Y2K readiness through close partnerships with process control users

ABB has developed a Group-wide programme to minimize the potential impact of the so-called 'millennium bug' on customers' software-based products and systems and on its in-house IT processes. Active steps are being taken to ensure that ABB products are 'year 2000 compliant' and that there is only a minimal risk of customers' processes being disrupted. To evaluate the susceptibility of the installed process control systems and provide a platform for corrective measures, ABB has created a 'four pillar' concept that offers maximum support to customers. More than 60 pilot projects show that a close partnership between the supplier and operators is the only way to successfully tackle the Y2K problem.

Large sections of the infrastructure on which society relies, eg electricity and water supplies, telecommunications and public transportation, are supervised and controlled by software-based process control systems. As has been widely reported, the software in older electronic devices was programmed to recognize only the last two digits of a year, eg '98' in the case of '1998'. Therefore, at mid-night on December 31, 1999, when these two digits change to '00', devices based on such software may read '1900' instead of '2000'. This Year 2000 problem, or 'Y2K bug' as it is also popularly known, may cause systems with such devices embedded in them to malfunction, or in the worst case shut down – as system tests carried out by ABB have shown – unless a professional and concerted effort is made to correct the situation. The same holds true for the huge number of industrial plants in which the systems are installed.

The economic implications of the Y2K bug could be enormous if corrective measures are not taken in time. Control system suppliers have already done a great deal of work, alone and in collaboration with plant owners and operators, to find solutions that will minimize the threat. This experience has shown a strong need for plant operators and control system suppliers to work together. Both parties have know-how and skills which are critically important, and only when both sides make their best and most knowledgeable people available will there be the resources needed to complete the work by December 1999.

Dr. Klaus Ragaller
ABB Year 2000 Task Force

The Y2K process control challenge

The investigation of process control systems with regard to their Y2K susceptibility is a complex undertaking despite the fact that the elementary failure mechanism (the 2-digit representation of a year) is a very simple problem. This is because in addition to the two dimensions of technical complexity ('vertical' and 'horizontal') there are all kinds of organizational complexity involved.

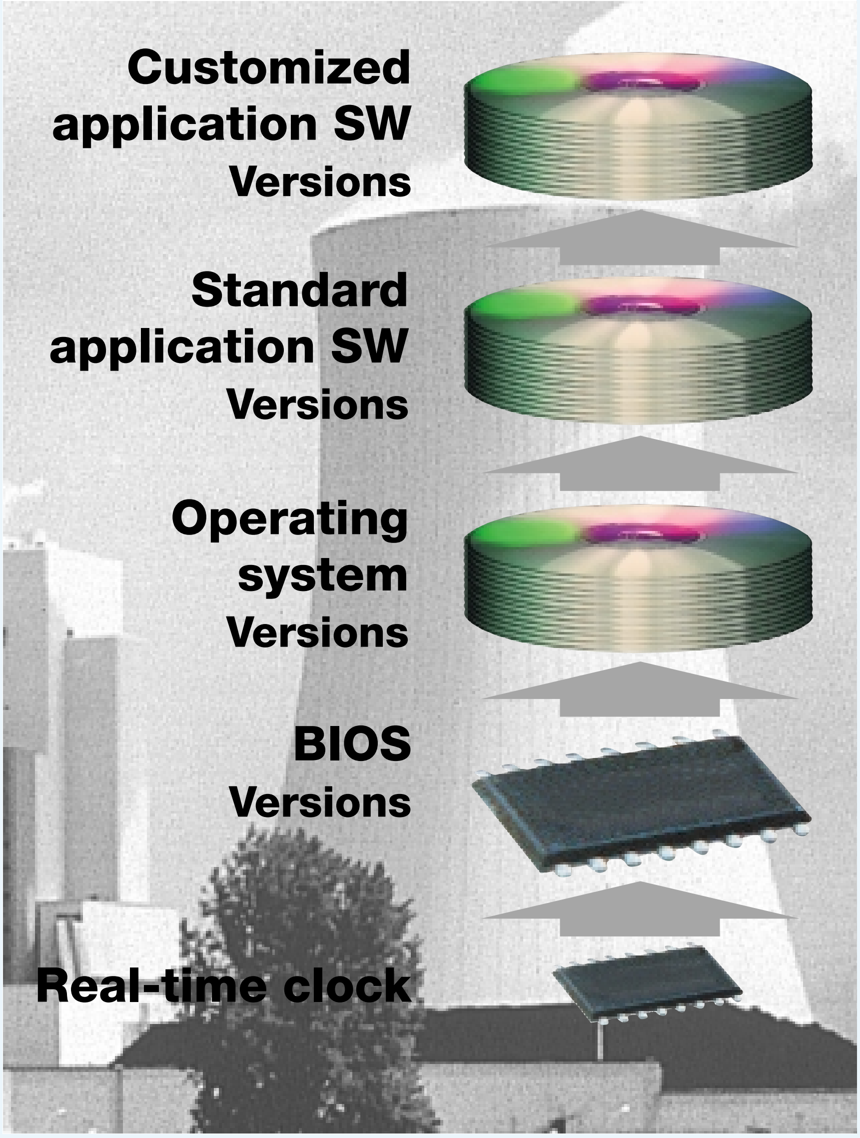
Vertical complexity

'Vertical' refers in this context to the different hierarchical levels in a control system **1**.

At the highest level there is the application software (typically consisting of a project-specific and a standard part) which may or may not use date functions and may or may not be Y2K compliant. The application software runs on a PC or workstation with an operating system which likewise may or may not be compliant. Below this operating system is the BIOS (Basic Input/Output System), and finally the real-time clock chip.

Over a period of time, different versions of the products in use on all four hierarchical levels will have been developed, so that many different combinations of these product versions may be found in the plants. Even at the individual product level this can lead to surprises (eg, two seemingly identical electronic balances, one with and one without a Y2K problem).

The total number of complex products of this sort connected together in a modern control system is very large, often reaching several hundred. In addition to the com-



Vertical complexity of a process control system. Over time, different versions of the products on all four hierarchical levels will have been developed, resulting in many different combinations existing in plants. **1**

BIOS *Basic input/output system*

plexity of each product in itself, there is also the complexity of the interactions to be considered.

As a supplier of control equipment, ABB tests the products used to build the systems as well as the basic configurations, which typically form the core of plant automation. However, the obvious complexity of any large system test configuration, although suitable for verifying Y2K compliance of all known modules within a system, makes it impossible to guarantee total compliance for the system and all its interconnections.

Horizontal complexity

Even more challenging than the vertical complexity is the complexity which results from the interconnections between different types of systems **2**. In a typical industrial plant, the process control system which controls the core process (eg, turbine control in a power station) is connected to a large number of other control and information processing systems. Examples of these are fire alarm systems and dedicated subsystems, eg for lube oil control, compressor control, etc. Often, there are also connections to other parts of the plant which may be controlled by a control system from another vendor or by a PLC-based control system.

Also very important are the sensors used to detect the process parameters which are environmentally sensitive or critical for safety. If these sensors malfunction, the plant might be shut down immediately.

Recent years have also seen a trend towards horizontal connections to the plant management information systems. These are made in order to automate the data transfer between process control and accounting, scheduling and other plant management tasks.

Control systems responsible for the control of, for example, a single unit are usually also connected to a more complex system, which in turn is connected to an overriding system of control centers. For instance, a power plant control center is connected to the control centers of other power plants, which are linked to the network control centers.

Typically, too, control systems are time-synchronized by an external clock system. Increasingly, a radio clock or the GPS (Geographical Positioning System) is used for this.

All or any of these system components and their interactions can be a potential cause of Y2K problems. One of the difficulties is that more than 90 percent of the components used in a system are not affected at all by the Y2K bug. However, the remaining 10 percent that can cause problems are distributed across the vertical and horizontal dimensions of the systems. Again, most of these problems will not be severe. It is in the remaining small percentage of problems that the real danger lies. The search for these 'needles in the haystack' is what makes the millennium problem such a challenge.

Organizational complexity

Superimposed on the mentioned technical complexities are a number of organizational complexities. Manuals, drawings and other system documentation can often not be found or are outdated and no longer reflect the present-day situation. Often, the engineering procurement company originally responsible for specifying a system and then documenting it in the form of pipe and instrument diagrams is not involved in later extensions or modifications to the system; also, the plant personnel and suppliers who collaborated in the work may have neglected to update the documentation. The first priority is therefore to assemble a complete, up-to-date plant inventory to serve as the basis for all further work. Every time a change is made to the installation after it has been confirmed 'Y2K ready', a check must be performed to ensure that there is no change in the system or component compliance.

The large number of different suppliers is another organizational challenge. What is needed for efficient Y2K project handling is information on the compliance status of the different products. Larger suppliers make this information available on the Internet, whereas smaller suppliers have to be contacted with special requests for information. Experience to date shows this source of information not only to be poor but – even more worrying – often unreliable. Suppliers and partners in the computer industry pose a specific problem: the general practice in this sector is to provide support only for more recent products, ie those not more than a few years old. In contrast, as a plant control system supplier ABB typically provides customer support for 30 to 40 years. This poses a dilemma as ABB uses equipment from the computer vendors in the control systems it sells to its customers.

For economic reasons, many industrial plants have to be kept running day and night. Because of this, maintenance has to be carefully scheduled and often can be carried out only within a very short timeframe. In the case of a paper mill, for example, this can consist of just a few days around Christmas time, while for a power plant or an oil platform maintenance may be scheduled just once every two years. As tests on the control systems can only be performed during these plant shutdowns, the scheduling of the Y2K tests in these plants is severely restricted. In other plants the boundary conditions for testing may be better, eg network control centers typically feature dual redundancy, allowing one of the two systems to be used for testing without having to interrupt operation.

Each type of plant usually also has its own specific security and environmental documentation as well as other regulations which have to be observed.

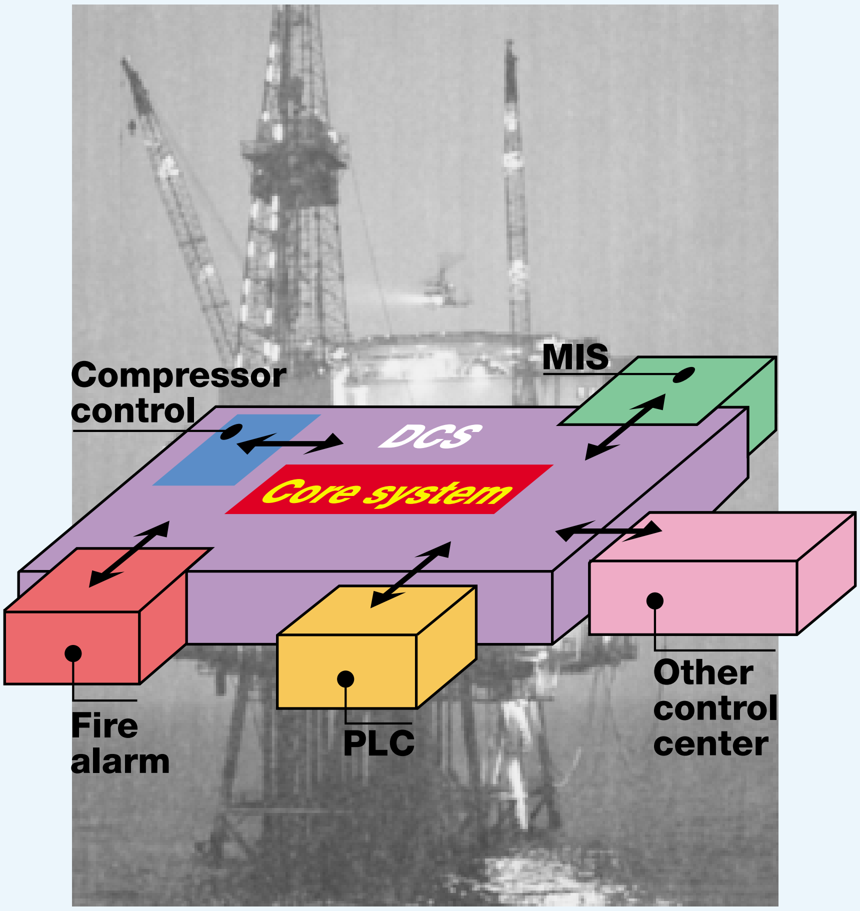
Achieving plant Y2K readiness

General

The first step, as has been said, must always be to establish a complete inventory based on the documentation available from the supplier and/or plant operator. How-

Horizontal complexity resulting from the interconnections between different types of systems **2**

DCS *Distributed control system*
MIS *Management information system*
PLC *Programmable logic controllers*



ever, a physical check also has to be carried out, as experience shows that there are always deviations from the existing documentation, which may even be incomplete (eg, the exact product designations or versions may not be given). This plant inventory should be stored in a database in a format that allows an automatic link-up to the supplier product database **3**. Thus, the compliance status is automatically indicated for all products installed in a specific plant.

In the case of third-party products with unknown statuses, a supplier inquiry must be started. This has to be given a high priority. Written inquiries frequently do not produce sufficiently reliable results fast enough; direct contact at the technical expert level is therefore often needed.

On the basis of this updated inventory, a plan for corrective action can be established. It must indicate which products have to be retrofitted with a patch, which products have to be replaced and which products can be left as they are although not compliant, since the type of non-compliance has no consequences for the specific application.

A second area to be worked through is the plant-specific application software typically installed in a variety of products. Examples are the ladder diagrams in the controllers and high-level application programs in the operator or maintenance stations. Different languages are used for this software: vendor-specific languages for the controllers, and Fortran, Pascal, C, C++ etc, for the high-level programs. These application codes must be scanned for entries that involve the date. For the code scanning, tools are available that automatically identify the critical code lines. The scanning can be done off-line, eg by downloading the code to a PC. On the basis of the identified critical code lines, it must be checked if the date function could cause a problem (this will seldom be the case), in which event a solution has to be programmed.

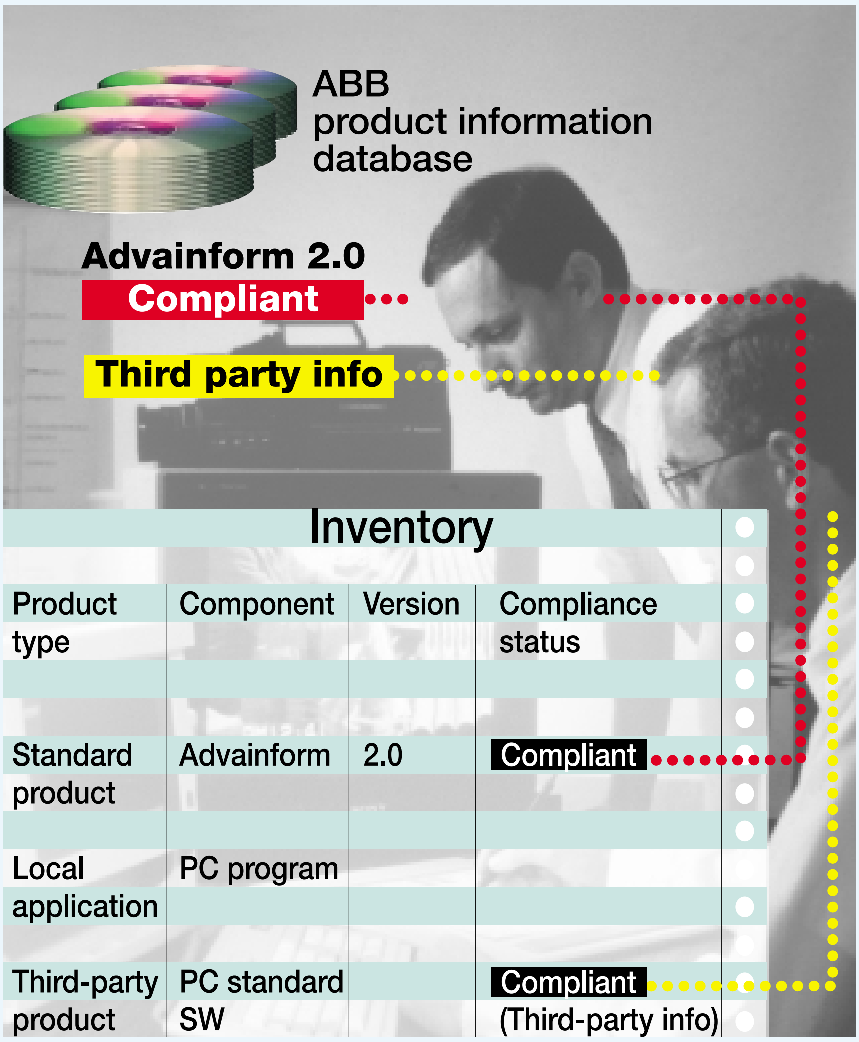
In certain application areas (eg, ABB power plant control) the design of the control system is based on highly standardized systems which are then customized by means of parameterization. In terms of Y2K compliance, the fact that no project-specific application software is installed in these systems is a huge advantage.

The next step is to identify the key subsystems used to build the overall system. The compliance status of the subsystems should be checked with the system suppliers. As mentioned, ABB is testing products and basic configurations. Although they cannot completely replace site tests, the results of these tests can considerably simplify site testing, as only those items not yet tested then have to be checked.

Next to be checked are the interfaces between the subsystems and the other system parts, again by scanning through the protocols in order to identify date-sensitive information. As with the application software, system designers must then evaluate the implications and, if there is a problem, program a solution.

As a next step, subsystem tests can be planned. This is exacting work: the tests involve the system clocks being set forward

The first step towards Year 2000 compliance: the establishment of a plant inventory based on the documentation available from the supplier and/or plant operator and its storage in a database that can be linked to the supplier product database. **3**



and then back again to test several critical dates 4. Before testing begins – in the case of critical subsystems the plant has to be shut down – a back-up of the complete system status has to be performed to be sure that the pre-test status can be re-established (date shifting can lead to the deletion of files, etc). Connections to other system parts have to be disconnected or must be simulated.

Finally, the system designer and plant operator have to decide together whether or not a complete system test is required.

Each of the above-mentioned steps has to be carefully documented. It is very important to realize that the described procedure relies heavily on sound engineering judgement. A widely recognized difficulty in software development is that it is not possible to test all possibilities. Thus, there is no guarantee that a system, although it has gone through all of the described procedures, will be free of problems.

Critical dates for testing subsystems 4

Example: oil platform is Y2K ready

The following example describes the procedure adopted for the control and safety system installed on Shell's Draugen oil platform in the North Sea 5.

The control system is an ABB Advant OCS (Open Control System). A rough indication of its size is given by the following figures: 9000 I/Os, 7 controllers, 4 operator stations, 9 security systems for fire and gas and for emergency shutdown, 5 communication links to other systems.

Due to the high complexity and criticality of this installation the plant operator requested that the support from the system supplier include engineers who had been involved in the system design. The plant operator also made his most experienced people available for the Y2K project.

The man-weeks required for the steps which have been described were as follows:

- 2 man-weeks to update the inventory
- 2 man-weeks to work through the products
- 1 man-week to scan the application code
- 2 man-weeks to check the communication links
- 2 man-weeks to perform the subsystem and system tests

As a result of the work carried out, this installation is now Year 2000 ready.

Partnership between plant operator and control system supplier

General

From what has been said, it is clear that the task of making a plant fit for the Year 2000 roll-over can only be tackled through close cooperation between the control system supplier and plant operator. Independent experts also confirm this. GartnerGroup,

Shell's Draugen oil platform in the North Sea.
The control system on this platform is now Year 2000 ready. **5**
(Photo: A/S Norske Shell)

one of the leading consultants in this field, states: 'The mission critical tasks within the process chain must be identified and the critical tasks must then be checked for embedded systems. This is best done in cooperation with the operation or maintenance personnel. They know where the critical tasks are and whether or not these tasks depend on embedded systems. The operation and maintenance personnel usually also know what must be done in the case of a failure.'

The importance of plant personnel playing a leading role, however, goes beyond the technical issues. As mentioned above, operating experience is essential if the systems and subsystems are to be structured for testing in a way that will keep operational disturbances to a minimum.

Especially important is the involvement of the plant personnel in the development of mitigation and contingency plans. Depending on the plant type and the operating constraints, a plant shutdown and a well-prepared reboot process in January 2000 might be the safest and most economical solution. This assumes that the customer's business process will allow a plant shutdown and that the reboot process works; several cases are known where rebooting has not worked during Y2K testing. Other options that can be considered are isolation of critical subsystems or manual operation of certain system parts, etc. Here again, close cooperation between the system supplier and operating personnel is the secret to an effective solution.

ABB's Year 2000 fourpillar concept

Based on the described experience, ABB has developed a fourpillar concept designed to give optimal support to customers operating plants in which ABB control systems are installed **6**.

Pillar 1: Investigation of ABB products for the purpose of evaluating their compliance status. Possible ratings are 'not applicable' for products which have embedded computers without a date function, or 'compliant' for products which have been tested in accordance with the BSI compliance definition (see box) and for which a test protocol exists. Products are rated 'non-compliant' when the tests reveal problems in meeting one or more compliance criteria. In such cases it is very important to clearly define whether the product will be made compliant or will remain non-compliant. In the latter case, information should be given about the exact nature of the non-compliance, as in many cases non-compliant products can still be used without problems.

Pillar 2: Establishment of an inventory of installed plants. This acts as the basis for all further work, for planning the needed resources and for scheduling the required training courses, etc. As already mentioned, these are not trivial tasks. Plant evolutions have to be traced back 15 to 20 years, a time frame within which the industry, suppliers and plant operators will all have undergone major changes. In the meantime, some suppliers may have ceased to exist, or plant operators may have changed owners, etc.

Pillar 3: Execution of pilot projects for the purpose of developing a methodol-

British Standard DISC PD2000-1:

- Product operation will not be interrupted when the date reaches the '00' value.
- Date-based functionality must behave consistently for dates prior to, during and after the year 2000.
- In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.
- The year 2000 must be recognized as a leap year.

'Four pillar' approach developed by ABB to give optimal support to customers operating plants in which ABB control systems are installed *(Photo: PRISMA)* **6**

Pillar 1: *Investigation of ABB products*
Pillar 2: *Establishment of an inventory of installed plants*
Pillar 3: *Execution of pilot projects in order to develop a methodology for each type of plant*
Pillar 4: *Training programme for customer's and ABB service personnel*

ogy for each type of plant. Although there is a general process which can be followed for every plant, there can be important differences between the plants, eg differences in the level of automation, extent of the integration with other systems, training and strength of the operating and maintenance staff, facilities for isolating certain parts of the plant, possibilities for tests, etc. All of these aspects are worked on in the pilot projects and put together in a methodology for a given type of plant.

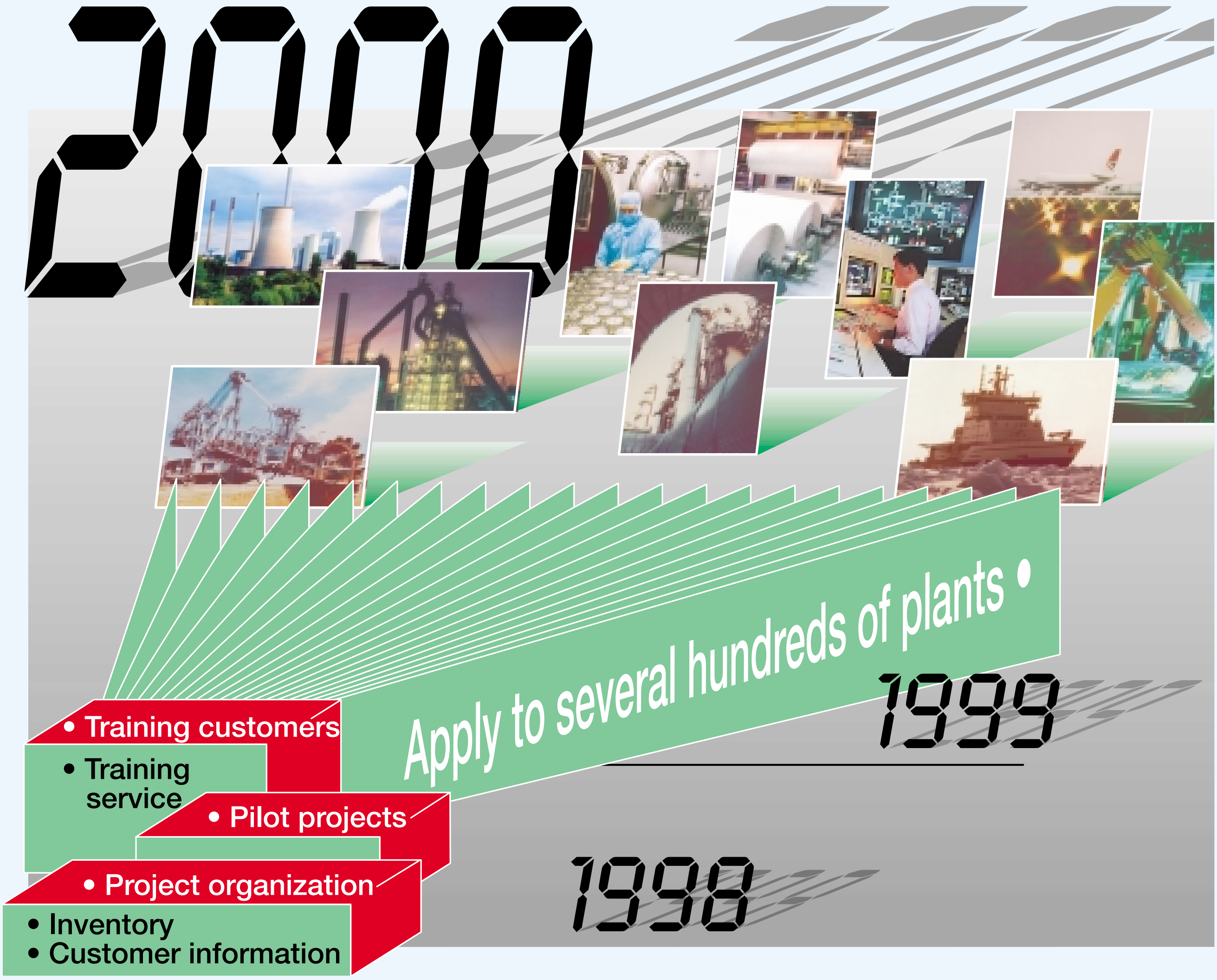
Pillar 4: Training of the customer's personnel and ABB service staff. The knowledge gained from the pilot projects must be passed on to a large number of people. The sheer number of plants in existence and the limited number of personnel at the disposal of the control system suppliers indicate the need for both parties to work on this, and the necessity for training on a large scale. ABB has several worldwide training organizations, and these are being used to achieve the necessary multiplication effect **7**.

Current status

More than 60 pilot projects being run by ABB are almost completed. In all cases, the cooperation with our customers, who operate the plants, is excellent, and the four pillar concept has been well-received. The training courses are also well under way, with a significant portion already completed.

Concluding remarks

The only way to tackle the Y2K problem is for the system supplier and system oper-



Expanding from pilot projects to full-scale, industry-wide realization **7**

ators to work together. Besides the technical and organizational arguments for such a partnership, only close cooperation can effectively avoid dangerous misunderstandings and misconceptions. The Year 2000 problem is not the fault of one party or the other, neither of the suppliers nor of the plant operators. It is a result of a convention adopted decades ago to save chip-memory costs, and its continued and widespread use since then by software development groups across all of industry. Suppliers, customers and users are all being confronted with this problem in much the same way. What must be avoided at all costs is finger-pointing and the apportioning of blame for the situation, neither of which will solve the problem.

Only a shared effort in which all parties able to contribute to the solution participate will allow an adequate response to the Y2K challenge.

There are also some beneficial side-effects of the Year 2000 cooperation. As a result of the closer relationships between suppliers and operators, opportunities for plant upgrades and other improvements, leading to better service, may be identified. Hopefully, too, industry will learn from the Y2K issue. Systems, especially those which play such a vital and universal role in society, must be designed in such a way that they will be incapable of causing similar problems in the future.

Author

Dr. Klaus Ragaller
ABB Year 2000 Task Force
ABB Asea Brown Boveri Ltd
CH-8050 Zurich
Switzerland
Telefax: +41 1 317 79 68
E-mail:
klaus.ragaller@abbzh.mail.abb.com