Argus Oversees and Protects All

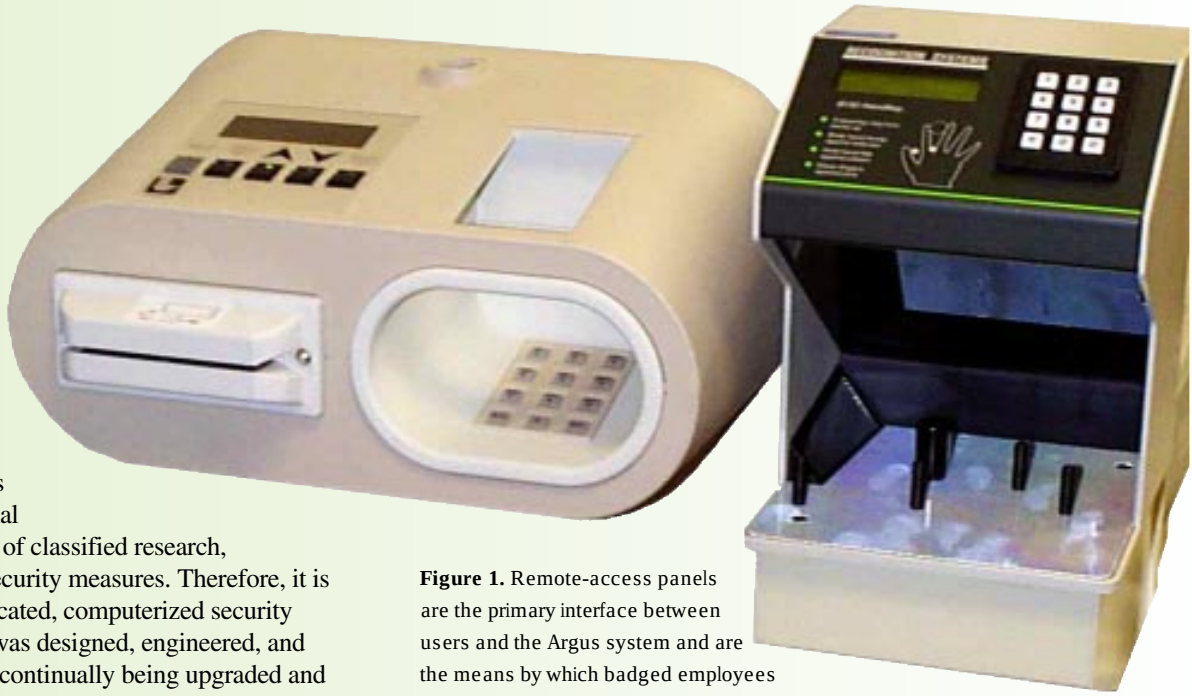


Figure 1. Remote-access panels are the primary interface between users and the Argus system and are the means by which badged employees enter controlled buildings and areas.

FROM outside Lawrence Livermore National Laboratory, the public sees a site protected by chain link fences and guards at entry gates. But this Department of Energy national laboratory, home to a variety of classified research, requires much higher level security measures. Therefore, it is guarded as well by a sophisticated, computerized security system called Argus. Argus was designed, engineered, and installed at Livermore and is continually being upgraded and enhanced. It is also available to other Department of Energy and Department of Defense facilities.

Although named for the hundred-eyed monster of Greek myth, Argus security comprises much more than visual capabilities. A highly interconnected network engineered with comprehensive security features, Argus lives up to such stringent security requirements that DOE's Office of Safeguards and Security has cited it as the standard for physical security systems protecting facilities where the consequences of intrusion are significant. In addition to Lawrence Livermore, the Argus system has been installed at three other DOE sites and at one DOD site to protect top-priority assets or nuclear material.

As it monitors and controls entry into the Laboratory's high-security buildings, Argus is simultaneously monitoring the entire site for security threats and can alert and direct security forces to those threats. Argus security is all-encompassing and omnipresent, but it is surprisingly noninvasive. Employees of Lawrence Livermore enter and move about the Laboratory campus with relative ease. Yet, the Laboratory's Top Secret documents, materials, and facilities are thoroughly protected, intruders can be detected in real time, and intrusions and emergencies get instantaneous response from police and investigative personnel. The Laboratory is provided with maximum security 24 hours a day, 7 days a week.

This security results from a software system that comprises some 1.5 million lines of code, offering a wide range of security features. Extensive features are necessary, because Argus must accommodate many different configurations of security rules within one security complex, and sometimes one complex may have multiple geographical locations (for example, Livermore's Argus system controls the main site and the nearby Site 300 high-explosives testing facility). Moreover, Argus must be reconfigurable at any time. Extensive features also translate into flexibility and simplicity for end users. That's important because every authorized person in a high-security site accesses and interfaces with the Argus system. To ensure that designers, operators, and users understand Argus, DOE's Central Training Academy in Albuquerque, New Mexico, has 14 classes available, ranging from one hour to one week, that cover the complete set of Argus features.

While protecting a security complex, Argus also protects itself. A high degree of redundancy has been incorporated to prevent system failure, and tamper-indicating devices and data encryption have been used throughout to protect

surveillance equipment and data from intruders and thieves. Insider threats to weaken the system have been addressed with a comprehensive set of system-enforced and procedural measures, including consistency checking, captive accounts, and a rule prohibiting people from working alone.

How Users Work with Argus

Argus is implemented through four integrated computer subsystems. One subsystem controls access into buildings and areas. Another monitors alarms and sensors installed throughout the site. A third integrates and displays security data so security personnel can assess and control incidents. The fourth provides central computing and data storage to support the overall system configuration and databases. These four elements provide what Greg Davis, the manager of Livermore's Argus program, calls a "God's eye view" of the site. They connect into a real-time, interactive security assessment and response system.

User interactions with the Argus network are made possible through two hardware components: a remote access panel (RAP) and the Argus field processor (AFP).

The RAP (Figure 1) is a microprocessor-based, programmable input–output device connected to an AFP (Figure 2). It is the primary user interface to the Argus system. When Livermore employees are "badged," they are enrolled into the Argus system and can then use RAPs to gain entry into controlled buildings and areas on site. They swipe their badges, which have been coded with a unique identification number and a decryption key. The RAP communicates the badge information to the AFP, another microprocessor-based device, which verifies it against locally stored encrypted access authorization databases.

Figure 2. Argus field processors are microprocessor-based devices that verify badge information transmitted from remote access panels against locally stored encrypted access authorization databases.

Argus software allows access based on credentials (determined by a badge), a user's identity (determined by personal identification number and biometrics), clearance level, and privilege. Although access rules can be very restrictive, the access system provides flexibility by being able to make fine distinctions within those rules. Thus, it might allow a person into a high-security building within a classified area but prevent that person from entering an even higher level security vault within that building. The access system also allows changes in user privileges, within rule confines; for example, regular users can be enrolled to escort visitors through high-security areas. The system eliminates the need for labor-intensive badge checking, and it monitors, tracks, and logs all badge usage.

In addition to controlling and monitoring the RAP access controls, AFPs also control and monitor the networks of thousands of electronic sensors and other surveillance equipment that comprise the alarm stations of a security complex.

The AFP determines the status of security in the alarm station by polling its sensors, controls station operating mode (that is, whether the station is open or secured, in maintenance, etc.), and provides entry authorization via the RAP interface. Alarm station caretakers can also use the RAP to modify access lists, change the rules of the alarm station, and authorize maintenance on the station.

Alarm stations are of many types—outdoor perimeter exclusion zones, normal interior rooms, vaults of concrete or steel, or even entire buildings. They can have sensors and surveillance equipment installed on walls, floors, and ceilings. Because as many AFP modules can be installed as necessary to monitor alarm stations, site security is scalable. At the same time, its modularity restricts problems and makes maintenance and diagnostic work easier.

Real-Time Command and Control

Occasionally at the Laboratory, police cars with flashing lights and howling sirens speed through the streets in response to an alarm or other security incident. They have been dispatched by security personnel who monitor site security 24 hours a day from Argus consoles (Figure 3). The consoles

Figure 3. Security personnel monitor site security 24 hours a day from Argus consoles like this one at Lawrence Livermore.

integrate and display graphical data from controlled entryways and alarm stations, and they are linked to telephone, radio, and intercom systems. They provide Livermore security staff with a real-time command-and-control capability.

At each console workstation, an operator controls two high-resolution, color display screens that show maps of security areas and the security equipment contained in them (sensors, entry control devices, cameras). The system display lists any security anomalies that are occurring and indicates the security status of surveillance equipment by color code. Green, for example, indicates normal or secure, while red indicates a potential security threat, an alarm, or a failure. When security anomalies occur, an operator is alerted by the lists and can view them on the screens; the views can be enlarged or adjusted for seeing additional details.

Operators may also be able to zoom in on the anomaly. Consoles can be linked to closed circuit televisions. Console video subsystems have computer-controlled switches capable of delivering signals from any linked television camera simultaneously to any display monitor and to all recording devices. Video options also include pan–tilt–zoom cameras and video motion detectors.

The consoles are ergonomically designed, providing comfort and ease of use to operators. The number of consoles in operation depends on site requirements and operator workloads; Argus can support any number of workstations without degradation.

Continuing Improvements, Ever More Uses

The installation of Argus at a major DOE nuclear weapons storage and dismantlement site is nearing completion. There, Argus was modified to accommodate access authorization procedures that require observation of the two-person rule for entry and exit. In addition to RAPs, the entry portals have devices that read stored hand-geometry data, and booths may have special detectors to monitor the transport of sensitive materials. To serve this site and other users, Argus program staff are developing a 24-hour help line.

They are also moving ahead to evolve Argus to the next technological level, with such features as topology-independent network-based sensors and capability to simulate intrusions and attacks. In the first, Argus staff are in the midst of developing a neuron chip that can be embedded into sensors, adding the capability to communicate with sensors instead of merely receiving signals from them. This feature will enhance AFP line supervision of alarm stations, enhance sensor security, and dramatically reduce installation costs. In the second, Argus staff are beginning research and development to endow Argus with simulation capabilities that can be used in conjunction with conflict simulation exercises. Argus console operators will soon be able to detect simulated attacks and send virtual security dispatches to contain and control them. Such simulation would hone a site's emergency response tactics and provide realistic training to console operators.

—Gloria Wilt

Key Words: Argus, Argus field processor (AFP), remote access panel (RAP), security technology.

For further information contact
Gregory Davis (925) 422-4028 (davis19@llnl.gov)

Of Josephson Junctions, Quasi-particles, and Cooper Pairs

IF Josephson junction brings to mind an intersection of two small back roads, it's time to change gears and think science. This term, along with quasi-particle and Cooper pair, is part of the large area of superconductors.

Simon Labov and his colleagues in Lawrence Livermore's Physics and Space Technology Directorate say these concepts and discoveries show great promise for applications in areas such as wireless communication, energy storage, and medical diagnostics. Labov and his fellow researchers are using superconductors to create a new generation of supersensitive detectors for nondestructive evaluation and astrophysics.

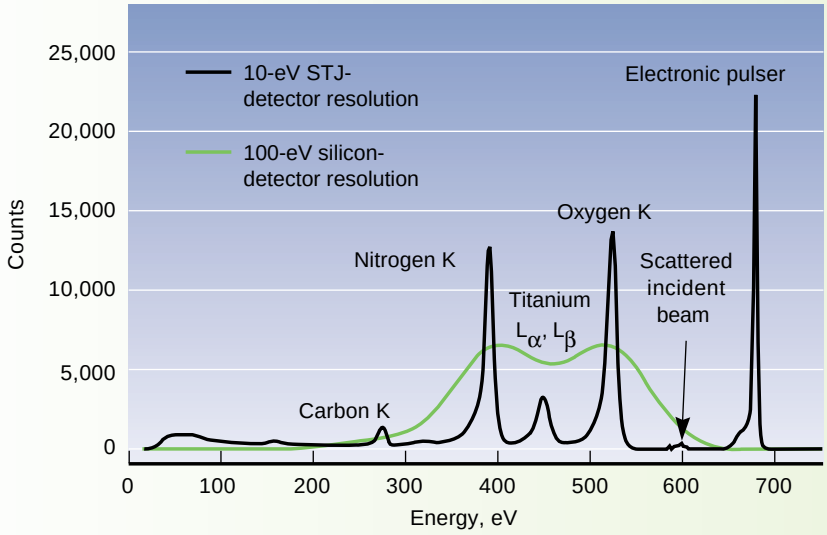
Stephan Friedrich inserts a sample in the Lawrence Livermore superconducting-tunnel-junction (STJ) detector cryostat at the Stanford Synchrotron Radiation Laboratory. X rays from the synchrotron enter the cryostat through the beamline on the left and strike the sample, producing x-ray fluorescence, which is measured by the STJ detector.

When ordinary metal conducts electricity, the electrons carrying the current collide with imperfections in the metal, thereby creating resistance. But when a superconducting material is cooled to its critical temperature, electrons pair off into Cooper pairs, named for Leon Cooper, one of the scientists who won a 1972 Nobel Prize in physics for explaining the now widely accepted theory. Any movement of one electron is matched by equal and opposite movement of the other. As a result, they don't hit the imperfections, no electrical resistance is generated, and electrons flow freely, without the addition of more energy.

But to put these theories to practical use in detectors requires a Josephson junction. Named for Brian Josephson, who described the theory when he was a graduate student at Cambridge University in 1962, a Josephson junction is two pieces of superconducting material linked by a weak insulating barrier. When an x ray hits a Josephson junction, the Cooper pairs break up, and quasi-particles are created. These quasi-particles, which are electronlike or holelike excitations in the superconductor, can tunnel through the weak insulating barrier of the Josephson junction, producing a pulse of electrical current. By measuring the number of Cooper pairs that are broken, scientists can determine the energy of the x ray up to ten times better than with conventional technology and can identify the material that emitted the x ray. These superconducting-tunnel-junction (STJ) detectors also work with optical, ultraviolet gamma-ray photons and large biomolecules. Labov and his team are working to use this new technology in applications for analyzing all of these particles.

Measuring Large, Slow Molecules

The Livermore group has, for example, teamed with scientists at Lawrence Berkeley National Laboratory and a commercial firm, Conductus Inc., of Sunnyvale, California,



X-ray fluorescence measured with a superconducting-tunnel-junction (STJ) detector shows ten times better energy resolution than can be achieved with a conventional silicon detector. A titanium nitride sample was irradiated by 600-electron-volt (eV) x-ray photons at the Stanford Synchrotron Radiation Laboratory. The STJ detector cleanly separates the titanium L lines from the nitrogen K line and the background oxygen K line.

to measure massive, slow-moving macromolecules in DNA research. In a typical time-of-flight mass spectrometer using a microchannel-plate (MCP) ion detector, large ions move too slowly to be efficiently detected. Using an STJ detector, the team found that they could achieve close to 100% detection efficiency for all ions, including the slow, massive macromolecules. "A comparison of count rates obtained with both detectors indicated a hundred to a thousand times higher detection efficiency per unit area for the STJ detector at 66,000 atomic-mass units," Labov says. "For higher molecular masses, we expect an even higher relative efficiency for cryogenic detectors because MCPs show a rapid decline in detection efficiency as ion mass increases."

Even more exciting, STJ detectors can measure independently the mass and charge of the molecule. Current MCP detector technology cannot measure the charge of the molecule, and this inability often causes confusion in interpreting mass spectrometer data. According to Labov, if nonfragmenting ionization techniques can be perfected, cryogenic detectors could make possible the rapid analysis of large DNA molecules for the Human Genome Project and might be used to analyze intact microorganisms to identify viruses or biological weapons materials.

High Resolution for Soft X Rays

In another experiment using an STJ, Labov again teamed with Conductus and seven other Lawrence Livermore scientists to study energy resolution for soft x rays with energies between 70 and 700 electron volts. The results showed that STJ detectors can operate at count rates approaching those of semiconductor detectors while still providing significant improvement in energy resolution for soft x rays. "In this region, the STJ detector provides about ten times better resolution," Labov adds.

Astronomers also are looking to STJs as single-photon detectors of both x rays and visible wavelengths. In the visible band, silicon-based, charge-coupled devices cannot measure a photon's energy, but STJs can. One photon, depending on its energy, can generate thousands of quasi-particles. By measuring the photon's energy, STJ detectors will allow astronomers to study galaxies and stars that are barely bright enough to be seen with the largest telescopes.

Detecting Impurities as Semiconductors Shrink

As semiconductor devices continue to shrink, the industry needs to detect and identify small amounts of contamination on the devices. Microanalysis systems with conventional energy-dispersive spectrometers "excite" contamination on chips with fairly high (10-kiloelectron-volt) energy, which results in the surrounding material also being excited. When the surrounding material is excited, a flood of unwanted signals or noise is created, making it impossible to detect the contamination. But STJ detectors can operate with excitation energies of less than 2 kiloelectron volts, which produce signals from the contamination only, allowing the imperfections to be detected.

Helping to Enforce Nonproliferation

One of the Laboratory's important missions is to help guard against the proliferation of nuclear weapons. Labov and his team are conducting a research and development project that involves using a superconducting tantalum detector to improve gamma-ray resolution. This technology provides better

diagnostic capability, particularly when there are large amounts of one isotope and small amounts of another. For example, when small quantities of nuclear materials are present, most of the gamma rays detected will be from background sources. Conventional detectors aren't sensitive enough to distinguish clearly between gamma radiation from the background source and from the nuclear material.

The team's high-resolution, superconducting spectrometer can detect special nuclear materials by isolating emissions from different radioisotopes. For example, if an inspector suspected that a heavily shielded barrel of spent plutonium from a reactor plant also contained weapons-grade plutonium, the superconducting spectrometer can measure the composition of the materials in the barrel much more accurately than a conventional detector. The technology also holds promise in environmental monitoring for the analysis of trace contaminants because it can detect levels that conventional detectors would miss.

Looking toward the Future

Traditional energy-dispersive and wavelength-dispersive spectrometers are fully developed technologies, leaving little room for significant performance improvements. Cryogenic detectors are still in a developmental stage, with significant progress having been made over the past few years. STJ detectors, although an "old" concept, are now better able to resolve low-energy x rays without sacrificing count-rate capability, and the x-ray collection efficiency of these detectors can be increased by orders of magnitude with focusing x-ray optics, which concentrate the x rays on the detector. These developments could greatly increase the use of these detectors in a wide range of applications.

—Sam Hunter

Key Words: atomic spectroscopy, Cooper pairs, detectors, Josephson junction, mass spectrometry, quasi-particles.

For further information contact
Simon Labov (925) 423-3818 (labov1@llnl.gov).