

Utility Security Upholds Uncompromising Standards

BY MAY CHU

Utilities are like a country's nerve system — any harm could result in serious consequences. After Sept. 11, utility sites have focused on defending vulnerabilities against threats.

The protection of critical infrastructure, such as water systems, became a high priority after Sept. 11 for U.S. federal agencies, such as the Department of Homeland Security and the Environmental Protection Agency. Both agencies developed guidelines for the security of water and wastewater facilities. In June 2002, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act, which requires vulnerability assessments and emergency response plans for community drinking water systems serving more than 3,000 people. Electric utilities follow the North American Electric Reliability Corporation's guidelines, starting a program for self-reporting and certification in 2008.

Security professionals believe that the U.S. regulations on utilities will result in more regulations for other parts of the world as well. The security market will need to apply these regulations to products in order to comply. "Before, if you found a problem with water, you could hide and try to fix it," said Gilad Chitayat, International Director

of Sales, Orsus Systems. "But now, you need to report to the government (in the United States, for example), following a standard procedure and reacting much faster than before."

Security providers agreed the security market for utilities will increase. Ariel Frischhoff, VP of Sales for EMEA and APAC, Agent Video Intelligence, said the market is roughly US\$300 to 500 million. Rajeev Kaushal, Division Head of infochips, estimated the global market size to be billions of dollars. Other interviewees felt it was difficult to put a figure on utilities, since threats differ from region to region.





▲ Rajeev Kaushal, Division Head of einfochips



▲ Tom Wallace, Sales Manager for Utilities, Security Systems Division, Southwest Microwave



▲ Karl Philbin, Business Development Manager for Asia, Australia and the Middle East, Gallagher Security Management Systems



▲ Adam Rosenberg, VP of Marketing, Magal Security Systems

THREATS

Utilities face several threats. One threat is physical attacks that would inflict damage or destruction to vital infrastructure. “These attacks can include terrorism, sabotage or vandalism,” said Tom Wallace, Sales Manager for Utilities, Security Systems Division, Southwest Microwave. “For water utilities, these acts can threaten raw water supply, water treatment plants and storage or distribution facilities. This could potentially affect water and power delivery, or public and environmental health and safety.”

Other threats include planting of explosive devices and arson. Dumping of flammable or toxic substances into water, treatment facilities or distribution systems could be a potential risk. Theft of material such as copper or destruction of assets is also a big concern.

Utilities also have to assume the risk of hacking into a facility’s supervisory control and data acquisition (SCADA) system or deletion of critical files and databases. In addition, liability risks are real, such

as injury or death to individuals by drowning or electrocution from high-voltage equipment.

Internal threats cannot be ignored, such as employees stealing information, materials or equipment. “Employees of critical utilities site are exposed to sensitive information about the site,” Frischhoff said. “For example, a nuclear plant contains information on nuclear energy processes that are confidential. Employees may have access to it and try to steal it to sell it on the market.”

PERIMETER

Perimeter systems are the first crucial layer of security for utility sites. It has to both deter and detect, often with barriers, cameras and monitoring systems.

“Perimeter sensors allow security personnel to detect an intrusion attempt to the outer perimeter,” Wallace said. For example, fences topped with razor wire, are an effective



delay to unauthorized entry. Monitoring equipment provides visual assessment of the disturbance, allowing security personnel to respond quickly.

“The perimeter system should actually provide a deterrent to intruders,” said Karl Philbin, Business Development Manager for Asia, Australia and the Middle East, Gallagher Security Management Systems, who recommended electric fences.

Environmental conditions have to be considered when implementing perimeter systems. “Usually utility sites are very big in size, and are located in areas where environmental elements are very strong, like wind, snow or hot deserts,” said Frischoff. “This makes them very difficult to safeguard.”

“If there is no illumination or the area suffers from heavy fog, these problems must be addressed,” said Adam Rosenberg, VP of Marketing for Magal Security Systems. To overcome harsh weather conditions, Magal’s taut wire is designed for installation near the sea in humid conditions, snow or strong winds. It offers high probability of detection and a low false-alarm rate.

FALSE-ALARM CONTROL

Several types of sensors can be used for perimeter security. The most important criteria for perimeter intrusion are the number of false alarms and the associated technologies to reduce them.

“It has to be considerably low,” Philbin said. “Otherwise, sites will pay unbelievable prices, having security guards — even police — running back and forth to remote and expansive sites.” Electrified fences have fewer false alarms because a physical action is required to initiate an alarm. Magal Security Systems said its false-alarm rate for its taut wire system is one false alarm per kilometer in three months.



▲ Uri Engelhard, President and CEO, Mate Intelligent Video



▲ Oren Feldmann, VP of Marketing and Sales, EVT



▲ The protection of critical infrastructure, such as water systems, became a high priority in the United States after Sept. 11.

However, some experts considered a few false alarms good, to keep security personnel alert. “It’s better to have a few false alarms rather than having misdetections,” said Uri Engelhard, President and CEO for Mate Intelligent Video.

ACCESS CONTROL

At many utility sites, employees enter through a detection gate and have their belongings searched. Between gates, there are different levels of security for employees, with different authorization granting access to different areas.

Oren Feldmann, VP of Marketing and Sales at EVT, said access control for utilities is usually combined with other systems, such as alarm-triggered video or video analytics. “If someone has gone through a gate, a video will pop up and be viewed live from the control room,” he said. “Or if someone has stayed in a gateway where everybody is supposed to pass in a few seconds, then the video analytics will tell the operator what the person is doing.”

Access control can play a larger role in an integrated system. “In a hazardous environment, access control supports automated mustering,” said Susan Alderman, Project Marketing Director for EMEA and India, Honeywell Building Solutions. “It can track who is in a facility, their real-time location and in the event of an emergency, direct first responders to that exact point.”

It can be governed down to the smallest details, such as working with ID card management, authenticating contractors and visitors on prespecified locations, times

and training credentials, Alderman continued. Access control can also be used to protect intellectual property, along with tracking valuable portable assets to predetermined boundaries.

At highly sensitive utility sites, any identification breach could cause serious problems. "The solution to avoid faulty access is to have multilevel authentication, such as fingerprint, smart card and facial recognition," Kaushal said.

PRODUCT TRENDS

Perimeter security will always be the first protection for utility sites. "Utility companies are still perimeter-oriented and typically spend more on perimeter protection than for internal security," said Andrew Minnikin, President of Pacom Systems U.K. and Northern Europe. "If trespassers cannot get in, then there's less dependence on internal security."

System integration is another trend for utilities, owing to a need for operational efficiency as well as security. Frischhoff estimated this market to grow at 25 to 40 percent annually.

Integration will offer financial gains to utilities. "In our experience, this equates to at least a 20-percent saving on operational costs — more if a fully integrated design process is applied at the initial design stage," Alderman said.

Integration will lead to improved situational awareness and real-time responses. For example, Chitayat said, the Orsus Situator can automatically notify the relevant agencies and personnel when certain events occur, such as water pollution, resulting in faster responses.

FUTURE OUTLOOK

Utilities are important locations, but the perception of danger is not always present. "The main challenge — not just for utilities but everywhere — is that people don't believe anything will happen," said Dave Foster, Director of Utility Security.

More technical challenges are ahead, with the development of systems involving network technology. "Improvement of IT and network infrastructure has given rise to the requirement to perform all security functions remotely," Minnikin said. "I would suggest customers think wisely before considering a product that sits on their LAN/WAN. They should check that it has a proven track record, that it doesn't substantially impact bandwidth traffic."

Increased situational awareness is a goal that security providers strive for. "All sensors, all systems and all information will drop a conclusion through one procedure to the security person of what is happening and what they need to do," Feldmann said. "An operator goes to site one to site 20, and all sites will need to look the same and feel the same."

Video analytics are getting smarter, with demand growing to detect more unauthorized intrusion and eliminate false alarms. "The money will be spent much more smartly in the future," said Eli Gorovici, President and CEO for DVTel.

"While governments are cutting budgets, they will spend money on proved technology, not on 'cool' unproved technology which may or may not work," Gorovici said. The bottom line is: "We don't see any slowdown in this industry — typically homeland security, but utility security is a big part of it." **AS**



▲ System integration is the trend for utilities, owing to a need for operational efficiency as well as security.