

Y2K Problem and the Impact on Chemical Safety

The Year 2000 Technology Problem, also known as the "Y2K Problem" or the "Millennium Bug", stems primarily from a simple two-digit year representation. In the early days of computing, computer memory considerations caused programmers to represent years in a two-digit format – for example, "99" instead of "1999." This practice became standard for the computer technology, both for software as well as embedded microchips. The microchips, numbered in billions, are embedded in almost everything we use today. The Gartner Group estimates about 50 billion microchips in embedded systems worldwide and about 1 percent of these microchips will have Y2K-related failures leading to shutdowns, erroneous results, and chaotic behavior. Of this, a fraction is in mission-critical systems, leaving on the order of 25 million microchips (deployed in systems) which must be repaired worldwide.

The chemical process industry relies on software and microchips for the operation, maintenance, and control activities that are vital to the safe operation of the plants as well as the profitable manufacture and distribution of chemical products.

Software or microchips that store dates as two digits could render incorrect results. For example, a control device may have been programmed to provide a reading or report every six months using the two-digit arithmetic. Such a device could interpret the year 2000 as "00" and calculate a negative number. The outcome of such an event could pose a problem. The question is: would the computer ignore the incorrect answer, or could it cause the hardware to malfunction, or cause a major process upset? The potential for catastrophic events stemming from Year 2000 Non-Compliance can be divided into three categories. First, failures in software or embedded microchips within the process plants may cause process excursions or control problems resulting in accidents. Second, external Y2K-related problems, such as power outages could cause various problems, such as accelerated shutdown of processing, monitoring, and safety systems. Third, multiple Y2K-related incidents may strain emergency response organizations.

The chemical process industries, irrespective of size and type of operations, use a variety of software and embedded microchips to operate, maintain, and control their processes. Y2K-related failures, can at the minimum, cause off-specification products or shutdown of the process and at the extreme cause process malfunctions leading to accidents. For example, the agitator on a batch reactor may fail to operate causing the initiation of a runaway reaction. Many other examples exist for both batch processes as well as continuous processes used by the chemical process industries.

Potential Y2K-related power outages represent another set of problems for chemical and petroleum facilities. First, plants without auxiliary power backup systems face a threat to parts of their processes that do not shutdown in a fail-safe mode. Batch chemical processes are especially susceptible because the safety of the process is quite often dependent on time-dependent factors such as precisely timed heating or cooling requirements. Second, a potential scenario is that widespread power outages may cause shutdowns of many plants, which in turn will require simultaneous startups. Although startups of chemical plants are infrequent and their durations are short compared with the life cycle of a plant, process safety incidents occur five times as often as they do during normal operations. Thus, large number of simultaneous startups will increase the potential of incidents in one or more process plants. In addition, the simultaneous restarts of large power-consuming facilities will pose tremendous liabilities on the electrical grid.

It is reasonable to assume that emergency response organizations may also have Y2K-related difficulties. However, even under the best of circumstances where the emergency response organizations continue to operate without any major problem, multiple incidents could strain the system.

There is no doubt that the impact of the Y2K problem is pervasive. Various estimates ranging from millions to billions of embedded microchips and software programming lines are quoted by different sources. However, there is quite a bit of disagreement in terms of the potential outcome. Some experts claim that they could not identify a single catastrophic failure that could be attributed to Y2K-related events. On the other hand, other experts are quite persuasive in their argument that because of the underlying causes, there is a reasonable potential for major accidents. Even though there is significant disagreement on the catastrophic extent of the Y2K problem, there is unanimous agreement that the prudent approach is to take remedial measures. In general, this means a Year 2000 compliance program that includes four basic steps:

- Inventory,
- Assessment,
- Remediation, and
- Testing and Certification.

Inventory includes compilation of inventory of all hardware/software systems that are susceptible to Y2K failure. For process industries, this could mean complete control systems, pumps, compressors, automated agitators, and a host of other devices and equipment.

The assessment step requires an analysis to determine if the system (large or small) is safety-critical; could an individual failure or failure in combination with other systems result in a process safety incident. The assessment step is quite similar to hazard analysis conducted by process plants. A classic hazard analysis approach for finding Y2K-related safety-critical problems is to answer three questions:

What will happen if this system fails because of the Y2K problem?

Will a Y2K problem occur in this system?

Will the consequences be severe enough to cause any concerns?

The remediation step requires the fixing or replacement of safety-critical systems identified in the assessment step.

Testing and certification is the final step that ensures Y2K compliance using accepted industry standards. Vendors and other organizations have made available testing and certification standards. Some are also providing services for testing and certification of different devices. The testing includes integrated testing across several devices, and not just the evaluation of individual devices.