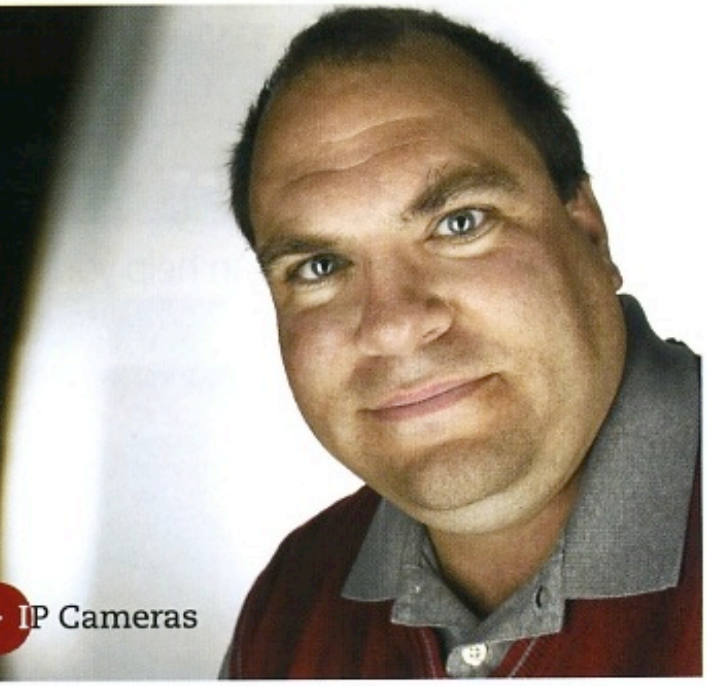
Gaining Focus

Take your best shot at collaboration and surveillance using IP cameras.

By Logan Kugler



↑ "Cameras that we wouldn't want the world to have access to are protected. Cameras that show off to the world what we do are available to anyone from outside to take a look," says Jeff Terry, who operates a facility at Argonne National Laboratory.

ROBERT RANDALL

When physicists at the Argonne National Laboratory wanted to let researchers around the world observe and participate in lab experiments, they hit on a novel way to mix security with accessibility. Alongside their normal array of security cameras, the physicists at the lab installed a set of web-accessible Axis Communications cameras that selected observers could access online from anywhere in the world.

"We have cameras that are secure and password protected that no one has access to, and we also have public cameras," explains Jeff Terry, the researcher who developed the system used at Argonne. "Cameras that we wouldn't want the world to have access to are protected. Cameras that show off to the world what we do are available to anyone from outside to take a look."

The technology that makes this possible at the Energy Department lab outside Chicago is the Internet Protocol camera, the next generation replacement for traditional analog cameras running on closed-circuit TV networks. While traditional analog cameras use proprietary hardware and software, IP camera networks share infrastructure with existing computer networks, which makes IP cameras more accessible and more extensible than their analog counterparts. Plus, increasingly powerful video analytics software sends automated alerts under specified conditions, which makes IP cameras especially useful as surveillance tools that can, for instance, spot a sudden rush of activity or a foreign object left unattended.

But implementing an IP system can be a demanding undertaking, particularly if you are considering upgrading an existing analog system, says Eric Cole, a fellow with the SANS Institute in Bethesda, Md., and a security consultant. To make sure your agency gets the best possible return on its investment, take particular care with five things: defining your requirements, planning for network load, integrating your IT and security programs, setting security for the cameras themselves and training users.

PLAN for your specific needs.

IP-based systems offer a number of benefits over traditional analog cameras, but they are not the best and only answer for every situation, says Terry. Before choosing, you should thoroughly explore the physical, technical and personnel requirements of your situation and plan accordingly. When you know what you'll be using your camera system for, you'll be able to determine the type of network you need, the particular hardware and software you need and how your camera should be placed, adds Cole.

For instance, if your needs tend more toward surveillance than collaboration, you'd likely want to pair your cameras with analytics applications. That requires establishing procedures for when an alert will be sent, to whom it will be sent and how the recipient should respond. You also need a procedure for handling the recorded data, Cole adds, because it will provide forensic evidence for any investigation.

KEEP three things at the top of your priority list: bandwidth, bandwidth, bandwidth.

The most crucial limiting factor in any IP camera installation is the amount of bandwidth you can allot, says Casey Beard, emergency management director for Morrow County, Ore., which runs surveillance at the Army's Umatilla Chemical

Depot. Streaming full-frame, real-time video can slow even the most robust network to a crawl. In most cases, your existing network infrastructure won't be enough, unless you are willing to settle for reduced video quality, Beard says.

But for Umatilla, reduced capacity was not an option. Its network of dozens of cameras deployed wirelessly over an area of 1,000 square miles is an essential component of the facility's evacuation system, and local law enforcement also uses the cameras, Beard says. The life-or-death context demands full-speed, high-resolution imagery, so the system's planners turned to wireless fiber, a point-to-point technology providing fiber-like bandwidth through the air, he says.

Server hardware also will limit bandwidth. Beard points out that while wireless fiber solved part of the bandwidth problem at Umatilla, "the bigger issue was having enough server capacity to handle all the data and avoid things like latency, so we have the ability to dynamically control the system."

CREATE a partnership between IT and security.

Installing and operating an IP security system requires a unique blend of skill and expertise, says Dilip Sarangan, a security analyst at Frost and Sullivan. The best approach, he says, makes use of both an agency's IT department and its security team. "A security manager may not be equipped with all the necessary information or the knowledge to be able to control these systems and make them as efficient as they should be," Sarangan says. "But if it's handed off to the IT department, they're more worried about how much bandwidth it takes up than the security situation."

Sarangan describes an effective relationship as a marriage between IT and security, with clearly defined roles and responsibilities — basically, a technology pre-nup. Creating this marriage requires extensive training and an open relationship between departments that might not have a history of cooperation, which means the team leader needs to be an exceptionally skilled facilitator, Sarangan says.

MATCH the security requirement to the content.

"When you're working at the national labs, security has to be an utmost concern at all times," says Terry. "It's not something you can plan for after the fact. You can't just say, 'We're going to do this,' and worry about securing it later. You have to think about security right from the start." At Argonne, established in 1946 as the first national lab, teams of scientists conduct applied and basic research in a wide range of areas.

Like many federal organizations, the lab manages information, including images gathered by its cameras, that runs from the mundane to the classified. Extra care must be taken to secure IP cameras from both unauthorized users on the internal network and malicious outsiders who can potentially access the system over the Internet, Terry says.

At a minimum, he suggests use of intrusion detection systems and regular probes of the camera firmware and other hardware on the network to check for vulnerabilities. In most situations, a separate virtual private network should be established for each camera or block of cameras. If the content gathered by the cameras is extremely sensitive — as it is sometimes at Argonne — IP cameras may need to operate on a separate network.

REMEMBER your human resources.

The focus of designing a system should be on simplicity, elegance and ease of use. As security systems grow more powerful, the amount of information the end user — a security guard, field officer or inspector — has to deal with multiplies rapidly and can easily become overwhelming, says Cole.

Unfortunately, it's all too easy to skimp on usability to meet a budget. "When it comes to security functionality, you're always going to pay," Cole says. "You either pay up front to do it correctly, or you pay after the fact when there's an incident or breach."

Cole recommends a custom interface that's built around the different responsibilities of the people who will use the system. "You need to limit and control what access each person has and make it simple," he says. "You're not restricting that person, you're giving them everything they need to do their job."

Although it's easy to get swept up in the whiz-bang aspects of IP-based security technologies, the most crucial elements of a functioning system still are planning and training, Cole says. With this in mind, you can develop a system that will make the best use of the power this technology offers and that can grow and develop as your needs change. FT

SECURITY WITHOUT WALLS

Both Internet Protocol cameras and traditional analog cameras can handle the task of securing a fixed area such as a building or data center, but what if the area your agency needs to secure keeps shifting? What if you're trying to secure a battlefield or an operation deep behind enemy lines?

MacroSwiss, a Swiss manufacturer of specialty cameras for military use, focuses its R&D on the question, "Where *can't* you put a camera?"

The company's SpyRobot 4WD and its little brother, MicroSpyRobot, ride only a few inches off the ground on all-terrain paddle wheels that work in water as well as on land, allowing soldiers to remotely drive the cameras into situations that they cannot reach.

MacroSwiss' Short Range Throwing Camera, or SRTC, looks and works like a grenade. The user remotely lobs the camera, in its hardened case, into chaotic situations so observers can get a handle on what's happening before entering the fray.

The GunCam, another MacroSwiss product, mounts on the barrel of a gun and streams images to a wrist-mounted monitor, enabling soldiers to look safely around corners and react instantly to any threats they might find.

Finally, the experimental HydroBot packages a motor and camera system into a flotation device shaped like either a seagull (for saltwater deployment) or a duck (for freshwater use).

SHOU SASAKI/GETTY IMAGES