Applied Occupational and Environmental Hygiene

ISSN: 1047-322X (Print) 1521-0898 (Online) Journal homepage: https://www.tandfonline.com/loi/uaoh20

Occupational Safety and Health Implications of the Millennium Bug: Embedded Microchips

Vernon P. Anderson

To cite this article: Vernon P. Anderson (1999) Occupational Safety and Health Implications of the Millennium Bug: Embedded Microchips, Applied Occupational and Environmental Hygiene, 14:6, 359-364, DOI: 10.1080/104732299302738

To link to this article: https://doi.org/10.1080/104732299302738

Published online: 30 Nov 2010.

Applied Occupational and Environmental Hygiene
Volume 14: 359–364, 1999

1047-322X/99 $12.00 + .00

IH Interface

Occupational Safety and Health Implications of the Millennium Bug: Embedded Microchips

William J. Daniels and Stanley Salisbury, Column Editors

Reported by Vernon P. Anderson

Abstract

Personnel working in the field of environmental safety and health need to be aware that their exposure monitoring equipment as well as various laboratory and work site test and safety systems are candidates for a Y2K problem. The focus here is on the Y2K problem associated with embedded microchips contained in measurement and analytical equipment with internal date functions. With the turn of the century, the year 99 (i.e., 1999) will turn to 00 (i.e., 2000). The expectation is that the date change over will result in some form of malfunction or failure. The media has provided us with basic information on Y2K, particularly as it impacts computer hardware and software users. We know less, however, about how the Y2K issue may affect date-sensitive embedded microchips in safety and health equipment. To manage this problem, we propose a familiar public health strategy involving risk assessment (surveillance and prioritizing) and risk management (intervention/contingency planning). Success in dealing with Y2K-embedded chips will be increased by engaging managers, operators, employee-management safety teams, safety professionals and their organizations, trade associations, local, state and federal regulatory agencies, and the public, where appropriate. A list of Internet sites is provided with information on managing problems arising from date-dependent embedded chips and the Y2K problem.

Introduction

Personnel working in the field of environmental safety and health need to be aware that their exposure monitoring equipment as well as various laboratory and work site test and safety systems are candidates for a Y2K problem.* The focus here is on the Y2K problem associated with embedded microchips contained in measurement and analytical equipment with internal date functions.** The Y2K problem has evolved because of a need by programmers to conserve costly computer memory in the early development of software and hardware applications. This led to the tradition of using two digits to represent the year instead of four digits. With the turn of the century, the year 99 (i.e., 1999) will turn to 00 (i.e., 2000). The expectation is that this will result in some form of malfunction or failure whenever date-dependent calculations are performed. The media has provided us with basic information on Y2K, particularly as it impacts computer hardware and software users. Also, a scan of the Internet yields more than three-quarters of a million pages describing various facets of this problem, originating from more than 200 Internet sites around the world. We know less, however, about how the Y2K issue may affect date-sensitive embedded microchips. To manage the problem, we propose a familiar public health strategy involving risk assessment (surveillance and prioritizing) and risk management (intervention/contingency planning).

Background

Many experts believe that electronic systems that do not correctly recognize certain dates in 1999, and after December 31, 1999, will malfunction or shut down due to "date-discontinuity" prior to, on, or during the year 2000.[1] Strictly speaking, this is more than a once-every-thousand-year event occurring at a specific point in time. There are a series of dates now, and in the near future, that may pose a risk of some form of system or equipment failure (Table I). Professor Haselkorn, Chair of the Institute of Electrical and Electronic Engineers (IEEE) Year 2000 Coordinating Committee, suggested that a more accurate name for Y2K is the "Century-Digits Change" problem, or CDC for short. The reference to the acronym CDC for the Centers for Disease Control and Prevention is intentional, because the phenomenon is more similar to an epidemic than to a typical technical problem. Moreover, a plot of the curve for Y2K technological failures and recovery closely resembles the course of an epidemic and then recovery. This epidemic analogy is not lost in the way computer scientists describe the problem and solutions. For example, the exchange of data is described as "transmitting the bug"

* For consistency, the acronym "Y2K," referring to the Year 2000, will be used throughout this article. Analogous terms include Millennium Bug, Y2K Time Bomb, and more recently, the Century-Digits Change (CDC) problem.

** Embedded microchips are written in a low-level language, usually Assembler. The object code is burned into the chips' Read Only Memory (ROM). This ensures the code cannot be altered, unless the ROM is of a special type that can be updated. The microchips are inserted or "embedded" into the electronic hardware of equipment and serve to control the product's functionality.

TABLE I
Dates that may affect occupational safety and health[A]

Dates	Why it may be a problem
January 1, 1999	Some systems use 99 as a trigger or as an end-of-file marker (the last record in a file or list). This may be the case if the system handles the year portion of the date as two digits.
September 9, 1999	Some systems use 9s as an end-of-file marker (the last record in a file or list).
January 1, 2000	If a system handles the year portion of the date as 2 digits ONLY, actions and calculations may be incorrect.
February 29, 2000 (leap year)	This is a leap year day and may not appear in some system calendars. When adjusting systems for Y2K, this date needs to be programmed.
December 31, 2000	This is the 366th day, which has been known to cause problems in systems.
January 1, 2001	Some systems are being adjusted only for the year 2000.

[A] A more exhaustive list of problematic dates for the Y2K can be found at http://www.bug2000.co.uk/business/testing/shtml.

from system to system; "fire-walls" are used to "quarantine" systems; and prevention follows a triage approach, seeking to save those systems that have the best prospects. Furthermore, the focus on prevention deals not only with the existing cases, but also on the growth rate and on potential future cases. Finally, Haselkorn stated that "we need to carefully define the disease and provide guidelines for its management."[2] The epidemic analogy for those of us in the health sciences may serve two purposes. It provides a familiar context for managing the problem and it provides a perspective on the insidious nature of the millennium bug.

Despite the widespread publicity in recent months about this problem, the actual extent of the damage to computer systems and control systems is unknown. There are technical experts who predict the Y2K malfunctioning could lead to massive catastrophic failure of industrial processes, resulting in increased risk of death and injury to both the workforce and the general population.[3] Not only will many computers fail—but any item containing a microchip may also fail. Table II lists examples of systems that could fail, and thereby affect the safety and health of workers and the public. Examples of failures of embedded systems are being reported with increasing frequency, particularly on the Internet. For some interesting reading and examples of failures from Y2K testing, scan the Y2K-Status.Org: Examples of Failures of Embedded Systems (http://www.Y2K-status.Org/EmbeddedFailures.htm) and a site listed as Year 2000 Problem Sightings (http://info.cv.nrao.edu/y2k/sightings.htm).

TABLE II
Systems that may fail and affect the safety and health of workers

Affected system	Effect on workers
Electrical supply (including backup lighting and generators)	Entry and exit from work sites ability to perform tasks
Fire control systems	Ability to know about fire and fire location
Valve control systems	Malfunction of systems that contain hazardous materials
Security systems, cameras, vaults	Inability to assess potential dangers
Time recording systems	Inability to determine the legal date

The scope of the embedded microchip problem can be appreciated when you consider the experience of the Department of Defense. A review was performed of one small sector of their Year 2000 project inventory. Of the 3,962 applicable systems with embedded microchips, they found 582 were acceptable, 623 were being renovated, 628 were retired, and the balance of 1,900 needed further investigation. The conclusion was that about 25 percent of all the embedded systems would require some level of fixing. Similarly, an industry executive in the automotive industry was quoted as saying, "Amazingly enough, machines on the factory floor are far more sensitive to incorrect dates than we ever anticipated. When we tested robotic devices for transition into the year 2000, for example, they just froze and stopped operating." Above all else, Y2K is a new challenge to management that demands a coordinated effort and an overall plan with proper metrics for assessing project completion, the extent of the problem, and the establishment of realistic dates for completing the tasks.[4]

In response to the Y2K problem, on October 19, 1998, the president signed the "Year 2000 Information and Readiness Disclosure Act."[5] The law (S. 2392) was drafted to address what the president described as the "first global challenge of the information age." The law, also referred to as the "Good Samaritan Act," was drafted "to encourage the disclosure and exchange of information about computer processing problems, solutions, test practices, and test results, and related matters in connection with the transition to the year 2000." This legislation provides a degree of liability protection to promote and *encourage greater information sharing* about

Y2K experiences and solutions. Certainly, for small business and services provided by local communities, the exchange of information on the Y2K problem is critical. Few small businesses have the internal resources or expertise to deal with this problem. In an effort to improve communications and centralize information sharing, the U.S. Government established an Internet site (http://www.Y2K.gov/) that contains information targeted to specific industry sectors, for example, small business, health care, transportation.

Small Business Challenge

According to the GartnerGroup,[6] as of October 1998, 23 percent of small companies (2,000 or fewer employees) have not started any Y2K remediation. Yet 50 percent of companies that have significant health and safety risks will experience at least one critical system failure during the first quarter of 2000. Industries in this category include chemical processing, utilities, construction, transportation, pulp and paper, food processing, and agriculture. Recovering from a single failure is estimated to cost a company between $20,000 to $3.5 million.

Given that any programmable electronic system may fail, rendering existing safety systems ineffective, and given the cost of recovery from failures, the incentive for mounting a prevention program for the Year 2000 should be self-evident. At the simplest level, the responsibility of a person working in a small company who oversees the plant's ventilation and exposure monitoring equipment would entail a call to the manufacturer of the equipment/software to verify Year 2000 compliance status. The manufacturer already may have developed hardware and software fixes to rectify the Y2K bug. Alternately, the manufacturer may no longer be in business and/or the equipment may be considered obsolete with no fixes available. Certainly, lack of information would necessitate some unplanned and potentially costly expenditures for replacements or customized fixes. The cost associated with a prevention approach, however, should be easy to justify when weighed against the uncertainty of doing nothing and the potential risks to equipment, employees, and production schedules if Y2K problems exist.

Risk Assessment and Risk Management

As Professor Haselkorn noted, there are a number of similarities between the Y2K problem and an epidemic. As such, the public health model provides a familiar and simple strategy for assessing, managing, and staging the problem. To gauge the extent of the problem, a basic risk assessment is performed to survey inventory that includes date-dependent microchips. The inventory is prioritized, perhaps using a triage strategy to assess and rate the accompanying safety and health risks. Risk management may be the most challenging phase involving the development of contingency plans and implementing fixes, where possible. Finally, information on successes and failures with Y2K solutions needs to be disseminated and shared with others.

Risk assessment. Risk assessment begins with surveillance. A single inventory needs to be constructed of all the equipment, systems, and software in an organization that contain embedded microchips, or computer source codes that maintain yearly timekeeping functions (see Table II). A major problem is that embedded microchips and software with date-dependent functions are ubiquitous in process control operations, controlling everything from power grid systems to ventilation systems. The difficulty lies in identifying which components contain date-dependent functions and which software applications use yearly dates as data points. Few organizations have an inventory of their computer program source codes or even the sub-components of their process-control systems. Typically, process-control components are linked into larger systems involving a feedback mechanism. This results in inter-connected systems, such that when one unit fails, they all fail, not unlike a string of Christmas lights strung in series. Finally, the problem can occur at any level of the system: the computer clock, the basic input/output system (BIOS), the operating system, the application software, or the data held.

In general, systems that operate using embedded microchips typically fall into one of the four categories listed below. Categories 1 and 2 are unlikely to fail, unless they are programmed to work differently on different days, or have a maintenance schedule built into their functioning, in which case a Y2K-compliant replacement is usually the only option. Categories 3 and 4 pose the greatest risk for failures.[7]

1. Individual microprocessors (e.g., temperature sensors, smoke and gas detectors, circuit breakers).
2. Small assemblies of microprocessors with no timing functions (e.g., flow controllers, signal amplifiers, position sensors, valve actuators).
3. Subassemblies with a timing function (e.g., switches/controllers, telephone exchanges, elevators, data acquisition, monitoring, and diagnostic.) Sensors in these subassemblies systems usually send data to computers that run database programs. Y2K failures may occur within or between subassemblies and even before the year 2000, because the system may project a future action that would not be recognized.
4. Computer systems used in manufacturing or process control, which also usually include embedded microchips, are candidates for Y2K failures. System failures would be expected because the software and hardware are usually based on commercial data processing languages that were developed years ago, such as COBOL and FORTRAN.

A basic inventory should include at a minimum the following: the unit name, manufacturer, model number, serial number, software release dates and patches, and the purpose of the unit, reference documentation, information on

the format of the date, if available, and any electronic linkages with other equipment or software. A more detailed format for an inventory containing 39 informational fields is provided by the Institution of Electrical Engineers (IEE) from the United Kingdom (http://www.iee.org.uk/2000risk/w-104.htm). Regardless of the detail, a comprehensive inventory will define the work to be done. The inventory will also be useful for deciding whether you have the personnel resources and expertise in-house to deal with the problem.

Once an inventory is assembled, the items need to be prioritized. The highest priority in the event of Y2K failure should be given to those systems that have the greatest impact on the safety and health of workers, as well as the public, followed by those systems that have an impact on business operations. The problem is that the two systems are often intertwined in production-oriented industries. Moreover, priority setting cannot be done without some knowledge of the costs and benefits of proposed actions. The options for risk management need to be explored at an early stage to assure that priority is given not only to those systems in which the severity of the problem and the greatest number of workers/tasks are affected, but also consideration needs to be given to those systems that are the most amenable to intervention, that is, have the best chance of succeeding given the time frame available.[8] The U.K. Health and Safety Executive also provides a useful synopsis of the risk assessment approach entitled, *Health and Safety and the Year 2000 Problem—Guidance on Year 2000 Issues as They Affect Safety-Related Control Systems*, http://www.open.gov.uk/hse/dst/2000indx.htm.***

Risk Management. Following the initial prioritization, the manufacturers and suppliers need to be contacted. Usually, they are the only ones who understand the detailed characteristics of the hardware and software. If the equipment and software is more than few years old, the suppliers may be difficult to locate as a result of company mergers, business failures, or name changes. The *Thomas Registry of Manufacturers* and the original equipment reference materials provide good starting points for locating manufacturers.[9] A useful database of manufacturers is being constructed on the Internet that includes information on companies that produce measurement equipment, controls, or anything that could have an embedded processor inside. The database lists the type of controls a manufacturer produces, whether they have Y2K web pages, and whether the manufacturer has Y2K information related to its products.[10]

Another site on the Internet that is strictly commercial offers a unique compliance database containing information on 10,000 microprocessors, related control devices, and software from more than 1000 vendors of products that may be used on the factory floor. The vendor indicates that the software can evaluate Y2K capabilities for robots, computers, microprocessors, and systems with embedded software that are used to guide automated vehicles. Once an inventory of microprocessors and software is compiled, a client company can access the company's commercial database to determine whether the maker of each item can supply a Year 2000 update, or whether the equipment should be replaced.[11]

Information obtained from equipment suppliers concerning the Year 2000 compliance of their products could be restricted, refused, or worse yet, may be misleading. Suppliers may fear a lawsuit stemming from any admission that their products may fail. They may also fear that any negative information about a lack of Y2K compliance could be publicized on the Internet, affecting their competitive status and future sales. Finally, suppliers may simply be uncertain as to whether their products are Year 2000-compliant.

The Good Samaritan Act was passed, in part, to allay suppliers' fears of sharing Y2K information. Concerned suppliers also have joined together and established independent third-party auditors who are entrusted with gathering Y2K information from suppliers and then providing reports to customers with the stipulation that the customers forgo any rights of litigation and unfair use of the data. This agreement is referred to as the "Compliance Cooperative Protocol."[12] How effective either approach is in ensuring accurate information sharing has yet to be determined.

There are at least four choices or actions that can be taken when systems and equipment are found to be at risk of failing due to Y2K conditions: workaround, repair, replace, or retire. Each of these actions/choices are described by the IEE in a comprehensive monograph available on the Internet.[13] This instructive monograph provides definitions, criteria, and examples for making decisions about carrying out each of these actions to achieve Year 2000 compliance. To minimize disputes about what constitutes Year 2000 compliance, a uniform definition is needed. Although the definition of Year 2000 compliance and the actions that achieve compliance would appear self-evident, this is a hotly debated issue. The U.S. Institute of Electrical and Electronics Engineers (IEEE) published a "Standard for Year 2000 Terminology" that broadly states that equipment, systems, and computers are compliant when they are capable of processing date-dependent data within and between the 20th and 21st centuries.[14] The federal government's Y2K Interagency Committee (IAC) also has been addressing Y2K compliance definitions and compliance standards since January 1996, http://www.itpolicy.gsa.gov/.

Good risk management requires the development of a contingency plan. A Y2K contingency plan will identify what the organization must do to keep operations running while realizing that some of the organization's critical systems are not Year 2000-compliant. Each contingency plan should provide a description

*** Requires Acrobat Reader Version 3 to open document.

of the resources, staff roles, procedures, and timetables needed for implementation. The contingency plan may also identify the risks, costs, and benefits of alternative strategies.

Contingency planning involves the preparation and partial implementation of alternative work processes in the event of a safety and health failure of varying proportions. It is perhaps the most difficult aspect of solving the Y2K problem, because it involves a disciplined investigation into all areas of an organization's operations and locating those points where safety and health risk can occur which could pose a risk to workers. Likewise, one of the primary values of contingency planning is that the planning has taken place before the crisis. The risk can be reduced by building into the action plan an adequate post-implementation interval. Most information technology industry experts agree any application should be implemented no less than six months before the Year 2000. Comprehensive testing also needs to be conducted during the post-implementation interval. Prior to implementation, the organization should thoroughly test and certify that the equipment and the tests performed can advance their dates into the next century.

There is no simple solution, short of talking to, and working with, the manufacturers and suppliers of equipment being used that contains embedded microchips. Each person responsible for such equipment should be developing and carrying out a plan for evaluating the impact of the Y2K problem on their operations, particularly as it affects the safety and health of workers and the public. Dr. Jerry Poje, Chemical Safety and Hazard Investigation Board Member, captured the sentiments of many concerned professionals in this field when he noted, "... that the novel, time-definite, and pervasive Y2K problem is a major test of the system of safety in the United States and beyond. This means every component of the system will need to be effectively engaged: managers, operators, safety professionals, professional safety organizations, trade associations, local, state, and federal regulatory agencies, emergency response agencies, surveillance agencies and research agencies, and the at-risk populations in the nearby communities."[****]

More detailed guidance for each of these steps is available at various Internet sites. Appendix A contains a list of the sites that we have found informative on the subject of date-dependent embedded microchips and Y2K problems.

Acknowledgments

Appreciation is extended to the following individuals for their comments and reviews of various drafts of this paper: Martin Abell, Cathleen Anderson, Edward Dacey, William Halperin, Vivian Morgan, Richard Niemeier, Jerry Poje, Scott Schneider, Paul Schulte, James Seligman, Rodger Tatken, and Eugene White.

REFERENCES

1. A Call to Action: the National and Global Implications of the Year 2000 Embedded Systems Crisis, http://www.year2000.com/y2kcurrent1.html, Reid, W.S., The Year 2000 Titian, MidRange Systems Magazine, http://www.year2000.com/y2kcurrent1.html (August 17, 1998).
2. Haselkorn, M.P.: Engineering the Year 2000 Problem; Professor and Founding Chair of Technical Communication, University of Washington, Chair, IEEE Year 2000 Coordinating Committee, Member, President's Y2K Conversion Council, Working Groups on Information Technology, Science & Technology, and Non-Profits & Philanthropic Organizations, http://www.ieee.org/tab/tsld001.htm (November, 1998).
3. de Jager, P.: An Open Letter to President Clinton, http://www.year2000.com/y2ky2kclinton.html (November 17, 1998).
4. Webster, B.F.: The Estimated Impact of the Year 2000 Problem in the United States... A Survey of the Membership of the Washington, DC Year 2000 Group, 21 April 1998, http://wdcy2k.org/survey/.
5. Year 2000 Information and Readiness Disclosure Act (S.2392), signed into law October 19, 1998. http://www.Y2K.gov/.
6. Marcoccio, L.: Year 2000 Global State of Readiness and Risks to the General Business Community, Testimony to U.S. Senate Special Committee on the Year 2000 Technology Problem, Washington, DC, http://gartner5.gartnerweb.com/gg/static/itjournal/testimony1.html (October 7, 1998).
7. The Institution of Electrical Engineers (IEE), The Millennium Problem in Embedded Systems, London, United Kingdom. http://www.iee.org.uk/2000risk (September 25, 1998).
8. U.K. Catalogue of Year 2000 Information, http://www.bug2000.co.uk/business-bug/search/index.shtml (December 10, 1998).
9. Thomas Publishing Company, 5 Penn Plaza, New York, NY 10001. Thomas Register on CD-ROM, http://www.thomasregister.com/ (December 17, 1998).
10. Embedded Processors Y2K Page. A Database of Select Manufacturers of Equipment with Embedded Microchips. http://www.geocities.com/SiliconValley/Grid/6729/ep/ep.htm (February 2, 1998).
11. Jenkins, J.: TAVA Technologies Plant Y2kOne™, http://www.planty2kone.com/fr-main.html (November 25, 1998).
12. Ross, G.: The Y2K Compliance Cooperation Protocol (CCP), http://www.alertuk.com/ (July, 1998).
13. The Institution of Electrical Engineers (IEE), The Millennium Problem in Embedded Systems, London, United Kingdom, http://www.iee.org.uk/2000risk/, (Section: w-205.htm) (September 25, 1998).
14. IEEE Standard for Year 2000 Terminology, IEEE Computer Society, Portable Applications Standards Committee, (IEEE Std 2000.1-1998) http://standards.ieee.org/ (October 1996).

Appendix A

Sources of Y2K Assistance

1. Year 2000 project management checklist and building system

[****] Personal communication, December 16, 1998.

inventory form. The building checklists are from BOMA's publication *Meeting the Year 2000 Challenge: A Guide for Property Professionals*. This document was distributed from BOMA International's Web site. http://www.boma.org; http://www.boma.org/year2000/download/checklist.pdf (1998).

2. IEEE's Y2K Resources: *http://www.ieeeusa.org/usab/Y2K/*. December 14, 1998.
3. Huntress, J.: Dealing with Y2K impacts in a business [or government organization] The Year 2000 and Embedded Systems: For Most Businesses, This Does not Have to Be a Major Problem. *http://www.year2000.com/archive/embedded.html*.
4. Kling, J.: The impact on research organizations. Act Now to Avoid Doom When the Year 2000 Comes. http://www.the-scientist.library.upenn.edu/yr1998/ January 5, 1998.
5. EDS "Vendor 2000" web site of commercial products Y2K compliance. *http://www.eds.com/vendor2000*.
6. Small Business Administration web site dealing with Y2K. Http://www.sba.gov/y2k/indexsba.html. (December 12, 1998).
7. Commercial site for Y2K videos: *http://www.y2kvideos.com/*.
8. Two excellent guides from the U.S. General Accounting Office: Year 2000 Computing Crisis: An Assessment Guide: *http://www.gao.gov/special.pubs/publist.htm*, GAO/AIMD-10.1.14 [Available in PDF version only] Year 2000 Computing Crisis: Business Continuity and Contingency Planning. GAO/AIMD-10.1.19 [Available in PDF version only]. (October 1, 1998).
9. Chemical Safety and Hazard Investigation Board-Chem Links-Library Electronic Reading Room, Year 2000 issues. *http://www.csb.gov/*.
10. U.S. Food and Drug Administration, Year 2000 Impact on Biomedical Equipment. http://www.fda.gov/cdrh/yr2000/year2000.html. (December 15, 1998).
11. The Centers for Disease Control and Prevention (CDC). Agency of the Department of Health and Human Services. Centers for the Division of Laboratory Systems. *http://www.cdc.gov/phppo/dls*, Go to: "DLS Year 2000 Resource Guide for Laboratories."
12. National Institute for Occupational Safety and Health (NIOSH). One of the Centers for Disease Control and Prevention (CDC). Providing Y2K information: (See ICON on Homepage) *http://www.cdc.gov/niosh/homepage.html*.
13. U.S. Department of Labor, Occupational Safety and Health Administration. Provides Y2K link on homepage with fact sheets on Y2K, plus a web forum (chat room). *http://www.osha.gov/*.
14. This site contains numerically and functionally ordered chip lists, chip pinouts, and lists of chip manufacturers, controller embedding tools manufacturers, electronics books, CD-ROMs, and magazines: *http://www.hitex.com/chipdir/*.