COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 23.11.1999
COM(1999)545 final

**REPORT FROM THE COMMISSION
TO THE COUNCIL, THE EUROPEAN PARLIAMENT,
THE ECONOMIC AND SOCIAL COMMITTEE
AND THE COMMITTEE OF THE REGIONS**

EU Infrastructures and the Year 2000 Computer Problem

♦

Q1 1999

Table of Contents

1   EXECUTIVE SUMMARY

Understanding of the nature of the Year 2000 computing (Y2K) problem has continually evolved during the past few years. It is not simply an IT system problem, nor primarily a management problem, nor even a general business problem, **it concerns interdependencies**. These interdependencies exist at many levels, the most fundamental of which are those basic infrastructures which provide the essential services upon which all depend.

Organisations completing their Y2K adaptation and testing activities are shifting their efforts to contingency planning. Their scope of interest thus becomes much wider than their own internal environment, and they must assess the effect of external factors. Inevitably, concerns arise regarding the **preparedness of the suppliers of essential services, in particular, areas such as energy, transport, telecommunications, finance, and water**.

The information which is presented in this report is intended to provide a **broad overview of the Y2K-related activities and issues in each of these sectors from an EU perspective**, and is aimed at national authorities, Industry in general, infrastructure operators, and the public. A comprehensive list of websites with additional information is annexed. The relevant administrations, regulatory and supervisory authorities in the Member States, as well as European and international associations, all contributed to the report.

Although the situation naturally varies between sectors and in different countries, a number of **important trends are now emerging across all sectors**, and throughout the EU as a whole. Positive developments are:

- *Regulatory and supervisory authorities are increasingly involved in monitoring and auditing vital infrastructure sectors.*

- *Co-ordination efforts are being carried out by sectoral, national, and international associations.*

- *Bilateral, multilateral, end-to-end, and national testing is occurring.*

- *Information campaigns are being planned or ongoing to maintain public confidence.*

- *Greater information on progress, results, risks, and contingency plans is available.*

- *Forerunners are helping those who are still lagging behind.*

Nevertheless, every sector consistently reported that **smaller organisations continue to lag significantly behind large companies** in addressing the millennium problem, and all organisations retain a **strong dependency upon their IT system suppliers to provide an accurate disclosure of the compliance of their products and to deliver timely compliant upgrades**.

Companies and organisations throughout the EU are vigorously tackling the Y2K problem and are now starting to demonstrate their success in doing so. The **overall assessment is that the risk of significant disruption to EU infrastructures during the millennium period is limited.** Any **problems are likely to be localised and occur in smaller organisations**. Since such risks,

however minor, still exist, efforts are ongoing in every sector to establish thorough, comprehensive contingency plans in mitigation.

The format of the report involves a general overview of each sector in the Y2K context, followed by a summary of the activities undertaken by international bodies, including specific sectoral Commission activities where relevant, and then an outline of the current EU situation. A brief synopsis of the Commission internal situation and the general Y2K-related activities of the Commission is also provided.

The Commission has, with the close co-operation and support of the Member States authorities and international organisations, undertaken a significant effort to prepare quarterly reports on EU progress in tackling the millennium bug. Various administrative difficulties have delayed publication of this Q1 99 report, and thus the response of the Commission to the request of the Council and European Parliament to be kept regularly informed of the Y2K situation in the EU. However, the adoption of the Q2 99 report will follow shortly during November. A Q3 99 report is currently in preparation and will be adopted before the end of 1999.

Each report is complete in itself, and contains useful background information which has emerged as the problem evolves. Given the international aspect of the problem, having this information available in all EU languages is important for EU business and citizens.

2   INTRODUCTION

The information on the Year 2000 computer problem (Y2K) which is presented in this report has been provided by the relevant administrations, regulatory and supervisory authorities in the Member States, as well as European and international associations. Countries which made specific contributions include Belgium, Denmark, Germany, Greece, Spain, France, Italy, Luxembourg, the Netherlands, Portugal, Finland, Sweden and the United Kingdom. Both Switzerland and Norway also reported on their situation. The reporting timeframe was mid-March 1999.

The intention of this report is to provide a current overview of the Y2K preparations of essential infrastructures, in order to assist industry and the public in gaining a greater understanding of the EU situation. The specific choice of infrastructures to be reported on was agreed in consultation with Member States. It is recognised that other domains such as health and food supply chains are also important, but health is primarily a national concern, and it is not possible to provide an EU overview of food supply chains.

This report presents the information as provided by Member State authorities and the other sources cited above. The report is not a comparative assessment of country preparedness, but rather an analysis of the main issues and the activities which are being undertaken in vital infrastructure sectors, particularly in an EU context. The role of the Commission in this domain is to facilitate the exchange of information and experiences between EU countries and organisations, focusing on areas in which there are potential cross-border impacts. The individual companies and Member State authorities concerned must carry out the necessary actions to ensure that the business continuity of essential services is maintained during the millennium changeover.

Throughout 1998, the Y2K Problem received high level political attention in the EU. The Communication of the Commission on the subject (COM(98)102), issued in February 1998, aimed to establish a shared and common understanding in Member States of the scope, the potential risks associated with the problem, and the need to take appropriate action.

This action was followed up by a Commission report presented to the Vienna Council in December 1998 on *How the EU is Tackling the Year 2000 Computer Problem* (SEC(98)2100). The purpose of this report was to provide an overview of Member State preparations and to identify areas where progress might be insufficient and greater action should be taken. Although substantial progress took place during 1998, with both the financial and telecommunication sectors demonstrating significant activity, concerns were expressed for local administrations, and for the energy and transport sectors. These concerns arose primarily from the lack of available information in these areas.

In 1999, the level of political attention being given to the issue has further intensified. The topic continues to appear on the agenda of high level meetings within the EU, including the Telecommunications and Energy Councils, and internationally in fora such as the G8.

In the first quarter of this year, as countries and organisations are completing their adaptation activities, the focus of their efforts is shifting to contingency planning. Such planning is now taking place at various levels. Individual organisations are developing plans to ensure the continuity of their own business operations. Certain sectors are in the process of establishing much more elaborate sector-wide contingency plans. This is particularly apparent in the energy, water, aviation, telecommunications, and finance areas. In several countries, government initiatives are co-ordinating the plans of emergency services at local and national level.

As organisations and sectors concentrate on contingency planning, their interest moves from the internal environment to the external environment, and specifically to the essential services upon which they rely to continue their operations. The Consumer Committee, an advisory committee to the European Commission, emphasised, in its opinion adopted the 24 September 1998, the need of consumers to receive more information on Y2K preparedness. This need is crucial in the context of services, such as telecommunications, energy supply, and transport, since consumers are entirely dependent on the capability of providers to address Y2K-related problems.

The report also provides useful pointers to the enormous wealth of additional information which is available on Internet websites. Access to clear, comprehensive information on potential implications and contingency plans is essential for consumers, particularly evidence of the 'Year-2000 compliance' of services and products, and reassurances that quality and continuity will be ensured. This information need could also be addressed through 'checklists', prepared for consumers by providers, which would help them to identify individual risks and provide instructions on how these risks could be minimised, as well as giving advice on how the impact could be reduced in case of any disruption. The Internet also provides easy access to information about the numerous technical software solutions which are available to assist organisations to identify potential problems and facilitate their adaptation efforts.

The format of the report involves a general overview of each sector in the Y2K context, followed by a summary of the activities undertaken by international bodies, including specific sectoral Commission activities where relevant, and then an outline of the current EU situation. A brief synopsis of the Commission internal situation and the general Y2K-related activities of the Commission is also provided.

3   ENERGY

3.1   Overview

The provision of energy is clearly a vital service for every aspect of an economy and the welfare of its people. In addition, with the date change in the EU occurring in the middle of winter, the need and demand for energy will be high, particularly in the more northern countries. The overall continuity of energy supplies is essential.

*Various energy forms
rely on each other, and
on other infrastructures*

This is particularly important for electricity supply, which is not stored and where supply failure could lead to failures in other areas, including telecommunications and some transport systems, building equipment such as lifts and control systems, the vast array of electrical equipment, central heating installations, and lighting. Interruptions to other energy sources, and in particular to natural gas, for which customers do not usually have storage mechanisms, would also have serious effects. The inter-reliance of energy forms is also important. Gas compression for transport and distribution requires electricity, whilst a growing share of electricity is now generated by gas in the Community. The integrity of interacting energy forms is thus essential, as well as the reliability of other infrastructure sectors, notably telecommunications.

As in all sectors, the primary responsibility for tackling the Y2K problem lies with the energy supply companies and utilities themselves, excluding the issue of equipment after the meter. The firms in this sector are carrying out rigorous Y2K programmes for their energy supply systems, as well as other systems such as internal telecommunications, control systems, office equipment, security, safety, and even financial systems, since these could also jeopardise energy supply continuity. Typically, Y2K programmes of the energy supply industry are subject to external audits.

*...with comprehensive
contingency planning to
handle residual risks*

Despite their best efforts, a residual risk of failure will inevitably remain, to be addressed through contingency plans. These may be developed in co-operation with the authorities and often involve the adaption of existing contingency plans developed to deal with other possible emergencies. Such plans need to cover all major possible eventualities, including standby energy supplies for important customers, measures to deal with the failure of essential inputs or services, such as input fuels for power stations or communications, and measures to handle the failure of key equipment items in the supply chains for the different energy forms.

Another characteristic of the energy sector is that it operates on a commercial basis, with commercial relationships governing the supply of energy to the consumer, but also for supplies to energy companies, of primary fuels for example, and for exchanges, notably across borders, between energy companies. The primary responsibility for ensuring the continuity of supply in these areas also lies with the operators concerned, who must take all necessary measures to ensure that their commitments are fulfilled.

Given the vital role of energy supply, it is clear that national authorities must also become closely involved in Y2K programmes in this sector. Their activities include ensuring that energy companies are undertaking all necessary actions, through independent audits and other monitoring; providing a platform or forum for the co-ordination of activities and the exchange of best practice, which may occur across sectors; developing sectoral contingency plans; and providing information to the public on the progress of preparations.

3.1.1 International Activities in the Energy Sector

*...with relevant industry
associations also
playing a part*

The relevant industry associations also play an important role in exchanging information and co-ordination, including at international level, particularly for the network industries of electricity and gas. The European Commission is playing a role at this level too, providing a forum for Member States to exchange information and co-ordinate their activities, focusing on areas with significant cross border effects, such as electricity and gas.

The industry association UNIPEDE/EURELECTRIC, which facilitates a regular exchange of information between its European members, has supplemented the information which has been provided by Member State administrations in this report. EUROGAS fulfils a similar role in the gas supply sector.

Flows of energy between utilities and countries must be co-ordinated...

An important issue in this sector is the interchange of electricity between utilities and countries. These flows may consist of regular trade in a particular direction, or more fluctuating flows which depend upon short term economic and load characteristics. These exchanges are co-ordinated within the UCPTE (Union pour la Coordination des Producteurs et Transporteurs d'Électricité) and the Nordic System (NORDEL) in the EU. The UCPTE proposed the adoption of a "minimal load policy" for the changeover period and to increase the generation reserve. In essence, exchanges will be reduced to a minimum, subject to contractual obligations, with each country prepared to meet its own demand. Interconnections would remain connected to allow for mutual assistance if required.

...with mutual understanding and agreement on plans for the changeover period

For all such interlinkages, notably those between critical fuel suppliers and generators, between electricity utilities, (both horizontal and vertical links), and between suppliers and very large customers, including auto-producers, it is vital that there is a mutual understanding and agreement on plans and procedures for the date change period, including any linkages with non-EU countries.

3.2 Electricity

All countries in the EU have Y2K programmes for the electricity sector, which have been running for some time, and companies expect most of their systems to be compliant before the fourth quarter of 1999.

Most EU electricity firms plan compliance well before the end of 1999
To continue to meet demand....

It is a major challenge. The whole electricity supply chain must be assured as far as possible, from the supply of electricity generation fuels, through to the consumer's meter. Since electricity is not stockable, demand must be met on a close to instantaneous basis. This requires that adequate generation plant must be running at the critical time, with instantaneous spare capacity (spinning reserves) also ready in case of plant failure. Hydro plant and pumped storage plant, which can operate autonomously and which can also generate power at very short notice, are also very useful in this respect.

...extra stocks of fuel, alternative power sources and additional communication facilities

In preparation for a possible disruption to fuel supply, stocks will be increased where not already sufficient, particularly for coal- and oil-fired generation (nuclear reactor fuel is only changed periodically). For gas-fired generation, the role of the gas supplier is crucial, although some power stations are dual or even triple fired (oil/gas/coal), an important consideration if the continuity of gas supply is not maintained. Another problem could be the failure of a large consumer, causing a sudden drop in load, which would require an immediate reaction by the grid control/dispatching centre. The transmission and distribution systems must also be assured and be able to cope with potential unpredictable changes in supply and demand. Adequate communications between all the key components is also clearly vital, and some companies have installed extra facilities to manage the grid in case of loss of telecommunication networks.

It is recognised that risks of local failures in individual smaller production or distribution facilities may exist; however, such problems can normally be handled in such a manner that they are unlikely to cause a major disturbance to the electricity consumer. The general recommendation of the sector is that "each electricity consumer should take the measures against electricity cuts that they would do under normal circumstances."

Whilst the challenges for this sector are considerable, the electricity supply industry has been working very hard to meet them, co-operating with public authorities and through various international associations, and it is generally felt that, providing the full range of measures are pursued, there should be no major failures in supply.

3.3 Natural Gas

Natural gas supply has some similarities with electricity but also significant differences, making it an important energy form with respect to the Y2K problem. In terms of similarities, it is characterised by a supply chain structure, with one connection to each consumer. The most significant difference is the large dependence on supplies of natural gas from outside the EU. Currently, such supplies account for just under 40% of total demand in the EU as a whole, with the bulk provided by Norway, Algeria and the Russian Federation. This percentage varies considerably by Member State, as does their reliance on the three particular countries. In terms of indigenous production of natural gas, the Netherlands is a very large producer, exporting about 40% of its output to other EU countries. The UK is also a major EU producer, and is now connected to the continental grid with a link to Zeebrugge on the Belgian coast.

The relevant firms in EU producing countries have been making very extensive efforts to assure the continuity of their supplies, as has the gas supply sector as a whole, which has been working on this problem for a number of years. Co-ordination with upstream suppliers, between utilities, and with customers is taking place, though there are difficulties in obtaining information on Y2K compatibility for supplies originating outside the EU. Moreover, pipelines from two of the major external suppliers cross non-EU transit countries.

One of the main considerations for the gas sector is thus how to deal with a possible interruption in external supplies. In general, to ensure supply security, the industry has been building up over a long period very substantial gas storage facilities, flexible supply possibilities with indigenous sources, and greater interlinking and diversified supplies in the European grid. These measures are able to deal with interruptions to supplies of many months and longer, and could easily cope, with suitable preparation, with interruptions created by the Y2K problem. Nevertheless, the European gas supply industry must continue to co-operate together, using existing contingency plans and facilities, in order to be prepared in the event of a major failure in supply due to the Y2K problem.

Additionally, many of the other measures mentioned for the electricity sector also apply, such as the need for a common understanding and agreement on gas interchanges between utilities, as well as on the intentions of very large consumers. Equally, other vital services such as telecommunications and electricity supply must be assured. With all these measures adequately addressed however, there should be no significant failure in supplies to final consumers.

3.4 Oil and Coal

Oil is of less concern in the EU...

Whilst the oil sector is equally important for the economy and welfare of its citizens as electricity and gas, including a vital role in transport as well as for heating, its supply structure and particular characteristics are significantly different.

...due to substantial stocks...

Firstly, oil can be readily stored, thus those who are dependent on this fuel for heating can have stocks in place. Moreover, for the oil supply industry as a whole, substantial oil stocks should exist, to meet the levels required under EU legislation for general supply security reasons (90 days consumption required to be held by the industry or designated agencies for each Member State).

...and diversification of suppliers and supply routes

Secondly, the oil supply industry is very diverse, characterised by very large multinational companies and a multitude of often much smaller independent operators. The large companies have invested considerable efforts on the Y2K problem to ensure the continuity of their operations, whilst smaller companies are typically very quick in meeting any deficiencies in the supply chain which may arise. Furthermore, this diversity is reflected in the number of supply routes and main linkages in the supply chain, with oil transported by ship, barge, pipeline, train and lorry, between diverse and competing crude oil sources, refineries and distributors.

Nevertheless, the dependence on non-EU oil supplies, at nearly 80%, is high, and as with natural gas, it is not possible to be certain of the effect of Y2K on external producer countries. Member States should therefore ensure that contingency plans are able to deal with any disruption in supplies, and confirm that measures have been taken for the key installations within their territory, such as import terminals, production and storage facilities, refineries, and major pipelines.

Coal is the energy form of least concern

The coal sector is perhaps the energy form of least general concern with respect to the Y2K problem. In part, this is because indigenous production of coal in the EU has declined considerably, primarily in Germany, the UK and Spain. It is clear however that the companies involved must take measures to prevent disruption to their production. Likewise, consumption is rather concentrated, and is mainly accounted for by power generation, steel and other industry, though these users too will need to take measures to assure their supplies and to hold an appropriate level of stocks. In addition, as for the oil sector, Member States will need to assure themselves that key infrastructures, such as import terminals and bulk transport, are assured.

4 TRANSPORT

Co-ordination mechanisms between different modes of transport are essential

As in the energy sector, several EU countries, including the Netherlands and the UK, have established national transport platforms or ministerial bodies to co-ordinate Y2K activities throughout the sector. Although Y2K problems tend to be specific to particular modes of transport, a degree of co-ordination is essential in ensuring the continuity of multimodal transport throughout the EU.

There are common transport issues, for instance the systems responsible for the opening and closing of bridges, that are of concern to shipping, as well as road and railroad traffic.

4.1 Aviation

The aviation sector represents a complex international supply chain, where aspects such as flight safety, the carrier supply chain, and the customer supply chain must all be taken into consideration when addressing the Y2K problem. It is therefore an area in which co-operation at international level is essential. Various national and international organisations in the aviation industry are actively addressing the millennium problem.

4.1.1 International Activities in the Aviation Sector

A continuous effort is being undertaken by regulatory bodies to assess and audit the state of preparedness of air transport operators and service providers falling within their authority. Particular attention is being paid to the evaluation and testing of systems which interface between different players and countries, owned by aircraft operators, air traffic control and airports.

Given the inherent cross-border nature of air transport, where potential disruptions originating in one country could have repercussions on many others, international co-ordination requires setting common standards and agreeing specific timetables for achieving compliance of computer-based systems.

The International Civil Aviation Organisation (ICAO), in an Assembly which took place in September 1998, called on its members to disclose their readiness status . This disclosure will be based on questionnaires, using criteria developed by ICAO with the assistance of certain countries and IATA. These responses will be extremely important, since they will form the basis for a global assessment of the safety of airspace, leading to decisions by the civil aviation authorities on which countries/airports to fly to at the end of this year.

EUROCONTROL has been very active in the area of Air Traffic Management by raising awareness of the Y2K problem within its Member States, particularly in national administrations providing air traffic services; as well as co-ordinating and exchanging information with relevant international organisations. The emphasis of this co-ordination has now shifted to facilitating the development of contingency plans, where a special task force has produced a set of guidelines. Practical contingency measures are being developed within the Maastricht operational centre, which is responsible for air traffic management in Belgium, Luxembourg, the Netherlands, and Germany. These measures will entail the use of military facilities as a fallback solution in a comprehensive plan designed to address various scenarios involving technical disruptions.

In the European Civil Aviation Conference (ECAC), a special group is determining the scope of actions to be undertaken under the ECAC umbrella, to complement the Y2K initiative of ICAO. This group will prepare policy proposals for the Directors General of Civil Aviation.

An International Air Transport Association (IATA) Y2K project for the clearing systems which they operate for travel agents is progressing satisfactorily. A Y2K Industry Project began in June 1998. Within this project, IATA carries out site visits to certain airports and air traffic control services. The majority of these visits planned for Western Europe were completed by mid-February 1999. Although the global picture appears positive, several issues have been identified, particularly in the smaller airports. In some cases the necessary political will is

not apparent, and a low priority is being given to the problem. Several programmes suffer from a lack of finance and manpower. Dependencies on third-party providers are not always covered.

The Airports Council International (ACI) role continues to be one of raising awareness amongst its members, sharing expertise, and assisting in finding solutions. ACI has developed a check list for assessments and advocates contingency planning. The Joint Aviation Authorities (JAA) continues to pursue initiatives with responsible authorities and organisations in connection with certified aircraft and maintenance.

AECMA members (an association of aircraft manufacturers) indicate they are well advanced in their efforts to ensure compliance and confirm that there are no safety problems with non-modified original aircraft, or with aircraft modified by the manufacturer. Some remedial work remains to be done in non-critical areas, which is expected to be completed during the next few months.

Based upon the available information, the aviation industry appears well advanced in its preparations to combat potential problems, following a thorough methodology which includes raising awareness, assessing systems, rectifying problems, and developing, testing and validating contingency plans.

Nevertheless, there are outstanding issues. Where necessary, additional efforts to raise awareness must be made. Greater sharing and dissemination of information is important to avoid duplication of effort. Many organisations including ATC providers, aircraft manufacturers, airports, etc. are still lacking essential compliance information from third-party vendors and providers. Further efforts to develop and validate contingency plans need to be encouraged.

4.1.2 EU Aviation

Throughout the EU, all players in the aviation sector are actively co-operating to ensure that air travel remains as safe during the changeover period as it is today.

Major EU aircraft suppliers, such as Airbus, have extremely thorough Y2K projects, comprising design office and system rig tests, as well as a real flight rollover on both A320 and A330 aircraft, where the date was changed in flight during August 1998. The onboard data source (clock) accepts both manual entry and automatic dates from the Global Positioning System (GPS). The only error detected was created by the date change affecting the recording of the correlation between in-flight incidents taking place before and after midnight.

As far as aircraft navigation systems are concerned, the results thus far indicate that such systems make little use of dates in a format where there is an explicit reference to the year. In real-time systems, references to time are made almost exclusively on the basis of hours, minutes and seconds. Only systems used for regulating air traffic, as well as systems for recording and archiving data make use of the full date. Aircraft navigation systems are supported by a number of fallback systems, based upon the use of various different technologies and with comprehensive contingency plans for ensuring traffic safety. It is worth noting that the density of air traffic is generally lower at night, and even more so on New Year's Eve. In the event of problems, contingency plans take into account the need to delay or reroute aircraft.

Although extensive contingency plans are being developed and implemented by individual companies, information on international strategies and developments is needed to complete such plans. The aviation industry is being advised by regulators that if they are not satisfied with Y2K compliance programmes and they have safety concerns, action will be taken to withdraw operating authorisations.

4.2 Maritime Transport

There is little doubt that the millennium bug will affect maritime transport to a similar degree as it will other modes of transport. In this sector, there are two main levels where disruption could occur. These are the ship itself as a transportation unit, and the environment wherein ships operate, the ports and terminals.

The consequences on board vessels might be as simple as a failure in a timer or a GPS receiver, or as sophisticated as the malfunctioning of the monitoring and control system for the main engine plant or of the navigation and communication systems, which could result in a loss of power or steering. Ashore, the areas effected could be as diverse as the actual services offered by ports and terminals. Problems could occur in communication systems, in cargo and document handling systems, or in the provision of radio navigation assistance - essentially in any computer-based systems.

4.2.1 International Activities in the Maritime Sector

In order to assist the shipping industry in addressing the Y2K problem, the International Maritime Organisation (IMO) has issued two circulars on the matter[1]. The first circular invited Member Governments to bring this problem to the attention of ship owners, ship operators, shipmasters and other interested parties in the shipping industry. Referring to the guidance notes prepared by the United Kingdom on the issue, the circular encouraged all concerned to become familiar with the nature of Y2K problem, to assess the potential impact on their operations, and to take the necessary actions to upgrade, replace, or retire affected systems. The second circular recommended that ships participating in mandatory reporting systems be requested to co-operate with the relevant authorities in providing information on the status of their Y2K preparations.

At the initiative of the United States Coast Guard and the United Kingdom Maritime and Coastguard Agency, a meeting was held in IMO in March 1999 to consider issues relating to the Y2K problem. Representatives of non-governmental industry organisations were invited to participate. The meeting unanimously agreed to adopt "The Year 2000 Code of Good Practice", and defined key elements of a general Y2K contingency strategy for ships, ports and terminals. Member Governments of IMO were invited to bring these results to the attention of the maritime industry as a whole[2].

---

[1]   MSC/Circ.868 of 27 May 1998 and MSC/Circ. 894 of 17 December 1998

[2]   Circular letter 2121 of 5 March 1999

The Code of Good Practice recommends measures and precautions for ships, ports and terminals to reduce the risk associated with possible malfunctions of equipment which might be dependent on electronic date recognition. In particular, it recommends the use of a set of questionnaires to be filled in by shipowners and ports/terminals, and shared between them in order to facilitate communication on the subject. If the information which is provided creates concern as to whether a planned operation can be conducted safely, then masters, port authorities or terminal operators could decide to suspend or postpone the operation. The key elements of Y2K contingency plans for the industry are provided in a short guide, aimed at assisting those in the maritime transport industry to understand those elements which may supplement/complement existing emergency response plans.

The signatories to the Paris MOU on Port State Control[3] have decided to issue a letter, intended to raise awareness on the millennium bug, to all shipmasters of ships inspected in the framework of the Port State Control in Paris MOU ports. The Paris MOU group will also investigate the possibility of taking action against individual ships as the critical date approaches, should shipmasters fail to provide a satisfactory response to queries concerning how the potential risks have been addressed on board their ships.

The involvement of international organisations and the international exchange of information is thus essential to the overall co-ordination of the maritime sector. Other organisations which must co-ordinate with the IMO include the International Association of Lighthouse Authorities, as well as the organisations responsible for shipping for the larger rivers, such as the Rhine.

4.2.2 EU Maritime Transport

*EU Port Authorities
and shipping companies
are progressing...*

Throughout the EU, port authorities and individual shipping companies are generally making progress, although this is more apparent in the larger firms. Greater efforts are needed to develop common approaches to be implemented by port authorities, and increased attention needs to be paid to solving the millennium problem at the level of individual ships. The French navy, in its Y2K system inventory, noted that its distance navigation system (SYNEDIS) was currently not compliant, and decided that traditional means of navigation would be used as a fallback solution.

*...and certification
schemes for Y2K are
created...*

Contingency plans are being developed and implemented by each port. A certification scheme for ships is being proposed and will be implemented, which will mandate the need for a certificate to be provided before entry will be granted to major ports. As far as local shipping is concerned, in countries such as the Netherlands, ships will be licensed through a joint initiative between insurance companies and sectoral organisations. A similar scheme is proposed for ships registered in foreign countries.

---

[3] Composed of Belgium, France, United Kingdom, the Netherlands, Germany, Finland, Sweden, Denmark, Italy, Greece, Spain, Portugal, Ireland, Norway, Croatia, Poland, Russian Federation and Canada.

Several countries commented that for the most part, the maritime sector was providing relatively little information thus far, and that few companies had reported that they were establishing Y2K contingency plans.

4.3 Rail Transport

4.3.1 Overview

Rail operations and the rail infrastructure are very closely linked and numerous railway companies remain integrated, thus it is not appropriate to make a distinction between providers of infrastructure and operators of transport services in the context of the year 2000 problem.

There are a number of different IT systems used by railways in which problems of compliance could arise. These include both central and local IT systems, many of which are mainframe based and are used for general management purposes or to provide specialised services such as ticketing, reservations and passenger information, as well as the embedded chips located in locomotives, signalling, crossings, lifts and escalators, air-conditioning and ventilation systems, etc., and the interconnections between railway IT systems used to transfer data concerning international operations. Additionally, the IT systems of those suppliers on which the railways depend to provide electricity, telecommunications and diesel fuel may also experience problems.

In principle, non-compliance could create several problems. It is unlikely to compromise safety, since generally IT-based signalling is only one layer of a system, however, it could disrupt rail traffic or services to freight and passenger customers. Ensuring the compliance of the interconnections between the railways' IT systems is a particularly complex task (these systems are used for transferring information about international trains, rather than for signalling or traffic management). Data is exchanged through links between individual IT systems in a largely virtual network. While components of this network have been checked, end-to-end tests have not been carried out.

To respond to concerns about these potential difficulties, the International Union of Railways (UIC) intends to hold a seminar on embedded systems, to organise end-to-end tests of the interconnections between various railway systems, and to create a back-up team to help railways experiencing difficulties. The UIC has also facilitated the exchange of information on the Y2K problem in this sector.

4.3.2 EU Rail Transport

Compliance is being tackled by each railway on a national basis. The railways generally began their Y2K work during 1996 and 1997, starting with an inventory of IT systems and classifying each system as being critical or non-critical. They are now in the process of testing systems for compliance, with work on IT systems apparently in advance of that on embedded systems and international connections. A significant proportion of their IT systems are not compliant and are thus being modified or replaced (some railways see the year 2000 problem as an opportunity to modernise IT). Key systems which may be affected are those relating to the maintenance of trains, equipment, and buildings. In the systems for signal authorisation, and those authorising the speed of the French TGV, for instance, no use is made of dates. The railways are demanding certification of

compliance from major suppliers but will find it difficult to obtain information from all suppliers.

Compliance is being tackled by each railway on a national basis. Overall progress in this sector is therefore deemed to be satisfactory, with the larger firms making good progress. Generally, no sectoral contingency plans are being developed, the individual companies are responsible for their own contingency planning.

Regulators are generally taking the leading role in the assessment of business continuity aspects, as well as safety aspects. Audits are being performed and the results kept under review. Risks are limited in this sector, primarily associated with the power supply and the international context. Minor and limited disturbance to local information systems for passengers cannot be excluded.

The Netherlands noted that no rail transport is planned during any year end period for several hours before and after midnight.

4.4   Road Transport

The comprehensive EU road network makes use of a number of electronic systems in order to ensure a smooth flow of traffic. These include surveillance systems, weighing stations, toll booths, monitoring and management systems which collect, analyse and disseminate traffic information, signalling, dynamic navigation systems, and security systems for highway emergency services, as well as the technical systems responsible for the operation of equipment such as lighting and ventilation.

The risks associated with a malfunction may be direct, in the case of problems with signalling or the operation of lights, or indirect, should traffic management systems be unable to cope with a critical situation. Priority is generally being given to the overall traffic information systems at national and regional level, traffic signalling, highway emergency service networks, and central management systems for tunnels.

The large integrated management systems used to control traffic in urban areas are complex and it is consequently more difficult to assess the Y2K impact. The compliance of road traffic/transport systems is being addressed at various levels. Both private companies and public administrations are responsible for different components of the road network.

The Y2K impact on cross-border information services should be limited, as the European network of electronic traffic data exchange between the national/regional centres of most of the EU Member States will only become operational in 2000 and 2001.

5   TELECOMMUNICATIONS

5.1   Overview

The global telecommunications infrastructure as a whole is critical in assuring the flow of information to support the operation of many industries and services, as well as for the Internet, voice, data, fax, and other telecommunication services.

Consequently, even where individual elements of telecommunication services are considered to be Y2000 compliant, their normal functioning will still depend upon the reliability of interconnections within the overall infrastructure, particularly interconnections between operators and across borders. This is of course equally relevant internationally as within the EU, since a significant proportion of European communication traffic is routed globally.

As a result of the liberalisation of telecommunication services and infrastructure in many parts of the world, including the European Union, a wide range of competing operators are providing different parts of the communication infrastructure. It is therefore the responsibility of each operator to ensure that all their interconnections with other operators are Y2000 compliant. To ensure business continuity, operators may make use of alternative and redundant circuits and routing possibilities, as appropriate.

The risk of disruption to communication services is primarily associated with software used in network operators' systems. Most consumer equipment, such as telephones and fax machines, should continue to work as normal. Problems are more likely to be encountered by people using PCs to access networks (such as the Internet), where the PC may not be Year 2000 ready, or by small businesses with private switches which have date-dependent functions.

5.2 International Activities in the Telecommunication Sector

Recognising the scale of the threat posed by potential Year 2000 computer failures and the critical role played by the globally deployed telecommunications networks, the International Telecommunications Union (ITU) established a Year 2000 Task Force in March 1998.

The terms of reference of the Task Force are to:

- raise the awareness of all telecommunication Operators and Carriers of, and to provide information on, the Year 2000 problem (Millennium Bug);

- advise on compliance standards;

- seek to establish the position of all Operators and Carriers, including an understanding of their timescales for compliance and to influence this where appropriate;

- seek agreement to, and promote, a sharing of information within the telecommunications community and with customers;

- promote the cross fertilisation of year 2000 best practice amongst the membership.

In pursuing this mandate, the Task Force set out to ensure a high level of awareness amongst its members of the issues at stake and to establish a comprehensive set of guidelines and tools that would assist organisations in reaching identified levels of year 2000 compliance. As part of this activity, the Task Force has surveyed the major operators to obtain forecasts of readiness, both within Europe and internationally. The Task Force reports that the level of response to date has been high, with the majority of respondents reporting that they expect to achieve compliance by mid 1999 or earlier.

In recognition of the need to ensure not only the compliance of individual operators but also the requirement to ensure global interoperability, an Inter Carrier Testing Sub Group has also been set up. The goal of this Sub Group and its Global International Gateway Testing strategy is to publicly demonstrate the telecommunication industry's Year 2000 international readiness. The end goal of the testing effort is to ensure that the full inventory of international gateway switch types throughout the world are all tested, with results published by the third quarter 1999. Any identified gaps or problems will be addressed through contingency plans and testing during the fourth quarter 1999.

5.3   EU Telecommunications

As in other sectors, the overall indications are that larger businesses in the EU are making good progress in their preparations for the millennium date change, although smaller businesses may be less well prepared. Regulatory authorities are monitoring progress in the sector. Interconnectivity tests are taking place between suppliers and EU operators participate in the ITU activities.

The primary dependency of this sector is on the power supply. Public telecommunication providers have contingency plans and disaster recovery plans to enable them to deal with failures that might occur, as well as internal procedures for prioritising telephone calls in emergencies, and a dedicated emergency planning staff. Several countries reported that at national level, a private telecommunication service is available to government users in emergency services such as defense, the police, and civil protection authorities.

The operators in countries such as the UK have formed a self-help group to present a common front to equipment suppliers, and to ensure millennium compliant software and hardware are supplied on time. Network operators are working together to ensure that equipment manufacturers are carrying out tests of new network equipment. Peer assessment is also proving very effective at solving any detailed technical problems with companies' software and hardware.

Some countries, including the Netherlands and Sweden, report adopting an overall approach to communications, which integrates related services such as mail and broadcasting systems. Certain telecommunication providers are making information packs available both to corporate and private users of telecommunication equipment. They are raising customers' awareness of the possible effects to equipment at customer premises and taking steps to address this with the suppliers of terminal equipment.

It is recognised that companies outside the EU may not be equally well prepared. EU organisations are liaising bilaterally with other administrations, sharing best practice and encouraging overseas operators to do all that is necessary to ensure that their networks are prepared.

6   NUCLEAR SAFETY

6.1   Overview

There are a number of potential problems in nuclear power plants (NPPs) relating to safety which can be associated with the Y2K problem. The first of these are the direct safety issues, which concern the software, hardware, and embedded chips used in safety-related systems. The relationship between power plants and the

electricity grid or other generation facilities may also induce problems. Should grid problems arise, it is important that back-up mechanisms, such as batteries and diesels, operate to ensure emergency electricity supply to cooling systems. Finally, there are also concerns that multiple failures, though not intrinsically unsafe in themselves, could unduly overload NPP operators.

6.2   International Activities on Nuclear Safety

WANO, the World Association of Nuclear Operators, has taken initiatives since 1998 to raise awareness and share information amongst its members. The International Atomic Energy Agency (IAEA) has launched a special project to address the Y2K problem for NPPs (particularly in CEEC, NIS and China). It plans to organise a comprehensive assessment between March and June (based on guidance documents) followed by a phase of contingency planning. This assessment phase will be implemented by small teams of Western experts, in co-operation with local operators. In the short term, these Western teams need to be set up, managed and funded. The assessment teams will report in May or June, providing a clearer picture of future needs.

6.3   EU Nuclear Safety

Rigorous programmes are in place throughout the EU...

All Member States with operating NPPs have a programme to address the issue. Although each programme differs in detail, each requires the licensee to identify systems that might be affected, to rank them by nuclear safety significance, to test each in turn and to modify or replace any that fail. Regulatory authorities are reviewing the content of these programmes and are monitoring their execution. In some Member States, attention is now turning to risk mitigation planning, such as requiring increased operating staff numbers and avoiding maintenance activities over the critical dates.

The Commission is in regular contact with relevant industrial groups (FORATOM, WANO, EURELECTRIC, UNIPEDE) for information on their activities. The Commission has raised the Y2K issue for discussion with Member State regulators in the relevant working groups, promoting the spread of best regulatory practice. There is no perceived need to increase the Commission's activities with respect to Y2K compliance of NPPs in the Member States, since they are already adequately addressing the issue.

...which are closely monitored by regulators

All countries with NPPs report that these sites are monitored closely by the regulatory authority concerned, and are normally required to operate within strict rules and with adequate contingency plans, which are checked and validated on a regular basis. The design specifications of these sites require safe operation in case of emergencies. Safety mechanisms in these plants are generally independent of computerised systems, thus it is very unlikely that there will be problems created by Y2K.

6.4 Nuclear Safety in Central and East European Countries (CEEC) and New Independent States (NIS)

Despite the relatively limited use of digital logic in safety-related systems in eastern European NPPs, there are known to be Y2K problems with some systems. Special attention must be paid to recently installed equipment, some of which may have been provided with support of the PHARE and TACIS programmes. Given concerns that the preparations of the electricity sector in these countries tend to be less advanced than those of the EU, the likelihood of grid problems arising may be greater, also increasing the possibility of overloading operators.

All these countries are reportedly taking measures, however, it appears that the level of awareness and action is not homogeneous. WANO considers that it is currently hard to judge to what extent adequate action has been undertaken in CEEC/NIS, other than in the Czech Republic, Slovakia and Hungary. WANO is encouraging the more experienced of its Western members to second experts to eastern NPPs.

The Commission's CONCERT group, (consisting of the senior nuclear regulators of 25 EU, CEEC and NIS countries) discussed the issue in June 1998 in order to increase awareness. The success of this policy was demonstrated in January 1999, when all CEEC and NIS nuclear regulatory authorities presented action plans, several developed following the 1998 meeting. The content of these plans and their state of progress varies. Some countries report being as well prepared as their EU counterparts, while others are significantly less advanced. In the January 1999 meeting, the regulators encouraged the Commission to consider further action. They welcomed an offer of assistance to regulators (requests have been received from Bulgaria and Slovakia) and urged the Commission to support the IAEA programme addressing NPPs.

The G-24 Nuclear Safety Assistance Co-ordination (NUSAC) secretariat, hosted by the Commission, raised the Y2K issue at its March 1999 meeting. The meeting brings together CEEC and NIS countries and the donors of nuclear safety assistance. The meeting considered the role of donor countries in assessing the Y2K compliance of equipment that they have supplied.

The International Science and Technology centre (ISTC) in Moscow is establishing a special fund (1.35 M$ are currently pledged) to assist Russian and NIS institutions in solving issues related to the Y2K problem, involving individuals and teams from the former weapon research institutes. The ISTC funds will support co-ordination of the definition of appropriate methodologies, assist Minatom and other institutions in conducting projects leading to the implementation of practical Y2K solutions, and assist in the provision of specific international expertise.

Considering the tight time scale and the absence of any mandate for the European Union to take an initiative, the Commission should focus its main effort onsupporting the IAEA work, which is based on a clearly defined methodology, and supporting the ISTC initiative by reinforcing the current contribution to the ISTC budget foreseen for Y2K, the ISTC providing practical immediate assistance through concrete projects in the NIS. The Commission will make best

use of the TACIS on-site assistance programme with EU nuclear operators, who will be fully integrated into the IAEA scheme. Discussions are taking place with the IAEA to further assess the practicalities of Community support. In addition to supporting the IAEA assessment teams, the Commission will investigate whether resources could be put in place to address needs identified by these teams.

...and providing direct on-site assistance

The Commission has also asked that the issue be raised in the framework of the PHARE and TACIS regulatory assistance projects. In these projects, EU regulators are in permanent contact with their CEEC and NIS counterparts at working level, and so are well placed to raise their awareness.

In the framework of the EU TACIS on-site assistance programme, the issue has already been taken up by one contractor (at Leningrad NPP). At the Commission's request, the issue was also addressed at the last on-site assistance meeting organised by WANO in November 1998. In December 1998, the Commission requested TACIS on-site assistance contractors to ensure the Y2K compliance of equipment delivered under EU programmes. In the early 1999, the Commission initiated a new inquiry with all the EU utilities involved in the on-site assistance programme to raise awareness. The most recent on-site assistance contracts include a provision to address the issue at the specific sites.

EU countries also carry out bilateral activities

The UK Department of Trade and Industry funded a study[4], the results of which were circulated to utilities participating in the TACIS on-site assistance programme. Finland has provided assistance to the Leningrad NPP near Saint Petersburg and to the NPP in the Kola peninsula. Further reports on bilateral actions have been requested from Member States.

For all activities, the target date for completion is October 1999, since last minute modifications to NPPs or to procedures run the risk of introducing more problems than they resolve.

7   FINANCE

7.1   Overview

The financial sector considered most advanced

In the EU, as elsewhere, the financial sector is still generally considered to be the most advanced sector. Certain EU countries noted that their financial organisations had tended to delay their year 2000 adaptation processes, due to the changeover to the euro. However, this has had a generally positive result. All institutions of the four financial services sectors (banking, insurance, securities, payment systems) have undergone an exercise of parallel euro and Year 2000 adaptation projects. In some cases, new wholesale payment systems have been specially developed in the context of the introduction of the euro, taking into account the need to be Year 2000 compliant.

---

[4]   The Millennium Problem. Raising the awareness of nuclear power station operators and regulatory authorities in Central and Eastern Europe, September 1998

EU financial services have benefited from the introduction of the euro	The euro changeover has had another benefit, in that many of the contingency strategies for Y2K are being based upon the contingency measures adopted for the euro changeover. In particular, the preparations for the euro changeover weekend (internal task forces and help desk, mutual contact lists with external parties, back up of data-bases and applications, build up of additional processing capacity and disk space, postponement or reduction of certain operations), are all contributing to contingency planning for the Y2K rollover in the financial sector. The successful experience of EU financial institutions in coping with the similar euro changeover challenge has generated confidence in the ability of companies to implement such changes successfully.
The sector is in the testing and contingency planning phase	A positive widespread trend in the four financial services sectors is that firms are generally now in the process of completing the final phases of their Y2K projects, specifically testing and contingency planning. Less positive is another common occurrence in these sectors, which is a tendency to underestimate risks not directly associated with information system failures (credit risks, potential liquidity tensions, and litigation). Although these issues have been identified as potential problem sources, firms may lack the resources, time, or simply the ability to take appropriate measures in order to protect themselves against such risks.
The insurance sector is considering policy holder risks	The insurance sector is systematically taking into account the Year 2000 related risks of its customers, due to the fundamental nature of its activities. In deciding how to assess and handle these risks, two approaches are apparent in EU countries. Countries such as the UK have decided not to cover Y2K-related risks; others, including France and Belgium, have decided to cover them provided their clients have suffered a serious sinister, involving material and/or physical damage, in spite of having taken all appropriate possible actions to be Year 2000 compliant.
Information to the public could be improved	The supply of information to the public by the financial sector could still be improved. Many companies have yet to adopt proactive strategies to disclose to the public their Year 2000 situation. This lack of attention could impair the competitive position of the entire financial system, in spite of the substantial progress which has been made.

7.2 International Activities in the Financial Sector

International co-ordination activities	The main international organisations involved in the financial sector are the Global 2000 Group, an informal grouping of banks, security firms, and insurance which facilitates efforts by the global financial community to improve the readiness of financial markets to meet the challenges created by the Year 2000 changeover, and the Joint Y2K Council, a grouping of international associations of financial regulators and supervisors.
International testing	Global testing of payment and settlement systems is planned. EU National Central Banks (NCBs) are fully involved in these international tests. The impact of the transition to the year 2000 on the insurance industry and the measures needed to cope are under discussion[5]. The Y2K problem is also being analysed by both the OECD's insurance committee and IAIS.

---

[5]   111th Conference of EU insurance supervisors, Amsterdam, October 1998

IAIS, the International Association of Insurance Supervisors, sent a questionnaire to all its members in December 1998. 43 countries replied, including 12 EU countries. A summary of the results has been available since March 1999. The risks which were most frequently mentioned by insurance supervisors were the possible failure of internal IT systems leading to business disruption and corruption of records; their dependence on suppliers; and an increase in claims, particularly in liability insurance. Two thirds of the respondents reported that insurance companies in their country expect an increase in their liabilities in non-life insurance; only seven respondents also expect it in the life sector. Of greater concern is the fact that only 11 respondents report having given advice to the firms under their authority on the technicalities and consequences of additional claims. IAIS has developed a document on contingency planning in the insurance sector which will be widely distributed to insurance companies and national inspection bodies.

7.3   EU Finance

Close monitoring of banks

Various bodies are active in the supervision of banking institutions, including the European Central Bank (ECB), NCBs, supervisory authorities, national administrations and regulators, as well as professional organisations, both at national and European level. The Banking Advisory Committee, where national supervisors, NCBs and Finance Ministries meet regularly, represents another forum for the exchange of information on national monitoring activities in the banking sector. This monitoring involves both information recollection and ad-hoc checks, as well as the co-ordination of multilateral testing. Supervisors and other national authorities are using a wide variety of sources of information in this respect - the firms themselves, professionals engaged in tackling the problem (such as auditors), and commercial rivals. In addition, regulators in this sector tend to have extensive knowledge of the systems' expertise, controls and personnel of the firms supervised.

External testing foreseen in 2nd and 3rd quarter of 1999

Generally, those banks and financial institutions in the EU which are subject to supervision have completed their internal adaptations, with many involved in internal testing. Nearly every EU country reported that national external testing would take place during the second and third quarters of 1999. As far as payment systems are concerned, the ECB is requesting each NCB to monitor closely the progress of RTGS systems within the framework of the TARGET changeover to Y2K, implementing compulsory deadlines for action - internal IT testing to be completed by the end of April; multilateral testing to be completed by the end of July; final certification systems to be in place by the end of September; and contingency testing (no deadline has yet been defined). Testing tends to be complex, involving a series of integrated tests on national clearing and settlement procedures with the involvement of all payment system participants. Retail payment systems, including ATMs, credit transfers and TPOS (terminal payment at point of sale), are also being thoroughly tested.

Action is being taken against laggards

Some countries noted that delays had occurred to Y2K project schedules within the banking sector, primarily attributable to suppliers having delayed their delivery of year 2000 compliant products. Insitutions which appear to be falling behind schedule are being addressed in several ways. In Italy, formal letters are being issued and on-site examinations carried out. All companies under

supervision must submit a self-assessment declaration, signed by Senior Management and/or the Board of Directors, stating the preparedness of the institution. The Nederlandsche Bank will request those banks which continue to encounter problems and which are in arrears to report on further progress on a monthly basis. Regulators have made it clear that firms which fail to implement appropriate measures will face regulatory intervention.

Security firms are required to disclose status of readiness

As far as securities firm and the stock exchange are concerned, EU regulators supervise regulated markets and market management companies, including the behaviour of intermediaries, and ensure proper disclosure by issuers. In many countries, such as Finland and Italy, supervisors and regulators are requiring detailed information on Y2K readiness to be provided in financial statements and/or certain reports. National arrangements are in place to carry out appropriate testing on settlement dates. Italian firms report that as part of their contingency planning, a back-up link has already been established by intermediaries for orders and pre-matching, intended to assist with disaster recovery.

Insurers are being asked to analyse portfolios

In all EU countries, insurance companies have informed their customers, both individual and business, about Y2K risks and the coverage of such risks under their contracts, as well as their own responsibility for Y2K compliance. In some countries, companies have adopted exclusion clauses to be inserted in new and existing contracts. Certain insurers have even communicated with their larger customers through questionnaires, both to determine their state of preparedness and also to make them aware of the consequences of non-compliance. In Italy, insurance companies were asked to include in their 1998 annual accounts an analysis of the insurance portfolio subject to the Y2K problem, in this case arising from Y2K failures of policyholders, as well as a quantification of the associated costs. External auditors, appointed to certify the financial statements of insurance companies, will specifically evaluate each company's plans to manage such Y2K risks.

Some countries have created a platform to assess Y2K claims

The insurance company association- in France, the FFSA, has decided to create a 'technical platform' which will be available to all insurance companies from the end of 1999. A network of 150 to 200 experts on Y2K problems will be established, with knowledge covering many different aspects (PCs, embedded systems, electronic equipment, production process computing, office computing, etc.). Where insurance claims are made as a result of damages linked to the Y2K problem, a single expert per case will be designated to evaluate the cause of accidents due directly or indirectly to the Y2K changeover, and to assess the adaptation measures and contingency planning undertaken by the firms involved. The platform will be in place throughout 2000, and is intended to facilitate a quick, independent, consistent, and indisputable expertise, in order to prevent long-lasting claim procedures. Belgium is another country where the sector has decided to prepare itself by implementing a common technical platform.

8   WATER

Activities in the water sector are occurring at local level, ...

Although activities in this area have generally had a late start, the water supply and waste water treatment sectors in the EU have recognised the threat posed by the millennium bug and now report making progress. In most instances, monitoring activities in this sector tend to be carried out at local level. In many countries, there are no national regulators, but instead national associations of

water companies. In Denmark, the Ministry for Research and IT carried out pilot projects in this area, in co-operation with the National Association of Local Authorities, distributing the results to municipalities.

...where strict contingency regimens already exist

The water supply sector normally implements strict contingency regimens which are required by law. Compliance programmes are currently preparing Y2K contingency arrangements for water supply, distribution and reclamation, and reviewing major incident plans and manpower planning arrangements. In the Netherlands, for example, there is a general requirement for 10 days of full operations without new supplies of energy and chemicals (based upon individual back-up power sources), and 20 - 25 days supply of fresh water without need for a new intake of water, making use of existing water resources. Water company contingency plans normally address how automated systems can be replaced by manual control in the event of problems. Such plans are being checked for millennium-specific aspects.

Key issues are energy and IT supplier dependencies...

With respect to waste water, most countries report that separate ministry and local government bodies are responsible. Each is therefore responsible for its own millennium projects, including contingency planning. This sector is dependent upon energy for its operation. Limited services can be provided when normal resources are unavailable. The sector is making progress, although supplier dependencies are of concern because the lack of information on certain technical installations.

...with the main risk being pollution

The main risk identified in the sector is the possibility of pollution of water intake from major rivers as a consequence of the millennium problem, including pollution from nuclear sources.

9   INTERNAL COMMISSION ACTIVITIES

Commission initiatives continue...

The Commission continues to actively pursue the initiatives announced in its Communication COM1998(102).

...with priority given to internal systems...

Top priority is being given to making its own systems compliant. Regular meetings involving the Secretary General and Directors General keep progress under review through the Co-ordination Group on Organisation and Management.

...and good progress has been achieved

Since 1996, all DGs have been asked to include in their annual information plan a specific plan to adapt their information systems to the Year 2000, with priority given in the budget allocations to executing these plans.

End-to-end testing is planned...

Particular attention is being paid to ensuring that work in progress on those mission critical systems not yet compliant is completed in time. The verification of the underlying infrastructure (hardware, system software, third party software) is well advanced and compliance will be achieved in time. In 1999, a series of individual tests in the DGs and a Commission wide end-to-end test will be conducted. The end-to-end test will validate the compliance of information flows in the areas of administrative, financial, statistical, documentary and office information. Depending on the results, corrective actions will be strengthened and prioritised.

An inter-service group, led by the Secretariat General and with representatives of all DGs, oversees the ongoing Year 2000 activities within the Commission. Its tasks cover mainly non-informatic subjects, such as the co-ordination of contingency plans for assuring the continuity of essential services, the co-ordination of legal issues relating to Y2K, the general infrastructure aspects (including buildings, security systems, lifts, and all related supplies) and information campaigns targeted at Commission staff and the public.

As regards other European institutions, the inter-institutional committee for informatics (CII) is co-ordinating year 2000 compliant activities so as to ensure a common approach to the problem. The Commission has also organised a symposium with Member States and a joint conference with the Portuguese Government to discuss the adaptation of European information systems to the year 2000. Similar actions are planned with other Member States and for SMEs.

With regard to Commission actions to promote and facilitate an exchange of information on the Y2K problem between countries and sectors in the EU, the Commission continues to host regular meetings between national Y2K co-ordinators and representatives from industry associations, with an increased frequency during 1999. Throughout the Commission, the DGs concerned with infrastructure sectors are liasing with appropriate associations and collecting information.

Various actions are being carried out in the Member States to ensure the continuous functioning of alarm systems, including the mutual 112 number, and to prepare the Civil Protection authorities for emergencies that might occur in connection with the millennium date change. An exchange of experience on the readiness of the emergency services has taken place during the meeting of the directors-general for Civil Protection in Vienna on 21 October 1998, as well as in the regular meetings of the permanent network of national correspondents in the field of Civil Protection (PNNC). In accordance with the decision of the meeting of the directors-general, the civil protection unit of the Commission services ensures the circulation of relevant information.

10 CONCLUSIONS

It is important to note the substantial progress in addressing the Year 2000 problem in critical infrastructures which has occurred since the previous report of the Commission was published in December 1998. This progress is reflected in the much greater amount of information on the Y2K situation which is now available to industry, consumers, and citizens.

There are a number of important trends which are now emerging across all sectors, and throughout the EU as a whole:

- *The greater involvement of regulatory and supervisory authorities in monitoring and auditing vital infrastructure sectors.*

- *The co-ordination efforts being carried out by sectoral, national, and international associations, which are examining the problem with their members and establishing general contingency strategies and guidelines.*

- *The increasing emphasis on bilateral, multilateral, end-to-end, and national testing.*

- *The growth in national and sectoral Y2K information campaigns, aimed at maintaining public confidence by focusing on the state of readiness of essential service providers.*

- *The wider availability of information on progress, result, risks, and contingency plans.*

- *The development of "troubleshooting" actions by forerunners and associations, designed to assist laggards in their efforts to catch up.*

- *The recognition that, in infrastructure areas as in industry as a whole, smaller organisations continue to lag significantly behind large companies in addressing the Y2K problem.*

- *A dependency upon IT system suppliers to provide an accurate disclosure of the compliance of their products, and where necessary, to deliver timely upgrades.*

Involvement of sectoral and international organisations in contingency planning is critical to success

Prior to 1999, many sectoral, national, and international organisations seemed to be struggling to find an appropriate role for themselves in order to provide practical assistance to their communities in preparing themselves for the changeover to the year 2000. However, now that companies are starting to focus their attention beyond their internal systems, associations and organisations are able to facilitate the exchange of information, to develop common guidelines, and particularly important, to assist in contingency planning. The implementation of sectoral and international contingency strategies will undoubtedly become a critical success factor for addressing the Y2K problem on an international scale.

The reliability of public utilities in the EU is very high...

In the EU today, the reliability of public utilities is so high, that the consumer tends to take it for granted that they will continue to receive power and water, and that they will hear a dial tone when they pick up the telephone. Nevertheless, no utility provider would currently be prepared to give any consumer an absolute guarantee of uninterrupted service on a particular day. It is therefore not surprising that suppliers also refuse to provide such guarantees during the millennium changeover, at a time when the potential impact of external factors outside their control on their own business operations is very difficult for any organisation to quantify.

...and the risk of significant disruption is correspondingly low

It is clear that companies and organisations throughout the EU have recognised their responsibility to tackle the Year 2000 computer problem and are now starting to demonstrate their success in doing so. The overall assessment is that the risk of significant disruption to EU infrastructures during the millennium period is limited. Any problems are more likely to be localised and occur in smaller organisations. Since such risks, however minor, still exist, efforts are ongoing in every sector to establish thorough, comprehensive contingency plans to mitigate these risks.

11 ANNEX

The following is a list of websites from which additional information can be obtained.

National and government information:

UK   http://www.open.gov.uk/year2000 (UK plans/preparedness)

          http://www.bug2000.co.uk (UK infrastructures – the results of all assessments are provided on this website)

Greece   http://www.year2000.gr

Luxembourg   http://www.crpht.lu/an2000

France   http://www.premier.ministre.gouv.fr

              http://www.an2000.gouv.fr (government)

              http://www.industrie.gouv.fr/site/industrie/home/navi/page/industrie (industry)

              http://www.justice.gouv.fr/publicat/an2000.htm (justice)

              http://www.defense.gouv.fr/sdsic/a2000/index.html (defense)

              http://www.equipement.gouv.fr/an2000/1000.htm (transport/logistics)

              http://www.education.gouv.fr/actu/an2000/plan.htm (education)

              http://www.diplomatie.fr/actual/dossier/an2000.html   (foreign affairs)

              http://www.interieur.gouv.fr/an2000 (interior)

              http://www.agriculture.gouv.fr/index.html (agriculture)

              http://www.jeunesse-sports.gouv.fr/francais/misan2000/index.htm (youth/sports)

              http://www.santé.gouv.fr/htm/pointsur/an2000/index.htm (health)

Sweden   http://www.statskontoret.se/2000/sfs.htm

              http://www.2000-delegationen.gov.se/arbete/direktiv.htm

Spain   http://www.map.es/csi/2000.htm

Portugal   http://www.missao-si.mct.pt/P2000/index1.html (national site)

              http://www.iapmei.pt/idex/informacao/ano2000.html (SMEs)

24

	http://www.inst-informatica.pt/ANO2MIL/2mil001.htm
	http://www.min-plan.pt/menu/tforce/index.html
Switzerland	http://www.millennium.ch (national site)
	http://www.efd.admin.ch/aktuell/2000/index.htm (public administrations)

For the energy sector:

Netherlands	http://www.energie2000.nl
	http://www.emp.nl
Italy	http://www.enel.it
Spain	http://www.endesa.es/2000/index.htm
	http://www.repsol.es/webrepsol/esp/inversor/efecto2000.htm
	http://www.miner.es
Greece	http://www.dei.gr/dei-en.htm
	http://www.depa.gr/eng.index.html
	http://www.dep.gr
Sweden	http://el2000.com/index.html
	http://www.stem.se/om_myndigheten/y2k.html
Finland	http://www.finergy.com
	http://www.fingrid.com
	http://www.neste.fi/konserni/2000/index.html
	http://www.gasum.fi/frindex_eng.htm
France	http://www.edf.fr (electricity)
	http://www.gdf.fr (gas)
Luxembourg	http://www.cegedel.lu
Switzerland	http:// www.strom.ch (electricity)
	http://www.erdgas.ch (gas)
Norway	http://www.enfo.no/index.cfm
	http://www.statnett.no/y2k/index.html
	http://www.npd.no/y2k/

For the transport sector in general

Spain	http://www.mfom.es

For the aviation sector:

Finland	http://www.ilmailulaitos.com/english/ (Civil Aviation Authority)
Greece	http://www.olympic-airways.gr
Sweden	http://www.lfv.se/sakerhet/y2k/y2krs03.pdf
Switzerland	http://www.atraxis.com

For the maritime sector:

International	http://www.ship2000.com (joint web site of the International Chamber of Shipping (ICS), the United Kingdom P&I Club and Lloyd's Register)
Greece	http://www.yen.gr
Belgium	http://www.zeebruggeport.be
Sweden	http://www.sjofartsverket.se/frameset.htm

Norwayhttp://www.rederi.no/no/bibliotek/y2k/

For the rail sector:

Finland	http://www.rhk.fi/defeng.htm (Finnish Rail Administration)
	http://www.vr.fi (Finnish State Railways)
Greece	http://www.ose.gr
France	http:// www.sncf.fr
	http://www.ratp.fr
Sweden	http://www.banverket.se/framtiden/ar2000.htm
Switzerland	http://www.sbb.ch

For the road sector:

France	http://www.equipement.gouv.fr/an2000/1000.htm
Greece	http://www.oasa.gr (Athens Urban Transport Association)

For the telecommunication sector:

International	http://www.itu/y2k (summaries of individual company responses to questionnaires can be found on this ITU web site)
UK	http://www.oftel.gov.uk/bug2000.htm
Spain	http://www.sgc.mfom.es/efecto/efecto.htm
Greece	http://www.ote.gr (Hellenic Telecommunications Organisation)
	http://www.cosmote.gr/e_mainpage1.htm
	http://www.panafon.gr/en
Sweden	http://www.pts.se/aktuellt/2000-rap.pdf
France	http://www.france.telecom.fr
Luxembourg	http://www.y2k.lu
Finland	http://www.sonera.fi/english/year2000.html (Sonera Oyj)
	http://www.hpy.fi/yritys/vuosi2000 (Finnet Group)
Norway	http://www.telenor.no/bedrift/ar2000
Switzerland	http://www.swisscom.com/2000ok

For the Nuclear Power sector:

Finland	http://www.stuk.fi
Sweden	http://www.ski.se/
Switzerland	http:// www.hsk.psi.ch/aktuel.html

For the financial sector:

Netherlands	http://www.dnb.nl
Italy	http://www.bancaditalia.it
	http://www.cipa.it
	http://techinfo.sia.it
	http://www.consob.it
	http://www.borsaitalia.it
	http://www.cedborsa.it
	http://www.isvap.it

UK	http://www.bba.org.uk (information by the BBA on UK financial sector preparations)
	http://www.bankofengland.co.uk (contains the Bank of England's "Blue Book")
Spain	http://www.cnmv.es/A2000/efecto2000.htm
	http://www.ipyme.org/inipyme/prog4.htm
Greece	http;//www.hba.gr
Germany	http://www.bakred.de (Bundesaufsichtsamt für das Kreditwesen)
	http://www.bundesbank.de (Deutsche Bundesbank)
	http://www.bav-bund.de (Bundesaufsichtsamt für das Versicherungswesen)
	http://www.bawe.de (Bundesaufsichtsamt für den Wertpapierhandel)
Finland	http://www.bof.fi (Bank of Finland)
	http://www.rata.bof.fi/english/Faq/Faq.html (Finnish Supervisory Authority)
	http://www.hex.fi/y2k/index.html (Helsinki Stock Exchange)
France	http://www.afb.fr/pascfonb.htm
	http:// www.paribas.com
Portugal	http://interbolsa.pt/index.htm
Sweden	http://www.fi.se/fffs/1998/fs9818.htm
Switzerland	http://www.swissbanking.org/e/Pages/swissbanking.htm

Norwayhttp://www.finans.dep.no

For the water sector:

Sweden http://www.slv.se/vatten/index.htm

France	http://www.generale-des-eaux.com
	http://www.suez-lyonnaise-eaux.fr
	http:// www.bouygues.fr
Finland	http://www.vvy.fi
Spain	http://www.mma.es/2000.htm
Denmark	http://www.dkvand.dk/index1.htm
	http://www.kl.dk/siab.asp?o_id=1869

Norwayhttp://www.norvar.no