

## IT in the Plant

### Enterprise asset management software comes of age

By **Ken Mausey**, Contributing Editor

---

Selecting and implementing an enterprise asset management system is one of the IT challenges confronting power producers. Suppliers of ERP systems are muscling into the plant driven by top-down corporate initiatives, while CMMS packages, long-standing fixtures at the plant level, are being beefed up to meet corporate needs. With information flow accelerating, IT security looms larger too

---

Stanley Kubrick may have been just a little off the mark when his movie, 2001: A Space Odyssey, portrayed a computer with paramount artificial intelligence communicating readily and making complex decisions on behalf of the mission. For here we are in 2001, yet the goal of perfecting artificial intelligence within binary brains, and putting it to use in a real-world mission--such as the competitive production of electricity--remains as elusive as ever.



1. Enterprise asset management software is being implemented by scores of power producers seeking to link diverse software applications--from the control room to the board room.

---

To be sure, enterprise computing has become a valuable tool in today's competitive power sector (see box, below). But those who have struggled to implement the comprehensive software systems report that they are far from artificial intelligence, and by no means a plug-and-play application. Some even refer to the implementation phase as Operation Infinity, with tongue firmly embedded in cheek.

It's easy to see why the name might apply: Powerplants generate more than electricity, they generate tremendous amounts of data (Fig 1). Like steam surging from a boiler, the data represent a continuous flow that must be harnessed as it is formed if it is to be effective. Often, vast quantities of data are underused, or even lost completely because systems are not in place to handle the information overload.

### Battling Nimby

Another challenge: The not-in-my-backyard syndrome, or Nimby, so familiar to power-project developers, often applies to the implementation of an enterprise asset management (EAM) system. Nearly everyone in the organization wants the speed and flexibility of seamless, robust data delivered to his desktop. But when personnel realize that all of their existing data will have to be entered into the new system, few of them want the interruption, and even fewer want to be saddled with the job of actually entering it.

Point is, the decision to purchase an EAM system needs to be accompanied by a detailed plan--and sufficient funding--to implement it. The plan, IT specialists say, should figure on increased workload for plant staff, for six months or more. Many EAM systems never reach more than a moderately usable level because of staff constraints. Outsourcing the work is an attractive alternative, but this carries the increased risk of data being mishandled by people unfamiliar with your operations and business practices. Some plant managers also worry that contractors can sport loose tongues and compromise competitive data.

Funding needs don't stop the day the EAM system "goes live." Upgrades and ongoing management expenses will need to be included in both short- and long-range budgets. "Maintenance of the system is critical," says Dave Taylor of Idaho Power Co, Boise, Idaho. "You must take great care to upgrade the product to prolong its life."

Idaho Power recently implemented the Passport system, supplied by Indus International, Atlanta, Ga. The solution, as customized for Idaho Power, includes Work Management and Supply Chain solutions across Generation, Transmission, Distribution, and Corporate Services, explains Terry Maxey, VP of strategic initiatives at Indus International.

"To expedite the implementation, Taylor and his colleagues chose to leave legacy systems in operation if the data they contained were not valuable enough to integrate into the new Passport system. "We kept legacy systems available, and implemented the new system with new data," Taylor explains. "We did convert catalog information for parts inventory, but we used Idaho power employees because they were most familiar with the data."

PPL Corp, Allentown, Pa, used a variety of methods to enter data when it implemented the "InfoWorks" EAM system, supplied by Scientech Inc, Bethesda, Md. Some data were installed using automated means; others were entered by hand. "The best way to insure that data are entered and maintained is to get the involvement of the people who care the most about the accuracy of the data," says Ray Harris of PPL. "Don't even start if you don't have the involvement of the users."

In addition to PPL Corp, InfoWorks has been installed by such power producers as Arizona Public Service Co, Phoenix, and Constellation Nuclear, Baltimore, Md, reports Harold Burton, senior VP for Scientech Generation Services.

### **On-time training**

Some level of training always is included with the purchase of any product of this size and magnitude. But the critical issue for EAM systems, IT experts emphasize, is not the inclusion of training so much as it is the manner in which it is scheduled. The installation of the new system inevitably will include problems and setbacks, which in turn affect deployment schedule. But the training typically goes on as originally planned.

All too often then, the employees have forgotten much of what they learned by the time the new EAM system goes live. The basic functionality they will remember, but the time-saving shortcuts and important details will be lost in the fog. The true value of software often comes when employees effectively use the time-saving measures built into the application, particularly for data retrieval. But during the initial startup, employees are concentrating most on data entry. Properly timed training can ensure that important shortcuts are remembered when the data-retrieval phase finally begins.

PPL Corp's Harris has strong feelings about the need for training, and retraining. "Refresher training is the best way for your people to learn the tips they need to use the software most effectively," says Harris. "Advanced training on unfamiliar software is necessary, but the students will not remember the tricks they need to be efficient." Harris feels that training should be considered an ongoing project, one that must be revisited as often as necessary to keep the staff performing at peak levels.

Idaho Power Co's Taylor agrees, pointing out that training should be scheduled for deployment time, and then again after a reasonable period of system use. Though he is very satisfied with the Passport system, he is quick to point out the need for ongoing training. "The people that work with [our EAM system] everyday love it. The people who casually use it sometimes struggle," he says. All EAM systems, regardless of supplier, are large in scope and complexity, making them difficult for casual users to operate. Taylor reports that Idaho Power personnel were trained "just enough" to use Passport in the beginning, but that they needed refresher training three weeks after the system went live.

The productivity boost that comes from retraining will in many cases more than offset the additional cost, IT specialists agree. The costs can be kept to a minimum if refresher training is included in the purchase price of the system. This is when a customer is most likely to receive a discount from the supplier.

### **Cost accounting**

In today's competitive market, the cost of fuel is one factor in a much larger equation. The EAM system can help manage that equation.

Implementing an EAM system allows for work requests to be generated that automatically include a complete list of parts required for a particular job function. This reduces the need for time-consuming inventory searches of the past. Also, with an EAM system, inventory is removed from stock and marked for reorder as it is used. The work request may also show the quantities that remain. In addition, trends can be spotted more easily, and accounting personnel can track spending more accurately. Expenses can even be "rolled up" into a report to track equipment reliability based on individual vendors and equipment models, which, in turn, can be used when deciding future purchases--both for repair parts and for capital equipment.

Inventory management has entered the on-line sector, with such offerings as Scientech's Rapidpartsmart, a powerful on-line parts search engine. Rapidpartsmart uses plug-ins to integrate search functions with computerized maintenance management systems (CMMS) as well as work management and enterprise resource planning (ERP) systems. In addition, it acts as a "navigator" to access supply chain networks and preferred net markets for e-commerce applications. Parts data are updated daily through the site's Gateway feature.

Larry Brodsky, VP, Scientech Utility Services, says the site benefits utilities, vendors, and e-commerce net markets by providing "one source, where anyone searching for engineered parts can find the right part, in the least time, at a good price." Brodsky believes that the rapidpartsmart data base will help utilities reduce inventory and carrying charges, lower operating risks, increase procurement options, and promote more disciplined purchasing decisions.

### **Data availability**

The successful EAM vendor will make sure the customer establishes the right level of data access for each employee. Excessive viewing or editing rights for some employees are easily seen as risky (see box), but less evident is the loss of effective resource management if insufficient viewing or editing rights are awarded to other employees.

A popular acronym in the EAM field is CRUD, for "create, read, update, and delete. These are the basic policies the user manager must consider when deciding access rights. The conventional approach to data has been to hide them. This insures security, but at the possible loss of economic value.

PPL Corp took an opposite approach. All data were assumed to be potentially accessible, then each item was reviewed to determine if it should instead be hidden from access. "Why hide data if it isn't necessary?" Harris asks. "Don't control what people can see, control what they can't see."

Taylor echoes the thought, and recalls, "We had to shift our security thinking 180 degrees. We stopped looking at data from a 'need-to-know' basis, and started from one of 'open access.' "

With viewing methods under control, both the Idaho Power and the PPL teams were able to free up time and resources. A tremendous amount of the security effort then went into user rights for create, update, and delete. "Expect to spend a lot of time doing CRUD, determining who can enter (create) data, who can view (read), who can maintain (update), and who can delete data," adds Harris.

## **Open standards**

Open standards for information exchange are of paramount importance in the selection of an EAM system. If a proprietary (often couched by vendors in the word "innovative") method of data exchange is used, the flow of information within an enterprise-wide deployment may be severely limited. The purchaser is well-advised to determine if an industry-accepted means of information exchange is being applied, without "special modification." This allows the purchase of additional services/platforms from competing vendors to seamlessly communicate with your EAM system.

The users' desire for open standards was clearly evident at last year's Powerplant IT Workshop, hosted by Power magazine in Phoenix, Ariz (see box, p 62). Many of the powerplant IT specialists in attendance stated that an effective EAM system should revolve around open standards, using industry-accepted methods of data exchange. One participant observed, "You can never win the operating system war. Every user has a strong belief regarding which one is best, and vendors must adapt to those wishes."

Scott Lowes of Ontario Power Generation Inc, Toronto, Ont, Canada, shares the fervor for open protocols. "It is imperative," he says, "to be able to access data using open protocols so that engineers and managers can compare or evaluate information that originates from different systems."

Toward this end, the dot-com boom that imploded in failure last year may have at least succeeded in perfecting data exchange over a wide variety of platforms. Alan Cox, developer on the Linux project, explains, "Most of the great leaps of the computer age have happened despite--rather than because of--IPR [intellectual property rights]. In fact, before the Internet, the proprietary network protocols divided customers, locked them into providers, and forced them to exchange much of their data by tape."

## **Selling the standards**

Dr J Patrick Kennedy, founder of OSI Software Inc, San Leandro, Calif, understands that the sources of information available in a powerplant are vast, and often hard to access. They range from real-time control systems--such as the distributed control system (DCS) and programmable logic controllers (PLCs)--to intelligent relays, smart meters, manual log sheets, laboratory data, operator inputs, weather stations, and files on engineers' PCs. To exchange information with so many varied systems, OSI includes over 200 standard interfaces, Kennedy explains, providing the ability to instantly trend and view data from the DCS, and from balance-of-plant systems--such as the electrostatic precipitators, sootblowers, ash handlers, and water treatment systems.

Several prominent power producers--Mirant International, Atlanta, Ga, Exelon, Philadelphia, Pa, Southern California Edison Co, Rosemead, Calif, and Ontario Power Generation Inc, Toronto, Ont, Canada--recently selected an enterprise data historian called "eDNA." Developed by Industrial Peer-to-Peer LLC (Ip2), Chicago, Ill, the package is billed as a decision support tool for predictive maintenance, forecasting, and other reporting and analytical functions. It captures, archives, and time-stamps historical and real-time data from plant equipment--including heat rates, fuel costs, and process parameters--then integrates the data with other enterprise systems and trading-floor programs.

"Power and processing plants need tools to monitor thousands of data points, sometimes down to the sub-second," says Tony Maurer, nuclear engineer, co-founder and vice president of InStep Software LLC, parent company of Ip2. "Not having instant access to this data can mean the difference in millions of dollars in profits or losses."

### **IT security: It's not what you think**

The mainstream media associate computer security with evil, pony-tailed hackers pounding away at a keyboard in a pile of Coca-Cola cans and Cheetos. But missing from your nightly newscast is any mention of physical security. Within the hallowed walls of corporate networks, employees often do more damage to information technology (IT) systems through physical intrusion than outsiders do through computer viruses and Web site attacks.

Physical security is low-tech, boring stuff. But that, according to many IT specialists, is what makes it so prevalent. It requires no technical knowledge, and can be performed by unskilled staff. Preventing physical intrusions may not build your reputation as a computer guru, nor will it endear you to your non-IT department colleagues. But it will reward you with fewer IT system problems.

### **Lock 'em down**

Vincent Danen, founder of Danen Consulting, Edmonton, Alta, Canada, says, "We always advise our customers to [physically] secure their servers as much as possible. Statistics have proven that the majority of information theft and damage is caused by people having physical access to systems that they have no business accessing." For example, the room that servers are in should be locked. Sounds like a no-brainer, but many power plant servers sit unattended just on the other side of an unlocked door.

Many IT failures occur, for instance, when the cleaning crew inadvertently disconnects funny little wires from their funny little homes. In their diligent efforts to get that last dust bunny, cleaners can shut down an enterprise-wide IT system.

Another very boring physical threat is the floppy disk drive found in most servers. There are hundreds of Web sites on the Internet where an employee can download a simple program that automatically extracts data. If allowed physical access to the floppy drive on a key server, the employee can then obtain full access to the confidential data contained within, simply by inserting the floppy disk. The employee needs no special training, for the instructions have been provided with the program. The hackers have, in essence, given the employee all the access he wants.

Do not let unauthorized people have unsupervised access to any IT system, period.

### **Keep 'em separate**

No matter how remote your plant location or how few your number of employees, the power plant process-control network should be on a separate network from the administrative one. There are many reasons why.

Dial-up connections tops the list. Do you really know what lies on the other end of that modem connection? The bad guys in the black hats do not come up to the front gate and ask to schedule an appointment. They send out viruses and such to remotely do their bidding; all they need is a dial-up connection. Typically, viruses are designed to erase hard drives or crash computers, but they also can quietly reside for months and collect passwords, power plant data, and so on.

By placing a router with suitable security settings between your administrative users and your operational users, the tech-savvy IT administrator has a fighting chance to filter out the traffic that passes to the control system. A router does not have to take the form of a magic little black box. It could be a computer with multiple network cards, or a hardware box made just for the purpose of filtering traffic.

Danen says that security measures don't have to cost a lot. For example, hardware that you may consider obsolete makes an excellent router. "The solution we often end up implementing," he says, "is a low-end computer physically secured and running the Linux operating system with two network cards, one connected to each network. If you have the hardware floating around already, the cost is minimal because Linux is free" (Power, July/August 2001, p 58).

### **Patch 'em up**

Once your security is in place, make sure that you keep all of your network computers updated with the most recent security patches. Some of the latest break-in stories revolve around software flaws that were fixed years ago. Recently, a two-year-old security hole in Microsoft Corp's Internet Information Server software allowed a computer cracker to download thousands of credit-card numbers and post them on the Internet. The patch for this problem had been out for 18 months, yet many servers were running without it

To be sure, keeping up with all the patches is burdensome. Many companies complain that they do not have the time or resources to keep up with the many Microsoft patches. Some network insurers have even started charging a 15% penalty to clients running Microsoft Windows, citing security as the cause. Danen advises his clients to steer clear of Microsoft products for secure applications. "For your security to be effective, you must base it upon effective solutions. Using a Microsoft product in a secure environment is like putting a 'Kick Me' sign on the back of your network." He recommends operating systems that are more robust, stable, and reliable, yet retain the same functionality as their Microsoft counterparts. "Operating systems like Linux and OpenBSD work extremely well to protect your servers and workstations," he says.

## Shut 'em out

Perhaps the thorniest issue for IT specialists arises when managers or key administrative staff request the ability to view process-control information via a simple Internet connection (figure). Office politics and personal feelings can run high at this point, so keepers of the IT key must dig deep into their "people skills" for solutions. Discussing network security and establishing firm policies during staff meetings can help fend off these requests before they are made.

As Danen advises, "The only way you can regulate who gets in and out is with the proper tools and the proper policy, both of which must be enforced and monitored on a constant basis."

## Reading the alphabet

A variety of terms are bantered about in the field of enterprise computing. Here's a primer on the three most commonly applied in the power generation sector.

- Enterprise resource planning (ERP) systems are the largest, most comprehensive, and most complex. They typically cover finance, production, sales, purchasing, inventory, human relations, maintenance, and automated data collection. Born from the needs of large manufacturing interests, ERP systems have seen only limited acceptance in the power industry.
- Enterprise asset management (EAM) software, compared to ERP, is a mid-range product, although enhancements by EAM suppliers, coupled with increased attention to work management functions by ERP suppliers, are blurring the lines between the two. An EAM system typically includes integrated modules for use by the various departments, but falls short of the monolithic properties of a well-crafted ERP system.
- A computer-based maintenance management system (CMMS) is the veteran player in the powerplant stadium. This is also referred to as a work management system (WMS). If you need to schedule someone to do something, and arm him with useful information to accomplish it, a CMMS is your servant-at-large. Most ERP and EAM systems include a WMS module as an integral part of their offerings to the power industry.