NEED TO KNOW
a national security newsletter

Volume 4, Number 2 April 2004

Revealing Images:

INEEL Portal Detects Concealed Weapons

The first INEEL-designed concealed weapons detector was installed at the Bannock County Courthouse in Pocatello, Idaho, in 1998. Over the years, it has stopped thousands of weapons from entering the courtrooms, everything from penknives to axes. But more interestingly, it has stopped many weapons from even entering the building. Its reputation for detecting hidden items is so good that groundskeepers continue to find an arsenal stashed behind bushes and trash cans, abandoned by owners who would rather risk losing their property than discovery.

Fast-forward a few years to 2003. The next-generation INEEL concealed weapons detector, now commercialized and marketed as SecureScan 2000 by View Systems, Inc., is installed in Washington Irving High School, in New York, N.Y. Students carrying lunches, books and backpacks walk through the portal as if they were walking through a doorway. But some of the students carry more than the paraphernalia of today's teenager – the MP3s, pagers and cell phones. Some carry weapons.

The New York City Police Department School Safety Division reported an incident last year after an alarm sounded as a student passed through the portal. The monitor indicated that a weapon was concealed in the student's mouth. The subsequent search revealed that the student had hidden a razor blade in the upper palate area of his jaw.

According to the NYPD, student slashings are a major

See **PORTAL**, *page 2*

04-GA50120-01

PN03-0437-01-21

The new INEEL weapons detector is sophisticated enough to discriminate between threat and nonthreat items such as keys and coins. And it is sensitive enough to identify threat items as small as a box cutter or razor blade.

IDAHO NATIONAL ENGINEERING AND ENVIRONMENTAL LABORATORY

INEEL
Home of Science and Engineering Solutions

PORTAL *(continued from page 1)*

threat citywide. The police stated that standard metal detectors often resulted in false detections and an increase in man-hours to conduct hand searches. They said jewelry and coins were being detected instead of razor blades and other weapons.

The new INEEL weapons detector is sophisticated enough to discriminate between threat and nonthreat items such as keys and coins. And it is sensitive enough to identify threat items as small as a box cutter or razor blade.

How they work

Typical airport metal detectors use an active electromagnetic technology based on pulsed induction. PI systems send pulses of current through coils of wire within the panels of a portal. The pulse creates a magnetic field, which reverses polarity and collapses when the pulse ends. This collapse results in an electrical spike. The spike causes a short – about 30 microseconds – reflected pulse. If there is metal within the magnetic field, it makes the micropulse last just a bit longer.

Historical data have shown that the responses from typical magnetic monitoring sensors have extreme variability and generate numerous false alarms. Many factors impact and alter performance, including the gait of the person walking through the portal, speed of passage and position in the portal. This makes it difficult to discriminate between threat/nonthreat responses and requires labor-intensive skilled supervision to operate.

The INEEL system is a passive device that senses disturbances in the ambient Earth's magnetic field – disturbances such as that caused by a weapon passing through the aperture of the portal.

The detector uses 16 magnetic gradiometer sensors, arrayed on both sides of the portal aperture. Data are collected from each of the gradiometers, and the change in the magnetic field over ambient background is determined. After the individual sensor responses are computed, the data from all of the sensors are processed as a group to determine the detected object's location and size.

The system provides a graphical interface to the operator by using freeze-frame video capture technology, and places filled circles – dependent upon the number of items detected – over the video image indicating where suspected weapons may reside on a person. The circle sizes vary in proportion to the strength of the measured signal.

Since the original weapons detector was placed in the county courthouse, INEEL researcher and electrical engineer Dale Kotter has designed new enhancements to increase system sensitivity, further reduce false alarms and recognize evolving weaponry.

The system provides a graphical interface to the operator by using freeze-frame video capture technology, and places filled circles – dependent upon the number of items detected – over the video image indicating where suspected weapons may reside on a person (photos at left). The detector uses 16 magnetic gradiometer sensors, arrayed on both sides of the portal aperture (detail below).

A security staff member displays a small sample of the weapons that have been found by the groundskeepers outside the courthouse. INEEL's Concealed Weapons Detector has proven to be a formidable deterrent to people bringing dangerous items into the courtroom.

The Science behind the System

The INEEL detector uses a proprietary method to process and transform thousands of real-time data points from the portal detector array into a signature pattern for analysis.

Threat items, such as guns and knives, and nonthreat items, such as cell phones and pagers, produce unique magnetic signatures, almost like fingerprints. The signature is variable and can be impacted by some of the same factors as those affecting electromagnetic detectors – gait and speed of passage, proximity to center of portal and background clutter. Additionally, the orientation of the weapon can impact the signature.

Kotter employs several signal process methods to analyze the magnetic signature. The data is filtered to remove environmental noise and passed through threshold analysis to discriminate low-level nonthreat alarms. While the simplest way to reduce false alarms is to ignore events close to background, the INEEL system employs other methods so that it doesn't miss almost baseline threats.

Kotter worked with Quantum Mechanics – the sensor manufacturer – to improve sensor sensitivity by imbedding microprocessors into the sensors. Now it can detect that box cutter heading into an airplane or that razor blade into the schoolroom.

Over time, research showed that operators at the Bannock County Courthouse began to recognize signature patterns and could identify the cause of the weapons detector alarms. Simply stated, this human 'learned' response has been optimized and automated.

Kotter has developed advanced signal processing algorithms using statistical analysis tools and a variant of a Probabilistic Neural Net to analyze the magnetic spectrum. The algorithms perform a type of pattern recognition and calculate a probability factor that the collected signatures correlate to a database of weapons and nonweapons.

Test Results

Exacting science must stand up to the rigors of the field and the weapons detector is no exception. Any detector system must smoothly and accurately process snaking lines of travelers or students. Kotter continues to test the INEEL detector for accuracy reproducibility. He, along with colleague Lyle Roybal, replicated field conditions and ran various threat/nonthreat items through the detector.

They tested against the dead zone – the mid-portal area where many standard detectors are unable to identify a weapon – and found that the advanced signal analysis techniques could identify a cell phone, even at levels approaching baseline.

They performed experiments on items that have a high tendency to generate false positive alarms, such as watches, cell phones and PDAs. Proof-of-concept experiments demonstrated a 94.7 percent correct classification between cell phones and weapons and 91 percent classification among nonthreat items.

They verified that a weapon placed at hip, shoulder, mid-body and feet created unique responses that could be classified.

The researchers also conducted experiments on classifying multiple weapons on an individual. In 86 percent of the test cases, the detector correctly classified a razor blade in a pocket, a cell phone on the hip and a knife in the shoe.

Thus far, the National Institute of Justice has funded the INEEL research. Kotter is looking beyond NIJ for future research, actually quite a bit beyond. Kotter traveled to Russia last December and met with scientists from the Russian Institute of Radio Engineering and Electronics. They have developed an active RF technology to detect tumors in bodies. Kotter believes the signal – about the frequency of radio and just as harmless – could be adapted to detect weapons and contraband. He is pursuing a joint project through the Department of Energy's Initiative for Proliferation Program (*see Need to Know July 2002*). View Systems, Inc., the commercial provider of the current version of the INEEL's weapons detector, is also interested in partnering in the research.

Everyone who has ever boarded a plane, entered a federal building or attended high-profile events such as the Salt Lake Winter Olympics wants an efficient weapons detector; one that can spot a tiny, but deadly weapon but one that won't result in false alarms from under wire bras and hiking boots.

The INEEL is developing a solution that can pinpoint the location of a hidden knife yet allows to pass the average traveler, laden only with cell phones and keys.

Dale Kotter
kotr@inel.gov

INEEL Security Expert Spearheads VA Center of Excellence

U.S. Department of Energy and National Nuclear Security Administration laboratories regularly perform vulnerability assessments related to theft and sabotage of special nuclear materials and radiological sabotage. VA analysts conduct detailed examinations of facilities, buildings and vaults to determine the ability of the overall protective system to detect, assess, delay, interrupt and neutralize adversarial threats against strategic quantities of the nuclear or radioactive materials. Not only does the process define risk, but protection strategies and training are also tailored on the outcome of the analyses. And in many cases, significant funding is also requested and allocated to reduce or mitigate risk based on the identified weaknesses.

The VA process is essential and thorough, but it has had a vulnerability of its own – the execution at each facility is dependent on the knowledge, training and experience of each analyst. And until now, there has been no formal training program or certification process for personnel conducting assessments within NNSA or DOE.

That's all about to change.

Sponsored by DOE headquarters and NNSA, National Security's Greg English spearheaded the creation of a Vulnerability Assessment Center of Excellence at the INEEL. The Center will offer certified training to VA analysts across the complex to improve the quality, consistency and completeness of each NNSA site's vulnerability analyses, which, in turn, will improve the accuracy of risk reported.

When it comes to protecting the DOE's assets, English has all of the right qualifications. He says it all started because he was lucky enough to be at the right place at the right time.

Twenty years ago, after finishing his bachelor of science degree in corporate training, English – who was then an INEEL Special Response Team member – volunteered for a rigorous and challenging counter-terrorism selection process at the INEEL. Several former Delta Force personnel from Special Forces Operations Detachment arrived to plan and conduct a six-month, intensive training program for the Laboratory's first counter-terrorist security force. They warned the 60 new recruits that, although they planned on four teams of 11 members each, they would make no exceptions for anyone to pass, and would operate with whatever number made it through selection. English made it through the first time.

"I was lucky to receive that level of training," said English. "From the ground level up, we were taught everything about security from the tactical viewpoint." English used this knowledge to first become a special response team leader, then an SRT Training and Operations manager. Special Operations personnel continued to come to the INEEL for training because of the security mission of the Laboratory and the diverse terrains – desert operations, urban environment – available in one location. For the next few years, he trained along with, and competed against, some of the best security forces in the nation.

National Security's Greg English spearheaded the creation of a Vulnerability Assessment Center of Excellence at the INEEL. English has handled personal and site security in a variety of countries and situations.

PN03-0406-01-19

He then took the only available vulnerability assessment training so that he and others at the INEEL could more aggressively protect the Laboratory by buttressing any identifiable weaknesses.

English's renown in the field of vulnerability assessments and security force training grew, and with it, some unique opportunities.

Through DOE's Material Protection Control and Accounting program – an international cooperative effort to secure and account for nuclear weapons and materials – English traveled to the former Soviet Union to help train the Russian military to better protect their sites. He brought with him eight Russian-speaking, former special forces operators.

"My job was to get the Russians up to speed," said English. "We could do this better if we spoke the same language and didn't have to rely on interpreters external from our unit."

In Columbia – the kidnapping capital of the world – English trained CEOs in how to avoid ambushes or survive kidnapping. In Trinidad, English arranged security for a foreign country president and ambassadors attending a business meeting with

One of the first special response teams that trained at the INEEL (top). A sequence of explosions during an on-site training exercise (above).

an international oil company. And in the United States, he set up protection for a United Arab Emirates head of state.

Closer to home, DOE headquarters sent him to sites in Tennessee, New Mexico and California, and had him take part in internal department assessments. English – and the INEEL – were subject to these same audits. But in the case of the Idaho Laboratory, the auditors liked what they saw.

During these audits, English noticed inconsistencies around the complex in how vulnerabilities were identified and how different sites were tested. English wrote a paper on what he saw and suggested one method to correct it with a report he entitled, "An Evaluation of DOE's Exercise Process," which recommended a different and more comprehensive approach to evaluating protection effectiveness. But like a lot of good ideas, it sat unnoticed.

That is, until 9/11.

After the attacks in New York and Washington, D.C., the whole country took a new, hard look at just how vulnerable we were and DOE was no exception. From English's report, the Iterative Site Analysis process was initiated, which consisted, in part, of a red or adversarial team that had to collect intelligence and formulate attack plans based on pre-attack detection. This was tested at each weapons site. For months on end, English, along with other INEEL experts, visited site after site. During one six-month period, he was home a total of seven days.

English's reputation won him calls from NNSA Director, Ambassador Linton Brooks through Admiral Mies – at home – for assistance with independent analysis of the weapons complex security.

In between traveling, English initiated a concept to provide training to improve VA programs complexwide. He crystallized his vision and came up with a complete program of instruction, consisting of seven logical and sequential modules, each building on the information learned in a previous course. He added two courses as an overview for managers with vulnerability assessment oversight and senior management having the authority to accept site risk. The total program of instruction is more than 260 hours.

The first course – lasting a full two weeks – began in February. David Telles, an experienced VA analyst from Los Alamos National Laboratories, attended the inaugural session.

"I was skeptical at first," said Telles. "I expected them to say 'you will do it this way.' Instead, they delivered a comprehensive course that offered new ways to look at things." Telles is committed to attending all of the courses and, depending on available time and funding, plans to send his VA team to the courses.

"Two weeks is intensive," said Telles, speaking of the first course, "but it flows and I think it's the only way to do it right."

DOE recognized that inconsistencies among the different sites' VA analysis could result in significant differences. VA programs have a major role and influence in determining protective strategies, protective force training, protective system effectiveness, risk and substantial funding requests. Simple differences in VA analysis execution between Site A and Site B might result in one site requesting several million dollars in facility upgrades, that are either not identified by the other site, or perhaps not needed.

"There is only so much money to fix things," said English. "If everyone is looking at it differently, it can drive up security costs."

English is the first to admit that he could not, and did not, develop this program on his own.

"The course is so comprehensive that no single person has the technical experience to teach it all," said English. "We are really fortunate to have some of the best in the business here at the INEEL." He points to Matt Pincock, Jerry Weber, Monty Mortensen, Scott Patrick and Vern Kubiak, all with years of experience, and a new INEEL employee and explosives expert, Greg Clemens.

The Training Accreditation Program (TAP)-certified courses began in February. Many applied for space in the first course, but could not attend due to tough pre-requisites and restriction to 12 students. Enrollment remains limited to allow for intensive, site-specific training.

Greg English
gre@inel.gov

National Security physicist James L. Jones has developed a technology with the ability to rapidly and accurately detect shielded weapons-grade materials hidden within cargo containers.

Taking direct aim at terrorism:

INEEL scientist demonstrates nuclear materials detector

A cutaway of a commercial cargo container sits on the concrete floor of a laboratory at the Idaho Accelerator Center in Pocatello, Idaho. Hidden deep inside, under thick blocks of wood and layers of polyethylene and lead, is an innocent-looking vial, about the size of an aerosol can. National Security physicist James L. Jones aims an accelerator beam at the huge container and in less than 120 seconds, reveals the vial contains uranium.

An audience of scientific peers and representatives from Department of Homeland Security and the Defense Threat Reduction Agency was on hand to witness the INEEL-developed technology's ability to rapidly and accurately detect shielded weapons-grade materials hidden within the container – the same type of cargo containers that daily enter U.S. borders by the thousands.

"Nuclear smuggling is a real threat," said Jones. "I've demonstrated just what this technology could do against it." For several years, DOE's National Nuclear Security Administration has funded research projects to address nuclear smuggling. Jones and others had been working under the auspices of DOE, until program oversight was transferred to the newly formed Department of Homeland Security.

Jones teamed with DOE's Los Alamos National Laboratory and a commercial company to develop the system that could be deployed at the nation's ports of entry. The technology Jones demonstrated has the added benefit of being adaptable to a variety of commercial inspection platforms.

Jones uses a transportable electron accelerator – not much bigger than automobile diagnostic equipment – to produce energetic photons. These photons interact with the interrogated object, in this case, the cargo container. This process, which occurs in less than the blink of an eye, induces fission – divisions in the atomic nucleus – in nuclear material. Other materials do not fission. Jones has designed a patent-pending cylindrical detector that can pick up and characterize this fission event. The pulsed photonuclear neutron detector detects the presence of shielded nuclear material and can differentiate between highly enriched uranium, depleted uranium or thorium when a second beam at a different energy level is directed at the object.

Jones has designed a patent-pending cylindrical detector that can detect and characterize fission in nuclear material.

Sonya Bowyer from Homeland Security attended the demonstration in her role as active interrogation program manager.

"Nuclear smuggling isn't just a Homeland Security issue, it's a global issue," said Bowyer. "One of the jobs I have is evaluating the best technologies to address it. James' is one."

Bowyer plans on identifying the technologies with the best chance of solving real problems and then testing them methodically. Jones agrees on the need for independent testing along with consistent test and demonstration criteria.

"There are thousands of ways to configure a cargo container," said Jones. "We've picked a couple of challenging ones to demonstrate. We are developing standard testing configurations so we can compare our results with other technologies."

This demonstration took place at the Idaho Accelerator Center on the Idaho State University Campus. The Idaho Accelerator Center is operated by ISU in collaboration with the INEEL.

James Jones
jlj@inel.gov


PN03-0003-02-05

State of the Division

Laurin Dodd,
Associate Laboratory Director, National Security

Change at the INEEL is accelerating and it is good. While preparing for an upcoming external review of our progress against laboratory goals, I was struck by two things. First, our client base is continuing to diversify. Second, we are increasingly engaged in major research, development, testing and evaluation areas today that did not exist for us two years ago.

In January 2002, the National Security Division's External Review Board noted that a vast majority of our work is related to 'critical infrastructure' and recommended that we build on that. The Board also observed and complimented us on the fact that we, by and large, were not trying to replicate other national laboratories' efforts. INEEL, as an engineering laboratory, located on a large, isolated site has the capabilities to do many things that would be very difficult to accomplish at other DOE laboratories.

Since that time, we have focused on:

- Developing and bringing into operation numerous 'test beds' on our unique site, and
- Applying our engineering talents to developing solutions to client needs in a broad range of areas that relate to 'critical infrastructures.'

As a result, the INEEL today is increasingly engaged in addressing significant national security challenges. In so doing, we are using core capabilities in process control systems, cyber security, protective security, power transmission, communications and contraband detection.

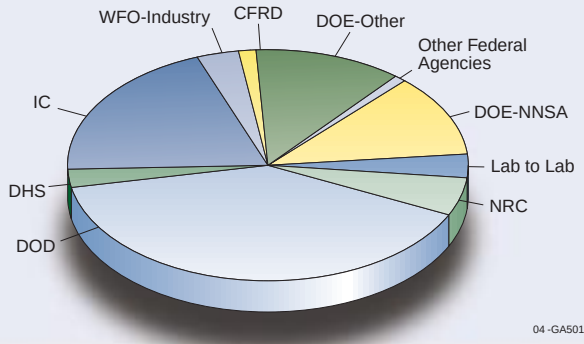
One measure of our increased contributions to the nation's security is the growth rate in our business volume. Since 2002, the Division is experiencing an annual growth rate that exceeds 30 percent.

The chart displays our diverse client base. The makeup of that chart is quickly changing as we see increasing demands from growth areas such as Homeland Security. The fact that DOE represents less than one quarter of our business base is a solid indicator that we are not trying to replicate other DOE laboratories' work. Although we would like to see a larger role with DOE, we recognize that its mission is relatively stable and well addressed by other labs.

Early next year, major changes under way today will culminate in the creation of the new Idaho National Laboratory (INL) – a merger of the INEEL with Argonne National Laboratory's Idaho site. The INL will be a 'nuclear energy and national security' laboratory and will become the focal point of the nation's nuclear energy research and development as well as a center for technology development and testing in support of our nation's security.

It is an exciting time to be associated with this institution. Rapidly, today's challenges are evolving into opportunities for both the laboratory and the staff. We should all welcome the continued change.

National Security Client Base



04 -GA50120-08


04-GA50120-09

Need to Know Wins International Design Award

The Society of Technical Communication (STC) has recently awarded INEEL's *Need to Know* National Security newsletter with an Excellence award at its international technical art competition. In order to compete at the international level, the newsletter first had to win a Distinguished award at the regional (Intermountain) competition. There are three levels of award given by the STC; Merit, Excellence and Distinguished. By the time the newsletter reached the international competition, it was competing with companies like Microsoft, Hitachi, Yamaha Corporation and other international giants.

Domestic Terrorism

Contributed by Gene Johannes

Terrorism – observed in every part of the world – is defined as using, or the threat of using, criminal violence against persons or property with the intent to further a political or ideological objective. Terrorists, who are usually a small minority of the population, attempt to force their views on the majority. As long as humans pursue different objectives, and some of them are inclined to take violent steps to attain their goals, the phenomenon of terrorism will persist.[1]

Terrorists may give numerous explanations for their violence; however, these rationalizations are frequently related to three basic concepts:

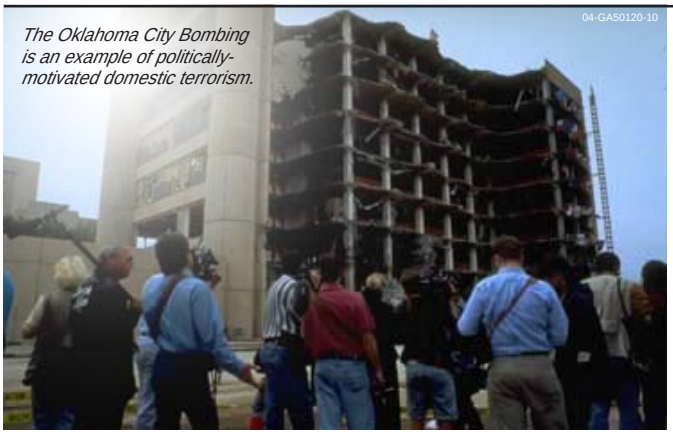
1. Society is sick and cannot be cured by half-measures of reform.
2. The state is in itself violent and can be countered and overcome only by violence.
3. The truth of the terrorist cause justifies any action that supports it. While some terrorists recognize no moral law, others have their own "higher morality." [2]

U.S. domestic terrorism generally falls into one of the following general groups: religious, anti-abortion, hate groups, environmental, world order, political[3] or animal rights.[4] These groups are often categorized in more general terms of either left wing or right wing organizations. Many of these groups may have legitimate complaints, goals or objectives. But by choosing violent methods to further their goals or objectives, they depart from the normal established procedures to effect change in society and cross into the realm of terrorism. Recent examples of domestic terrorism include:

- September 2003, San Diego, Calif., fires in a housing construction area and $50 million destruction to an unfinished condominium complex
- September 2003, destruction to much of the Louisiana State University School of Veterinary Medicine office
- August 2003, $1 million in vandalism and arson damage to sport utility vehicles at a California automobile dealership
- January 1999, an individual was convicted of plotting to blow up federal property and threatening to attack and murder government officials
- October 1995, where, at the site of a 12-car Amtrak train derailment – in which one person was killed and 12 seriously injured – the FBI found four letters mentioning The Bureau of Alcohol, Tobacco, and Firearms, FBI, "Ruby Ridge" and "Waco"
- April 1995, the Oklahoma City bombing in which 168 people were killed and hundreds injured.

With each new act of terrorism, the public is conditioned to accept the terrorists' actions as regrettable, but an understandable expression of the terrorists' grievances. Any tolerance or expressed understandings of these acts adds a certain amount of legitimacy to the terrorists' cause, which usually results in more acts of terrorism.

What can we as INEEL employees do? Be aware. See terrorism for what it is – not a means to effect change in society, but violence. Most terrorist acts are preceded by some sort of surveillance of the intended target. Watch for suspicious vehicles, people, anything out of the ordinary, or those things that are just not normal for the respective location. Remember JDLR. If it "Just Doesn't Look Right," it probably isn't and should be reported. Contact your INEEL Counterintelligence Office at 526-2223/4023/3661.



The Oklahoma City Bombing is an example of politically-motivated domestic terrorism.

1 Ray S. Cline and Yonah Alexander, TERRORISM as State-Sponsored Covert Warfare, Hero Books, Fairfax, Va. 1986, pp 5

2 Albert Parry, TERRORISM from Robespierre to Arafat, Gage Publishing Co., Agincourt, Ontario. 1976, pp 12.

3 http://directory.google.com/Top/Society/Issues/Terrorism/US Domestic Terrorism/Groups/

4 http://dmoz.org/Society/Issues/Terrorism/US Domestic Terrorism/Causes/

NEED TO KNOW *is a publication of the National Security Division of the Idaho National Engineering and Environmental Laboratory. The INEEL is a science-based, applied engineering national laboratory dedicated to supporting the U.S. Department of Energy's missions in environment, energy, science and national security. The INEEL is operated for the DOE by Bechtel BWXT Idaho, LLC. Requests for additional copies, story ideas or questions should be directed to the editor at (208) 526-1058, kzc@inel.gov. This is printed on recycled paper.*

Editor ..... Kathy Gatens
Graphic artist .... David Combs
Photographers .. Mike Crane, Chris Morgan, Ron Paarmann
Copy editing ..... Rick Bolton
Research ..... Steve Paschke

Visit our national security website at: www.inel.gov/nationalsecurity