There is a prevailing thought that a utility can have either an integrated and intelligent system OR a safe system, but not a combination of the two. This article will review the current thinking about integrating intelligent systems to help secure utilities; compare threat scenarios; and discuss a model of a secure, integrated system.

## *CURRENT THINKING: Either Integration Or Security Systems, but not Both*

Most utilities view security and technology integration as an either/or proposition; however, this view limits the payback on technology investments and forces inefficiencies into the system.

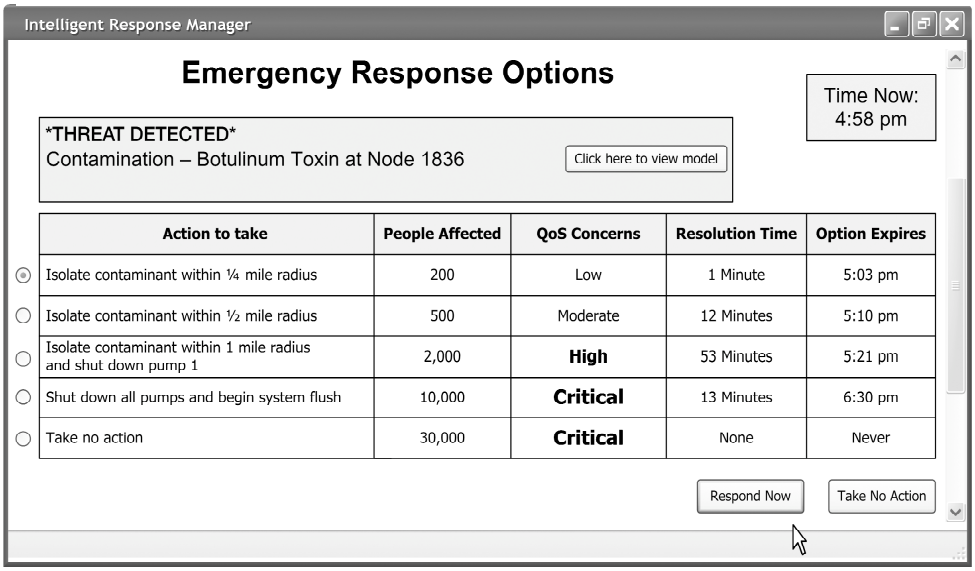
While on the surface, security seems to warrant segregated systems, we believe that just the opposite is true. Basic physical security is sufficient even in today's environment. Oppressive fences, cameras, checkpoints and the like are not the most important elements of security; what is most important is the ability to ability to respond quickly and accurately–with a full understanding of how actions will affect outcomes. Responding inappropriately to a situation can actually create more damage than the initial event by exacerbating a problem.

It does not matter how much money you throw at physical security–it won't be enough. There are ways to infiltrate a system from one's own home, so why spend a fortune on protecting a few key assets when the rest of the network is at risk? Yes, build basic security and prevention into the mix of protection, but don't focus solely on physical security–the Constantine and camera approach–to the exclusion of operational improvement.

Instead, integrate your software systems. This may sound like blasphemy to many, but why should you not reap high returns on your software and systems expenditures by integrating them? With significant digital security (which can be affordable), you can protect your data and systems from outside infiltration as well as from internal mistakes or sabotage. After all, the biggest risk to a utility is not terrorists, but employees.

Integrating your systems does *not* mean sacrificing security. In fact, we think that having access to your data from anywhere in the world i

## Proposed Secure, Integrated Systems Model




This sample Intelligent Emergency Response System interface shows the expiration of options and the effect of each option on the population and service quality. Not all scenarios would be so bleak.

Most utilities operating today have physical security measures and basic cyber security in place, but the physical security measures can get in the way of operational efficiency and the cyber security is often a weakness that needs to be bolstered.

Information technology is often used as a foundation in utilities, but not as a key strategic asset. Most large utilities have modeling software, which is typically used in advance of a change in the network to model the effects and provide the best solution. SCADA (Supervisory Controls and Data Acquisition) is present at most utilities in some form or another, and GIS (Geographic Information Systems) is nearly ubiquitous, not always within the utility itself, but as part of the larger municipality or organization.

For the most part, metering occurs at the access point and is not automated. Monitoring and detection systems are available, but are not real-time in most installations. They are also not effective for detecting biological agents. As technology improves, new detection methods can be incorporated into the system.

Most operational, accounting, and billing activities are automated; however, accounting and billing are usually not integrated with the other technological components, yielding fragmented workflow and duplication of effort.

The proposed model for a secure, intelligent system integrates all operations and depends upon artificial as well as personal management for response to an emergency situation. An intelligent system does not preclude or denigrate the very important role of people during emergency situations. Instead, it offers electronic support and decision support to help alleviate the situation as quickly as possible, with the least impact upon the fewest number of customers.

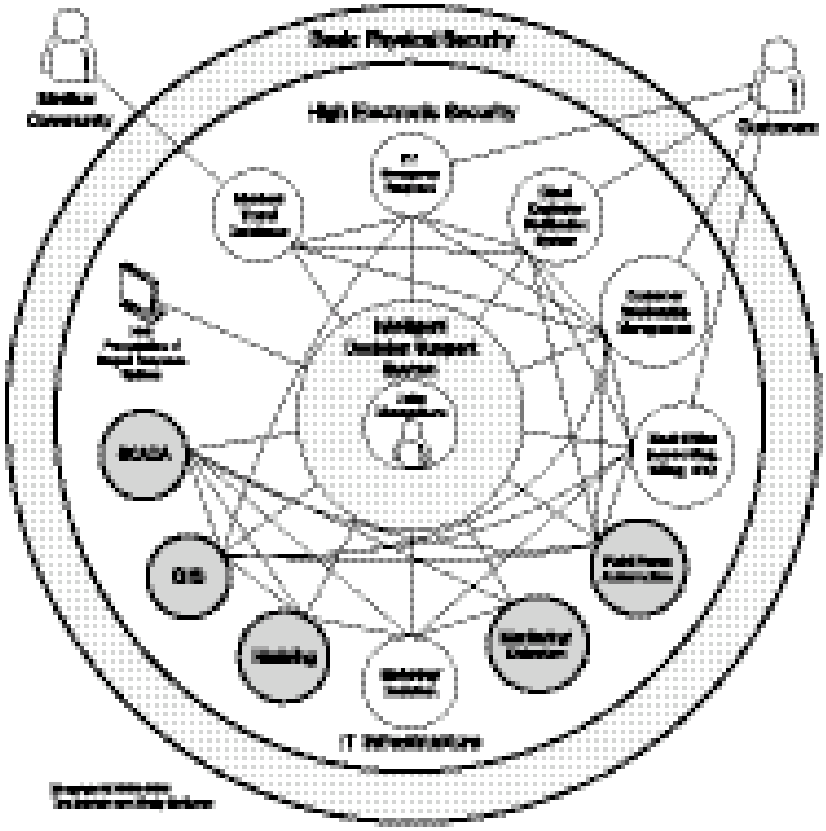
The options provided by the decision support system allow operators to make better decisions faster, based on real-time data and current system demands. Because the intelligent system provides decision options based on modeled scenarios, the options will identify the time, risk, and other factors associated with resolution.

The benefits of this intelligent model are numerous:

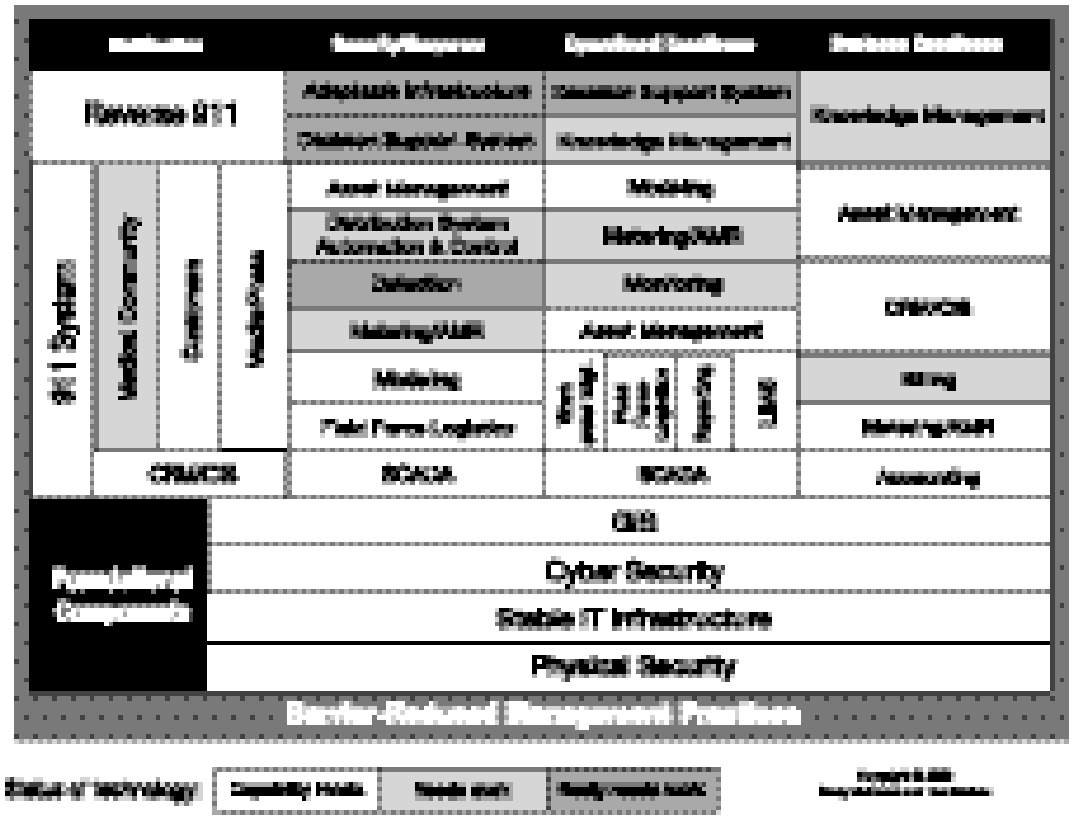
- **It focuses on good operational procedures, integration, and efficiency.** Including operational, security, business, and management elements of the utility into one overall intelligent system streamlines the functions of the utility and improves efficiency.
- **It reduces the drag caused by excessive physical security.** Utilities can supplement their physical security measures with decision support systems, thereby protecting the utility from interior and exterior threats.
- **It augments skills of operators.** Operators will learn to operate and maintain the decision support system, which in turn boosts their skill levels.
- **It increases response ability and effectiveness.** An effective decision support system can vastly reduce the amount of time required to contain an intrusion into a water supply system.
- **It decreases operational costs.** Streamlining systems saves money.

*Continued on page 24*

## Secure, Integrated Systems Model:
### Operational Efficiency and Effective Response



## Integrated Systems Component Model




*Continued from page 23*

Right now, numerous organizations are working to prevent or reduce the threat of terrorist attack on water utilities. Here is a list of technologies that fit within the proposed secure, integrated system model and are available today.

**Technology Infrastructure**

Data networks are capable of significant speed and reliability. Wireless network options, which have become more prevalent in businesses, are available to help organizations communicate with workers who need to move around frequently. Shop-floor personnel can carry a Tablet PC or PDA (personal digital assistant) with them to enter maintenance data and still be connected to the network through wireless means.

There is a price for this ease of communication, though, because many wireless networks are insecure. There are ways to secure wireless networks, but doing so is not as common as you might think.

In addition to the physical communication structure, servers and server-based applications support the business of the utility. From database servers to customer relationship management, or CRM, servers, these information and transaction servers allow people to share data and better support the business. These servers can also drive efficiency if properly utilized and aligned with the utility's strategy.

**Digital Security**

There has been a huge groundswell of products in this area. From the movie *War Games* in the '80s to the security present in *Mission Impossible* of the late '90s, digital security has come a long way. What to look for is the point at which there are decreasing returns for additional investment.

High digital security is easily accomplished for local area networks but becomes increasingly difficult and expensive when dealing with wireless and radio communications. Fortunately, those links can be limited to the types of data that can be transmitted and, thus, the exposure allowed without impacting overall security.

**GIS**

GIS is the foundation for integrated systems. Because of geographic information related to most assets in a utility and because of its rich database, GIS should be part of the foundation for integrating systems. Many other applications can already interact with GIS or run directly on top of it. GIS databases are extremely rich in the various types of data that can be stored, and most are also extensible, allowing the utility to customize and add data sets for new functions.

**Intelligent Systems: SCADA**

The only artificial intelligence/decision support system that exists in most utilities now is SCADA, and that is an expert system (you must tell it how to respond to specific events) that deals with just a small portion of the model. To our knowledge, no one is looking at an intelligent decision support component to tie everything together.

SCADA has advanced to a level where the computer systems can handle many, if not most, of the routine issues facing a utility. To a large degree, these systems are intelligent in that they are programmed to respond to specific events; however, they would not be able to respond effectively, if at all, to an event that is not programmed. To this extent, the person who programs the SCADA system must think through all issues in order to maximize the effectiveness of the utility.

**Systems Integration**

There are numerous firms that can help utilities integrate their systems today, for a price. What to look for is a way to create standard models that can be used for integrating systems from various vendors to accomplish the goal of integrated systems.

**CRM**

Customer relationship management (CRM) applications are contact managers that usually have several additional pieces of information linked to the contact, such as call history, service issues, and bill payments. The idea behind CRM is to capture everything possible about an individual in order to better serve that person and, in the case of for-profit business, to sell more to that person.

Several CRM applications exist today, from Seibel™, Microsoft™, Oracle™, and many others. These systems are designed to collect data about people and help you make decisions about servicing those people.

**Monitoring and Detection**

There have been no significant electronic breakthroughs in the areas of monitoring and detection.

The framework illustrated on this page shows where development work needs to occur. It also shows four starting points for reaching the ultimate goal of secure, integrated systems. After the foundational components of physical security, IT infrastructure, cyber security, and GIS are in place, the utility can choose any of the four columns to begin building out the system. Later, as funding and capability allow, additional functionality can be added to achieve additional goals.

## The Future is Out There

What electronic advancements are on the horizon?

**Monitoring and Detection**

Researchers are working on M/D systems that are closer to real-time and can detect a broader spectrum of contaminants. The experts we have spoken to say this field still needs significant progress before real-time or near-real-time detection becomes reality for all but the crudest contaminants. It will be even longer before those technologies yield affordable solutions. Having a significant number of utilities looking for this capability, combined with the new Department of Homeland Security, could spur researchers to step up their efforts.

**Intelligent Systems**

The technology exists to create realistic intelligent systems that can respond to situations and present valid options to the operator. Whether they are expert systems, neural networks, fuzzy logic, genetic algorithms, or Bayesian networks, methods exist to model the intelligence needed for this centralized intelligence.

As far as can be determined, the only problem is that nobody is applying artificial intelligence to water systems beyond the task-specific use. Haestad Methods is beginning to use AI in its WaterCAD™ product to help with pipe-decay assessment, but not for controlling an integrated system.

**Medical Trending**

There are apparently some efforts out there to keep up with trends of disease and illness, but currently these efforts have not been tied back to the water utilities. Information like increasing sickness in a particular community could be tied back to water-quality issues and is important for determining possible causes and solutions.

## Sounds Great, but How Do We Get There?

Here is a brief summary of the recommended process for getting to your desired goal of secure, integrated systems:

**Assess Where You Are**

Start by assembling a team of experts inside and outside your organization to assess your current capabilities and infrastructure. You will need to know where you are–realistically–to make a plan for going somewhere else. Don't gloss over this aspect of the integration process. Without a proper assessment of your existing situation, you will not effectively move anywhere.

A SWOT (Strengths, Weaknesses,

*Continued on page 26*

*Continued from page 25*

Opportunities, and Threats) analysis can help identify ways you can improve and help you think through potential threats and weaknesses. You will need to look at all of the following aspects of your utility:

- Physical Security
- IT Infrastructure
- Cyber Security
- GIS
- Components of the Model that are Currently in Place

**Determine Where You Want to Be**

Identify your goal for integration (or not). What will your system look like when it meets your goal? This process will involve intensive brainstorming, discussions with experts, vendors, and other utilities. Having a long-term (20 years out) timeframe allows you to plan more effectively than the limited horizon of the next year's budget. In fact, taking the long view allows you to plan more effectively now by adding components in a logical manner that help you reach the long-range goal. Technologies change, but a component-based model will allow you to replace items as things change.

**Create the Roadmap**

You have your starting and ending points, so create a rough map. Don't get too detailed yet. The technology can't take you to the endpoint doorstep—yet. But if you're going from North Carolina to California, start by going west; that will get you 90 percent there. Think about the big issues of integration. Smaller details will need to be addressed as technology develops. You can build the map based on existing technology, but then you won't be traveling very far.

**Follow the Map**

Start moving toward integration by getting the key components—people and security—in place. Once you have assembled a (not too big) team, assure that your physical and electronic security is in place and then work on your physical and digital infrastructures. Finally (and hopefully not years down the road), begin the systems-integration effort. Some of these issues can be done concurrently.

**Ask for Directions along the Way**

No one knows everything, so get the experts involved at critical junctures. When you've lost your way, stop and ask directions; otherwise, frustration will overtake the effort. For some issues, even experts may not know the way, so be sure to include creative thinkers who can turn ideas into implementable solutions.

**Did You Get There?**

Be sure to have clearly defined outcomes so you know when and if you arrive. This should be a continuing assessment of progress.

## *FAQs*

Here are some common concerns:

**If I integrate my systems, won't I be asking for more electronic attacks? Won't it be easier for hackers to get at everything if they get into one system?**

Not at all. Significant electronic security (computer security) is essential for all your systems now. This security net does not have to block out access to the system. In fact, the utility manager should be able to check statistics from home if there is a need. An appropriately designed security plan will allow him/her to do that and still prevent unauthorized access.

Even if someone were to hack into the system, he/she still would not have access to everything because the integration occurs at the data level, not the interface level. SCADA will still operate the basic mechanical devices in the water network, but the information in SCADA will now be observable by the manager making system-wide decisions.

**Why should accounting personnel have access to SCADA?**

They don't need it and shouldn't have it. Just because systems are integrated does not mean that everyone sees everything in the system. That integrated view of the utility is mostly needed at the executive level to help make decisions and allocate funds.

**If I don't spend more on physical security, won't it be easy for someone to infiltrate my plant?**

No easier than it is right now. Obviously, you don't take down the fences and rip out the locks, but further expenditures beyond a basic level of physical security to prevent the teenagers and pranksters are not necessary. A well-funded terrorist group will be able to bypass or destroy any physical security you can put in place.

**Isn't electronic security inherently insecure? Won't I be opening myself up for an attack from the Internet?**

Yes and no. There is nothing foolproof and totally secure, electronic or physical. But state-of-the-art electronic security is almost impossible to crack—even by the best hackers.

The biggest threats to your water network are not the outsiders, but insiders. They are the ones with direct access to your systems now. Electronic security can prevent or reduce the ability of insiders to do harm, intentionally or not.

Electronic security can be extremely effective against intrusion if well planned and implemented. A security specialist is needed to set up the system, but also to test the ability to gain access. Testing is important because a good security specialist can identify the weak links in your electronic fence and can help you fix them.

**I already have enough problems with false alarms. Won't an integrated system just compound this situation?**

Just the opposite. The integrated system can check and re-check conditions in the field through monitors upstream and downstream from the alarm location, allowing the system to sort through many of the false alarms and assign probability and severity to each alarm. This capability can help operators sort through the hordes of alarms to determine which are most likely real and then determine priorities based on predetermined criteria. The intelligent system helps the operators and managers deal with issues more effectively.

**What if the intelligent system isn't?**

Then you wouldn't buy it. But let's say you go on the cheap and get Joe's Discount Intelligent System. Even if it is not that intelligent, there are still the operator and the decision maker who will perform necessary actions and make the final decisions. The system will not make all the decisions for you; it just assembles all the available data from your integrated systems and returns the most important information that can be helpful for making decisions. It tells you what you've told it to tell you, nothing more or less.

**Does this intelligent system replace my operators?**

No. People are at the heart of the system. But it does help eliminate the need for everyone to know everything about the system. Knowledge can reside within the system with easy access to it from any authorized person, reducing the need for gut-feel decisions that could turn sour.

People will make the final decision in any scenario unless you want the computer to handle certain tasks on its own, like your SCADA system does now.

**Won't I spend tons of money and time integrating my systems?**

Probably. And you'll love doing it when you start seeing the payback. Remember, this is largely money that would otherwise have gone into physical security or new systems that didn't have the same operational improvement opportunities. What we're proposing is that you begin aligning your systems and security expenditures toward the common goal of integrated, secure systems.