

Y2K AND GPS WNRO: A FITTING FINALE TO THE SECOND MILLENNIUM

Ray Claflin III
Claflin Associates

ABSTRACT

This paper discusses the successful passage past the Year 2000 (Y2K) Rollover and GPS 1999 (Week Number Roll Over) WNRO. The reasons the glitches seen at those events were relatively minor and the lessons learned to help enter the Third Millennium with careful optimism are reviewed.

KEY WORDS

Y2K, Millennium Rollover, GPS Week Number Roll Over, WNRO

INTRODUCTION

This paper is the third in a series presented at ITC covering Timing issues including GPS WNRO and Y2K. The focus of this paper is strictly Y2K and GPS WNRO and how the world successfully avoided major disruptions with either event. The lessons learned are applicable to tackling the technology problems anticipated as we soon begin the Third Millennium.

GPS 1999 WEEK NUMBER ROLL OVER (WNRO)

The GPS Week Number Roll Over that occurs every 1024 weeks and happened on August 21, 1999 at 23:59:47 UTC provided an excellent pre-test for Y2K. Like Y2K, GPS WNRO was a rollover issue. The difference is that it was a rollover at the end of 10 bits versus two digits. As most military and commercial timing instruments now use GPS receivers as their engine, there could have been a number of problems similar those anticipated for Y2K. The US military upgraded their elements of the system and performed validation tests in early 1999 to confirm that the system itself and military users were ready for GPS WNRO and Y2K. Manufacturers of both OEM and Instrument GPS Timing Receiver Systems performed GPS WNRO and Y2K reviews or tests and mailed information to customers or posted notices on their web sites as to which models were compliant and how to upgrade older receivers. The most thorough

companies acquired GPS simulators to provide full validation testing. Some companies stationed service personnel on duty during the GPS WNRO and Y2K events.

Due to these efforts, there were few reported problems for GPS WNRO. There were some users who found out from WNRO that they had not upgraded older non-compliant receivers, but as a member of the timing community I have not heard of any critical timing systems being disrupted. At the “Thirty First Annual Precise Time and Time Interval (PTTI) Systems and Applications Meeting” December 7-9, 1999 a Panel Discussion on “Post GPS End of Week Rollover and Upcoming Y2K” was held to discuss feedback about WNRO and what might happen at Y2K. The Panel Chairman was Mr. Don Mitchell, VP of Sales at TrueTime, Inc. In private conversations with me in January and May 2000, Mr. Mitchell stated that no one came forward with any actual WNRO problems and the discussion turned to Y2K. The Proceedings of the PTTI conference are being published under the auspices of the US Naval Observatory (USNO) and will be available in print by ITC 2000. The PTTI conference is sponsored and attended by timing community specialists from military and civilian agencies across the country and that panel discussion was the best place to have heard about WNRO effects from critical timing users.

Y2K: WHAT COULD HAVE HAPPENED

Scenarios ranging from 3 days to three years (Dick Mills, page 79 and Michael Hyatt, page 94 of Harris’Farmer’s Almanac Presents How To Survive The Y2K Crisis) of electrical blackouts and societal problems before a return to normal were proposed by pundits. Even the President’s Council on Year 2000 Conversion noted that it was felt by many in early 1998 that the problem was too big, complex, and interrelated to be successfully solved. There was a lot of work to be done just to make many US Government Departments compliant and a 1998 World Bank study showed that only a quarter of countries worldwide had even a basic plan for addressing Y2K (“Final Report of the President’s Council”, page 3). What was feared was the simultaneous crashing of many systems leading to the crash of other systems feeding a positive feedback loop that would grow larger and larger and overwhelm systems and response capabilities across different areas and infrastructure segments. The simultaneity of power outages leading to communications, hospital, water plant, transportation disruptions leading to public safety disorders were physical concerns and the most dramatic. Problems in a tightly coupled “just in time” supply chain combined with the possibility of hoarding and financial system disruption were less dramatic but more likely. Public hysteria over such physical or financial issues and loss of public confidence in governments and institutions in the end became the most likely part of any scenario.

Y2K: WHAT DID HAPPEN

A review of the Press Reports and Briefings from the International Y2K Cooperation Center (IY2KCC) tells the story of what did happen (“International Y2K Cooperation Center, What’s New”).

28 December 1999	Many Y2K Inconveniences Expected, But Few Serious Incidents
01 January 2000	118 Countries Report Normal Y2K Status In All Sectors

02 January 2000	Update on Gambia – All is Normal
03 January 2000	All IY2KCC scheduled briefings cancelled as of 3 January 2000
04 January 2000	Major Y2K Successes Permit Reduced Monitoring
03 February 2000	Numerous Y2K Glitches Experienced Globally, Impact Limited
01 March 2000	No Significant Leap Year Computer Problems Reported

The International Y2K Cooperation Center (IY2KCC) was set up by the United Nations in February 1999 and funded by the World Bank. IY2KCC worked with Y2K coordinators from 170 countries including the United States. It acted as a central clearinghouse and facilitator of Y2K related activity, posted only confirmed reports on its web site, and maintained a country by country and sector by sector status in near real time.

The goal of national and international Y2K efforts was to prevent severe disruptions of crucial services. There was no expectation that all systems everywhere would be compliant. There were scattered glitches in almost every sector worldwide and undoubtedly a number that were never reported. Medical instruments, building systems, meters, military satellites, security systems, aluminum plants, oil pipelines, train controls, government services, media, finance systems, telecommunications, aviation, and just about every sector experienced a glitch somewhere (“International Y2K Glitch Report”). There were a limited number of hacking incidents. The glitches did not get out of control and cascade into severe disruptions of crucial services, so the goal was achieved.

THE REASONS FOR THE SUCCESSFUL Y2K TRANSITION

The first reason that Y2K was a successful transition was that from the top down and bottom up people were motivated into action to resolve the issue. From the IY2KCC to the President’s Council on Y2K to local governments to every segment of key infrastructure down to individual agencies and businesses, individuals in organizations took effective action to meet Y2K. Money is one indicator of serious action. Per the “President’s Council Report” page14, a Commerce Dept. study predicted that 100 Billion Dollars would be spent by governments and businesses in the US on Y2K. Leaders taking full responsibility is another reason for success. From the President’s Council on Y2K with every agency and cabinet department represented to industry associations to individual companies, the management of the enterprise took responsibility to ensure that Y2K was a full enterprise issue, not just an Information Systems Department issue. It became obvious that any enterprise in government or business that failed Y2K while others passed would definitely receive a change in management. The interest from the top included key personnel spending December 31 to January 1 on watch, not on vacation as usual with only junior people on duty.

The actions taken included careful inventory of the situation, planning, allocation of resources, deploying new systems or code, testing and cross testing in isolation and combined systems, and demanding compliance from partners. The latter was extremely effective in the US where Y2K Compliance was

required by law from every government vendor and made it easier for commercial businesses as well to demand such compliance. Per a private discussion in May 2000 with Mr. Robert Martin of MITRE Corp., Bedford, Mass., this was very effective overseas where the multi-national corporations demanded compliance by their sub-vendors and partners as well as assisted them in achieving it.

A huge factor for Y2K success was cooperation within and across industries and countries. The US Justice Dept. agreed that anti trust suits would not be brought against companies simply for cooperating in Y2K work. In his "January 3 Statement", Bruce McConnell of IY2KCC noted that an "unprecedented international cooperation" and "dedicated efforts of millions of Y2K workers" were reasons for success. Cooperating across established groups and empowering the creation of new groups in pursuit of a common goal provided a network of resources that could be coordinated voluntarily in many cases. This included both public and private individuals and groups. The cooperation across as well as within enterprises helped reduce institutional rigidity or found ways around it.

The use of knowledge databases and internet technology to organize, coordinate, and then make available usable information provided a way for millions of diverse enterprises and people to access a solution once it was developed or found. This permitted a vast reduction in costs and labor required and allowed "leapfrogging" to an effective solution by enterprises and nations that were behind in finding solutions ("Y2K: Starting the Century Right!", page 8). Once a product or system was found to be compliant or unaffected by Y2K and the knowledge communicated or available for access by those who needed it, vast resources were freed up.

Prioritizing and taking care of critical systems first was crucial to effective resource allocation and successful attainment of further objectives. Keeping key systems from failure was vital to preventing the feared cascading positive feedback loop. Ensuring that key systems were compliant and communicating that information was vital to creating public confidence and accurate expectations.

Contingency plans and actual drill in those plans was also an important factor in Y2K success. Numerous glitches occurred but were prevented from causing problems because of manual backup or other contingency methods. The fact as mentioned above that qualified, capable teams were in place and on duty at Y2K and ready for action was vital for public confidence as well as effective action. While many utilities were already prepared and effectively organized for various kinds of contingencies, this was additional training in both contingencies and effective coordination for many enterprises.

Leveraging internet communications with the other factors created a synergy that cascaded into a positive feedback loop that so markedly reduced the time and increased the effectiveness of effort that a successful solution became a reality. This multiplying synergy factor while totally dependent on the other factors for its creation nonetheless is perhaps the most significant factor in the total solution. It is likely that its negative counterpart resulting from the lack of those other factors would have similarly been the greatest factor in a doomsday Y2K scenario.

Y2K: THE FUTURE

Y2K is not quite over. For those who rely on day of year numbers, making sure to use 366 instead of 365 days means that Y2K really is not over until Midnight December 31, 2000/January 1, 2001 which is the start of the Third Millennium. Also, many Y2K solutions used a 100 year Window Method to reduce costs and complications. Users of those systems must keep track of when they need to move that Window. Other methods such as 28 Year Bridging or rolling back the clock also require ongoing maintenance. (See "Dealing with Dates", page 5)

The effective response to Y2K provides a fitting finale to a millennium and a technology problem created in the last years of that millennium. The inventory, update of computer system assets, and elimination of systems with unsupported code combined with the much clearer knowledge of systems interaction is a worthy housekeeping exercise to start the twenty first century. The promise of personal empowerment through computer networking technology also brings with it the threat of malevolent hacker attack by small yet capable groups or even individuals. The proof that networks of individuals and groups of common purpose and good will can be created and coordinated efficiently through networking to resolve problems provides optimism for entering the Third Millennium.

REFERENCES

Mills. Dick, "Power Grid Breakdown," Harris' Farmer's Almanac Presents How To Survive The Y2K Crisis, USA Issue No 14, Year 1999, Page 68

Hyatt, Michael, "The Y2K Crisis," Harris' Farmer's Almanac Presents How To Survive The Y2K Crisis, USA Issue No. 14, Year 1999, Page 6.

"The Journey to Y2K: Final Report of the President's Council on Year 2000 Conversion",
March 13, 2000,
<http://www.y2k.gov/docs/LASTREP3.htm>

"International Y2K Cooperation Center, What's New,"
<http://www.iy2kcc.org/WhatsNew.htm>

"International Y2K Glitch Report",
<http://www.iy2kcc.org/Glitches2000.htm>

"Statement of Bruce W. McConnell, Director, International Y2K Cooperation Center", January 3, 2000,
<http://www.iy2kcc.org/News20000103.htm>

"Y2K: Starting the Century Right!", February 2000,
<http://www.iy2kcc.org/ExecutiveSummary.htm>

“Dealing with Dates: Solutions for the Year 2000”,
http://www.mitre.org/research/y2k/docs/DEALING_DATES.html

Note: IY2KCC.ORG Web Site is only guaranteed available through January 1, 2002.