The Year 2000 threat to the electrical grid

Industry and society in general are making a large-scale effort to identify and fix problems threatened by the 'millennium bug', ie the failure by certain older software to recognize correctly the date 2000 when the last two digits of the year change from '99' to '00'. Maintaining a functioning infrastructure, especially a reliable supply of electricity, is central to this effort. ABB is working closely with power utilities to make sure that everything is done to meet the Y2K challenge.

Across the whole of industry and throughout society, intensive work is going on to identify and fix potential Year 2000 problems in computer systems, process control equipment and all other kinds of system with embedded intelligent devices. The key priority is to ensure a functioning infrastructure, ie telecommunications, water, oil and gas supplies, transportation and other public services. Central to this work is the necessity to maintain a reliable supply of electricity, without which banks, petrol stations, food stores, railways and traffic lights, to name just some of the vital services and systems on which we depend, will cease to work.

This overwhelming reliance on electricity has developed as a result of the electrical engineering industry building systems and developing procedures which guarantee a very high reliability for its supply. Local blackouts occur only occasionally, usually being caused by excavators accidentally cutting into cables or lightning causing short circuits. Service teams on continuous standby respond to problems immediately and restore the supply within a short time. Blackouts affecting larger areas are extremely rare. When they do occur they are thoroughly investigated and the lessons learned are invested in more robust system layouts and made generally available.

Against this background, the Year 2000 (Y2K) problem raises the following questions:

- How vulnerable is the electrical grid to the Y2K threat?
- Which are the most critical system components?
- Is the established system layout robust enough to withstand the specific Y2K threat?
- Are the existing service and emergency procedures adequate?

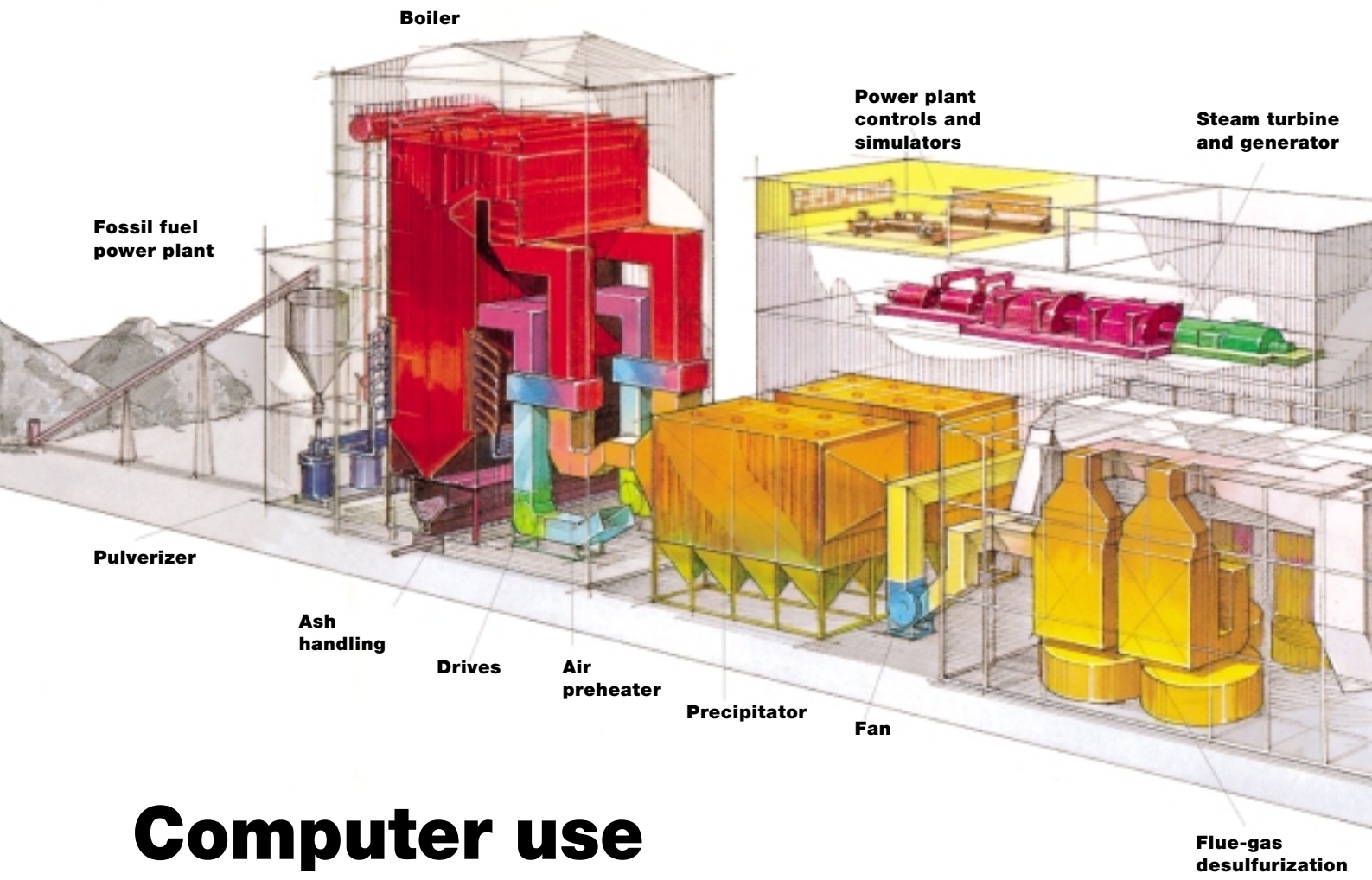
ABB, as a leading supplier of equipment to electric utilities, has done extensive work in this area [1] involving most products, systems and plants supplied by the company. In particular, pilot projects have been worked through for each type of system (eg, each type of power plant, network control center, substation, protection system, static var compensator, HVDC system, etc). ABB is also working with utilities in all parts of the world, involving operators of smaller, insular systems (eg, in Ireland) as well as large interconnected systems (eg, UCPTE). This work has allowed an extensive and unique 'experience base' to be built up for the purpose of addressing the Y2K issues.

Besides knowing the critical system components and their Y2K vulnerability, there is also the highly important question of overall system behaviour. System studies and simulations of every kind are the responsibility of the utilities, who have the tools and the data necessary to carry them out routinely. However, to mitigate the Y2K risk it is suggested that these be applied in close cooperation with the product and system supplier. All the available experience and field data have to be combined to achieve the highest possible reliability for the electricity supply.

Dr. Klaus Ragaller
ABB Year 2000 Task Force

Computer technology in the electrical system

All the main parts of an electrical system, from the generation of the electrical power through its transmission over the high-voltage lines to its distribution via medium-voltage and low-voltage systems to industrial and domestic users, are shown overleaf. Originally, these systems were built without any digital devices. Due to the installations having a service life of 40 years and more, much of the original non-digital equipment is still in service. Digital devices are found either in the more recent system extensions or replacements, or in add-on equipment installed to improve the moni-

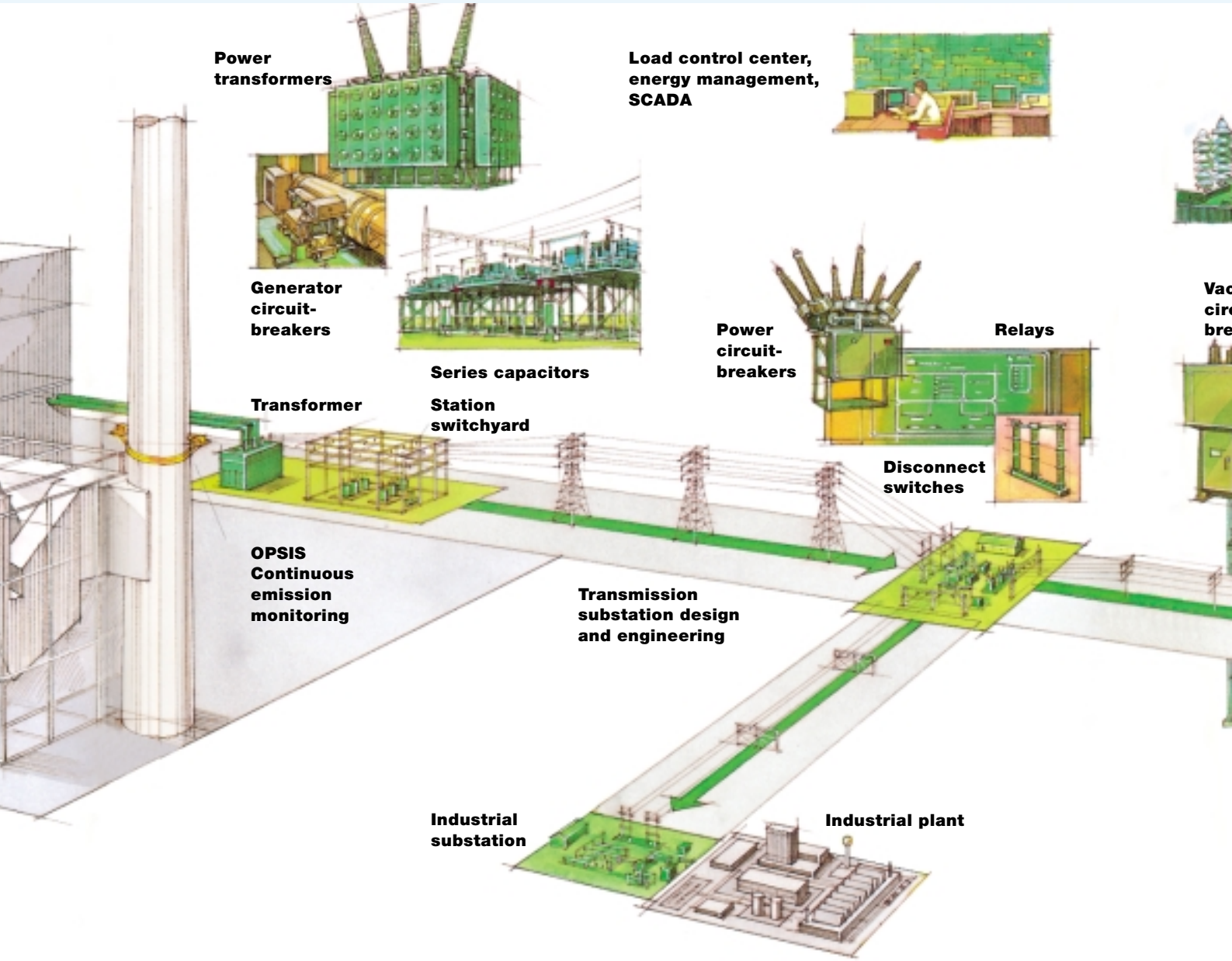


Computer use in the electrical system

Power plant

- **DCS (distributed control systems)**
- **Auxiliary system controllers**
- **Interfaces to other systems**
- **'Black boxes' with computers**
- **Intelligent devices**

toring and supervision of the system. As a rule, these extensions and additions have no adverse effect on the robustness of the system, eg the flow of electricity does not directly depend on proper functioning of the computers in the network control center; in fact, it would continue to flow if the computers were switched off. Also, the digital devices are typically of a robust design, without 'nice-to-have' add-ons. As a result, digital relays and protection devices are, with very few exceptions, Year 2000 compliant. The system control loop, which has to ensure that the generated power and consumed power are balanced at all times, is based on local frequency control in certain, selected generation plants. These fre-



Transmission

- Network control systems
- SVC, HVDC controls
- Communication computers

Substations

- Intelligent devices
- Protective relays

- RTUs
- Meteri
- Commu

Infrastructure Systems

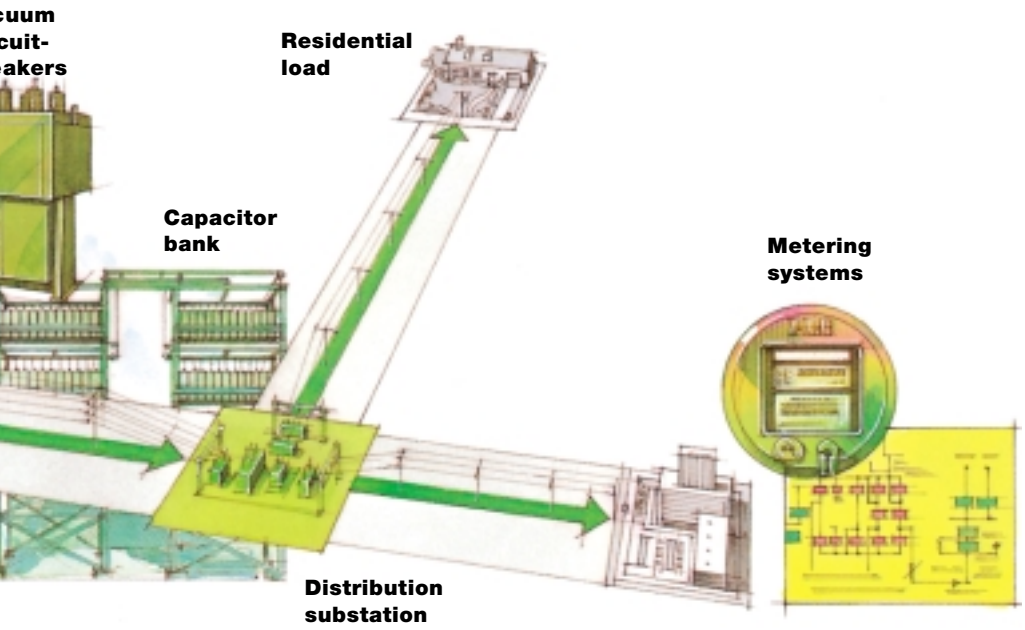
- Building access
- Fire alarms
- Power and water supply

quency control loops usually do not depend on digital technology, and where they operate with computers no date or time function is normally found in the control loop.

All of this is important in order to understand the starting point for the Year 2000 risk evaluation. In spite of this more or less sound platform the criticality of the power supply demands, as a kind of 'defence-in-depth' strategy [2], that certain questions be addressed: namely, is the system really so robust, what could still go wrong, and how could it be avoided?

It can also be seen above that the typical computer-based functions in the electrical system are concentrated in three areas:

Power equipment parts and service



Distribution

ng devices
unication links

- Digital control systems in power plants
- Computer-based network control centers and connected substations
- Intelligent measurement or protection devices or primary equipment with built-in computer control

www.abb.com/y2k

Visit the ABB Group Y2K web site for more information on Year 2000 compliance of ABB products.

Problems and risks in power plants

As mentioned, only those power plants with modern digital control systems should be focused on. For the large number of older plants without any digital control equipment, the so-called 'millennium bug' is obviously not an issue. Hydropower plants are usually in the latter category, and even those built more recently and which do have digital control are equipped with comparatively simple systems for which ABB has not been able to identify any serious Y2K threat.

A careful check nevertheless has to be carried out in these plants, targeting especially auxiliary systems such as the fire alarm or access control systems, which may have been installed later and could, if not working properly, indirectly affect plant operation.

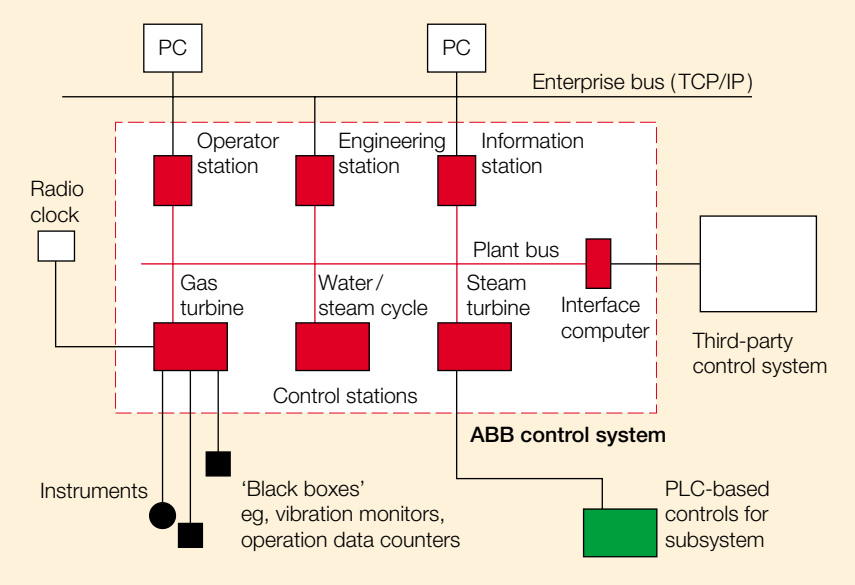
The Y2K problem is a bigger issue in coal- or gas-fired plants and nuclear power plants equipped with distributed control systems (DCS), simply because these plants are highly complex and many auxiliary functions are needed to make them work properly.

2 shows a typical structure for such a control system. Normally, ABB delivers the main system responsible for controlling the core equipment (eg, the steam or gas turbine) as a complete package. ABB has tested the system components and also typical system configurations with the main equipment components connected by communication buses. These systems are also very robust and are not likely to experience Y2K problems, as demonstrated by the compliance status of the widely used ABB Procontrol system components [3]. The exceptions are the operator stations, which are based on workstations from different computer vendors. Some earlier versions of these have been found to be seriously non-compliant, and would lead, unless corrected, to tripping of the plant. For example, unclear or unreliable operator information about the status of the plant may be displayed. In such a situation, the operator would be forced to shut the plant down after a short while. Another serious Y2K problem found in earlier generations of computers is an inability to reboot after 2000.

Since the locations of such non-compliant computers are known and a remedial concept has been developed (replacement or a software patch), every possible effort has to be made to eliminate this very serious risk through close cooperation between the system operators and suppliers. After the remediation work had been done, the part of the control system marked red in **2** successfully passed the various Year 2000 tests.

A second category of problems and risks results from those devices and interfaces connected to the control system. The system clock is set by means of a signal from a radio clock (more recently the GPS signal). A Year 2000 non-compliance can lead here to synchronization failure, so that the system runs on its own time. The time drift which this may cause can create severe problems in the communication with other systems. This is one example of an effect which, although not leading to immediate problems, can cause severe distortions later, sometimes much later.

Other critical equipment connected to the DCS includes intelligent measuring and monitoring devices, eg vibration monitoring devices for rotating machines. Some of these devices perform highly complex functions and therefore use extensive computing power. Normally, dates are not involved in this primary function. Dates are used, however, quite often to monitor maintenance intervals and to time-stamp the measured signals. Non-compliant time-stamps run the risk of being misread or rejected by the DCS, which could mean that a signal is shown as 'invalid' on the display. In the case of an important (eg, safety-re-



Typical structure of a power plant control system. The core part of the system (marked red) successfully passed the various Y2K tests following remedial measures. 2

lated) signal this may force the operator to shut down the plant.

Interfaces to control systems of other suppliers (eg, when the DCS for the boiler and the turbine island come from different suppliers) are critical. The data exchange between the two systems must be carefully checked for date-related data and their mutual understanding of the data verified. As a rule, non-compliances in this area do not have serious consequences. Quite often, however, they can lead to malfunctioning of certain services, such as archiving and documentation. For example, in one installation where an ABB control system was connected to a third-party archiving computer the system test showed the computer to be non-compliant.

While non-compliant archiving obviously does not place plant operation at risk, it can have serious consequences if regulations specify such a function as a precondition for plant operation. For nuclear plants, in particular, there exist a number of regulatory requirements which are mandatory for plant operation; in other plants, certain environmental sensors also belong in this category. Many of these functions are computer-controlled and are connected to monitoring and documentation devices.

As already mentioned, all kinds of auxiliary functions are important. A large coal-fired plant has a large number of such functions, some of which are obviously critical for plant operation (eg, those for coal transportation, cooling-water and compressed-air systems). Often, these peripheral systems make use of programmable logic controllers (PLCs). PLCs are a major Year 2000 concern as they perform their functions on the basis of an application-specific program with numerous timing functions. The documentation of such programs is often poor. A typical remediation process involves eliminating PLCs and implementing the required function in the existing DCS.

ABB has developed a methodology for a systematic Y2K risk classification of the numerous systems in a power plant (*Table*). Relevance to personnel safety, plant safety and plant production continuity represents one type of classification, while another is the time available for correcting potential problems before plant operation is placed at risk. Using this procedure, it is possible to focus on the important system parts.

Based on the described analysis and ABB's experience, the risk of losing a power plant due to Year 2000 non-compliance of some components must be taken very seriously, especially in the case of plants with a complex and diverse control and supervision computer infrastructure originating

Y2K: Power Utilities

Risks in power plants

- **Third-party, PLC-based controls for auxiliary systems which are important for personnel or plant safety or for plant operation**
- **Intelligent devices which perform functions required for operation of the plant (environmental sensors, archiving and documentation)**
- **DCS interfaces to the radio clock and other systems**
- **DCS**
- **Supplementary systems (access control systems)**

Y2K Task Force
G/SCT/Y2Kplant.ppt

from different suppliers. Even if individual components have been certified as being Year 2000 compliant, the plant operator must verify that the complete chain is Year 2000 ready and will function smoothly.

Problems and risks in network control and dispatching centers and in connected substations

Network control centers allow monitoring of certain areas of an electrical grid. Information about the status of the breakers and current and voltage transformer measurements from substations, power plants, etc, are processed and transmitted over remote terminal units (RTUs) to the central database in the network control center. The status of the grid, which lines are active, how much power is flowing over which lines, etc, is displayed, while a large number of supervisory functions are performed on the basis of the available data. Thus, operators receive early indications of changes in power production or consumption in an area. Based on this information, generation requests are dispatched to the different power plants in the area. An optimum grid structure in terms of routing of the power flows, lines in operation, etc, can be established. From stations in the network control center, breakers in the area can be remotely operated to obtain the required system configuration.

This briefly described functionality determines the main features of these very complex and large computer systems, which are based on high-performance workstations with millions of lines of code in the operating systems and the application software. The level of customization is very high as the systems have to be configured according to the specific structure and needs of the different parts of the grid.

The highly complex network control software and the workstation operating system on which it runs complicates the Y2K issue. Typically, the operating systems in use are earlier versions, and are neither maintained nor investigated by the computer vendors. Due to the complexity of the installations, upgrades to the latest versions are not usually possible. An adequate methodology therefore involves combined tests carried out on the overall systems and checks made on the main functionalities, supported by engineering judgement based on the release notes from the computer vendors.

ABB meanwhile has experience with a large number of such tests carried out on different network control center products and generations. Not one single case of complete system failure (dark screen or shut-down of the computer) was observed.

Typically, however, several cases of malfunctioning have been observed in earlier systems with functions involving date-sensitive data. Such malfunctions are normally corrected with a software patch or, in the case of very old systems, replacement by a new system, which also offers considerable additional functionality. Some of the typical malfunctions are: non-synchronization with the external clock; wrong time-tagging of data; wrongly archived data; erroneous event lists and reports; incorrect 'alarm filtering' (selection of alarms within a predetermined time window); inability to reboot computers after the Year 2000.

Table:
Prioritization of plant equipment. Example of methodology developed by ABB for a systematic Year 2000 risk classification of systems installed in a power plant

		Relevant to personnel safety	Relevant to plant safety	Relevant to production continuity	Not relevant
D1	*Steam turbine set & water/steam cycle*				
D1-02	Steam turbine & turboset (Bentley Nevada)			A	
D1-03	Generator output, metering			A	A
D1-04	Water condenser & evacuation			A	
D1-05	Condensate transfer, preheating, dumping device		A		
D1-06	Live steam & feedwater			A	
D1-07	Closed cooling-water system		A	A	
D1-08	Dosing			C	
D1-09	Sampling			C	
D1-10	Laboratory	C			
D1-11	Compressed air		A		
D1-12	Central lube oil supply & treatment system	C			
D1-14	Condensate cleaning system	C			
	Instrumentation			A	
	Heating, ventilation, air-conditioning	C			
	Fire protection		A		
D2	*Boiler area*				
D2-01	Heat recovery steam generator			A	
	Steel structures, cladding				
	Duct & stack				
	FAA lighting				A
	Blowdown vessel				
	Anchor devices				
	Soot blowers, incl control	C			
	Supplementary firing		A		
	Selective catalytic reactor (pumps & instrumentation)			A	
D2-02	Exhaust-gas analysis		B		
D2-03	Ammonia supply equipment for SCR		B		

A *Reaction time < 1 hour*
B *Reaction time < 1 day*
C *Reaction time < 1 month*

The RTUs connected to the network control center are, as a rule, Y2K compliant. What are critical, however, are the protocol converters acting as interfaces between the RTUs and the communication channels. The RTUs or control centers within a system may not be from the same supplier.

Particularly important for the system stability is the communication of the generation setpoints to the power plants. The entire communication chain must be carefully checked together with all the interfaces between the different system components. Two potential errors are dangerous in this chain: a wrongly communicated setpoint, which would cause problems immediately, and a loss of communication for the updating of setpoints. In the latter case, the previous setpoint would remain valid and over time, if the deviation became too large, the state of the system would become critical. This example illustrates the extremely important role that communication plays in the electrical system, and emphasizes the need to check all of its critical functions.

Patches are developed as a corrective measure for the malfunctions identified in system tests.

Based on its field experience, ABB sees the following two main risks in network control centers if remedial measures are not applied to all the installations in time: loss of some communication to substations and alarms and reports shown in the wrong sequences on the screens.

The effect of this could be to reduce the operational availability of network control centers.

While this alone would not have immediate and dramatic consequences, in combination with other disturbances in the system such occurrences could become dangerous and trigger cascading effects.

Y2K: Power Utilities

Risks in network control centers

- Loss of communication with some substations
- Loss of communication with power plants
- Wrong sequences and dates for alarms and reports
- Computer cannot be rebooted after 2000
- Auxiliary systems (water and power supplies)
- Supplementary systems (access control)

Y2K Task Force
G/SCT/Y2Kplant.ppt

Problems and risks with intelligent devices or primary equipment featuring built-in computer control

The intelligent devices most commonly found in electrical systems are protection gear (relays). Most of the installed relays, however, do not work with digital technology, only the more recent generations being microprocessor-based. The protection algorithms are time-critical and quite sophisticated. For this reason and because of the criticality of the protection, all unnecessary functions are avoided, ie either no date function is used at all, or when it is it is not close to the critical functions. Thus, the Y2K investigation usually shows protection devices to be compliant [3].

Metering devices also seem to be generally compliant. Any non-compliances that there are do not effect the supply of electricity since these devices are primarily for commercial transactions, which can be backed up by 'work-arounds'.

What are important are the systems and devices used for automatic load management. These systems work with date functions and, as they influence large loads, have a strong impact on the system dynamics.

Examples of primary equipment with built-in computer control are static var and HVDC devices used for the transmission of bulk energy, for coupling asynchronous systems and stability control. These make use of power semiconductors connected to a control system. Design reviews and system tests have shown that such systems use no Y2K-critical date functions for direct loop control.

In view of the complexity and importance of some of these installations, an appropriate Year 2000 assessment has to be performed for each installation. However, based on its present experience, ABB does not expect significant risks to arise from these devices. If prioritization is necessary, ABB proposes that the work in such installations be focused primarily on making sure that the environmental systems and auxiliary functions (eg, water and electricity supplies, cooling systems, etc) will not be disturbed.

Specific Y2K risks and potential crisis scenarios

Assuming that not all systems can be made fully compliant – a back-up procedure based on this assumption should at least be thought through as a 'defence-in-depth' strategy – what will be the consequences? As already mentioned, it may be expected that the electrical power will continue to flow undisturbed.

From what has been said, it is possible to derive some 'typical' Year 2000 risks. These range from malfunctioning of certain devices – most likely peripherals – in a power plant to the incorrect display of information from the power plant control system. If not remedied, such malfunctioning has the potential to cause tripping of the plant. This will not necessarily happen immediately after the millennium roll-over; the effects can show up later, since some of the errors have a delayed effect. Also, the independent real-time clocks in some of the black boxes may exhibit a considerable drift. In many cases, enough time is available to respond to this problem providing its source is properly understood and the correct course of action can be decided upon.

The main risk in the network control centers is a loss of system overview, eg due to an excessive number of alarms or wrong alarm sequences. Another risk is the loss of communication to one of the substations, making it impossible to operate certain breakers by remote control. While this once again has no direct consequences, in combination with other events it could lead to the system state becoming critical.

A hypothetical crisis scenario, eg requiring intervention by the operators, could be as follows: as a result of increased demand for power from a certain area due to a local plant tripping, the power flowing over an important feeder line rises to a critical level, ie it approaches levels where thermal overload relays would trip the line. Under normal service conditions the operators would order a plant in the area of high demand to increase power generation or alternatively activate a parallel line to reduce the load on the critical line. If the available information does not allow this response, the overloaded line could trip.

Such an event, namely the loss of a critical system component, can trigger cascading effects in the system. The history of brownouts and blackouts shows the root cause in most cases to be a combination of incidents that leads to a cascaded sequence of events. An actual case illustrates this: in July 1996 the electric service to about 2 million customers of the WSCC system in the western United States was interrupted [4]. The event triggering this was a short circuit on a HV power line caused by a tree growing into the line. At nearly the same time another line failed for totally different reasons. From this point on, there was a cascading series of events. In addition to the specific reasons that triggered the situation, the overall status of the system at the particular moment was another important reason for the severity of the outage: near-record hydropower generation in the Pacific Northwest, high power transfers on the transmission lines between the Pacific Northwest and California, power transfers through Idaho to Utah, high levels of coal-fired power transmission from Wyoming to Utah, and record demand for power in Idaho and Utah. In addition, the system status was affected by a combination of unfavourable conditions. This actual example shows how important it is for system-wide aspects to be taken into account in the Y2K preparation of the electrical grid.

The specific Year 2000 risk for electrical systems, namely that which makes it different from normal emergencies, is the risk of multiple coincidence failures: ie, whatever happens in the different system components will happen at the same time or within a limited period of time, and the events can occur in different geographical areas. 'Normal' system failures are restricted to a certain area. The utilities are able to deal with local events of this kind, since they have crews on standby which can be sent out at short notice to fix problems. However, not enough emergency crews are normally available to handle several such occurrences at the same time in different areas.

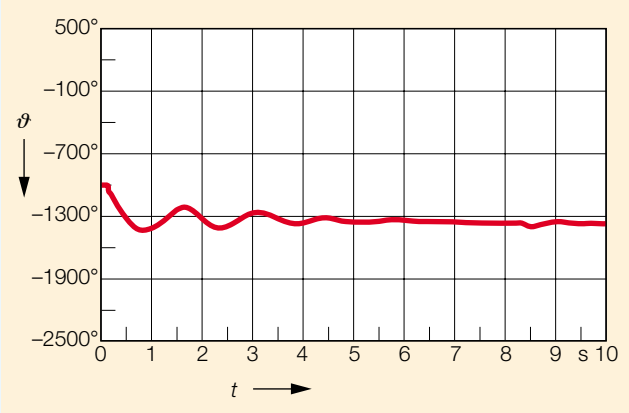
The biggest risk therefore comes from cascading system events which develop from multiple sources, as described in the hypothetical example above.

The enormous reliability and robustness of electrical systems are due to their rugged design, interconnections between different system parts which allow a critical area to receive support from the rest of the grid, and the ability of network control centers to correct trends leading to less stable system load distribution at an early stage, before safety margins have to be reduced.

Since the Year 2000 effects will occur simultaneously, it is not absolutely clear to what extent these advantages can be relied upon and to the extent a large, robust system offers a real benefit, especially if there is also a risk of some of the network control centers not working properly.

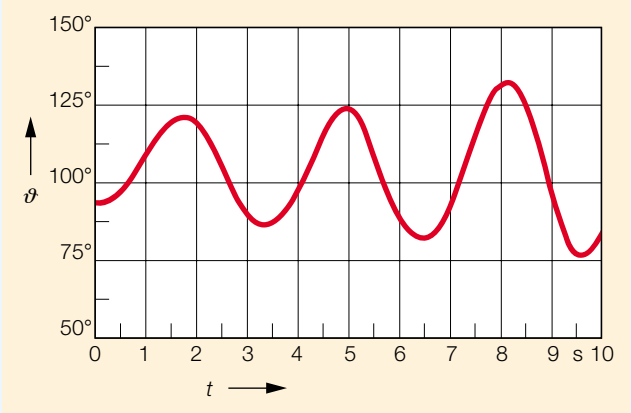
System studies based on simulations

In spite of the efforts made to identify and fix Y2K problems in all the critical areas, the huge importance of the power systems calls for extra precautions to be taken to cover the possibility of not all the problems being remedied. It is especially important to address the specific Year 2000 risks that have been mentioned since, by their very nature, they can be the cause of surprise effects with all their attendant dangers. The risks can be assessed and preventive measures worked out with the help of system studies based on simulations. To study the system dynamics, computer simulations are per-



Simulation of a power plant trip with recovery to a stable system state **3**

ϑ Phase angle t Time



Simulation of a power plant trip with growing instability **4**

ϑ Phase angle t Time

formed using models of a complete, wide-area, interconnected system, derived from important parameters such as the generation and transmission dynamics, relay settings, load distributions, etc. The utilities have such models already and use them mainly for system design work. ABB, as a leading system supplier, also uses such simulation software for system layouts and optimization, and has now started work on specific Y2K simulations with it [5].

Based on Y2K field experience, a certain percentage of failures is assumed for critical equipment: eg 10% of power plants with digital control systems will trip over a period of one day. The impact on the system dynamics is then simulated. The simulation model gives an immediate answer in terms of the impact of the assumed failures on the stability. If a power plant trips, the frequency of the system drops and the other generating units respond with a power increase. This leads to an oscillation, for which one of two cases apply: either the system can cope with the distortion and becomes stable again after a few seconds **3**, or the plant is at a critical location in the system, which becomes unstable and causes the oscillations to increase with time, leading to underfrequency protection relays initiating tripping of further generators. A cascading sequence of this kind leads to a blackout **4**. ABB recommends that the simulation models be tested and calibrated using historical events. The examples in **3** and **4** show simulations based on a hypothetical Y2K-related blackout in the WSCC system.

The described simulations allow particularly sensitive system components to be identified and given a high priority for the application of corrective measures. Such simulations can also be used to configure a more stable system, while another, extremely important use is to provide data and scenarios for training operators specifically to deal with potentially critical Y2K situations.

Problem solution and risk mitigation

The first step towards solving the Y2K problem and mitigating the risks involved is to establish an inventory of the Y2K-critical equipment and work with the suppliers to find out the compliance status and correct non-compliant components. This work has been under way on a large scale for some time.

In view of how important it is to ensure an uninterrupted supply of electricity, ABB recommends that the described system simulations be carried out for all systems. ABB offers support to utilities performing such studies and in developing scenarios based on field experience. The results can help utilities to set the right priorities for implementing corrective measures:

- Highest priority must be given to the power plants and the systems in them which could lead to loss of the plant.
- Second priority has to be given to the network control centers, where the focus must be on the functions needed for early correction of drifting of the system towards an unstable configuration. This means that all components working together, eg for the communication of setpoints for power plants, have to be checked to see that they really work together across the involved interfaces. This work is much more demanding than obtaining compliance statements for the individual components.

In the next step, system solutions have to be developed which minimize the impact of potential Y2K outages on the grid. The solutions must address in particular the dispatching of generated power and the issue of increased spinning reserves. Increased local generation in and near load centers has two important and beneficial effects:

- It reduces the power transfers necessary on the high-voltage transmission network, which in turn will lessen the impact of transmission line outages.
- It increases the spinning reserves so that the impact of a loss of remote and major