

THE MILLENNIUM BUG

Y2K

ITS POTENTIAL THREAT TO NUCLEAR FACILITIES

A REVIEW

CLIENT: GREENPEACE INTERNATIONAL

REPORT REF N^o R3031-A1

9 DECEMBER 1999

First Issued 22 May 1999

THE MILLENNIUM BUG - Y2K - THE THREAT TO NUCLEAR FACILITIES

SUMMARY

This review examines the potential for system failures in nuclear power plants and other nuclear facilities (excluding military nuclear systems) during the transition to the new millennium and at the passing of other key dates:-

Types and Age of Nuclear Systems at Risk

There is no particular decade or year of nuclear plant design and construction before which a nuclear plant could be reckoned to be insensitive to Y2k. Although the essential nuclear safety systems of nuclear facilities designed and constructed in or before the 1970s are expected to be less sensitive to internal Y2k disruption than later plants, most if not all earlier plants have undergone upgrades and refurbishment which would have introduced modern, digital equipment that could be Y2k sensitive.

For nuclear plants designed and built in the 1980s and 1990s, the dependency upon digital systems is widespread and reaches deep into the safety systems. Even if the primary safety hardware is analogue 'hard-wired', virtually all of the equipment, monitoring instrumentation and control room displays are now digitally based and thus susceptible to Y2k glitches. Even Y2k failure of a small proportion of these digital systems could result in a multiplicity of Y2k malfunctioning systems presenting, overall, a very confusing and demanding situation to the operators.

Not only are digital systems used extensively across all functions of modern and upgraded nuclear plants, there is also a great deal of networking and integration between individual systems. Importantly, these systems not only receive and transmit information amongst themselves but also are most likely to; both individually and severally, import and export data on and off the nuclear plant site. This networking provides opportunity for a single Y2k glitch to act as a *common cause* failure across the entire plant. Moreover, since data and information is imported into the site, the glitch could be generated somewhere off-site, completely beyond the control of the nuclear plant operating personnel.

Internal within Plant Y2k Failures

The consensus of the worldwide nuclear industry is that the protective safeguards operating within most nuclear power plants are sufficiently robust to withstand a number of unexpected Y2k failures within the plant and its systems. After all, it is argued by the nuclear industry, the safety reasoning of the plant allows for individual systems to fail, so a computer or safety system going down by Y2k would be handled in much the same way as if the same system had crashed or malfunctioned because of some Y2k unrelated internal component failure.

There are a number of possible exceptions to this.

For example, the Y2k glitch might act as a *common cause* across the entire plant bringing all systems down or, of greater likelihood, it might cause a high rate of simultaneous failures and/or malfunctions sufficient to disrupt continuing safe operation of the plant. Another realistic possibility is where the Y2k date generates erroneous *data* that, although in error, is passed along to another part of the system at which an incorrect action is implemented.

Both of these types of failure and/or malfunction could give rise to a high demand on human resource at a time of high levels of stress, resulting in a climate susceptible to human error.

Off-Site or External Y2k Failures

Those countries advanced in their preparation for millennium transition identify the dominant Y2k challenge to nuclear installations to arise from a series of external events triggered by Y2k anomalies, specifically nominating nuclear installation *blackout* (no off- or on-site power) as the candidate event.

This risk-significant challenge to nuclear installations arises from a localised or regional power outage of the electricity distribution grid accompanied by a failure, again localised or regional, of the telecommunications systems that are crucial to both the grid and nuclear power plants. The telecommunications systems are, in themselves, critically dependent upon electricity so at Y2k each of these systems, power plants, transmission grid and communications, could interact adversely with each other, creating a rapid cascade to failure of one or more of each.

Thereafter the marooned nuclear installation, be it a nuclear power plant, fuel reprocessing facility, or whatever, has to fend for itself deploying its internal systems to shut itself down and, in doing so, it exposes more of its stand-alone and interconnected systems to Y2k failure.

It is this extended exposure to Y2k, both from internal and, particularly, external systems that continue to give concern to the safety regulators in the Y2k advanced nations.

Sleeping-Through and Work-Around

For certain isolated systems it is possible to turn the system off over the critical dates (*sleeping-through*) or to reset the system date to a 'safe' date (*work-around* - the nearest past safe date is leap year 1972).

Sleeping-Through the new millennium date will probably apply to most functions of fuel cycle plants since it is unlikely that these will be in production over the millennium change. However, vigilance will be required during the sleep through period because many functions of such plants cannot simply be turned (ie high-level waste cooling, discharge and emission processes) and extra care will be needed when these plants restart in the new millennium.

Work-Around can only be applied to totally isolated systems where the data, or date dependent data, is not transmitted to or received from some source beyond the system boundary. Since virtually all commercially-sized nuclear power plants are directly connected to electricity distribution and telecommunications grids, which are date dependent in themselves, *work-around* cannot be applied to nuclear power plants with any certainty.

Those nations whose nuclear safety regulators have addressed Y2k generally reject *sleeping-through* and *work-around* approach, particularly if these constitute the rump of the Y2k remediation effort undertaken. Even so, some nuclear plant operators continue to overly rely upon these two means to fend off possible Y2k failures.

State of Y2k Readiness

In addressing this concern, the nuclear regulators of those countries that have examined Y2k compliance require each nuclear installation operator to demonstrate Y2k readiness. Where these compliance programmes are advanced, particularly in the United States, it is acknowledged that it is not possible to be absolutely certain that all potential problems have been detected and/or will be corrected. In recognising this, the nuclear regulator requires the operator to lay down contingency plans and, in doing so, there is tacit acknowledgement of a lowering of the acceptable risk of accident criterion of the pre-Y2k safety case.

The US nuclear regulator anticipates, for US nuclear power plants alone, that one or two nuclear plants will have to completely close down in an unplanned manner some time over the millennium transition and that there will occur a dozen or more breaches of the regulatory safety regime at other US nuclear plants and facilities. In fact, the uncertainty of the US situation is illustrated by US plans to monitor the situation in the Far East, that is noting a few hours in advance problems arising as the new millennium sun dawns across the globe.

International Co-Operation and Y2k Contingency Planning

Although there are a few examples of international co-operation, published details of these projects are sparse and virtually nothing is available indicating the extent of the resource being provided by the nuclear plant manufacturing nations – the problem extends beyond the basic nuclear plant to the equipment, control systems and instrumentation that may have been introduced to and adapted into the original plant design by the operating nation.[†]

Russian Federation and Territories, etc., Aligned to the former Soviet Union

It may seem odd that the main text of this review does not include a section dealing specifically with the state of preparedness of nuclear plants in and around the ex-Soviet Union. The reason for this is that, other than the non-technical snippets of Table 6 some of which seem to be little more than ill-based speculation, there is virtually nothing to report.

Just a decade ago the then Soviet Union was a major manufacturer and user of nuclear power plants. Today, following the dissolution of the Soviet Union, the Russian Federation itself has about 30 commercially-sized nuclear power reactors in operation and the former territories and aligned states account for another 35 or so operational power reactors – about 12 power plants are at various stages of construction. Also, there are several fuel manufacturing and reprocessing plants in the Federation, numerous research and development reactors and a staggering 320 or so marine nuclear propulsion reactors in various states of operation, disrepair and decommissioning on board the surface ships and submarines of the Northern and Pacific Fleets, and icebreakers serving the Northern Passage.[‡]

The Russian Federation itself seems to be tackling Y2k on a do-it-yourself (DIY) plant-by-plant basis and it was not until June 1999 that the Federation government, the Duma, made it obligatory for all state and commercial enterprises to address and report upon the potential problems of Y2k – the government ministry, Minatom, reckoned that the \$3B required to resolve the nuclear power plant issues was six times the original estimate. In the former Soviet Bloc countries the situation is very confusing with, for example, Bulgaria (6 reactors) and Ukraine (14 reactors) both cash-strapped and unable to technically resource the Y2k audit their

[†] Just for example, nothing is available on the extent of assistance, if any, being provided by the French to South Africa for the two Framatome PWRs at Koeberg (Cape).

[‡] Large J H, Decommissioning of Nuclear Powered Submarines, Decommissioning of Nuclear Facilities, Conf, IBC London 1993

own programmes – these two countries are looking towards the European Community for assistance but, in the time remaining, it is doubtful that anything effective can be organized.

The lack of forward planning, failure to allocate resources in good time and, it seems, the absence of resolve on the ground, so to speak, in the former Soviet Bloc is nothing short of alarming.

Overall

Finally, it is noted that the nuclear regulators of some nations have, apparently, done very little or nothing to prepare for the millennium transition. A somewhat sorry state of affairs illustrated by the fact that only fifteen nuclear nations bothered to respond to the International Atomic Energy Agency's recent (February 1999) questionnaire to Member Nations on their state of Y2k readiness.

MILLENNIUM BUG - Y2K - ITS POTENTIAL THREAT TO NUCLEAR FACILITIES

CONTENTS

- 1 TRANSITION AND KEY DATES**
- 2 TYPES OF SYSTEMS POTENTIALLY AFFECTED - ORIGINS OF Y2K EVENTS**
 - NUCLEAR PLANT INTERNAL RISKS**
 - The Age of Systems at Risk
 - EXTERNAL RISKS**
- 3 NUCLEAR SYSTEM INTERACTIONS WITH Y2K EVENTS**
 - INTERNAL SYSTEM IN-BUILT COMPENSATION**
 - INTERACTION WITH EXTERNALLY GENERATED Y2K FAULTS**
 - ELECTRICITY GRID INFRASTRUCTURE FAILURE**
 - Plant Grid Disconnect - Loss of Off Site Power
 - Plant Blackout - Failure of Emergency Generators
 - Plant and Grid Common-Cause Failures
 - LOSS OF CONSUMABLES**
 - COMMUNICATIONS SYSTEMS FAILURES**
- 4 SLEEPING THROUGH THE TRANSITION AND WORK-AROUND**
- 5 Y2K MODIFICATIONS TO THE SAFETY CASE**
- 6 STATE OF Y2K READINESS TO DATE**
- 7 PLANT SPECIFIC AND FAILURE SCENARIOS**
- 8 CONCLUSION**

TABLES

- TABLE 1 - TRANSITION AND KEY DATES
- TABLE 2 - INTERNAL SYSTEMS AT RISK
- TABLE 3 - EXTERNAL SYSTEMS AT RISK
- TABLE 4 - IAEA REPORTED STATE OF READINESS ETC
- TABLE 5 - UK PREDICTED AND FOUND Y2K FAULTS
- TABLE 6 - SNIPPETS OF Y2K INFORMATION
- TABLE 7 - POSSIBLE AND POTENTIAL Y2K FAILURE CONSEQUENCES

GLOSSARY

REFERENCES AND NOTES

YEAR 2000 - Y2K - MILLENNIUM BUG

ITS POTENTIAL THREAT TO NUCLEAR FACILITIES

Millennium date induced events or malfunctions are those potentially arising from the inability of software systems, software applications, digital devices and/or date embedded electronic chips, to correctly process and act upon a numerical interpretation of a date.

Although the initial error generated by the Y2k date anomaly might be simple, just two digits misplaced, subsequent computation and processing of this erroneous data might result in a complex malfunction or total failure at some point in the overall system remote from the initial error. In effect, the Y2k computer problem has a potential to impact upon all aspects of digital technology as utilised in computer hardware, software and embedded systems.

In nuclear power plants and facilities such digital technology is commonly deployed in areas of communications, information technology, instrumentation and control, radiological management, protection and information systems, transmission and distribution systems, and other support systems.¹

1 TRANSITION AND KEY DATES

The most obvious date for malfunction is the transition to the new Millennium or *rollover* date, from 31 December 1999 to 1 January 2000. This is because many computerised systems adopt the last two digits of the numeric date string (12-03-99) to represent the year (ie 1999 by 99), so entry into year 2000 gives a numeric value of (00=) 0.²

Importantly, the Y2K problem revolves around the inability of some systems to handle not only the new millennium *rollover* date of 1 January 2000, but also other critical dates arising before and following the onset of the millennium:

TABLE 1 - TRANSITION AND KEY DATES

DATE	UK DATE NOTATION	COMPUTER SYSTEMS POTENTIALLY AFFECTED
1 January 1999	01-01-99	Computer systems that handle the year of a date with only two digits and that use the number 99 as a trigger or as an end-of-file marker (ie 99 is the last record in a file or list).
22 August 1999	22-08-99	Systems that interface with the Global Positioning System (GPS), for example, the transport of nuclear fuel where knowledge of its location is important. The original GPS design allocated a 10-bit register to handle the number of weeks which had elapsed since the base date (or GPS epoch date) of 6 January 1980 - the 10-bit week counter will rollover from its maximum value to zero on 22 August 1999.
9 September 1999	09-09-99	As in the case of 1 January 1999, this date is a problem for computer systems that handle the year of a date with only two digits and that use the number 99 (or 9999) as an end-of-file marker or 'STOP' instruction.
1 January 2000	01-01-00	Applies to systems that handle the year of a date with only two digits, because they may misread 00 as the year 1900 instead of the year 2000.
29 February 2000	29-02-00	Where the computer system that does not correctly identify the year 2000 as a leap year and risk failure at 29 February 2000, because it is a leap day.
1 March 2000	01-03-00	This date is a problem for computer systems that do not correctly identify the year 2000 as a leap year and therefore do not recognise 29 February 2000 as a leap day. Also, 1 March 2000 is the day after the leap day and these systems may carry erroneous data.
31 December 2000	31-12-00	This date presents problems for computer systems that do not correctly identify the year 2000 as a leap year and risk failure at 31 December 2000, because it is the 366 th day.
1 January 2001	01-01-01	Where the system does not correctly identify the year 2000 as a leap year and may carry erroneous data on 1 January 2001, because it is the day after the 366 th day (31 December 2000).

Thus, the use of such two-digit date formats in computation, both in software codes and [embedded chips](#), will result in anomalies which, if not compensated, will give incorrect results, instructions and actions.

Obviously, the specific dates (such as Leap Day, Year 2000) are limited in potential for disruption and failure to that particular day, whereas other date anomalies might occur at any time once the critical date has arrived or passed. For example, a system might not require to compute a date until some event, either pre-planned or situation triggered, requires it to do so - only at that time will that particular part of the system be tested for date compliance.

In another example, a system may become locked into an updating loop or [sub-routine](#) because it assumes '00' is an invalid date but it has no instruction to exit the routine. Similarly, the system might assume that '00' is a valid date and present this to another part of the code, which may then malfunction or crash.

If the date anomaly was encountered within a string of dates in, say, a trending or averaging routine, commonly used in control and surveillance systems, the invalid '00' zero value would result in an incorrect trend or average value being passed forward.

In summary: There are a number of readily identifiable critical dates which may give rise to difficulties in the continuing operation and reliability of control and surveillance systems commonly utilised in nuclear applications. Although the arithmetical functions that gives rise to the date anomaly are simple and straightforward, there remains a great deal of uncertainty to how the individual computer system will respond when confronted with its own error - it may pass over the anomaly without faltering, it might enter into an endless loop thereby unable to progress the required function further, or it might pass on the invalid date to another system which will, itself, trip over or crash with such an erroneous input.

2 TYPES OF COMPUTERS AND SYSTEMS POTENTIALLY AFFECTED

In some cases it may be immediately obvious that a computer system is present in a plant or control system because it is overtly visible, say, in the form of a digital time or date readout. However, in many instances a computer, in the form of a processing chip, may be embedded^{3,4} in a device without any outward indication of its presence or, sometimes, where it is obviously present its function may not apparently include a date reliant computation. In other applications, the embedded computer chip might retrieve an invalid date, or erroneous date dependent data, from a host computer or a network server or, in some instances, via a radio, telephonic or microwave transmission link.

Obviously, many aspects of the operation of a nuclear installation employ computers located on and off site. This means that the millennium date problem has the potential to affect every activity on a nuclear site, both the day-to-day and emergency operation of the nuclear plant itself. The initiating event itself, the date anomaly, might be generated locally on site or remotely somewhere off site.

NUCLEAR PLANT INTERNAL RISKS

The on-site or *internal* site generated date anomalies give rise to risks that could degrade, impair or prevent the operation or safety of the plant, and might involve undetected failure modes. Types of *internal* system risk include systems with multiple, integrated digital control devices or software sub-systems, and systems that use digital input from other systems,⁵ examples of which are given in [TABLE 2](#).

All of the systems of [TABLE 2](#) could or should have been reviewed by the nuclear site management,⁶ so for those potential problem areas identified, where a correction could not be reasonably made, a contingency plan could be laid.

The Age of the Nuclear Plant Systems at Risk

It might be reasoned that that equipment and plants designed and constructed before a certain date, by virtue of the technology available at that time, will be free of risk from Y2k anomalies - the transition to Y2k sensitive systems in nuclear plant could be, very crudely, allocated by decade:-

1950s-60s-70s

As originally designed and constructed, the incorporation of potentially sensitive Y2k digital technology was rare in earlier nuclear plants and, moreover, many such plants have by now ceased to operate.⁷

Generally, for advanced engineering applications and processes, the adoption of digital technology for control and processing tasks, then hitherto undertaken by electro-mechanical devices and analogue circuitry, commences in the early to mid-1970s in the West and about a decade later in the East, particularly for the former Soviet bloc countries.⁸

It follows, that the underlying control and safety systems for the reactor and nuclear components of earlier plants (say, pre-80s design and build) is likely to remain based upon electro-mechanical/analogue systems, that are digitally free and thus generally insensitive to Y2k, although there are some notable exceptions.²⁰ However, upgrades of the more accessible non-nuclear plant, such as the steam-raising equipment and turbines, would have taken place over the years with much of the older analogue control being replaced by digital systems, particularly stand-alone mini-and personal computers which controlled individual systems and processes. Similarly, peripheral monitoring and measurement systems would have been upgraded and introduced, with virtually all such systems incorporating digital technology.

1980s-90s

During 1980s, first, there occurred a transition from a few stand-alone computer systems to more centralised computer control (main-frame) and, later, the rapid introduction of stand-alone personal computers (PCs) which not only performed a primary function but data and job shared on a networked basis throughout the plant.

1990s

During this current decade the adoption of digital systems and processes has been widespread with applications ranging from critical safety tasks to relatively mundane functions such as cctv security systems. Typically, small desktop PCs are networked and linked to central servers, which may be on- and off- the nuclear plant site, and

data transfer and sharing is commonplace both by dedicated and public communication systems.

Running parallel to this widespread adoption and use of personal and networked computers, the incorporation of embedded chips and microprocessor is now so commonplace that even the simplest of devices commonly in use at nuclear power plants, such as radiation monitors, temperature recorders, etc., are likely to make reference to a date and/or undertake a computation related thereto.

In Summary: Although there is no strict demarcation decade or year before which nuclear plants could be reckoned to be insensitive to Y2k, essential nuclear safety systems of such plants designed and constructed in or before the 1970s are expected to be less sensitive to internal Y2k disruption than later plants. That said, most if not all earlier nuclear plants have undergone upgrades and refurbishment that would have introduced modern, digital equipment that could be Y2k sensitive.

For nuclear plants designed and built in the 1980s and 1990s, the dependency upon digital systems is widespread - not only are digital systems used extensively across all functions of the plant, there is also a great deal of networking and integration between systems and, importantly, these systems not only receive and transmit information amongst themselves but are most likely to, both individually and severally, import and export data on and off the nuclear plant site.

EXTERNAL RISKS

Risks arising from *external* anomalies may be indirect, more than likely not directly involving an invalid date but from a malfunction that itself resulted from a date problem somewhere down the line.

In this case, the nuclear site management may not have reasonable premonition of the nature, expected frequency and/or consequence of an external fault, for which no contingency can be made.

Externally induced risks within the nuclear plant might be triggered by any problem, be it a signal anomaly (incorrect data or a command) or a physical event, that intrudes across the boundary of the plant, including electricity distribution [grid](#) collapse or attempts to reconnect to the grid, loss of consumables, faults in emergency preparedness, etc.. **TABLE 3** gives examples of externally induced Y2k events that could affect nuclear plant performance and stability.

3 NUCLEAR SYSTEM INTERACTIONS WITH Y2K EVENTS

The occurrence of a Y2k anomaly, internally or externally generated, confronts the system with an unexpected situation to which it has to respond.

Where Y2k preparedness programmes have identified Y2k anomalies and glitches that cannot be completely remedied in time for the transition and key dates, the general expectation is that the plant operator would have ready a contingency plan. However because of the complexity of the systems and, correspondingly, the diversity of outcomes possible from an undefined Y2k glitch, the expectation is that a number of unexpected Y2k triggered events will be encountered and will have to be dealt with by the system acting in its pre-Y2k state.

In its pre-Y2k state, the system will have to respond to *internal* and *external* Y2k triggered events:-

Internal System In-Built Compensation

Of course not all of the internal systems, particularly the safety systems and logical devices listed in **TABLE 1** employ computers in a primary role. Where computers and processing chips are used, generally, those directly handling reactor and nuclear system trip and actuate actions have no need for a date reference in their in-line logic and hence, in themselves, these are unlikely to be at risk of Y2k anomalies. Again generally, the safety systems handling higher risk situations usually incorporate at least one degree of **redundancy** and **diversity** so, given a Y2k generated failure, either another safety system should activate (redundancy) or an alternative approach (diversity) to resolving would be adopted.

For hazardous plant, including nuclear installations, the regulatory approach worldwide requires, and has done so for many years, the systematic demonstration of a safety case that considers the effects of all credible, single and multiple system failures. Obviously, this includes failures of computer logic within these systems, initiated by Y2k or some other reason, so a date anomaly failure might be regarded as simply no more challenging than any other failure cause within the fault logic tree of that system. Although the Y2k failure mode may have been unforeseen at the time that the majority of the presently installed nuclear power plants and facilities were designed and commissioned, the nuclear industry will (quite justifiably in many respects) claim that such failures are covered by the generality of the so-called **Defence in Depth approach** to nuclear safety.

However, there two other potential Y2k initiated sequences that may give rise to safety issues at nuclear power plants and facilities that challenge *Defence in Depth*. These are i) the possibility that Y2k failures may be prevalent in individual systems across the plant as whole, that is acting as **common-cause** failure, and/or ii) that systems, prompted by the Y2k anomaly, will generate incorrect and misleading information and data to other parts of the system.

Both of these Y2k generated fault sequences could result in events not previously foreseen in the safety analysis. For example, simultaneous common-cause type failures

across the plant could stretch human resources and management in dealing with system rectification and, where systems had been rendered inoperative (crashed), computer operated functions might have to be undertaken manually. Where a potential exists for Y2k to generate erroneous information and data, which might give rise to incorrect and unsafe actions, this information and data would have to be checked before its commanding function could be allowed to proceed.

In summary: Low rates of single system failure (system crash) within a nuclear plant or facility initiated by Y2k should not, in itself, present serious safety issues for the plant overall. This is because most nuclear plants have sufficient degrees of redundancy and diversity in their primary safety systems, for which the fault control logic is not generally date dependent, and where many such systems are analogue *'hard-wired'*.

There is, however, a potential for serious disruption of the plant safety routines if the rate of individual system failures rises to an unmanageable level and/or where Y2k affected systems are generating erroneous information and data. This is because taking over failed and/or intervening in deviant systems will place additional and unpredicted workloads on the plant staff which, accompanied by increased stress, could produce a climate susceptible to human error - it is via this indirect route that the boundary of the operational safety case of nuclear plants and facilities might be seriously challenged and breached.

Interaction with Externally Generated Y2k Faults

As previously noted, external risks are beyond the reasonable premonition of the nuclear plant management, arising from conditions and circumstances that are completely beyond its control. Specific external risk areas that have received considerable attention in the United States and the UK (and elsewhere internationally - see **TABLE 4**) relate to telephonic and other forms of communication and, particularly, disruption of the electricity distribution grid infrastructures.

Electricity Grid Infrastructure Failure

At national and local levels, Y2k anomalies⁹ could result in electrical grid instability, in the form of voltage and frequency variations, loss of **synchronisation**, eventually cascading to a loss of power take up from the power plant and, with that, complete loss of off site power feeding to the plant itself.¹⁰ At international levels, where there are electrical inter-connectors across national boundaries, events triggered by a Y2k grid event in one country may cross the boundary to affect systems in another country.¹¹

Plant-Grid Disconnect - Loss of Off Site Power

For nuclear power plants, loss of grid connection (the loss of power take up and, thereafter, loss of off site power) is a pre-Y2k credible event that is prepared for and rehearsed.

In such an event, the nuclear power plant operator has to simultaneously and very rapidly:-

- a) dissipate the very large amount of thermal energy held in its reactor system that would have otherwise have been converted through its turbo-alternators to electricity exported to the grid connection – it does this by a variety of processes that, essentially, flash off the energy of steam;
- b) it has run down the nuclear reactor in a controlled way, keeping the reactor pressure vessel within a predetermined temperature-pressure management envelope, so as not risk the **primary containment** – for this the temperature of and pressure within the reactor pressure vessel have to be lowered in unison;¹²

and, to power the operations of *a)* and *b)*, within a few seconds of the loss of off-site power:-

- c) on-site emergency generators have to be started and switched into the power station and reactor system and, once these immediate and other sequenced events have been completed, the generators have to provide power to the reactor and power station ancillaries to cool the reactor and maintain nuclear and non-nuclear systems stable.¹³

For other nuclear facilities, such as irradiated fuel reprocessing plants, where there is risk of nuclear criticality, uncontrolled discharge to the environment, etc., there exists need for alternate energy supplies for fuel and waste silo cooling, continuing process control and auxiliary equipment, etc..

Obviously, loss of grid supplies to both nuclear power plants and nuclear facilities are credible and readily foreseeable events that covered by installed levels of contingency planning - all such nuclear installations have sufficient capacity of on-site emergency (diesel) generation to cover this type of off-site failure and many of the emergency action processes are undertaken automatically by the plant's safety systems.

Plant Blackout - Failure of Emergency Generators

If, in the event of a *loss of off-site power* incident, the on-site emergency generators fail to start and/or switch in then a very serious situation can rapidly develop – this situation is referred to as a *plant blackout*.

It is established that in a *plant blackout* the failure to provide key safety equipment with sufficient electrical power from the onset and throughout the *loss of off-site power* event (which may be a prolonged period at Y2k), could be a major contributor to reactor core damage (for PWR/BWR reactor systems).¹⁴

Plant and Grid Common-Cause Failures

For both *Plant Disconnect* and *Blackout* scenarios, the loss of grid supplies arising from an off-site Y2k event could present additional difficulties at the nuclear plant if it, itself, was experiencing Y2k *common-cause* failures¹⁵ with its own internal systems, especially if the rate of internal failures was drawing heavily upon the human resource at the plant.

Loss of Plant Consumables

Another possibility is that if grid disruption were so severe that connection could not be re-established for several days or, in the extreme, weeks to the extent that the emergency generator fuel stocks required replenishment, then the nuclear plant would require fuel and other supplies to be delivered. If the transition into the new millennium results in a significant breakdown of the state infrastructure then such supplies cannot be guaranteed.¹⁶

Communications Systems Failures

Communications is the other specific external event area that has attracted considerable attention for Y2k compliance. This is not only because the nuclear plants themselves are highly dependent upon a number of different forms of communications systems but, particularly, because many of the national electricity supply grids also have a high dependency upon these same communications systems.¹⁷

The control, management and transmission of electrical power across the national and international electricity grid systems is highly dependent upon microwave, telephone and VHF communications systems, and these systems in turn are highly dependent upon the availability of electrical power. It is the very complexity of telecommunications and the interdependency between communications, the electricity distribution grid and both conventional and nuclear power plants, that might provide a hidden opportunity for a Y2k date anomaly cascade resulting in, perhaps, a very serious breakdown of the electricity generating sector (both nuclear and conventional power plants).

In Summary: Of the three obvious areas of externally generated Y2k disruption reviewed, the combination of failures in the distribution grid interlinked with a communications *lockout* could give rise to a very serious situation indeed. It might transpire that such a coupled event would result in wide-scale regional, perhaps national and in part international disruption of electricity supplies (from both conventional and nuclear generators) and, with this, a serious breakdown in the supporting industrial and technological infrastructures.

Of course, nuclear plants require conventional fuel and other supplies to maintain both emergency generation and conventional support plant running throughout any extended loss of off-site power but these may not be absolutely secure.¹⁶ Also, even if the millennium transition is uneventful for nuclear plants, the continuing safe operation will be very dependent upon the plant operators procuring adequate quantities and quality of consumables (fuel oil, chemicals, etc) in the short, interim and, perhaps, longer term future if Y2k is damaging to other economic-industrial sectors.¹⁸

4 SLEEPING THROUGH AND WORKING-AROUND THE TRANSITION

Sleeping Through

It has been suggested¹⁹ that closing down Y2k sensitive plants over the transition critical and key dates would remove the greater part of the risk of malfunction. In fact, for a number of reasons (including maintenance outages, batch operation of reprocessing and fuel enrichment/fabrication plants) some nuclear plants and equipment will not be in active use over the transition dates.²⁰

However, withdrawing the plant from service may not necessarily obviate or reduce the Y2k risk since the date anomaly may result in the plant entering an unsafe and possibly hidden state of instability. Those plants that do '*sleep*' through the transition dates will have to be monitored throughout their slumber and, prior to restarting, it will be necessary to assess the post Y2k safety situation.

Working Around

An alternative to sleeping through is to '*work-around*' the millennium transition date by rolling back the system clock to a year equivalent in all respects to Year 2000 - 1972 is the equivalent year with January 1 being a Saturday and since 1972 was a leap-year that matches leap-year 2000.

This somewhat expedient means of avoiding the Y2k anomaly by rolling back the system clock by 28 years would only be failsafe if the system rolled back was completely isolated from any other system which also referred to, relied upon and/or calculated a date related function.

In summary: Arrangements to *sleep through* or *work-around* the Y2k problem would not alleviate the susceptibility of nuclear installations to failures at the millennium transition and other key dates.²¹

The UK regulatory body, the Nuclear Installations Inspectorate, has declared that the approach of taking no corrective action, on the basis that shutting down or working around over the critical periods constitutes an appropriate, alternative solution (ie *work-around*), should be regarded as unacceptable.²²

5 Y2K MODIFICATIONS TO THE SAFETY CASE

Generally, the basis of licensing nuclear plants and facilities is that the risk of accident is acceptable and that the consequence of any credible accident is tolerable. This compact results in a sliding scale of acceptable frequency of accident to the projected severity of accident - ie an inverse relationship between accident frequency and severity. Although the licensing procedures do allow for some margin of discretion, once the safety case of a particular plant is accepted then, as time passes, any significant departure from the established safety case criteria (ie *risk v severity*) requires further justification from the operator.²³

Of course, the safety cases of existing nuclear plants were compiled mostly in the absence of any recognition of inclusion of Y2k potential failures. However, the relevant Y2k glitch remains dormant until the arrival of each of the critical and key dates so, at that time, the original safety case *as a whole* no longer applies and requires review - the argument here is that, for each nuclear plant, the safety case *as a whole* should be reviewed on the basis of its original premise and construction.

It is quite clear that a generic approach has not been adopted internationally and nationally - some national regulators, such as the US NRC, have been proactive, quite demanding of nuclear licensees and published openly,²⁴ others like the UK, although active in the area have published little,²⁵ and certain states, notably the Russian Federation, seem to have made no plans at all - **TABLE 6** includes snippets of information found in the nuclear professional, etc., journals over recent years.

Importantly, the US and UK approach suggests that instead of reviewing the safety case *as a whole*, it is sufficient for each operator to isolate and remedy the Y2k glitches. This means that the assessment and 'solution' of the Y2k problem is by deterministic means (requiring each Y2k glitch being sought out and remedied), whereas the original and continuing safety case is based on a probabilistic approach.

In other words, the probabilistic-based safety case that satisfies the site operating licence can only remain valid, during and after the new millennium transition, if there is absolute assurance that all Y2k glitches (both internally and externally as these affect the plant) have been identified and remedied.²⁶

Since the Y2k glitches remain in a dormant state until activated by the millennium transition and key dates, absolute assurance in this respect cannot be achieved.^{27,28} Put another way, this approach to remedying the Y2k problem could provide the both operator and regulator with discretion to relax the safety regime through and following the millennium transition.^{29,30}

In compensation for this uncertainty the national regulators require the operator to put in place *Contingency Plans*, but the difficulty here is in knowing exactly what contingency to lay these plans against (but see **TABLE 4**).³¹

In summary: There seems to be tacit acknowledgement by the nuclear regulators (at least by the US and UK bodies) that the pre-Y2k regulatory regimes are unsuited to manage Y2k problems, should these arise during and following the transition date into the new millennium. In fact, the US NRC notes that its regulatory regime is not only too cumbersome but that addressing Y2k glitches via its procedures and routines could, by forcing unnecessary nuclear plant shutdowns, adversely impact upon public health and safety.

Put simply, the present regulatory approach cannot, itself, safely handle the Y2k problem and there is not enough time to root out and eliminate all Y2k glitches. So, in the absence of a reliable route of regulatory management of Y2k, the regulators (the NRC at least) seem prepared to permit some degree of discretion during the millennium transition period³² - such permissive discretion must, of course, compromise the licensing conditions and safety case.

6 STATE OF Y2K READINESS TO DATE

Recently the IAEA published the summarised results of a Y2k questionnaire³³ relating to civilian nuclear plants - the greater number of member states (including the major nuclear states such as Russian Federation and France) failed to respond.³⁴ **TABLE 4** summarises the response of those Member States participating.

In Summary: Although **TABLE 4** provides only a very small sample of the nations (16 from >120) that responded to the IAEA worldwide questionnaire, it can be seen that the most advanced and well-prepared country (via the openness of its publications, seemingly, the United States) still has to reach a number of its own mission targets.³⁵

Also, it is interesting to note the apparent corollary that the greater the effort put into identifying and exploring potential Y2k problems then, it results, that a greater importance is placed on contingency planning ahead of the millennium event. For example, the US NRC requires each plant operator to have in place contingency plans and itself, the NRC, has laid a nationwide contingency plan.

Those nations that have undertaken little Y2k investigation, judging from lack of published information such as the Russian Federation, have little or no contingency planning in hand.

7 PLANT SPECIFIC AND FAILURE SCENARIOS

The US Nuclear Regulatory Commission,⁵ the UK Nuclear Installations Inspectorate⁴¹ and, to a limited extent, the International Atomic Energy Agency³³ have identified and published systems and processes that include potential for Y2k anomalies.

The UK regulator has published a listing the types of Y2k anomalies³⁶ discovered during its Y2k compliance programme at various types of civil nuclear installations - with added anomalies from Ref 20, the UK Y2k anomalies discovered to date are summarised in **TABLE 5**.

The US NRC draws a similar list, although not quite as specific as **TABLE 5**, of *projected* Y2k sensitive systems likely to be found in nuclear power plants, reprocessing and fuel facilities, R&D reactors, irradiators and, indeed, its own emergency systems,³⁷ but it goes further to develop and consider the contingency plan for a specific Y2k scenario^{5,38}

This scenario draws a mean between the extremes of no Y2k problems being encountered at all to a worst case situation involving a widespread telecommunications outage, a complete loss of the North-American power grid and major incidents at nuclear power plants, including complete station blackouts, loss of feedwater, loss of ultimate heat sink, etc..

The actual scenario chosen by the NRC to develop and test its own contingency plan comprised:-

- Y2k prompted localised grid disturbances and power outages but not a major, regional power loss

-
- local or regional telecommunications failures, but not a complete loss of the public switched network and with other operating systems of the major communications companies remaining functional
 - at least two nuclear facilities affected directly or indirectly to the extent that NRC response will be required
 - unforeseen Y2k occurrences will place a dozen or more nuclear installations in situations that depart from the licence conditions or technical specification
 - and, Y2k problems will affect at least one nuclear power plant outside of the United States

Essentially, the US (and probably the UK) regulator is anticipating a Y2k situation in which one or more nuclear installations are isolated from the electrical supply and distribution grid at a time when the local/regional communications system has collapsed. Thereafter, the marooned nuclear installation, be it a nuclear power plant, fuel reprocessing facility, or whatever, has to fend for itself by deploying its internal systems to shut itself down and, in doing so, it exposes more of its stand-alone and interconnected systems to Y2k failure.

In the event of a grid disruption and/or disconnection a nuclear installation has to rely upon its own emergency power generating systems.³⁹ If it successfully starts and maintains its on-site emergency supplies, then it remains at an enhanced risk of failure via internal Y2k related problems. If it fails to start and/or maintain its emergency power supplies and is *blacked out*, then depending on the type of nuclear plant a very challenging situation could develop quickly - in fact, most probabilistic risk assessments identify total loss of power, station *blackout*, as a situation that most threatens overall plant safety.

In summary: As promoted by the nuclear regulators, events that are likely to be most disruptive to nuclear installations will, if such occur at all, derive from external sources. A combination of failure of the electricity supply grid and regional communication systems are postulated to be the most threatening - in most nations, neither the nuclear plant operator nor regulator have any control over the grid and communications systems.

Once a nuclear installation is isolated and fending for itself, even with its emergency power systems in operation, it is at heightened risk of failure. The fact that whilst it is in this vulnerable state it will also be at risk of multiple failures from its own internal Y2k sensitive systems, must result in further challenges to its safety systems. In

other words, the risk of accident during and following the new millennium transition must increase.

If the safety systems fail then the type and operational state of the nuclear installation will determine the consequences to the environment and humans, very generally:-

NUCLEAR POWER PLANTS

TABLES 2, 3 and 5 summarise the primary risk areas of nuclear power plants.

In the immediate aftermath of the new millennium transition: If Y2k failures are permitted to cascade then the expectation is that penetration through the safeguards, if such occurs at all, will be via weaknesses in and fallibility of the human resource, prompted by and in combination with a multiplicity of small system failures. If the situation results in a release of radioactivity to off-site, difficulties may be encountered in mitigation of off-site consequences particularly if there are simultaneous power-communications disruption and/or blackout underway in the off-site domain.

In the interim and longer terms: The breakdown of sub systems that support both nuclear and other functions (such as pond stored irradiated fuel cooling and water conditioning, waste processing control), and/or depletion of essential supplies, might result in a general degradation of quality assurance and management overall, with eventual release to off-site of radioactive substances.

FUEL CYCLE AND RADIOACTIVE WASTE FACILITIES

TABLE 7 identifies possible risk and consequence areas for nuclear fuel cycle and radioactive waste facilities.

Generally, fuel cycle and radioactive waste management facilities are highly automated and very dependent upon digital process control and safety systems. Compared with nuclear power plants, there is much more emphasis and reliance upon data processing systems for material flow control, inventory and quality assurance.

Although Y2k generated system crashes would, like the NPP systems, test plant safety and its response to malfunction, these plants would appear to be at greater vulnerability to an unnoticed incorrect calculation rendering changes to the physical and/or chemical parameters of a process, that might compound in magnitude as the process develops downstream.

The diverse array of fuel cycle and waste plants provides opportunity for chemically toxic and/or radioactive gaseous, particulate and effluent release in the **immediate aftermath, interim and longer terms**.

OTHER RADIOACTIVE MATERIAL PROCESSES, ETC

The nuclear industry produces a range of products that are routinely deployed for medicine, engineering, research and development and production. The effectiveness and safety of these products, particularly when used for diagnostic and therapeutic medicine, could give rise to problems associated with Y2k.⁴⁰

8 IN CONCLUSION

The dependency of nations, societies and communities upon electrical power is so entrenched that widespread and chaotic disruption of reliable supplies of electricity could result in very serious and wide scale consequences. The fact that we greatly depend on modern communication systems to control and order our society and, particularly, to mitigate the consequences of accidents and adverse events, means that we have to safeguard both electrical supplies and communication systems through the new millennium transition.

Electrical generating power plants, both nuclear and conventional, must be able to stay on line during the Y2k transition to ensure that the grid distribution system does not collapse. This is because failure to provide the essential public services with electrical power could result in health and safety consequences as transport, hospitals and other facilities run into turmoil.

Obviously, there has to be a degree of compromise, perhaps even gambling, that in maintaining the nuclear power stations on line over the Y2k transition this will stave off collapse of the broader electricity supply and other infrastructures, thereby minimising the potential health and safety impact of Y2k. If it does not, then the fact that the nuclear plants are operational and at their most vulnerable during a grid collapse could, in fact, significantly worsen the potential health and safety impact.

TABLE 2 - INTERNAL SYSTEMS AT RISK - NPP AND OTHER NUCLEAR FACILITIES

INTERNAL SYSTEM	TYPICAL FUNCTION/ROLE
GENERAL MANAGEMENT	
DATA AND DATABASES	where dates are stored along with other information and data in a database - where information is retrieved from or located in by searching for a data string, at Y2k the year string "00" would not locate at year 2000 - a diverse range of data is stored in this way, including radiation records, radioactive and other discharges to the environment, general day to day management records, etc
COMMUNICATIONS/NETWORKS	where transmitted information is date stamped or dated - internal telephone systems, equipment and materials ordering and restocking
HUMAN/MACHINE INTERFACE	devices used for inputting and outputting dates - a human entry that might be incidentally date marked, for example, logging on to a computer, using a swipe card in a door entry system, dialing on an internal/external telephone system, etc
DOSIMETRY SYSTEMS	date logged radiation dose rates, personal and building areas and in medical therapy and diagnostics
BUILDING ACCESS/ SECURITY SYSTEMS	access control to plant areas, system locked out - swipe card door entry
NON-NUCLEAR PLANT	
PLANT ITEMS AND EQUIPMENT	cranes, circuit breakers, instruments, lifts and road vehicles
STEAM PLANT SIDE	Condensate polishing and water quality
SAFETY SYSTEMS	
COMPUTER-BASED SAFETY SYSTEMS	surveillance and other safety initiation systems and, generally, networked computer systems that may have been individually evaluated to be Y2k satisfactory, but where the complexity and multiplicity of the interfaces means that it is not possible to check the number of interactions and condition for any given transaction and in which a single failure has the potential for impacting on the entire data communications structure
SAFETY SYSTEM SUPPORT SYSTEMS	automatic information collation and relay systems
PROCESS CONTROLS	systems where continuous processing is underway, for example the full flow condensate polisher or FFCP which maintains correct water (chemistry) quality on the steam side of the plant which could result in adverse water quality and loss of control in the boiler/steam generator boiling regime
CONTROL AND MONITORING SYSTEMS	system and operator function tracking - for example, the control rod position indicator system which provided information to the control staff for the assessment of the reactor core thermal values and for automatic positioning of the control rods
ACTIVITY-IN-AIR SYSTEMS	respiratory protection triggers
DOSIMETRY SYSTEMS	emergency area radiation dose rate monitoring
FIRE ALARM SYSTEMS	automatic relaying of call signals
BURST CAN DETECTION SYSTEMS	fission product release detectors ⁴¹
CRITICALITY DETECTION/ALARM SYSTEMS	reactor core, fuel stores, irradiated fuel ponds
EMERGENCY CONTROL CENTRES	collapse of emergency support systems via loss of the plant process computer which provides a common facility and distributes information during and after an adverse incident for emergency mitigating purposes - the information is passed to an off site information system to the emergency response data system (US plants) so that any emergency situation may be handles on-site, locally, regionally and nationally
EMERGENCY COMMUNICATION SYSTEMS	internal telephone and communications systems as disrupted by external Y2k triggered events

TABLE 3 - EXTERNAL SYSTEMS AT RISK

EXTERNAL SYSTEM	TYPICAL FUNCTION/ROLE
DIRECT RESOURCES	

LOSS OF ULTIMATE HEAT SINK	NPS condenser cooling - for example, where the river flows are disrupted by some upstream Y2k event, say at a hydro-electric facility where the flow is held back
EMERGENCY WATER RESERVES	loss of cooling water reserves via pipelines or similar
GRID CONNECTION	
ELECTRICITY TRANSMISSION GRID	loss of transmission and input power, particularly high voltage line system due to Y2k induced failure at other sites connected to the grid system, could result in NPP blackout and need for emergency on-site provisions
COMMUNICATIONS	
SATELLITES	including communications systems and grid demand/stability control, location or irradiated fuel and other radioactive substances in transit
TELEPHONES	loss of Public Switched and direct systems
MICROWAVE	grid and other communications
CONSUMABLES	
DOMESTIC WATER	loss of potable supplies
PIPELINES	disruption of oil, gas, water, etc supply/emission routes
FUEL SUPPLY NETWORK	loss of tanker supplies for emergency generators, etc
LOCAL DISTRIBUTION GAS	loss of gas supplies for emergency generators, etc
GENERAL PROVISIONS	delays in delivery of consumables, nuclear components, etc
EMERGENCY SERVICES	
EMERGENCY SERVICES EVACUATION	confusion in external emergency services systems and personnel, loss of direct communications, overload if available resource, introduction of inexperienced human resource (army), etc

TABLE 4 - IAEA REPORTED STATE OF READINESS ETC (REF 42)

STATE	INITIATED ON DATE	REQUIRED BY DATE	PREP TIME MNTHS	STRATEGY APPROACH	PROBLEMS ENCOUNTERED TO DATE	CONTINGENCY PLANNING TO DATE
BULGARIA	~	03-99	~12	Adopts IAEA	embedded systems - some suppliers did not answer or answers unreliable.	O In hand for 09-99
CZECH	97	02-99	~18	In house	none	II To be drawn up
FINLAND	03-98	03-99	24	1 st inspection date	Suppliers state Y2k failures	O To be drawn up
GERMANY	07-98	03-99 07-99	17	Interim and Final reporting stages	None identified	II Based on grid failure
HUNGARY	~	12-98	~12	Nothing specific	None identified	II Not prepared
INDIA	01-99	~	12	Adopts IAEA approach	None expected and identified	II In hand based on keeping emergency generators operating
INDONESIA	~	12-99	~12	In house	Fuel management code	O Under development

JAPAN	09-98	06-99	15	Simulation testing	JOYA & MONJU FBR radiation monitoring errors - unspecified problems at NPPs - fuel enrichment plant misprocessing and shutdown problems at Y2k	O	In preparation, based around grid failures
MEXICO	03-99	~	15	Adopts NRC generic letter	Some specific problems encountered at Laguna Verde NPP but claimed not safety related	O	Situation to be assessed by US consultants by 07-99, then if necessary contingency plan prepared
HOLLAND	01-98	06-99	24	adopts NRC	Building area access control system	O	Possibly halting export/import to/of other state power to minimise grid disruption - special training for loss of grid supplies
PAKISTAN	09-98	09-99	15	Compliance audit - adopts IAEA	None identified	II	Locally at NPP level
SPAIN	05-98	06-99	19	adopts NRC generic and IAEA	None identified	II	Decision Awaited
UKRAINE	08-98	09-99	16	IAEA adopted	Unspecified found in nuclear safety systems	O	Nothing beyond present contingency planning - but see Snippets of TABLE 6
UK	96/97	6 weeks staged	~36	Completion 6 weeks before each of a number of key dates - industry based compliance	Fuel flask leak detection equipment misinformation at 98/99 transition, satellite communication flawed	O	In house planning at NPPs etc., national strategy for infrastructure
US	95/96	07-99	~36	Y2k certificated readiness date	Plant security computers, data recorders, radiation monitoring systems, plant process systems (e.g., feedwater control systems, turbine control systems, and heater drain level control systems), steam leak detection systems, and diagnostic systems	O	All NPPs, fuel facilities etc now have contingency planning, in hand from 08-98 - NRC is to conduct simulation exercises of Y2k failure of its own mission critical system - NRC plans to look East to US type NPPs for advance warning and to interrogate Mexican and Canadian grid controllers to isolate across border problems ⁴³

TABLE 5 - UK PREDICTED AND FOUND Y2K FAULTS AT NPPS

SYSTEM	Y2K FAULT	POSSIBLE CONSEQUENCE
--------	-----------	----------------------

Data Processing Systems	Incorrect date-stamp on some entries in the alarm and event log, e. year set to 28 instead of 00, 29 instead of 01; the rod-drop logger would not accept a date set beyond 1999, although it did correctly work through the date change to 2000; the punch history programme which prints out data after a trip can, if the year is set to zero, follow a path which leads to an incorrect date being printed.	MINOR: Information record
Embedded Hardware	Some hardware stores date for internal purposes and this is inaccessible by user.	MINOR TO SERIOUS: Presents some level of risk, depends on application, but has to be covered by contingency plan
Embedded Instruments	Instruments using date for internal processing and date stamping - some instrument do not perform correctly and some do not recognise 29 February 2000	MINOR: Once known Ref 20 suggests using "a rubber stamp".
Security Systems	The provided access control systems fail due to excessive error messages being generated on transition to year 2000. Setting the date back or re-starting in 2000 is being investigated as a contingency measure.	MINOR TO SERIOUS: Could deny egress to and from to certain areas during emergency or accident situations.
Emergency Plume Gamma Monitoring System	Historical trend information is presented correctly if all data is in this millennium or all the data is in the next millennium, but trends do not appear correctly if the data is spanning the transition.	SERIOUS: Could, for a through the Millennium transition accident aftermath, result in the wrong countermeasures being implemented and evacuees being directed into contaminated/radiation zones.
Main Turbine and Main Boiler Feed Pump Governors	The version of the operating system used in this equipment has a problem that prevents it being re-started in Year 2000. Upgrades to address this problem are being progressed.	MINOR: Takes up human resource with manual over restarting.
Fuel Flask Leak Detection	This equipment includes a calibration date and a check that it is within a yearly calibration period. The comparison of current and calibration-due dates needs to address the transition from 1999 to 2000 (99 to 00). The software was intended to deal with this, but causes an illegal syntax error and halts the processor when it does this check on 1/1/1999.	MINOR TO SERIOUS: Calibration check system might be intentionally disabled thereby allowing leaking flasks to carry irradiated fuel in public domain.
Water Chemistry Control System	A water treatment plant control and chemical monitoring system has been found to work incorrectly in the year 2000. Whilst not causing a loss of feed water to the boilers, it had the potential to affect water quality resulting in the longer term in an increase in the number of boiler tube failures.	DEPENDS ON REACTOR TYPE, IF AGR POTENTIALLY VERY SERIOUS: Water quality degrade could result in rapid stress corrosion failure of tubes at boiling regime on 'once-through' AGR boilers, could knock-on to serious flooding of reactor, overpressurisation and rupturing of reactor pressure vessel.
Activity in Low Level Waste Drums	A system that monitors the activity of low level waste stored in drums will not operate after 31 December 1999 because its calibration routine is not able to handle the change from 1999 to 2000. In addition, it does not recognise 29 February 2000. If this system is not corrected it will not pose a direct safety hazard but could result in delays in the dispatching of solid low-level waste off the site.	MINOR TO SERIOUS: Could impinge on the leak detection systems.

Burst Can Detection System	A burst can detection system, which monitors a reactor's primary cooling system for activity fails to scan the several inputs located around the reactor. Although it is still able to detect a leak of activity into the cooling system, and will indicate this to an operator who will trip the reactor, the detection of this activity could be delayed, further worsening the incident.	SERIOUS: Burst can detection is a primary defence guardline, particularly in the AGR system following and emergency shut down when the rate of pin failures give a primary indication of reactor gas conditions and state - this type of situation arises after a loss of all off site power incident and then loss of on site emergency supplies, following which the reactor depends solely on natural circulation
Maintenance Scheduling Computer	A maintenance scheduling computer is year 2000 non-compliant and requires modification. Whilst not affecting safety directly, problems with this system could mean maintenance was not carried out at the correct time and that there was an increased burden on the maintenance staff.	MINOR TO SERIOUS: Could result in out of maintenance time equipment being in place.
Emergency Indication	A Remote Emergency Indication Centre has a number of date related non-compliances which need to be rectified. If this were not done, the efficient handling of emergencies would be in jeopardy.	SERIOUS: Could knock on to the wider emergency planning for a nuclear release incident
Site Mustering Systems and Site Access	Not detailed but assumed to include locking our plant personnel to certain areas.	SERIOUS: Could influence efficiency of evacuation of plant personnel during emergency incident.
Suppliers' Information	Suppliers' letters on Y2 information provide inadequate information on the outcome of the possible non-compliance.	MINOR TO MODERATE: Requires double checking by plant staff of all equipment, with consequential high demand on plant human resource.
Work Permit System	A system that is used to ensure the safety of personnel who are working on plant by preparing safety documentation has needed to be replaced. Failure to update this system would have resulted in a manual alternative having to be brought into use with the additional burden on the operational/maintenance staff.	MINOR: Although may have longer-term repercussions for record keeping of individual radiation dose exposure history.

TABLE 6 - SNIPPETS OF INFORMATION ON Y2K

COUNTRY	TOPIC	SOURCE
OECD	OECD workshop identified the major focus or NPPs to be Y2k national grid instability and failures	Ottawa February 1999
United States	Y2k compliance programme for ComEd's Braidwood and other NNPs has cost between \$40 to \$60 Million and involved more than 300 personnel reviewing more than 15 million lines of computer code and 30,000 embedded systems.	Nuclear Engineering International March 1999
Russian Federation	US EXPERTS HELPING SOVIET DESIGNED POWER PLANTS DEAL WITH Y2K: Several issues are pending: <ul style="list-style-type: none"> Some Y2K problems exist in secondary safety systems. The most important are plant process computers. Failure of a plant process computer is not an immediate safety concern but does require that the plant be shut down within 4 to 8 hours if the computer is not restored. With nuclear energy providing about 20 percent of the electricity in Russia and 50 percent in Ukraine, the concern is that the shutdown of several nuclear plants could disrupt power supplies in the middle of winter. Y2K problems originating in the electrical transmission and distribution system could cause a loss of offsite power to the plant, resulting in an unplanned reactor shutdown. Russian and Ukrainian transmission and distribution experts are confident they can operate their systems 	Pacific NorthWest National Laboratory - insp.pnl.gov - March 1999

	<p>manually to avoid any unplanned disruption of electricity supplies.</p> <ul style="list-style-type: none"> Additional evaluation and planning is needed at Soviet-designed nuclear power plants to ensure plant personnel understand possible Y2K problems and how to respond to them appropriately. Contingency plans must be developed to address the worst-case Y2K scenarios. 	
United Kingdom	<p>Recently, the UK Secretary of State for Defence (George Robertson) provided an interesting, albeit fumbled, insight into the Y2k problems confronting the UK's nuclear deterrent system in a talk show programme:-</p> <p>"...</p> <p><i>Question: At one minute past midnight on the 1st of January 2000, will members of the panel be flying at 30,000 feet or will they be covering in a nuclear shelter?</i></p> <p><i>Chair of Panel: On the 1st of January in the year 2000, two American senators want everybody who knows anything about nuclear power from all countries to assemble together to make sure there isn't some ghastly accident. George Robertson, where are you going to be on the 1st of January 2000?</i></p> <p><i>George Robertson: There is a serious issue behind the question and I think it is a perfectly fair test and, as somebody who runs one of the biggest government departments in this country, indeed one of the biggest government departments in the whole of Europe, I've got a very special responsibility here. And we have placed a very, very high priority in dealing with the Millennium Bug problem and the serious implications that it has. I believe that I will be secure in anything that we have dealt with up until that time. What I'm less sure about is that other people, other institutions, even in this country or abroad, might not have done the preparations that we're doing...</i></p> <p><i>Chair: What about these two US senators, who lead that committee in the States, who want everybody to assemble to avoid a false missile alert: do you take that seriously?</i></p> <p><i>George Robertson: Well, there are dangers involved in that and we're addressing them and Robin Cook will be addressing that specific problem in Moscow as we are speaking just now - because we are sharing our expertise with the Russians at this difficult time. So there is a task ahead of us to make sure that the sort of 'Armageddon scenario' does not happen. It requires urgency, it requires action by everybody to make sure that it is tackled and I would...</i></p> <p><i>Chair (interrupting); Is it possible to be a hundred per cent certain?</i></p> <p><i>George Robertson: Well, I can only be certain about those things that I am in control of but I think there are serious...</i></p> <p><i>Chair (interrupting): The nuclear deterrent?</i></p> <p><i>George Robertson: Well, the nuclear deterrent...</i></p> <p><i>Chair: Certain, no problem?</i></p> <p><i>George Robertson MP: Well, I think the point can be made that the [does not finish sentence] yes, yes, absolutely, absolutely, we have made sure that we can say that with certainty but a 'default' setting, you see, for nuclear weapons is that they don't work. Unfortunately, the 'default' setting for civil nuclear power is that it stops - and that is where one of the big dangers might well come in so we've got a period during which all of us - and we're not just talking here about those who handle big government departments but all of us in society have an obligation to make sure that we keep our attention focussed very much on this. and the Government has made this a huge priority because it matters.</i></p> <p>..."</p>	BBC TV C1 - 4 March 1999
Russian Federation	<p>Minatom claim to be on target to finish checking all computer systems for NPPs and fuel facilities by August 1999 - Y2k compliance programme has been underway since 1997 - each NPP has to allocate its own finance to programme and any remediation required but Minatom estimates that \$3 Billion is required, that is x6 the original estimate</p>	Nuclear Engineering International March 1999
United States	<p>Nuclear Information and Resource Service claims that the November audit of Seabrook NPP</p>	NIRS, March 1999

	discovered 12 safety related Y2k problems	
United States	The North American Electric Reliability Council (NERC) plans to conduct tests in September to simulate a partial loss of computer systems because of Y2k glitches.	Nuclear Engineering Int March 1999
United States	At Peach Bottom NPP computers failed for 7 hours during a Y2k simulation test on the reactor control rod positioning system - every computer screen in the control room crashed - eventually problem found to arise from human error.	Nuclear Engineering Int April 1999
Ukraine	Former head of Chernobyl RBMK plant, Sergei Parashin, and now head of Ukraine Energy and Information Research Centre, stated that millennium bug could paralyse Ukraine's nuclear plants, stating <i>"We have not yet received all information for our nuclear stations . . . but, unfortunately, I have to say that the Ukrainian energy authorities do not fully understand the problem"</i> .	Nuclear Engineering Int April 1999
France	EDF has spent F600 million on Y2K compliance issues and intends to shut down and sleep through some plants. Others like ours in Fessenheim, will be closed, in the process of its decennial revision and COGEMA la Hague will be closed for Christmas and New year holidays.	Fernex, 14 April, 1999
France	French agency IPSN as saying that between 45 and 80% of internal systems could be sensitive to Y2K, and that this could "weaken safety levels".	Reuters, May 4, 1999
Japan	TEPCO completed Y2k simulation in April 1999 at Kashiwazaki-Kariwa ABWR NPP and experienced no Y2k glitches	Nuclear Engineering International May 1999
UK	BNFL commences Y2k programme in 1995 with 125 members of staff devoted to compliance issues on a full time basis for fuel facilities and ageing Magnox power stations, total spend estimated to be between £25 to £30M	BNFL Press Release, May 1999
United States	President Clinton's Y2K Czar, John Koskinen, told Georgia Y2K officials to make contingency plans for a three week power outage states Georgia State Representative George Grindley.	Scott Portzline happen@pipeline.com , 1 June 1999
Russian Federation	REACTORS LARGELY FREE OF COMPUTERS: The Deputy Atomic Energy Minister Valentin B. Ivanov has good reason to promise that Russia's 29 nuclear reactors will be free of the year 2000 computer problem in January. The reactors, it seems, are largely free of computers. At the nuclear station nearest to Moscow, Mr. Ivanov said, <i>"the general engineer promises that he'll have a New Year's party, and he's invited me."</i> Although American experts said they would quite likely accept such an invitation, they still have nagging questions about how ready the reactors are. The experts said they were unsure whether engineers could locate and check all the microchips and other digital improvements that have been added to Soviet-era plants over the years. The experts worry that Russian engineers, adept at handling breakdowns in sometimes creaky plants, might be overwhelmed if four or five systems failed at once, and they wonder whether backup water and power systems are sufficient. Most of all, the experts wonder whether the cash-depleted Government can really oversee all the work at stations flung across 10 time zones, some so remote that it is tough to administer them even in normal times. <i>"They're taking it seriously,"</i> an American official said. <i>"Our concern is that they won't do enough, either because there are some pockets in Russia that still aren't taking it seriously, even though they've been ordered by the Government to do things, or because they lack the resources."</i> The official echoed an analysis by the Pacific Northwest National Laboratories of the United States Energy Department about potential year 2000 flaws in Soviet-style reactors. The report found that senior Russian officials had made reactor safety a priority, but that <i>"the level of effort devoted to date varied from site to site and organization to organization."</i> In particular, American experts worry that the nuclear-energy industry is so short of cash and time that even some obvious flaws will go uncorrected. Those experts stress that their views are only well-educated guesses. Although Americans have visited all 66 Soviet-style reactors in Russia and surrounding nations, they have not evaluated the plants for year 2000 vulnerabilities. In general, they said, the millennium bug poses a small threat. Analog devices control most "mission critical" functions, including crucial water pumps. Some flawed computers or chips could force a plant to shut down, but none appear vital to stopping reactors in an emergency. In an emergency, a reactor can usually be shut down instantly. But operators still need to pump cool water to the core for a few days, until the plant is completely stabilized. That underscores American experts' second concern, that reactors could be hampered by the failure of regional power grids or other utilities and that backup systems at cash-strapped reactors might prove inadequate. As in the West, Russian nuclear stations have emergency backups like multiple generators. But they can be thwarted by many factors like poor maintenance or a shortage of diesel fuel. <i>"Even in Western plants,"</i> an American said, <i>"the systems don't work right all the time."</i> Russian experts nevertheless said they were atop the situation. The top year 2000 official in the Atomic Energy Ministry, Yuri Sokolov, said in March	The New York Times June 23, 1999 Michael Wines

	<p>that experts had checked 97 percent of date-sensitive reactor components. Mr. Sokolov did not say what that review found, but he said his ministry would use all means at its disposal to correct any flawed hardware or programs. Mr. Ivanov said flatly that the only computer systems with potential problems were those that process data and that all systems that affected critical reactor operations had been deemed safe, as have the systems that contain radiation. Still, he indicated that Russian experts harbored some of the lingering concerns that nag American scientists. Russia, it turns out, is not the Americans' greatest concern. The greatest potential for problems is in Ukraine, which is in even worse financial shape. It has 14 reactors in operation.</p>	
European Union Ex Soviet Bloc	<p>BRUSSELS (Reuters) - The European Commission expressed alarm Wednesday about potential "millennium bug" disruptions in public services, saying it was especially worried about nuclear power plants in the former Soviet bloc. The European Union executive said there was a lack of confidence that plants in Eastern Europe and the ex-Soviet Union had properly addressed safety and other concerns related to the Year 2000 (Y2K) computer problem. But its report, which will be presented to EU leaders at their summit in Cologne this week, also cited a host of possible threats to public infrastructure within EU borders - including electricity blackouts, breakdowns of waste water pumping stations and overloading of telecoms networks with Y2K-related calls. <i>"There is a clear political responsibility of the public institutions at all levels to intensify work on the Y2K issue... and to pay particular attention to trans-border effects and contingency planning,"</i> it said. The Commission's report examined whether Europe's public service suppliers were prepared to cope with the looming millennium bug - the inability of some computers to process dates after December 31, 1999. The EU executive, which sponsored a meeting of EU infrastructure providers in April, said reliable information was hard to get, but that some sectors in some countries were apparently not fully prepared for the date hangover. <i>"Every sector consistently reports that, in particular, smaller organizations continue to lag significantly behind large companies,"</i> it said. It did not name the countries it believed were less prepared. The report expressed the most concern about nuclear installations in eastern Europe and the ex-Soviet states -- 50 power plants as well as research and other facilities. It said the two main concerns were that the Y2K problem could cause on-site systems at power plants to fail, endangering safety, or create disruptions on electricity grids due to shutdowns of power stations or major users. <i>"The general view is there is a lack of confidence that the two main sources of concern have been appropriately checked (including contingency plans),"</i> it said. The report noted that the International Atomic Energy Agency had already asked the Commission to support inspection missions to nuclear power plants in Kozloduy, Bulgaria; Zaporizhya, Ukraine; and a not-yet named location in Russia. The Commission urged Bulgaria last month to close four Soviet-made nuclear reactors at Kozloduy earlier than planned, saying they posed a safety risk. The report said Y2K preparations by Western Europe's airline sector were well advanced, but risks connected to interactions with the EU's neighbors needed to be more fully assessed. It said the EU's financial sector was also generally well prepared but may have underestimated risks not directly associated with information system failures - such as credit risks or liquidity problems.</p>	Suzanne Perry, Reuters, 2 June 1999
Ukraine	<p>Y2k programmer Valentin Ponomarenko with IAEA identifies 1 July 1999 as a Y2k problem date at Ukraine's NPPs - <i>"No one knows what will happen . . . in a very worse case scenario, a serious accident could result from a massive failure of the safety programme at a nuclear plant."</i> Apparently this is because 1 July is the date at which the NPP computer systems begin to recognise the impending year 2000 as the system commences the first of its six month safety checks. <i>"In an absolutely worse case, a nuclear reaction could get out of control, and the people watching would have no idea."</i> said Ponomarenko although official at the Chernobyl plant argued the contrary that <i>"It absolutely cannot happen here - we have the situation fully under control"</i>, although the Chernobyl management noted that it had not taken any special steps to deal with a possible onset of Y2k problems on 1 July.</p> <p>The US State Department fact sheet advises American citizens planning to be in the Ukraine over the New Year to prepare for weeks-long power outages and possible subsequent shortages of potable water, food and medicines.</p>	Kiev Post, 10 June 1999, Vol 5 Issue 23
United States	<p>NRC PLANS FOR Y2K CONTINGENCIES: The Nuclear Regulatory Commission has developed a contingency plan for dealing with computer problems that could conceivably develop at a licensed nuclear facility at the start of the Year 2000. Part of the plan includes a proposed policy statement on the use of enforcement discretion during the Y2K transition. The "Year 2000" or Y2K problem refers to computers' potential inability to recognize dates beginning with January 1, 2000, and beyond. It arises from computer programs that use two-digit numbers to represent a calendar year (such as "98" for 1998). For example, computer systems could read</p>	NRC, 14 June 1999

	<p>"00" as 1900, rather than 2000, potentially causing computer systems to malfunction. The NRC has been working with its licensees to ensure that potential Y2K issues have been identified and corrected and that the agency's own computer systems involved in emergency response communications with licensees will continue to function properly during the transition from 1999 into 2000. Based on NRC's Y2K reviews and audits of nuclear power plants and other licensed facilities, all licensees are expected to be Y2K ready well before December 31, and the Y2K transition will not affect continued safe operation of their facilities. Although the need for NRC action during the Y2K transition is considered unlikely, the NRC has developed a contingency plan for ensuring that public health and safety and the environment will continue to be protected, even if unforeseen Y2K problems occur at a licensed nuclear facility. The plan has three major facets: Incident response -- How the agency will be prepared to respond if a safety-significant event should occur as a result of a Y2K problem at a nuclear power plant or other NRC-licensed facility . Information Sharing -- Communicating any Y2K problems reported by U.S. nuclear power plants or those abroad and passing on the information to domestic plant operators. Regulatory response -- Monitoring licensee activities during the Y2K transition. Being prepared to respond to licensees' requests that certain requirements for licensed facilities not be enforced so long as the safety implications are small and using such "enforcement discretion" would help maintain a reliable and stable electrical grid. The plan calls for staffing NRC's headquarters Operations Center in Rockville, Maryland, beginning at noon on December 31. Backup will be provided by NRC's regional office in Arlington, Texas. NRC staff will be stationed at each nuclear power plant site and uranium enrichment facility site as well as in each NRC regional Incident Response Center in King of Prussia, Pennsylvania; Atlanta, Georgia; and Lisle, Illinois. In addition, portable satellite telephones will provide backup communication, if needed, at each plant and facility site. Comments received on the draft contingency plan published last December have been incorporated to the extent applicable. The proposed interim enforcement policy on exercising enforcement discretion during the Y2K transition is available for public comment at the same locations identified above. Comments will be considered in the next revision to NRC's enforcement policy.</p>	
France	EDF will finish 3 year programme on Y2k compliance with final tests in July 1999. EDF state that 80% of necessary corrective measures have been taken and F600 million has been spent to upgrade hardware - at Civaux-2 Y2k simulation trials proved successful	Nuclear Europe Worldscan, June 1999
Russian Federation	<p>Wake up to Y2K bug, Duma tells Russia (Recasts with Duma law, details) By - Russia's parliament told the nation Thursday to wake up to the dangers of the 2000 computer glitch, but a new law provided no real remedy for a problem Moscow has been slow to recognize. The law, passed unanimously by the State Duma lower house, obliged government and private entities to work out plans for averting chaos at midnight on December 31. Computer experts in the West have been busy for months to make sure that older computer systems do not go haywire by mistaking the year 2000 for the year 1900. The new law marks a growing realization that Russia too is exposed to the risks, which could shut down public utilities and throw air traffic into confusion. Shortly before the Duma vote, the government's top official overseeing the so-called Y2K problem dismissed the dangers. "Russia expects nothing terrible," Ilya Klebanov, deputy prime minister for the military industrial complex, told Ekho Moskvyy radio. Although Russia has fewer computers than the West, experts have raised fears because of the country's vast nuclear arsenal, atomic power stations and other industrial facilities. Fears of a Y2K flaw confusing military radar systems have prompted the United States to propose joint staffing of missile early warning stations to prevent a mistaken warning of a missile attack. Cooperation on Y2K military issues has continued despite a halt in other military ties because of the war in Yugoslavia. Klebanov also said a government commission was set to be formed next month and members would travel the country to check on progress against the bug. Former Prime Minister Yevgeny Primakov, who was sacked in May, had set up a commission in January to combine efforts by central and local government. "Work is proceeding fruitfully, but as always there is not enough financing," Klebanov said. He said some ministries, such as those for atomic energy and fuel and energy, were dipping into their reserves for funds to beat the bug. Russian government experts have said the country needs \$2-\$3 billion dollars to tackle the millennium bug. Military officials say they have just \$4 million to spend on upgrading the nuclear arsenal's computer brains. By contrast, the U.S. state of Texas alone is spending \$280 million to fight the millennium bug. The Duma legislation passed Thursday does not provide new funding but obliges those who own computer systems to bear Y2K- related costs. It also says entities with computer systems must warn users of possible failures in the system and work out crisis plans in case failures occur. Last</p>	Eastern Europe, Republics Nuclear Power News, June 24, 1999 Adam Tanner Moscow (Reuters)

<p>East Europe - not just nuclear</p>	<p>week President Boris Yeltsin also issued a decree urging measures to deal with the problem.</p> <p><i>"Most of Eastern Europe is between 18 and 24 months behind in preparations for the millennium bug,"</i> ING Barings said in a recent report. <i>"And while Turkey also shares in this lack of readiness for the problems the turn of the century will cause a wide range of computer programs, Israel is the fifth most prepared country in the world,"</i> the bank said. <i>"With the exception of Israel, most countries in the emerging Europe region are one-and-a-half to two years behind with their Y2K projects,"</i> ING Barings said. In a report based on a survey of companies in the region, ING Barings said a lack of resources and a scarcity of qualified programmers were some of the reasons behind the lack of preparedness. <i>"Lack of resources does not allow for investment in new equipment and is one reason why so few governments...had made early preparations for the millennium,"</i> it said. The report expressed particular concern about the impact of Russia's economic crisis on the country's ability to eliminate millennium bug problems. ING Barings said many governments in the region assumed that because the level of computerization is relatively low, the millennium bug won't have a major impact. The bank said that while \$8 billion was spent on information technology in eastern Europe in 1997, the corresponding figure for western Europe was \$104 billion. <i>"The levels of awareness...vary from not knowing what the Y2K bug is, to assuming that equipment which is quite 'newish' will remain unaffected..."</i>, the report said. <i>"This complacency has grave safety implications, in particular concerning nuclear power plants and air traffic control systems."</i> The fact that over 80% of software being operated in eastern Europe is pirated has also stalled efforts to correct the problem, the bank said. Romania is the least prepared country of those it surveyed, the report said, while Hungary is the most prepared in eastern Europe. ING Barings said Czech companies appear not to have confronted the problem in the belief that they won't be affected by it, while until recently the Czech government <i>"had not take any formal steps to set up Y2K programs or even to set its own house in order."</i> The report said the Polish government and most companies <i>"seem to have underestimated the Y2K problem."</i></p>	<p>Europe Unprepared For Millennium Bug - ING Barings LONDON (Dow Jones)-- Paul Hannon DOW JONES NEWS, June 1999</p>
---------------------------------------	---	--

Comments under Topics are verbatim or truncated extracts from sources cited.

TABLE 7 - POSSIBLE AND POTENTIAL Y2K FAILURE CONSEQUENCES - FUEL AND WASTE FACILITIES

RISK PROCESS	RISK-CONSEQUENCE
FUEL FACILITIES	
<p>REFINING: Ore to Yellowcake - Producing U concentrate from uranium bearing ore involves nitric acid dissolution, solvent extraction then one of three processes (TDN, ADU or AUC) to convert to UO₃ or UO₂</p>	<p>Generally, risks and dangers arising from malfunction of a chemical processing stage, particularly fire during solvent extraction and fines explosion during calcination stages. Main risk generally confined to plant areas - knock-on risks might apply to tailings ponds, containment bunds, etc..</p>
<p>U²³⁵ ENRICHMENT: Conversion to uranium hexafluoride (UF₆) involves reduction by hydrogen or ammonia to UO₂ in a kiln, hydrofluorination either by wet hydrofluoric acid or by dry reaction with hydrofluoric gas, then fluorination in a flame reactor and stripping with potassium hydroxide. Thereafter the UF₆ is fed through low-pressure cascades, either diffusion or centrifuge, to obtain enhanced levels (enrichment) of U²³⁵ for 2 to 4% for civil reactor fuel and, higher, up to >90% U²³⁵ for research and nuclear propulsion reactors and nuclear weapon fissile components.</p>	<p>Involves considerable UF₆ national and international flask traffic between nuclear fuel plants with, for charging and discharging the transportation flasks, heating to the gas phase of UF₆ is necessary, so Y2k related problems at filling and transportation stages could result in significant UF₆ release and rapid deposition to ground. Throughout the enrichment process inventory controls are applied and these may be Y2k sensitive which could result in incorrect enrichment and loss of quality, perhaps have future affect at some reactor core reload. Main risk generally confined to plant areas, although public domain risk with transportation by road, rail and sea.</p>
<p>FUEL FABRICATION: For dioxide fuel, one of three processes, either precipitation and calcination or pyro-hydrolysis and reduction to UO₂, thereafter addition of any neutron poison,</p>	<p>Dangers and risks arises from considerable amount of automated chemical process control and assaying, so many opportunities for Y2k glitches to arise, giving rise to excessive pressure and/or</p>

<p>gadolinium, and sintering the compacted pellets under a reducing hydrogen atmosphere.</p> <p>For metal fuels, such as Magnox, reduction magnesium combines to separate out the fluoride of the UF₄ feedstock with vacuum casting into the fuel rod, which is subsequently machined and canned.</p> <p>Mixed Oxide Fuel (MOX) receives plutonium dioxide from fuel reprocessing which is mixed in concentrations up to 10%⁺ with uranium dioxide. Thereafter following the pelletising and sintering route as for uranium dioxide fuels - particle sizes used in the pre-pelletisation mixing process are extremely fine.</p>	<p>overheating, failure to ventilate process areas and the formation of explosive products and, for base elemental metal fuels (Magnox), fuel pyrophorosity (ignition).</p> <p>Nuclear criticality for both highly enriched and also for low enrichment fuels where some localised disruption may have occurred, such as flooding.</p> <p>MOX fuels have enhanced criticality and radiotoxicity because of the presence of plutonium - air contamination presents major difficulties. MOX fuel fabrication plants are relatively new and incorporate high degree of automatic processing by digital system control - since in the event of an accidental release, particularly at the mixing and sintering stages, the Pu particles sizes are very small, the inhalation hazard zone could be very large and widespread, depending on prevalent meteorological conditions</p>
<p>FUEL REPROCESSING: Irradiated or spent fuel separation commences with pre-storage, usually under water, thereafter mechanical separation of the fuel rods (head-end chopping), dissolution in nitric acid, centrifuge extraction to remove non-soluble fission products and several stages of chemical separation involving aqueous (nitric) and solvent (butyl) stages, yielding high-level waste, uranium and plutonium streams - for further fuel use, uranium stream may be converted to UF₆ to be used as feedstock for uranium enrichment.</p>	<p>Some problems may be experienced in the United Kingdom with the leak detection equipment for transportation flasks of irradiated fuel - see TABLE 4.</p> <p>Accountancy procedures in modern reprocessing plants are highly automated and relate to the chemical separation of the fuel, waste storage and waste emissions.</p> <p>In the actual reprocessing, particularly at the pre-separation stages, Y2k glitch errors could have significant detriment downstream at the separation stages. Waste storage requiring continuous cooling, that is high- (both liquors and glass) and some intermediate-level wastes, requires guaranteed power supplies in the vent of a facility blackout. Waste emissions may be at risk of premature discharge of relatively short live radio-isotopes if date sensitive trending data is incorrect.</p> <p>The complexity of fuel reprocessing facilities and the very large quantity and variety of radioactive materials held and processed on such sites provides opportunity for a wide range of Y2k related accident and release scenarios.</p>
<p>WASTE</p>	
<p>HIGH LEVEL: Includes storage of untreated irradiated fuel, either long term for eventual disposal or awaiting reprocessing; storage of fission product waste in liquor form from reprocessing, and vitrification and storage of fission product waste.</p> <p>Reprocessing facilities such as BNFL Sellafield hold enormous stocks of high-level wastes - BNFL holds approximately 2,000m³ of liquor HLW @ 3.2.E14-1.28.E13αBq/m³ and 8.4E16-5.98E15 βγBq/m³ from Magnox fuel reprocessing, with a smaller amount of HLW from THORP reprocessing currently under development, although fuel awaiting THORP reprocessing is currently at several thousand tonnes.</p>	<p>Continuous cooling is required for air and water pond stored fuel, reprocessed recovered fission product liquors and vitrified wastes. Liquors require stirring, mechanically or by pulse, for temperature control and control hydrogen evolution rate, so emergency on-site power requirements crucial in the event of a facility blackout. Off gas and sparging systems are essential to vitrification process safety.</p> <p>Continuous operation of monitoring and alarm equipment essential - fission product inventory of the liquor stage very large and the small releases to the environment could have very significant environmental and health impact</p>
<p>INTERMEDIATE LEVEL: Preparation and packaging processes include bituminisation, cementation, ion-exchange, precipitation, flocculation and simply bulk storage awaiting natural decay.</p>	<p>Modern waste preparation and treatment plants are fully automated and process controlled by digital system - Y2k failures and glitches could result in incorrect mixing of key components and, importantly, premature release of radioactive emissions and effluents due to incorrect calculations relating to the radioactive decay process.</p>

LOW LEVEL: Includes incineration, drying, compaction and liquid and gaseous emissions from nuclear plants, laboratories, hospitals and other facilities.

Loss of incineration temperature control and off gas treatment quality could result in significant and widespread release of radioactive substances, corrosive and chemical compounds, including dioxins, HCL, SO₂ and NO_x.

GLOSSARY

Common-Cause Failure

This is where a single cause, ie an incorrect date, will cause failures in otherwise unrelated and or diverse systems - similar to Common Mode Failure.

digital

Correctly a system that transfers information by binary code, that is by a string or series of discrete values of either '0' or '1', but here where some action or measurement is translated into a digit and transmitted by wire or radio, etc., signal to another similar device which converts the digitised signal into some analogue action - for example, dialling out on the older type of telephone dial converts a radial analogue signal into a digital code (series of blips) - see '[hard-wired](#)'.

Defence-in-Depth

Generally, a multiple layered approach to safety, incorporating redundancy and diversity and, particularly, where a defaulting reactor system will tumble down to a stable situation - for example, in the event of a complete station black-out the UK AGR reactor is intended to automatically close down and its reactor core and fuel remain stable on natural (convective) cooling alone.

diversity

Where an entirely different means is available to achieve the same objective - for example, to close or SCRAM a nuclear reactor the boron control rods are driven into the core to quench the nuclear reaction but a standby diverse system would be (for the UK advanced gas cooled reactor) to inject a boron pellets into the core.

embedded chips

Usually a small (finger nail sized) microprocessor included with the circuit of an electronic device which performs a number of calculations or actions that are inaccessible to the user - for example, the chip inserted into a mobile telephone or smart credit card which identifies the individual user but which is also likely to complete some hidden date related function relating to the card expiry period or similar.

grid

The network of (usually) overhead electricity power lines that criss-cross a country linking power stations and users - the grid is divided into regions and local areas with connections (interconnectors) between countries - each power station has to be synchronised to the grid in both voltage and current wave forms and frequency, so that grid controllers have to continuously render adjustment to the grid to maintain stability and balance over large areas - this requires control signals being transmitted over long distances via (public) communication systems which may not be entirely under the control of the grid controller.

hard-wired

Jargon - means that there is a direct physical link between the actuating device and the function - for example, the pedals on a bicycle are '*hard-wired*' to the rear wheel via the chain.

NRC

Nuclear Regulatory Commission - the United States nuclear regulator.

primary containment

The first envelope of containment of a nuclear reactor, usually taken as the reactor pressure vessel which is usually located within the large secondary containment dome that characterises PWR and BWR power plants, although some reactor

systems do not have secondary containment, for example the UK Magnox and AGR gas-cooled reactors, the Russian VVER 440 and RBMK reactors.

PWR/BWR

Pressurised and Boiling Water Reactors, the dominant types of commercial power station reactors

redundancy

Where a second or more identical back-up systems are available - for example, where a second pump is always held in reserve in contingency for the primary pump failing.

sub-routine

Commonly used in computer code or programmes (software) for a repetitive action, such as calculating the time or date - the main program might visit or 'goto' a particular sub-routine several times in its operation so a) any error generated within the sub-routine will be passed back to the main programme at different points in its execution - some of these points may pass the sub-routine error whereas another point might fail on the error or b) the program might crash in the sub-routine.

synchronisation

Since electricity supply is alternating, each power station has to align its output with the frequency and wave forms of the grid - some of the international interconnectors operate at very high voltage dc or direct current.

VHF

Very High Frequency - a wave band set used in communications transmissions.

Y2k

Acronym - Year 2000 > Y2 kilo > Y2k.

1972

Like January 1 2000, January 1 of 1972 was a Saturday and since 1972 was a leap-year that matches leap-year 2000.

REFERENCES AND NOTES

1 For example, an NRC audit of the US Seabrook nuclear power plant, identified 1,304 separate software items and embedded chips that were affected by Y2k, of which 12 were described as having 'safety implications' including the safety important *Reactor Vessel Level Indication System*, another 13 could result in a reactor to trip and, of the remaining Y2k prone systems, 160 affected systems required by NRC regulations and 800 were 'significant to business' (ie the generation of electricity) - NIRS, <http://www.nirs.org/y2k/NUCLEARPOWERANDY2K.htm>, 1999 - in another example (see Ref 20) applicable to a group of about 12 power stations, 4,841 different types of items were identified as potentially Y2k sensitive of which 3,113 related to plant or engineering systems (here there is only entry for each type of item, so to total number of systems would be much higher) - of the 3,113 items about one-half were considered to be 'essential'

2 The fact that some systems refer to year 1999 by four digits as "1999" does not preclude Y2k failure since the first two digits ("19") of the date string might be *hard-coded*, hence year 2000 becomes "1900". Also, note that different number formatting adopted by different countries might result in an incorrect period either passing through or failing a system - for example, a date interval incorrectly calculated at, say 1000 days and represented thus "1,000" with the comma separator, might be read in the United States as 1000 days but in some European countries as 1 since the comma is used as a decimal separator. There are also so relatively distance dates that might fail - for example some Unix systems store the date in terms of the number of seconds lapsed since 1 January 1970 in a 32 bit register which will overflow some time in year 2038

3 *Embedded Systems and the Year 2000 Problem, Guidance Notes*, IEE Technical Guidelines 9:1997, ISBN 0 85296 930 9.

4 KRAIG M, *The Bug in the Bomb: The Impact of the Year 2000 Problem on Nuclear Weapons*, British American Security Information Council Report 98.6, November 1998 - this gives an unsourced Y2k failure rate of between 2 to 5% of all embedded chips in the weapons control and deployment systems of the United States.

5 US NRC *Contingency Plan for the Year 2000 Issue in the Nuclear Industry*, May 1999 - The NRC gives specific examples of internal facility risks at nuclear power plants to include computer-based control systems for feedwater control, turbine control, and generator voltage regulator control; plant process computer; control rod position information system; security computer system; and area radiation monitoring systems - see also *Effect of the Year 2000 Computer Problem on NRC Licensees and Certificate Holders*, NRC, Information Notice 98-30, August 12, 1998.

6 Ref 41 reports on the state of the UK nuclear power industry and gives a number of Y2k generated incidents found to date at commercial nuclear power plants in the UK.

7 In the UK, for example, some of the early Magnox power stations still in service date from the mid-1960s (Bradwell, Sizewell, etc), with Calder Hall (~200MWe) was originally commissioned in 1956 - the BNFL Magnox irradiated fuel reprocessing works (B206) dates from the mid 1960s although it has been extensively refurbished since its original commissioning.

8 From the author's general observations in visiting Russian Federation and former Republics, Territories and States of the former Soviet Bloc. The Russian Federation Y2k programme involves the Ministry of Atomic Energy (Minatom), Rosenergoatom (nuclear operator), Central Research and Science Institute (Atominform), Research and Development Institute of Power Engineering (RDIPE), All-Russian Science and Research Institute (VNIIAES), and Smolensk, Novovoronezh, Kalinin, and Balakovo NPPs. The State Communications Committee, Goskomsviaz, had issued a Y2K action directive, recognizing the need to address the Y2K problem. Minatom established a Y2K Coordinating Commission, which distributed an assessment survey to Minatom organizations. Rosenergoatom issued a letter to the nuclear power plants requesting they inventory and assess existing systems and components. The Russian regulator, Gosatomnadzor, has not issued any Y2K official guidance but has notified plants that Y2K inspections will be conducted.

9 US NAERC (North American Electric Reliability Council) *Preparing the Electric Power Systems of North America for Transition to Year 2000 - A Status Report and Work Plan*, September 1998 - this identifies a number of specific Y2k failures, including power circuit breaker malfunctions, loss of grid impedance and other controls and, beyond the grid itself, large load demand fluctuations if and when other industrial systems failed.

10 Jackson S A *Exterminating the Bug: Governmental and Industrial Challenges in the Face of the Year 2000 Problem*, Int Wshop Impact of Year 2000 on Nuclear Ind, Ottawa February 1999 - this provides an example of a cascaded grid failure in 1996 in Oregon, United States, where a grid transient, commencing from an overhead power line sagging onto a tree, resulting the loss of 30,000MWe of load and 25,000MWe of generating capacity comprising 190 generating plants, including 4 nuclear power stations, that tripped off load and underwent a station 'black-out' or 'loss-of-offsite-power' (no external power supplies).

11 Holland, for example, is considering whether to isolate its international interconnectors during the millennium transition, that is neither importing or exporting electrical power.

12 At close down it is necessary to apply a Temperature-Pressure Management Regime in order to protect the reactor containment (RPV - reactor pressure vessel) - this is particularly stringent for older plants where the RPV is likely to have undergone embrittlement by neutron irradiation over its years of service - for example, UK Magnox and former Soviet Union and Eastern European VVER 440 reactors are acknowledged to be a risk of RPV failure in the event of an uncontrolled shut down.

13 For example, a 300-500MWe rated UK Magnox reactor requires about 15MWe electrical supplies for reactor cooling immediately upon shut down of the reactor to dissipate the reactor decay heat and (radio)activity, a further 1 to 3MWe for out-of-reactor core irradiated fuel cooling and, with other station auxiliary power needs,

a typical UK twin reactor Magnox power station would demand about 40MWe of immediately available electrical power.

14 US NRC *Individual Plant Examinations - Initiators of Reactor Core Damage*, 1988 – reactor core damage is a very serious precursor to a large radioactive release should, with its fuel core damaged, the reactor primary and, where provided, secondary containment systems fail. For example, the Three Mile Island (1978) accident included a reactor core damage where a partial primary containment failure occurred, but where the secondary containment held – Chernobyl (1986) was a complete failure of the primary containment and where there was no effective secondary containment.

15 It might be reasoned that newer plants with digital control systems may be the most vulnerable - the control and protection functions that these digital systems perform often incorporate time-dependent algorithms.

16 US NRC *Contingency Plan for the Year 2000 Issue in the Nuclear Industry*, May 1999 - this gives example of a road delivery of water on route to the US Turkey Point NPP in the aftermath of Hurricane Andrew was diverted by local law enforcement officials for another use - another example, relates to the natural time scales of river flows that could affect nuclear power plants downstream of, in this particular case, an ice jamming of the Missouri River in January 1999 which took several days to manifest itself at the downstream NPP - the Y2k problem here is if telecommunications systems failed over several days - for continuing generation operation a NPP requires a considerable range of station consumables, including, for water moderated reactor plant, main generator hydrogen, nitrogen for the containment atmosphere, CO2 for fire fighting, sodium hypochlorite for chlorine injection, etc..

17 US NAERC (North American Electric Reliability Council) *Preparing the Electric Power Systems of North America for Transition to Year 2000 - A Status Report and Work Plan*, September 1998 - WILLIAMS L G, *The Millennium Bug And Nuclear Safety*, Director of Nuclear Safety Directorate and Chief Inspector of HM Nuclear Installations Inspectorate, London, February 1999

18 NEI/NUSMG *Nuclear Utility Year 2000 Readiness 98-07* - this gives example of the loss of heat sink (condenser cooling) of nuclear power plants located downstream of hydro-electric facilities, relating to failure of the systems that control the amount of water released from the reservoir or hydro-electric dam, with the US Army Corps of Engineers identifying a number of potential Y2k failures.

19 NEI/NUSMG 98-07 *Nuclear Utility Year 2000 Readiness Contingency Planning Guideline, 1998* - this report proffers a number of contingency plans which introduces a diversity element by proposing to set the backup computer time clock by 28 years from the current date - this being a novel form of 'work-around' - see also Ref 20 - see also NEI/NUSMG 98-07 *Nuclear Utility Year 2000 Readiness, 97-07*, October 1997

20 BOSLEY M J, *The Impact of the Year 2000 on BNFL's Magnox Power Stations*, Nuclear Engineer, December 1998 - gives example of a variation of 'work-around' at two UK Magnox power stations whereby a real time system, SWEPSPEED developed in the late 1970s, has had to have its real time clock set back by 10 years to avoid its termination date of 31 December 1995 at which the system would have failed.

21 In fact, the IAEA suggest another 'work-around' approach when referring to Y2k problems that might affect radioactive waste systems, inasmuch that *"the slowness of the process (a radioactive waste release to the environment) can be taken into account when dealing with Y2K problems but (this) does not justify ignoring the problem"* - see IAEA-TecDoc-1073 *Safety Measures to Address the Year 2000 Issue at Radioactive Waste Management Facilities*, March 1999.

22 IAEA, *Guidance for Achieving Year 2000 Readiness*, Department of Nuclear Safety, Division of Nuclear Installation Safety and Department of Technical Co-operation, Division for Europe, Latin America and West Asia, January 1999 and WILLIAMS L G, *The Millennium Bug And Nuclear Safety*, Director of Nuclear Safety Directorate and Chief Inspector Of HM Nuclear Installations Inspectorate, London, February 1999 - both sources recommend that a *Work-Around* is not a preferred Remediation Strategy, although the IAEA acknowledge that *Work-Arounds* are, however, a pragmatic reality but that they should be subjected to analysis to ensure that they are achievable and safe, and consideration should include failure modes, interaction effects,

and the consequences of failure upon staff resources, although see Ref 19 and 20 which contradict this, particularly Ref 20 which states *"Remedial work will only be taken when absolutely necessary and if work arounds are impracticable . . . one approach is to simply turn the system off and restart it some time later"*.

23 For example, the age related embrittlement of the reactor pressure vessel steel requires the operator to reassess the temperature-pressure management envelope (see Ref 12) which, to maintain the safety case for the RPV, results in modification to the TP envelope - for example, the UK Magnox reactors have, over the years of operation, undergone a series of temperature-pressure deratings to maintain RPV containment compliance.

24 The US NRC have been addressing Y2k since about 1995 with its first notification to licensees of the potential problems at NNPs and other nuclear plants, then in 1998 the first of the generic letters - NRC Generic Letter 98-03: *NMSS Licensees' And Certificate Holders' Year 2000 Readiness Programs* - and it constantly reviews the nuclear operators' and its own position via a series status reports - eg *Status of the Nuclear Regulatory Commission's Year 2000 Efforts* Quarterly Report for February 1999. The Generic letter stipulates that:-

" . . .

To gain the necessary assurance that action addressees are effectively resolving the Y2K problem and are in compliance with the terms and conditions of their licenses or certificates, and NRC regulations, NRC requires that all action addressees submit a written response to this Generic Letter, as follows:

Within 90 days of the date of this Generic Letter, submit a written response indicating whether you have pursued and are continuing to pursue a Y2K Readiness Program. Present a brief description of the program that has already been completed, is being conducted, or is planned, to ensure Y2K Readiness of the computer systems at your facility. This response should address the program's scope, assessment process, and plans for corrective actions, including schedules for testing and validation. If an addressee chooses not to take the requested action(s), provide a description of any proposed alternative course of action, the schedule for completing the alternative course of action (if applicable), and the safety basis for determining the acceptability of the planned alternative course of action.

Upon completing your Y2K Readiness Program, or, in any event, no later than December 31, 1998, submit a written response confirming that your facility is Y2K Ready and in compliance with the terms and conditions of your license or certificate, and NRC regulations; or, if your facility is not Y2K Ready by December 31, 1998, then submit a written response that contains a status report of work remaining to be done to become Y2K Ready, including completion schedules. For systems that may affect safety and safeguards, contingency plans to become Y2K Ready and Y2K Compliant should be included in your response.

For facilities that are not Y2K Ready on or before December 31, 1998, submit a written response, by July 1, 1999, updating the status and schedule of your Y2K Readiness Program submitted in (2), above. The response should contain a status report of work remaining to be done to become Y2K Ready, including completion schedules. For systems that may affect safety and safeguards, contingency plans to become Y2K Ready and Y2K Compliant should be included in your response

If you determine, as your review evolves, that your facility is not Y2K Ready after submitting information in response to this Generic Letter that states that your facility is Y2K Ready, submit a written response containing the information as requested in (3) above. The written responses should include sufficient detail to assess the licensee's or certificate holder's Y2K Readiness Program.

..."

25 In the UK, for example, the continuing justification of nuclear plant safety is determined by the submission of *Justification for Continued Operation* (JfCO) statements from each site licensee for each of the key dates, the first of which was 31 December 1998 - 1 January 1999 - ALLARS K J, *NII Quarterly Report for Dounreay*, April 1999 - this report notes that, but does not identify, a small number of systems across the UK nuclear industry had been identified as being potentially affected on this the 1998 to 1999 transition date but

none, it claimed, embodied any significant threat to safety, even prior to rectification - in addition, a few unspecified system faults actually occurred at around the date transition to 1.1.99, but generally these were found not to have been caused by a millennium date problem - the next identified critical date identified by the UK regulator is 9.9.99.

26 For example, say the safety case probabilistic risk for particular safety system in a nuclear plant was deemed to be acceptable at 1 in 10,000 failures per year of operation pre Y2k. Now if it is absolutely certain that all Y2k glitches had been remedied, the post Y2k risk frequency would remain unchanged. If, however, there was a chance of, say, 50% that a Y2k glitch remained hidden in the system, then the post Y2k risk frequency is reduced to $(0.5 \times 10,000)$ 1 in 5,000 per operational year which may be considered to be an unacceptable risk. Of course, it may be that the regulators are able to ensure that the operators use all possible means to locate and remedy Y2k glitches within the nuclear plant's internal systems, thus reducing the chance of a rogue glitch remaining to a few or a fraction of a percent, but that same degree of scrutiny and success cannot be applied to the external Y2k triggered events.

27 The NRC admit as much (see Ref 5) with the statement " . . . However, because of the nature of the Y2K issue, it is not possible to be 100 percent certain that all potential problems will be corrected. For this reason, the NRC established a task force to develop a contingency plan for ensuring that public health and safety and the environment will continue to be protected, even if unforeseen Y2K problems occur. "

28 The IAEA (see Ref 22) recommends in its advice to Member States that (thereby minimising the risk of primary containment breach during the Y2k transition and tacitly acknowledging that the risk of adverse incident during the Y2k transition is heightened):-

" . . .

Where possible, all invasive plant operations (e.g. on-line re-fuelling) should be avoided on critical dates. All required resources (e.g. fuel, communications, safety significant items) should be secured prior to each critical date. . . ."

29 Not so according to the NRC 's web page 'Frequently Asked Questions' (April 1999) in which the NRC requires that all nuclear power plants report their Y2K readiness by July 1 and should the NRC identify a situation where the Y2K issue results in a plant being in non-compliance with its license or NRC regulations, appropriate action will be taken and that, by September, the NRC will determine the need for issuing orders to nuclear power plant licensees to address Y2K readiness issues including, if warranted, shutdown of a plant.

30 In fact, the IAEA (see Ref 22) goes so far as to apparently condone a higher risk of operation during the Y2k transition with its advice:-

" . . .

Where licensees wish to continue operation with a number of degraded safety-related systems, then the synergistic effect should be demonstrated to be safe. Any information, obtained from other sources and used in support of the plant's JfCO, should be sufficiently detailed and authenticated to enable the safety arguments to be evaluated without the need to seek further information held by others.

. . ."

31 The ambiguity about what exactly to plan for is summed up by one UK nuclear industry manager " . . . It is impossible to guarantee absolutely that systems will not fail in 2000 and the aim of our work is to reduce the probability of failure to something which is acceptable, with any remaining residual risk being contained by contingency plans. We already have in place plans to deal with contingencies arising from normal operation (ie the Safety Case) and these will remain but will be supplemented by additional millennium specific plans. ." (BOSLEY M J, The Impact of the Year 2000 on BNFL's Magnox Power Stations, Nuclear Engineer, December 1998).

32 The NRC states⁵ that:

" . . .

In an effort to help ensure reliable power to the electric grid during the transitional period of the Y2K rollover date, as an important aspect of the protection of public health and safety in the broader sense discussed above, the task force recommends the following:

Licensees may invoke 10 CFR 50.54(x) to maintain continued plant operation, providing the licensee determines that no significant safety concern results during a Y2K transition period of several days beginning on January 1, 2000.

- or -

The staff may provide a revised enforcement discretion policy specific to the Y2K transition period with specific guidance on those circumstances under which continued plant operation would be permitted and no significant safety concern results.

The NRC will provide support staff consisting of projects and enforcement personnel in the Operations Center to assist licensees in making prompt operability determinations during this transition period.

..."

10 CFR 50.54 relates to the inspection and testing of the primary pressure containment, although Clause (x) does not seem to be available in the public domain.

33 Internet site IAEA *Y2k Activities of Member States*, May 1999 in response to IAEA, *Guidance for Achieving Year 2000 Readiness*, Department of Nuclear Safety, Division of Nuclear Installation Safety and Department of Technical Co-operation, Division for Europe, Latin America and West Asia, January 1999 - the IAEA undertook this activity as a result of Resolution GC(42)/RES/11 Measures to Address Year 2000 (Y2K), 25 September 1998

34 When asked to confirm if its web page included all of the Member State responses (16 responses in total) the IAEA replied by e-mail (M.Libby@iaea.org - 21 May 1999):

" . . .

We only post responses contributed and have received none with any restrictions. Many countries are so tired of responding to questionnaires (sic) that they just don't respond.

..."

In fact, the IAEA request for information on the state of readiness by Member States was agreed at the 42nd General Conference of September 1998 attended by over 120 countries, so the response of just 16 is somewhat disappointing.

35 In comparison, the UK claims to be 100% Y2k ready in its nuclear fuel cycle and 95% ready in its electricity generating sector, which includes conventional fuel fired plants – see *Action 2000 Report* published in most UK national newspapers. However, when the Action 2000 Helpline is approached for further details nothing is available to demonstrate the UK Y2k audit.

36 The UK NII list is not believed to contain all specific instances of Y2k non-compliance but, instead, examples of the types of Y2k non-compliance discovered to date.

37 JOLICOEUR J R, *Updating the Emergency Response Data System for the Year 2000*, NRC October 1997 - the NRC emergency communication system was Y2k sensitive.

38 NEI/NUSMG 98-07, August 1998 - Appendix B *Examples of Remediation Risk Planning* - this gives number of examples of the types of risk and remediation required - Appendix C Examples of Internal Contingency Plans necessary following the remediation actions of *Appendix B*.

39 In fact, emergency power supplies are not, in themselves, infallible as demonstrated by a recent incident at Peach Bottom NNP when, on 10 June 1999 at 1330 hours, the "A" diesel generator output breaker failed to

close during periodic testing, it was discovered that the plant had operated for a period of time with both required diesel generators inoperable. Based on the identified failure mode, the "A" diesel generator breaker was in an inoperable state since the last time it was tripped on 11 May 1999 with, on the same day, the "B" diesel generator was declared inoperable for the performance of periodic testing, which resulted in both generators being inoperable and the plant entering a 3.0.3 TS LCO action statement., NRC Notification, Power Reactor -Event Number: 35812.

40 For example, in radiography radiation dose calculations involve the calculation of elapsed time which may be returned incorrectly by the unit's software system - the requirement to keep accurate records may also give rise to problems and errors over longer term treatments in external beam radiation therapy, brachytherapy and shorter term treatments such as intracavity where radioactive seeds are implanted into the tissue or cavity, endovascular placements and surface plaques, etc., - see IAEA-TecDoc- 1074 *Safety Measures to Address the Year 2000 Issue at Medical Facilities which Use Radiation Generators and Radioactive Materials*, IAEA March 1999

41 WILLIAMS L G, *The Millennium Bug And Nuclear Safety*, Director of Nuclear Safety Directorate and Chief Inspector of HM Nuclear Installations Inspectorate, London, February 1999 - see also *Testing Safety-Related Control Systems for Year 2000 Compliance*, HSE, London 1998 and HENDERSON J / DAVIDSON G I. *Safety and the Year 2000*, HSE, Sheffield 1998 and *Assessment of Licensees' Safety Cases for the Year 2000 Computer Problem – NSD's Y2K Assessment Principles*, Draft – For Trial Use, Revision 1, Nuclear Safety Directorate (NSD): Health and Safety Executive (HSE), UK, 23 September 1998. *Health and Safety and the Year 2000 Problem – Guidance on Year 2000 Issues as they Affect Safety-Related Control Systems* HSE UK, INDG267 C1000 5/98.

42 Data for Canada is given on the AEC web site.

43 The NRC participates in the specialist forward planning groups *Catastrophic Disaster Response Group* and the *President's Council Y2K Emergency Services Sector Working Group*.