Loviisa Power Plant

4.1.1999

Paper to be presented at the International Workshop:
"Impact of Year 2000 on the Nuclear Industry",
Canada, Ottawa 8 – 10 February 1999

MANAGING YEAR 2000 AT A VVER-PLANT – A CASE STUDY FROM LOVIISA NPS

Ulf Lindén
Project Leader

Disclaimer:
This presentation is for informative purposes only. It should not be taken as an expert advice nor as any promise or guarantee concerning the year 2000 date change problem or the way it can be solved or other aspects connected with year 2000. The presented plans and opinions may change without notice.

IVO

1 INTRODUCTION

The year 2000 date problem is widely understood within the IVO Group and it is taken seriously. Electricity production and delivery systems are among the most important elements of the economic and social infrastructure. All other critical elements of the infrastructure depend on the availability of a reliable supply of electrical power. The functioning of the power system, especially the Loviisa Power Plant, takes the highest priority in the company's Y2K project.

This paper describes the basic year 2000 work done at the Loviisa Power Plant to ensure the compatibility of electronics and information systems. Results from the assessment are presented and discussed. A year 2000 project is more than finding and fixing problems. You also have to plan for continuity, contingency, and crisis. Background for this work and the goals is explained.

When talking about the year 2000 issue one must be aware that the transition from year 1999 to year 2000 not will be the only problem. There are also other critical dates. When we in this paper talk about Y2K compliance we mean that neither performance nor functionality shall be affected by dates prior to, during, or after year 2000.

2 LOVIISA POWER PLANT

The Loviisa NPS consists of two Russian VVER-440 units. The first unit was put into operation in 1977 and the second in 1981. The plant has been modified to meet Western safety requirements and the plant differs therefore in some ways from a standard VVER, e.g.:

- instrumentation and control systems are based on Western technology
- control rooms are based on Western technology
- the units have very extensive process information systems
- reactor buildings are equipped with containments

During the Loviisa plant operation many modifications have been made in order to improve the plant safety. The reasons for the modifications have been defects in the original plans, new, more detailed accident analyses, more stringent safety requirements, operation experiences both from Loviisa and foreign plants, and power upgrading of plant units.

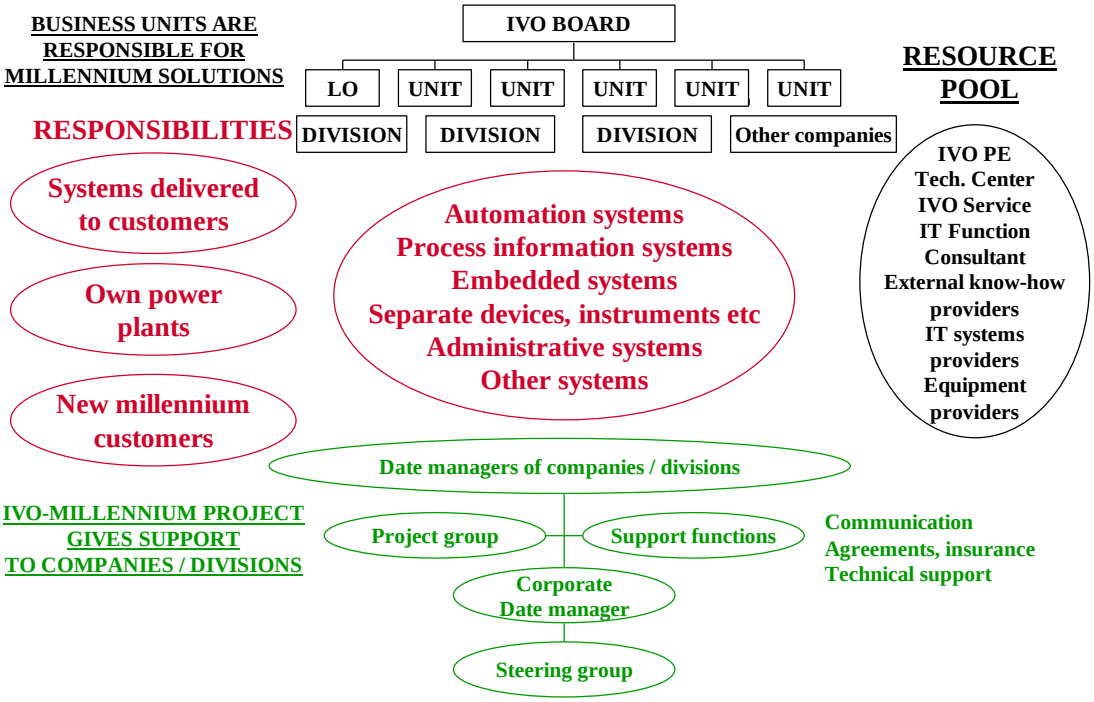
The plant has always used information technology (IT) extensively in several plant wide or dedicated information systems. Along with the backfitting work done during the 20 years of operation, a great deal of new digital systems with embedded components have been introduced to the plant.

High availability and short refuelling outages are characteristic of the plant. The mean energy availability for the two units after over 20 years of operation is about 85%.

3 Y2K PROJECT

3.1 Company Millennium Project

In addition to Loviisa Power Plant the company owns about 40 conventional power plants. The company also takes care of the operation and management of power plants in United Kingdom and Southeast Asia. The millennium project was organised as a centralised project with a strong steering group. The steering group required that Y2K projects should be started in every division and subsidiary of the company. A common resource pool was established to do the assessment. The resource pool set up a common database for the inventory and analysis of embedded components, and in this way shared experiences between power plants. The main role of the centralised project was to support the work done in the business units. It also supports other functions, such as legal questions, information/awareness, etc., and reports to the company management. The project organisation is shown in the following picture:



The main contractors in the resource pool are IVO Power Engineering, which takes care of the assessment, and IVO Technology Centre, which is responsible for the development of the testing method. IVO Technology Centre also deals with the exchange of information on Y2K issues with international organisations, like EPRI.

The main goal for the project was to achieve year 2000 compliance for all power systems by December 1998. Now we can see that this goal has only partially been met. All inventories have been completed and the analysis phase is over. The problem is that vendors have not been able to deliver year 2000 compatible upgrades in time and therefore some work had to be transferred to this year.

During the most hectic assessment phase over 100 experts were involved in the project. The project costs planned in 1997 exceeded 100 million FIM in Finnish operations.

3.2 Loviisa Power Plant Y2K project

The year 2000 project started in Loviisa in 1996 with the IT systems. This work has progressed in a very straightforward manner and is now in the state of final testing. The work on IT systems will be completed by the end of March 1999.

The Loviisa NPS got a high priority in the company's millennium project. A separate project organisation was established for the assessment of NON-IT components like programmable logic controllers and other embedded systems. This new organisation, which consists of experts from different areas of operation, continued with the Y2K work already started at the Loviisa NPS. This organisation is also using the central resource pool with their central databases containing component data.

The Loviisa NPS has, after the plant procurement, received very minimal support from the plant supplier. The plant organisation has therefore built up good competence and knowledge in the management, maintenance and operation of the systems and equipment in the plant. The key knowledge of the plant is possessed by the Loviisa personnel, and this has been very valuable in the millennium project.

3.2.1 Project Plan

The project plan is a normal plan aiming at Y2K readiness. The plan was drawn up before the publishing of NEI/NUSMG 97-07 and does not therefore directly follow that document. The plan consists of the following phases: awareness, assessment, remediation, contingency planning and risk management. The plan also includes requirements for quality assurance and documentation.

The awareness phase was initiated in November 1997. Information on Y2K problems was distributed to all site personnel via the site newsletter and group meetings. After that the project has been actively covered in the site and company newsletters, the regulatory authorities' newsletters, public newspapers, periodicals and seminars. The awareness phase also included training of the project group in how to find embedded components and how to perform simple tests.

The assessment of embedded systems started in December 1997. The tasks of assessment include inventory, prioritisation and analysis. The inventory is the most important phase in the assessment. The inventory at the Loviisa power plant included:

- all process automation systems
- all electrical automation systems
- building automation systems (lifts, ventilation,…)
- a hydro power plant used as a backup for emergency diesel generators
- telecommunications and data communication infrastructure
- gas turbines
- IT systems.

The basic inventory was carried out by the plant staff. Checklists based on process system identifications and system documentation lists (PI drawings, FSAR,…) were used. These were cross-checked using functional checklists (lists of controllers, inverters, etc.). The inventory was performed in several cycles by different teams to get a good coverage. Also spare parts storage was included in the inventory process. Procedures were written to handle the procurement of new components to ensure that all new deliveries will be year 2000 compliant.

All digital components were checked. If there were any doubts whether the component was digital or analogue then the component was handled as a digital component. Also if it was not clear if the component includes a real time clock (RTC) or calendar functions then the component was handled as containing an RTC.

During the inventory all components were classified and prioritised. The classification was based on the component safety class. In the prioritisation the following criteria were used:

1 Failure in the component will cause danger to personnel safety or damage to equipment.
2 Failure in the component will immediately affect production.
3 Failure in the component will have a delayed effect on production.
4 Requirement in Technical Specifications or affects the availability of safety systems.
5 The component is important for the operation or supervision of a process.
6 Non-essential

In parallel with the inventory, the analysis phase was started by sending a letter to all vendors asking for the vendors' statement of system or component compliance. The vendors' answers were followed up by utilising plant knowledge of the component and by component testing. It is important not to rely on vendors' statement only but to use multiple sources of information.

As mentioned earlier, several inventory cycles with component analysis have been performed and in our opinion all important components have now been identified. However, we would like to point out that the assessment is an iterative continuous process, that will go on until and even after year 2000.

3.3 Testing and validation

Testing is performed to validate vendor statements or to evaluate if a Y2K problem exists if the vendor cannot be located. Testing is also performed after remediation to check that the Y2K problem has been eliminated. A generic test procedure has been prepared. This procedure is then tailored for each component to be tested, often together with the vendor. The procedure consists of over 30 various steps for testing. Not only is the transition to year 2000 tested but also other critical dates. Mostly the testing is performed as unit testing, where only one single application or component is tested. More extensive system tests have also been conducted, e.g. all components and software modules in the plant information system were tested together. This test was

an integration test with 20 computers working together and ranging from the data acquisition system to the man-machine interface.

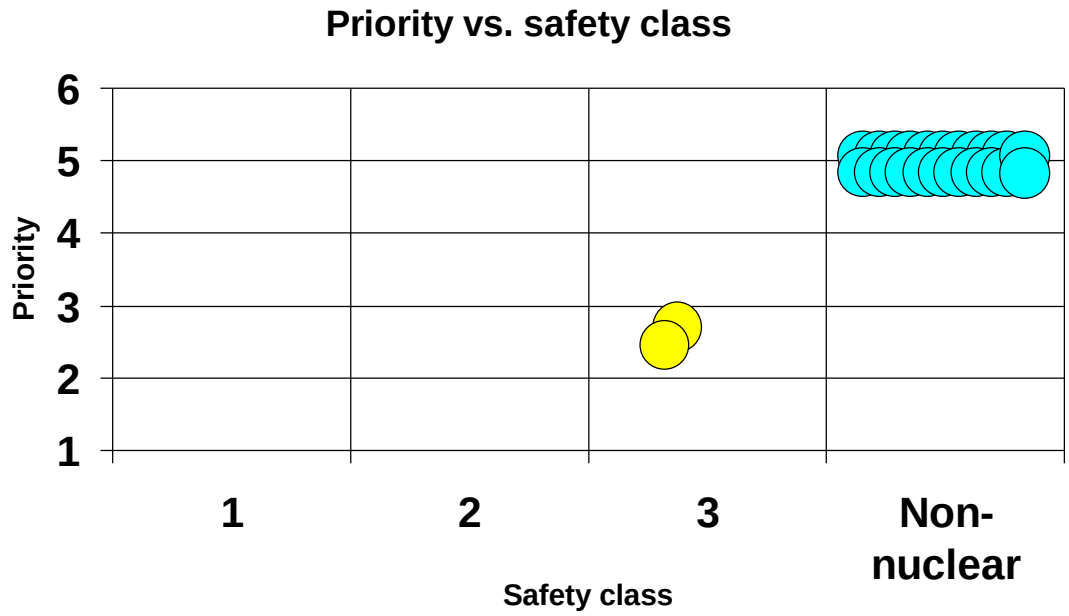
In the company wide project integrated testing of all embedded systems has been performed at two conventional plants.

3.4 Results from the assessment

A summary from the assessment is shown in the following table:

	Amount
Total amount of embedded components (types)	215
No RTC	95
RTC and year 2000 compliant	96
Not compliant	24

None of the found non-compliant components have any direct impact on safety or affect plant operation. Some of these components will, however, be important for the operation or supervision of some subprocess. None of these components belong to the original VVER design but have been installed during backfitting work after 1990. The following figure illustrates the non-compliant components as a function of safety class and prioritisation.



We believe this figure to be quite representative of a VVER plant. As a conclusion we can say that our experiences show that the original VVER design is very conservative and does not contain embedded components and should therefore also be Y2K compliant. A problem may be backfittings done during the last ten years.

The identified non-compliant components are listed in the following table. These components are all in non-safety systems but some of them are still important:

Component	Priority
– plant telephone exchanges (PBX)	5
– environment radiation monitoring system	5
– dosimetry systems	5
– body contamination monitors	5
– automation systems in low and intermediate-level waste repository	5
– sewage water purification plant automation system	5
– steam line activity measurement system	5

In addition to these some older PCs attached to tools or measurement systems have to be replaced.

3.5 Remediation

The purpose of remediation is to replace, fix, or eliminate items identified in the assessment as non-Y2K-compliant. The remediation work starts immediately when a component is found to be non compliant. The decision to replace, fix or eliminate the component is made in the line organisation in Loviisa. The plant's normal quality assurance procedures applied to the handling of system changes are used in the remediation work. After remediation, the component is tested according to the generic test procedure.

Modifications to existing equipment always carry an increased risk. Especially dangerous are temporary solutions and modifications executed in a hurry. None of the modifications made at the Loviisa NPS will directly affect operation. In our case the risks caused by the remediation will therefore be low but they will be taken into account in the contingency planning.

3.6 Documentation

The documentation produced from the Y2K program has an ongoing value, so it should be well organised and maintained. The Loviisa NPS will use a document management system based on Documentum® as a repository for the Y2K knowledge asset. Proper documentation and organisation will be a fundamental requirement as the accuracy and due diligence applied to the solving of the Y2K problem must be recorded carefully. Documentation is also vital to meeting Y2K schedules, maintaining compliance and providing proof of certification to nuclear regulator.

3.7 Interaction with the regulator

In Finland, the Radiation and Nuclear Safety Authority STUK acts as the regulatory agency. The ultimate responsibility for the safety and availability lies with the operating organisations of the nuclear power plants. However, the regulator has an important role to encourage the licensee to take proper actions in the Y2K issue. In the Loviisa Y2K project we have tried to establish good communication between the plant and the regulator. The regulator has been continuously informed about the progress of the project both by official reports and informal meetings and information exchange. This is important, because, as we all know, the project has a fixed non-negotiable deadline, which means that before December 31, 1999 both the licensee and the regulator should be convinced that the Y2K issue will not cause any safety threats to the power plant.

4 CONTINGENCY PLANNING

In parallel to the assessment and remediation work we have also started a project for contingency planning. This CCC project (**C**ontinuity, **C**ontingency, **C**risis) is a common project for the company's all power plants in Finland.

4.1 Electric grid issues

The power market in Finland is fully deregulated. Primarily all power producers are responsible for their own power balance. On the national level the company Finnish Power Grid Plc (Fingrid) is responsible. Fingrid is also responsible for the operation of the Finnish power system and takes care of the planning, construction, operation and maintenance of the national transmission network. The power industry's year 2000 co-operation is organised by the Finnish Energy Industries Federation, Finergy. Finergy is an organisation of the companies, member associations and other comparable societies involved in power and heat generation, procurement, transmission and sales, and building of the power transmission grid.

The Finnish power system consists of power plants, the main grid, regional networks, distribution networks, and consumers of electricity. It is a part of the joint Nordic power system, in co-operation with the Swedish, Norwegian and Danish systems. The peak load demand for electrical power in Finland varies from about 6 GW in summertime to about 12 GW in winter.

There are interconnections from the Finnish transmission network to:

- Russia
  - two 400 kV DC lines
- Sweden
  - two 400 kV AC lines
  - one 400 kV DC underwater cable
- Norway
  - one 220 kV AC line

There is co-operation between the Nordic grid companies via the NORDEL organisation. The time difference between countries (Russia +1 h, Scandinavia –1 h) allow some mutual backing up.

In the contingency planning Fingrid will focus on the 400 kV network. In the case of significant blackouts (anticipated events) Fingrid will be able to make a restoration within 15 minutes.

4.2 Scenario

The contingency planning will be based on the following basic scenario:
- temperature – 25 °C
- hydropower reserves low
- simultaneous big generating unit drop-outs (15 min rule)
- telecommunication network is overloaded.

The goal for the planning is to maintain the power balance. The combined plants shall also continue to supply steam and heat to customers. Power production facilities shall be kept safe by preventing damages to the facilities. The goal is to enable a fast response and mitigation even in the worst predictable case.

A list of all power plants was drawn up. For each power plant the dependencies were identified e.g. (see appendix 1):
- national power grid
- clean water supply
- communications
- logistics, fuel transport
- station service requirements
- regional alarm centre, fire brigade
- emergency power.

The maximum available power to the grid (1/1/2000) for each plant has been determined based on evaluation of the plant availability. The optimum mode for plant operation has also been analysed.

4.3 Process analysis

Process analysis will be piloted in some conventional power plants and may be applied also to the Loviisa NPS. So far we have analysed single components in the assessment phase. In the contingency planning we have checked external conditions. Now these two will be combined and we look at critical processes in the power plant. The availability of the processes will be checked in four cases:
- loss of power for 0 minutes
- loss of power for 0 – 15 minutes
- loss of power for 15 minutes – 2 hours
- loss of power for 2 hours –

Assessment/remediation project →		← Contingency planning
Electronics	**Processes**	**Continuity**
Embedded processors "critical dates" 1/1/1999 21/8/1999 9/9/1999 1/1/2000 1/3/2000 …	Phase 1. Identification of critical processes 1. LOOP 0 min. 2. LOOP 0 – 15 min 3. LOOP 15 min – 2h 4. LOOP > 2 h	External conditions: - fuel - transports - …
	Phase 2. Deterministic assumptions Special arrangements	

4.4 Special arrangements for the Loviisa NPS

The Loviisa power plant's contingency planning is tightly coupled to the company's CCC-project. The assessment phase already shows that the vulnerability is low for internal events at the Loviisa NPS. The year 2000 project started in time and the goal is to be 100% compliant by summer 1999. The main arrangements against internal risks will be the use of extra manpower and a higher level of preparedness in important areas.

The goal for the Loviisa NPS is to stay online during the transition period. The power may be reduced to about 70% to ensure the possibility to have a reserve for frequency control if needed. The more extensive the electrical grid is the better it can stand load fluctuations.

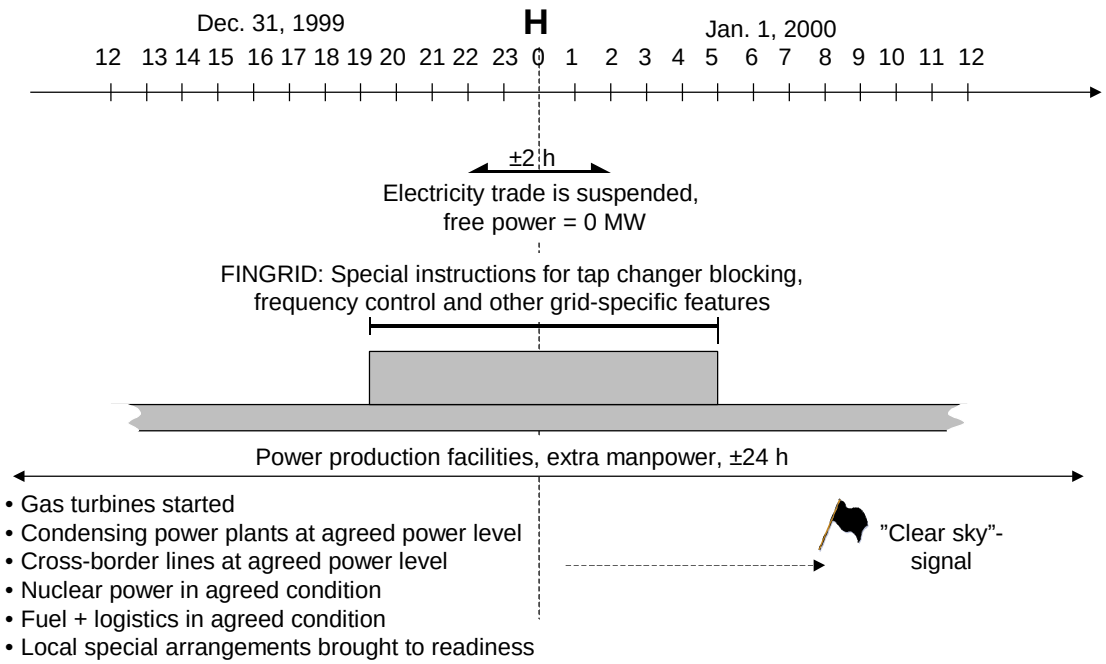
The analysis of external dependencies continues and the final contingency planning for the Loviisa NPS will be done during 1999. The Loviisa NPS has good access to the grid and in a case of loss of offsite power both units are equipped with emergency diesels (capacity 4 x 100%). The diesels have as a backup a hydropower plant. On the site there is also a gas turbine plant which will be able to make a black start in the case of loss of offsite power. Anticipated operational occurrences are already analysed in the Final Safety Analysis Report and the results can be used in the contingency planning. The plant has a wide range of procedures for handling of external events and some new procedures will be prepared together with the national transmission company. These procedures will focus on crisis situations related to major grid disturbances or outages.

In the scenario it was assumed that both the normal telecommunication and the mobile telephone systems are overloaded. New telecommunication networks, independent of the normal network, will be built from the power plant to the energy management control centre and also to the national transmission company.

4.5 Schedule

As mentioned earlier a draft contingency plan has been prepared and the final detailed plan will be ready before summer this year. Training will be arranged after the plant's refuelling outages (August –September). The readiness will be increased gradually from November 1999, although some programmed measures have to be taken as early as on the 21st of August. Full readiness will be required 24 hours before and after the transition to year 2000.

A preliminary schedule has been drawn up for 1/1/2000. This schedule is shown in the following figure:



4.6 Problems

There are still open questions and problems related to the contingency planning. One problem is the grid structure. About one thousand kilometres of network connects the big Y2K-safe hydro power plants in north with the industry and major population centres in the south. Another problem is the interconnections with Sweden, Norway and Russia. A big disturbance in these countries will also affect Finland. The connections to Sweden and Norway are also in the north and the long lines to the south are behind a complicated set of remote control equipment.

5 CONCLUSIONS

Analyses show that the Y2K issue will not cause any immediate safety or availability concerns at the Loviisa NPS. The year 2000 project started in time and the goal is to be 100% compliant by summer 1999. External events may however cause indirect threats to the plant and a contingency plan will therefore be implemented. This plan will be based on mitigation and restoration and will focus on an optimal recovery from any undesirable event during sensitive date rollovers. The findings at the Loviisa NPS show that the Y2K problems are not in the original VVER delivery but in later IT and automation upgrades. The problem is real and there is a need for assessing I&C systems at all VVERs.

APPENDIX: Continuity, contingency and crisis planning, functional review