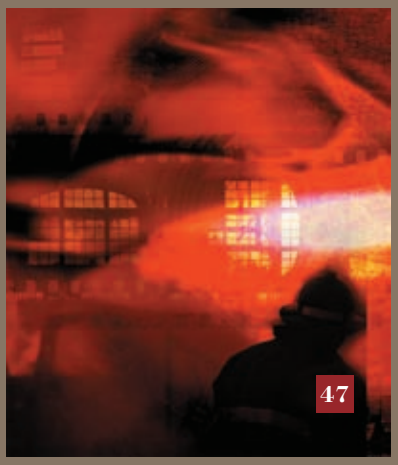
Defense Standardization Program
Journal
July/December 2007

DHS Standardization

RFID Devices in Homeland Security Applications
Reducing the Radiological and Nuclear Threat
Performance Standards for Urban Search and Rescue Robots

Defense Standardization Program
Journal

Contents *July/December 2007*



1 Director's Forum

5 ANSI-HSSP Leads Private-Sector Homeland Security Standards Initiatives

12 Development of Standards for Chemical and Biological Protective Equipment for Civilian First Responders

18 Meeting the Unknown
Standards for Detecting Biological Weapons Agents

25 Reducing the Radiological and Nuclear Threat
Standards for Radiation and Nuclear Detection

33 In God We Trust, X-Ray Everything Else!
Standards for X-Ray and Gamma-Ray Security Screening

41 Performance Standards for Urban Search and Rescue Robots
Enabling Deployment of New Tools for Responders

47 Indoor Localization
Technology That Can Save First Responder Lives

55 RFID Devices and Systems in Homeland Security Applications

61 Finding the Right Management Support Standards

69 The Last 1 Percent
Biometric Quality Assessment for Error Suppression

76 Making Biometric Systems Usable
Let's Not Forget the User!

82 The Multimodal Biometric Application Resource Kit
A Public Domain Framework for Biometric Clients

87 The Policy Machine
A Standards-Driven Enterprise-Wide Access Control Enforcement Mechanism

Departments

93 Events 94 People 96 DAU Courses—FY08

The *Defense Standardization Program Journal* (ISSN 0897-0245) is published four times a year by the Defense Standardization Program Office (DSPO). Opinions represented here are those of the authors and may not represent official policy of the U.S. Department of Defense. Letters, articles, news items, photographs, and other submissions for the *DSP Journal* are welcomed and encouraged. Send all materials to Editor, *DSP Journal*, J-307, Defense Standardization Program Office, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221. DSPO is not responsible for unsolicited materials. Materials can be submitted digitally by the following means:

e-mail to DSP-Editor@dla.mil
floppy disk (Windows format) to *DSP Journal* at the above address.

DSPO reserves the right to modify or reject any submission as deemed appropriate.

Gregory E. Saunders
Director, Defense Standardization Program Office
Timothy P. Koczanski
Editor, Defense Standardization Program Journal

Defense Standardization Program Office
8725 John J. Kingman Road
Stop 6233
Fort Belvoir, VA 22060-6221
703-767-6870 Fax 703-767-6876
dsp.dla.mil

For a subscription to the *DSP Journal*, go to **dsp.dla.mil/newsletters/subscribe.asp**

Director's Forum

In this issue of the *Defense Standardization Program Journal*, we are focusing on standardization efforts underway at the Department of Homeland Security (DHS). It is my pleasure to turn over my column in this issue to Mr. Jay Cohen, Under Secretary for Science and Technology at DHS, and Mr. Bert Coursey, DHS's Standards Executive.

Gregory E. Saunders
Director, Defense Standardization Program Office

Message from the DHS Under Secretary for Science and Technology

The Directorate for Science and Technology is aggressive in the development and implementation of homeland security standards. Such standards help us knit together the 22 legacy agencies of DHS into a cohesive department. However, DHS and the directorate are all too aware that ensuring technology and standards for homeland security extends far beyond the interests and efforts of a single federal agency: it takes a coordinated effort on the part of our federal partners as well as the private sector.

This special edition of the *Defense Standardization Program Journal* is a great opportunity for DHS to share a few of our key activities in standards with our federal partners and with the private sector. I hope that the articles will help generate new ideas, provide new perspectives on technology and standards, and foster close collaboration among government agencies and the private sector to make our nation safer.

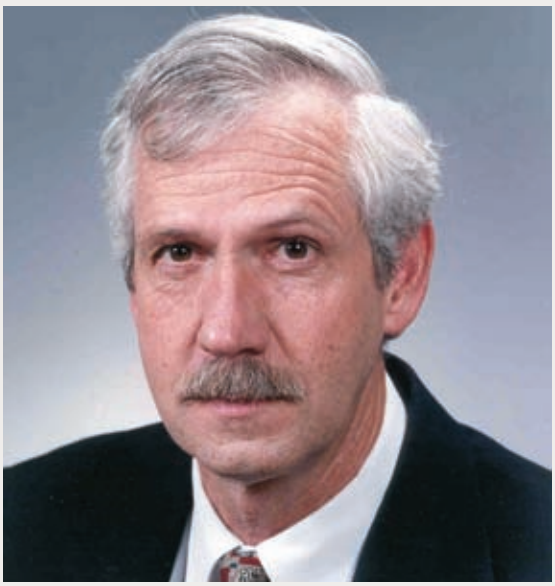
Jay Cohen
Under Secretary for Science and Technology, DHS

Message from the DHS Standards Executive

By Bert Coursey
Standards Executive, Department of Homeland Security

DHS's mission is to protect the nation from attack by terrorists and to prepare our nation to respond to and mitigate both terrorist attacks and natural disasters. Secretary Michael Chertoff has outlined these straightforward priority goals for the department:

- Keep terrorists, criminals, and unlawful entrants out of the United States
- Prevent dangerous materials, weapons, and illicit drugs from entering the country
- Strengthen screening of workers and travelers
- Secure critical infrastructure
- Build a nimble, effective emergency response system and culture of preparedness
- Strengthen core management to ensure that DHS is a great organization.



Bert Coursey
Standards Executive, DHS

Accomplishing these goals requires the nation—not just the department—to make a concerted effort to develop a measurements and standards infrastructure for homeland security. For example, the first goal will require working with other federal agencies to build on existing standards for law enforcement and data sharing. The second goal will require development of new standards for equipment used to detect chemical, biological, radiological, nuclear, and explosive agents. The third goal will require enhanced methods for biometric identification and credentialing of workers and travelers. The fourth goal will require standards, mainly for use in the private sector, on assessing and managing risks to critical infrastructure; these will build on existing safety and security standards, with the added dimension of protecting against terrorist attacks. The fifth goal will require the nation to strengthen and build on our public health and safety standards and make them an integral part of a culture of preparedness for incidents of national significance, whether they are man-made or natural disasters. The last goal will require management standards, which are essential to a well-disciplined and effective agency of 184,000 employees.

DHS does not have statutory authority to promulgate standards except in limited legacy programs such as U.S. Coast Guard marine safety equipment. Thus, a program to develop national standards for homeland security will be built on cooperation and coordination of standards activities at several different levels:

- *DHS Standards Council.* The DHS Standards Council—established in August 2006 with senior staff members from each DHS component—focuses on intra-agency standards. The council was needed because standards policies differed greatly among the legacy agencies that now constitute DHS. Some of these agencies, such as the U.S. Coast Guard, were closely aligned with DoD and already had a robust standards program. Other components, such as the Transportation Security Administration and the Federal Emergency Management Agency, built on existing programs for standards for transportation security and emergency preparedness and response, respectively. New activities in DHS required immediate focus on standards development, and teams were formed to address standards for detection of chemical, biological, radiological, nuclear, and explosive agents, as well as for response, recovery, and forensics. The DHS Standards Council provides a forum for representatives from each of these disciplines to discuss evolving policies on standards for the department.
- *Interagency Committee on Standards Policy (ICSP).* The ICSP focuses on interagency standards, in compliance with Section 12(d) of the National Technology Transfer and Advancement Act (Public Law 104-113), which directs federal departments and agencies to achieve a greater reliance on voluntary consensus standards. The use of voluntary consensus standards is also required by Office of Management and Budget (OMB) Circular A-119, "Federal Participation in the Development and Use of

Voluntary Consensus Standards and in Conformity Assessment Activities" (revised February 10, 1998). In addition, Circular A-119 spells out responsibilities for a Standards Executive for agencies that have a significant use and interest in standards. DHS is an active participant on the ICSP, in compliance with policy established in the Homeland Security Act of 2002 (Public Law 107-296). For instance, the DHS Standards Executive has hosted meetings of the ICSP and prepared the report to OMB on DHS's use of voluntary consensus standards.

- *American National Standards Institute's Homeland Security Standards Panel (ANSI-HSSP).* This panel, actively supported by the DHS Office of Standards, was formed in February 2003 (before the formation of DHS) as a public-private partnership to coordinate the development of non-government standards for homeland security. The HSSP identifies existing consensus standards, or, if none exist, assists DHS and other entities with accelerating the development and adoption of consensus standards critical to homeland security. The HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area.

The ANSI process for American national standards (and international processes through the ISO and International Electrotechnical Commission) ensures consensus in the development of standards, such that all the stakeholders have a chance to provide input.

Participants in voluntary standards processes are well aware of the perception that the consensus standards process is slow. The canon of standards for the nation contains more than 100,000 government and non-government standards. Moreover, the processes for revising standards or creating new ones vary from one agency to another and from one standards developing organization (SDO) to another.

As a nation, we realized after 9/11 that the gaps in standards had to be filled quickly. But, creating standards on a fast track is not the same as cutting corners. Two fundamental criteria for standards must be met: consensus and credibility. The ANSI process for American national standards (and international processes through the ISO and International Electrotechnical Commission) ensures consensus in the development of standards, such that all the stakeholders have a chance to provide input. Credibility relates to ac-

ceptance by the user community; this community—whether it is in the public or private sector—will not accept a standard unless the developers can demonstrate that they have relevant qualifications.

When ANSI established the HSSP, several ANSI-accredited SDOs reorganized their standards activities to focus on emerging needs for standards for homeland security. They include the National Fire Protection Association (NFPA), International Committee for Information Technology Standards (INCITS), Institute of Electrical and Electronics Engineers, Inc. (IEEE), and ASTM International.

NFPA has developed scores of useful standards, such as NFPA 1600, "Standard on Disaster/Emergency Management and Business Continuity Programs." The department adopted NFPA 1600 following the recommendation of the 9/11 Commission.

INCITS standards are particularly important for biometrics and travel documents. DHS worked with INCITS on the development and adoption of INCITS 385, "Information Technology—Face Recognition Format for Data Interchange."

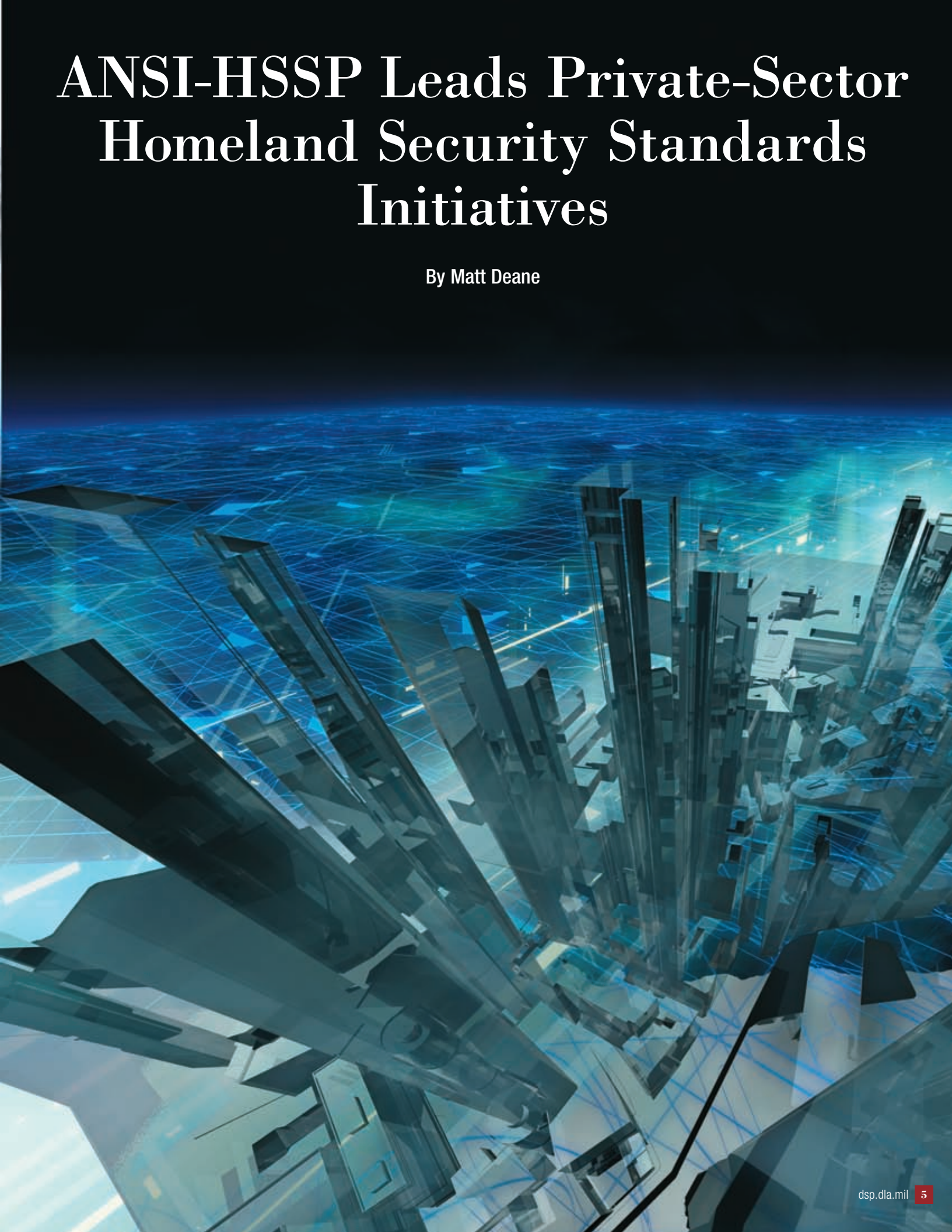
Two other standards activities used a fast-track process to develop important standards for detecting chemical, biological, radiological, and nuclear agents. One, the IEEE/ANSI N42 committee, developed standards for radiation detectors in 12–15 months. The other, a cooperative effort of multiple federal agencies, AOAC International, and ASTM International, took just 18 months to develop a standard method for sampling powder suspected of being a biological agent. The fast-track process still allowed time for all stakeholders (state and local emergency responders, manufacturers, federal and state agencies) to meet at regular intervals and participate in developing the standards.

These standards are addressed in two articles in this issue. Other articles highlight the work of our partners in DoD and the National Institute of Standards and Technology in developing standards to enhance security. These include standards for personal protective equipment, communications, access control, radio-frequency identification, emergency management, biometrics, and urban search and rescue robots. Still, the information in this issue is only a snapshot of the many standards development activities under way in DHS components; in other federal agencies such as the Centers for Disease Control and Prevention, Environmental Protection Agency, Department of Justice, and Department of Transportation; and in the technical committees of the SDOs that are participating in the ANSI-HSSP.

DHS is the newest federal department and one of the largest. But, we are starting with a strong commitment to standards and benefit from a nation that has enormous resources to bring to bear on the problems it faces.

ANSI-HSSP Leads Private-Sector Homeland Security Standards Initiatives

By Matt Deane



An often overlooked but crucial component of our nation's homeland security is voluntary consensus standards and the related compliance programs. When, in 2002, the National Strategy for Homeland Security identified the need for standards to support homeland security and emergency preparedness, the standardization community rallied to address the needs of security stakeholders in the United States and around the globe. Although there is still work to be done, much has already been accomplished. One of the key contributors is the Homeland Security Standards Panel (HSSP) of the American National Standards Institute (ANSI).

About the ANSI-HSSP

ANSI, facilitator of the U.S. standards and conformity assessment system, established the HSSP in February 2003. The first of ANSI's five current standards panels, the ANSI-HSSP was created in direct response to a call from government and industry for standards and conformity assessment programs that would support the nation's stakeholders and the burgeoning homeland security industry.

Specifically, the panel identifies and promotes consensus standards that are critical to homeland security. Where there are gaps, the ANSI-HSSP assists the Department of Homeland Security (DHS) Directorate for Science and Technology's (S&T's) Office of Standards, as well as other stakeholders, by accelerating the development and adoption of the consensus standards that are needed. The ANSI-HSSP provides DHS with a single forum in which officials can interact with the broad homeland security standards community.

One of the panel's primary goals is to promote a positive and cooperative partnership between the public and private sectors. Successful collaboration with various security initiatives has solidified the panel's reputation as the place to go for consideration of high-level homeland security standards matters.

The panel builds upon ANSI's expertise and reputation as an open and neutral forum, conducting its work primarily through plenary meetings and workshops. Hundreds of homeland security experts from government and from a broad cross-section of industrial sectors have become actively engaged in the five plenary meetings and workshop activities that are described in this article. This interaction has led to many instances in which groups were able to learn of complementary efforts and make contacts that foster collaboration.

The commitment of ANSI and the standardization community is documented in *United States Standards Strategy*, which highlights the importance of standards coordination to address national priorities such as homeland security.

Examples of success can be found in the alignment of resources for security-related conferences and initiatives and in the growing numbers of participants engaged in the technical activities of standards developers. The ANSI-HSSP secretary serves as a resource for homeland security standards inquiries—connecting people and groups working on similar issues.

To this end, and with support from DHS, ANSI also developed the Homeland Security Standards Database (HSSD) (www.hssd.us) as a one-stop comprehensive resource for homeland security standards information. The HSSD contains records pertaining to thousands of standards categorized via a DHS-developed taxonomy. This free database provides guidance to state and local first-response agencies that need standards for an expansive array of new security, personal-protective, and communication products. As the information in the HSSD continues to evolve, ANSI is working with other online systems to share and leverage homeland security information.

Considering recommendations from S&T's Office of Standards, DHS has adopted a number of these standards and guidelines to assist local, state, and federal procurement officials and manufacturers. Included are American National Standards from ANSI-accredited standards developing organizations such as the National Fire Protection Association (NFPA) and the International Safety Equipment Association on personal protective equipment for first responders, the Institute of Electrical and Electronics Engineers on radiological and nuclear detection equipment, and the InterNational Committee for Information Technology Standards on biometrics.

Working closely with ANSI, the DHS S&T's Office of Standards planned the ANSI-HSSP September 2005 plenary meeting not only to bring together the homeland security standards community, but also to facilitate contacts between security user requirements forums and standards developers. The user requirements forums that participated at that meeting, and that continue to work with ANSI-HSSP, are the Association of Public Safety Communications Officials International, Biometrics Consortium, InterAgency Board for Equipment Standardization and Interoperability, Council on Ionizing Radiation and Measurement Standards, Process Control System Forum, and Federal Geographic Data Committee.

A focus on emergency preparedness at the September 2006 plenary meeting provided DHS with the opportunity to brief the standards community and receive feedback on preparedness activities such as the National Incident Management System, National Infrastructure Protection Plan, National Preparedness Goal, and Target Capabilities List (TCL).

Security standardization is a global effort, and the ANSI-HSSP has actively incorporated international outreach into its program of work. The panel engages regularly with the Strategic Advisory Group on Security (SAG-S), which was formed by the ISO, International Electrotechnical Commission, and International Telecommunication Union. Chaired by Dr. George Arnold of the National Institute of Standards and Technology, the SAG-S helps to oversee standardization activities relevant to the field of security in each of the three parent organizations.

In addition, partnerships have been forged between the ANSI-HSSP and the European standards organizations, including the European Committee for Standardization working group on "Protection and Security of the Citizen" and with Standards Australia's National Centre for Security Standards.

ANSI-HSSP Workshop Deliverables

As mentioned earlier, workshops are the panel's primary mechanism to address homeland security subject areas. Workshops typically entail a series of meetings during which subject matter experts examine a subject and produce a final report and recommendations. The following areas have been examined by panel workshops.

EMERGENCY PREPAREDNESS AND BUSINESS CONTINUITY

At the request of the 9/11 Commission, the ANSI-HSSP organized a workshop with the goal of identifying an existing standard, or creating an action plan for developing one, in the area of private-sector emergency preparedness and business continuity. The workshop recommended NFPA 1600, "Standard on Disaster/Emergency Management and Business Continuity Programs." ANSI's recommendation was included in the final report published by the 9/11 Commission. ANSI/NFPA 1600 has since been promoted by the panel, referenced in national campaigns, and included in national legislation on the subject of preparedness.

As the U.S. member body representative in the ISO, ANSI led an ISO-sponsored meeting on emergency preparedness in April 2006. The event was hosted by New York University's International Center for Enterprise Preparedness (InterCEP)—a member of the ANSI-HSSP Steering Committee—at its facility in Florence, Italy. More than 70 emergency management and business continuity professionals from 16 countries gathered to discuss this subject and the role of standardization at the international level. Five prominent national standards and guidance documents from around the world were reviewed (including ANSI/NFPA 1600); the final outcome was the publication of ISO International Workshop Agreement 5:2006, "Emergency Preparedness."

Following the events of Hurricane Katrina, the ANSI-HSSP convened a workshop to further examine emergency preparedness and the role of standards and conformity assessment programs. More than 100 experts from dozens of public- and private-sector stakeholder organizations and the professional preparedness and business continuity community were involved in the 10-month effort to produce a final workshop report. The workshop once again recognized ANSI/NFPA 1600 as the preeminent standard on emergency preparedness and business continuity. The Hurricane Katrina workshop report highlighted the value of compliance with ANSI/NFPA 1600, recommended updates for NFPA to consider during the standard's next review cycle, and identified areas where supplemental standards are needed.

ENTERPRISE POWER SECURITY AND CONTINUITY

Continual availability of electric power at the enterprise level is essential for business functions, safety, and the public well-being. Yet many practical challenges exist related to keeping critical operations, equipment, or facilities powered when the

Perimeter security involves rapidly advancing technology that is needed to complement and enhance traditional means of perimeter security such as guards, gates, and personnel verification, as well as other newer technologies.

electric grid is not available. The ANSI-HSSP workshop report on standardization for enterprise power security and continuity, published in May 2006, defined the relevant standards and guidance documents pertaining to this topic. Like other reports, the outcome document also identified gaps in standards and conformity assessment programs, made a series of recommendations for addressing these gaps, and identified areas in which further work was needed.

PERIMETER SECURITY

Perimeter security involves rapidly advancing technology that is needed to complement and enhance traditional means of perimeter security such as guards, gates, and personnel verification, as well as other newer technologies. In January 2007, the ANSI-HSSP's final workshop report on perimeter security standardization provided basic concepts and definitions for perimeter security, presented conceptual frameworks for considering the need for standards for perimeter security, and in-

cluded a number of specific issues, factors, and recommendations that standards developing organizations should consider when developing perimeter security standards.

EMERGENCY COMMUNICATIONS

The ANSI-HSSP workshop on emergency communications standardization focused on standards that would help protect the safety of citizens and critical infrastructure, as well as support response and recovery efforts for emergency communications. The report focused on three categories:

- Individuals/organizations-to-individuals/organizations (including employer-to-employee, employer-to-employer, and employer-to-customer)
- Individuals/organizations-to-government
- Government-to-individuals/organizations. (Government-to-government emergency communications are being addressed by other programs such as DHS SAFECOM.)

The workshop considered the June 2006 release of an Executive order on public alerts and warning systems; the October 2006 Warning, Alert and Response Network Act; the Federal Communications Commission's Commercial Mobile Service Alert Advisory Committee; and legislation to create the Office of Emergency Communications within DHS.

Related discussions on citizen preparedness led to the creation of a targeted resource web page on the ANSI-HSSP website (www.ansi.org/hssp).

TRAINING PROGRAMS FOR FIRST RESPONSE TO WEAPONS OF MASS DESTRUCTION EVENTS

To assist the first-responder community, another ANSI-HSSP workshop focused on standards that support training programs and that can be used to help measure their effectiveness. This workshop's report, published in February 2006, contains a standards matrix that organizes existing standards by first-responder category, cross-referenced against the DHS TCL. The report also examines the important role of accreditation and certification to identified standards.

BIOLOGICAL AND CHEMICAL THREAT AGENTS

One of ANSI-HSSP's largest reports addressed the important concern of biological and chemical threat agents. A 400-page final report published in December 2004 contains an index of relevant published standards and projects under development, categorized by a subject-specific taxonomy developed by workshop participants.

BIOMETRICS

The ANSI-HSSP's final report on biometrics standardization—the foundation of many highly secure identification and verification solutions—was published in April 2004. In addition to highlighting existing standards and projects under development, the report recommended addressing five key issues related to biometric standardization and conformity assessment.

Looking Forward

Much progress has been made, but much more needs to be done. The following new focus areas are being explored through the ANSI-HSSP workshop process:

- Public transit security (nationally through the panel and internationally via an ANSI-hosted World Standards Cooperation workshop)
- Credentialing and access control for disaster management
- Security/emergency preparedness for persons with special needs and disabilities
- Mobilization of private-sector resources to disasters.

ANSI invites all interested stakeholders to join in the panel's examination of the vast landscape of homeland security and to participate in the development of standards-based solutions that address this critical national priority.

Information about the ANSI-HSSP, as well as reports and recommendations from all the workshops described above, can be found on the HSSP website (www.ansi.org/hssp). Questions or comments can be directed to Matt Deane (212-642-4992 or mdeane@ansi.org).

About the Author

Matt Deane is the director of homeland security standards at the American National Standards Institute.

Development of Standards for Chemical and Biological Protective Equipment for Civilian First Responders

By Elaine Stewart-Craig

Performance standards for military protective equipment have existed since World War I, but until recently, no such standards existed for chemical and biological (CB) protective equipment used by civilian first responders. The U.S. Army's Edgewood Chemical Biological Center (ECBC), with its long experience in researching and testing CB agents, was selected to help remedy this situation.

Background

ECBC, DoD's premier chemical and biological defense laboratory, has some 90 years of expertise in providing chemical detection, protection, and decontamination equipment to the military. In 1996, ECBC began assisting the civilian responder community through its participation in the Domestic Preparedness Program (DPP). According to Public Law 104-201 (National Defense Authorization Act for Fiscal Year 1997), the DPP was to enhance the capabilities of the federal, state, and local emergency response communities to respond to chemical, biological, radiological, and nuclear (CBRN) terrorism incidents. One task, the DPP Expert Assistance (Test Equipment) Program, tested commercially available CB protective equipment and provided test results to the response community. However, the test results were open to interpretation because of the lack of performance standards for civilian CB protective equipment.

Why are performance standards so important for the community of first responders? They specify the minimum acceptable performance requirements for equipment intended to be used in a CB event and the evaluation and testing criteria that will be used to ensure that equipment manufacturers meet those requirements. In other words, they ensure that equipment meets minimum quality, reliability, and interoperability requirements. Without such standards, responders have no assurance that the equipment they purchase will meet their needs: detect CB agents, protect them from those agents, and decontaminate them if they are exposed to such agents.

Leveraging ECBC's Expertise

To develop the needed standards for CB protective equipment used by the civilian response community, the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) partnered with ECBC to leverage its long history of military expertise in CB countermeasures. The ECBC established a Standards Development Team consisting of four technical-support components: detection, personal protective equipment (PPE), respirators, and personnel decontamination.

To ensure that the performance standards address the responders' needs, ECBC is a member of the InterAgency Board (IAB) for Equipment Standardization and Interoperability. In addition, the team works with standards developing organizations such as the National Fire Protection Association (NFPA), American National Standards Institute (ANSI), AOAC International, and ASTM International.

ECBC Successes and Next Steps

DETECTION

The detection component of ECBC's team is responsible for developing performance standards for area warning and personal detection equipment. The team has leveraged efforts initiated by the PPE component of the team to determine the concentration of chemical warfare agents (CWAs) that pose health risks. That determination will lead to the required detection levels.

Utilizing the priorities identified by the IAB, the team developed, and staffed through ASTM, the first standard for a Chemical Warfare Vapor Detector (CWVD). The published CWVD standard is a broad-based performance document that defines CWA detector performance criteria, as well as environmental, interface, and safety requirements. The team modified an ECBC CWA test protocol that was developed and used during the DPP Expert Assistance Program and performed the validation associated with the CWVD standard. The team partnered with an independent, nationally recognized test laboratory for the development and validation of all non-CWA test methods associated with the CWVD standard. The validation process will ultimately pave the way for DHS, NIST, and ANSI discussions regarding accreditation and development of a certification program. The standard development and certification of future chemical and biological detectors will follow the same protocol.

Subsequent chemical detection standards will narrow the field-of-use parameters and define specific-use requirements based on IAB prioritization. Near-term standards development efforts will focus on the identification of toxic industrial chemicals (TICs) and toxic industrial materials (TIMs), which pose a threat to first responders. Future detection standards will focus on biological detection devices.

In the long term, standardized reference materials will be needed for TICs, TIMs, and biological agents. The U.S. Army Chemical Agent Standard Analytical Reference Materiels program will likely be leveraged and potentially expanded to include those materials.

PERSONAL PROTECTIVE EQUIPMENT

The team has several ongoing PPE projects, including validation of Man-in-Simulant Test (MIST) procedures, identification of dermal vapor hazards for TICs, development of test methods for TICs, and support of the Law Enforcement CB Protective Ensemble Standards.

The team tested MIST procedures at the U.S. Army Dugway Proving Ground (DPG), using five commercially available protective ensembles and one baseline ensemble. The purpose of the test was to evaluate the overall protection level on an entire protective ensemble by having people wear the ensemble, including a certified respirator, and then perform predetermined motions in a chamber full of an agent simulant. This method has been previously used to test

military ensembles, but was modified to address the different requirements of the emergency response community. The work at DPG was to validate the procedures identified in the draft ASTM standard. The test was planned and conducted prior to finalization of ASTM F2588-06, "Standard Test Method for Man-in-Simulant Test (MIST) for Protective Ensembles," and incorporation of the MIST procedure into NFPA 1994, "Protective Ensembles for First Responders to CBRN Terrorism Incidents," 2007 edition. The test report, released in June 2007, provides recommendations for modifying the current standards. The test results and recommendations were briefed at the ASTM International F233000 subcommittee meeting in June 2007.

During the past few years, the nation has witnessed several large-scale incidents involving hazardous, commercially available industrial chemicals. The incidents prompted the PPE team to begin investigating TICs with an initial focus on dermal toxicity. The team, using the technical expertise of the U.S. Army Center for Health Promotion and Preventive Medicine, identified the large data gap for dermal toxicity of TICs and initiated a multiphased project. The first phase was to identify the dermal toxicity of a selected number of TICs, with the overall goal of ensuring that the TICs identified for testing are appropriate. Additional phases of the project will determine the dermal toxicity levels for additional TICs.

In conjunction with the TIC identification is the validation of standardized test methods to ensure that the TIC permeation requirements can be tested consistently in accordance with current ASTM standards. The chemical makeup of each TIC is unique; therefore, the testing procedures need to be validated for each of the TICs. The first phase of the project was recently completed. Using a select group of TICs, the team identified specific solvents, sorbent materials, and analytical instruments required when performing testing on each of those TICs. The team determined that the time and expense required to conduct permeation testing until the TICs break through the materials were unwarranted because the material performance requirement is for a specific amount of time. A real-time testing system is now being developed, and a prototype will be completed in late 2007. The full test system is anticipated to be ready for use in late 2008.

A program to identify potential CWA simulants that can be used by ensemble manufacturers is ongoing. The intent of the program is to identify chemicals that can be used by the material and ensemble manufacturers for a pretest to indicate which materials are unlikely to pass the CWA testing requirements; this will enable manufacturers to concentrate on materials that have a higher chance of passing the CWA test requirements. The initial program results are anticipated to be available in late 2008.

The team is providing technical support to the National Institute of Justice's Law Enforcement CB Protective Ensembles standards' program. ECBC will provide technical information on the hazard analysis already performed for the standards development program as well as in-

formation collected from ECBC ergonomic studies on specific concerns and issues brought up by the law enforcement community. These ergonomic studies include research on range of motion, mass properties of selected equipment and their effects on head and neck strain, hearing effects, aural effects, and noise effects that occur while wearing various PPE configurations and law enforcement items (protective armor, vision goggles, radio transmitters, and so on). Testing is being conducted at ECBC to document the effects of the add-on items on the protection factor of the respirators. MIST will be performed to document any effects on the overall CB protection level when these items are added on. The law enforcement community has expressed a concern that the current ensemble designs and standards do not address the effects of the add-on equipment. These test results will be used for the development of future PPE standards in both law enforcement and other response areas involving CB protection.

RESPIRATORS

The ECBC team is providing technical support for the development of chemical standards and test methods for respirators. It also is performing selected portions of the certification process for candidate respirators. For both of these tasks, the ECBC is working with the National Personal Protective Technology Laboratory (NPPTL), a laboratory within the National Institute for Occupational Safety and Health.

The ECBC is using its expertise with military CB protective masks to assist NPPTL with the development of various testing requirements for respirators. NPPTL was able to modify the military test requirements and ECBC test methods for application to civilian respirators. ECBC validates the test procedures prior to approval of the consensus standard. This modification and validation process was used to develop the CBRN standards for the Self-Contained Breathing Apparatus, the Air Purifying Respirator, and the Powered, Air-Purifying Respirator. Ongoing activities include development of requirements and test procedures for the Closed Circuit Self Contained Self Rescuers.

The team is also active in the respirator certification process. The ECBC laboratories provide testing capabilities to NPPTL for environmental, protection factor, and CWA testing. The NPPTL uses the results of the ECBC testing in conjunction with other tests results to determine whether or not a respirator will be certified to their CBRN standard.

PERSONNEL DECONTAMINATION

This component of the ECBC team is developing performance standards for personnel decontamination equipment. To develop these standards, the team must determine the expected level of contamination for a person in the contaminated environment and the required level of decontamination when the person exits the decontamination system—how clean the person must be.

Early investigation by the team revealed no existing model for categorizing indoor chemical events. Therefore, the modelers modified the parameters of the outdoor model to account for indoor environments. The resultant preliminary model was used to generate expected contamination levels for nerve and blister chemical warfare agents and selected TICs in multiple indoor scenarios.

The team is verifying its indoor model using simulants. The verification testing will be expanded to incorporate CWA comparison testing within the next 8 to 12 months. The team's intention is to modify the existing model to include a scenario for a large enclosed space.

Conclusion

The establishment of consensus standards for civilian CB protective equipment is essential in order for the response community—including law enforcement, fire service, hazardous materials, and emergency medical services personnel—to have confidence that the equipment it purchases will meet its needs: detect CB agents, protect responders from those agents, and decontaminate them if they are exposed to such agents. ECBC will continue to support our nation's responder community in the development of CB protective equipment standards.

The standards and results of subsequent performance evaluations will be disseminated to the public safety community (to help them make informed equipment purchases) and to manufacturers, developers, and the test and evaluation community (to enable them to ensure product compliance). The ultimate goal is to link performance standards and certifications with federal equipment grants programs. Ultimately, all CB protective equipment purchased using DHS grant money will require certification.

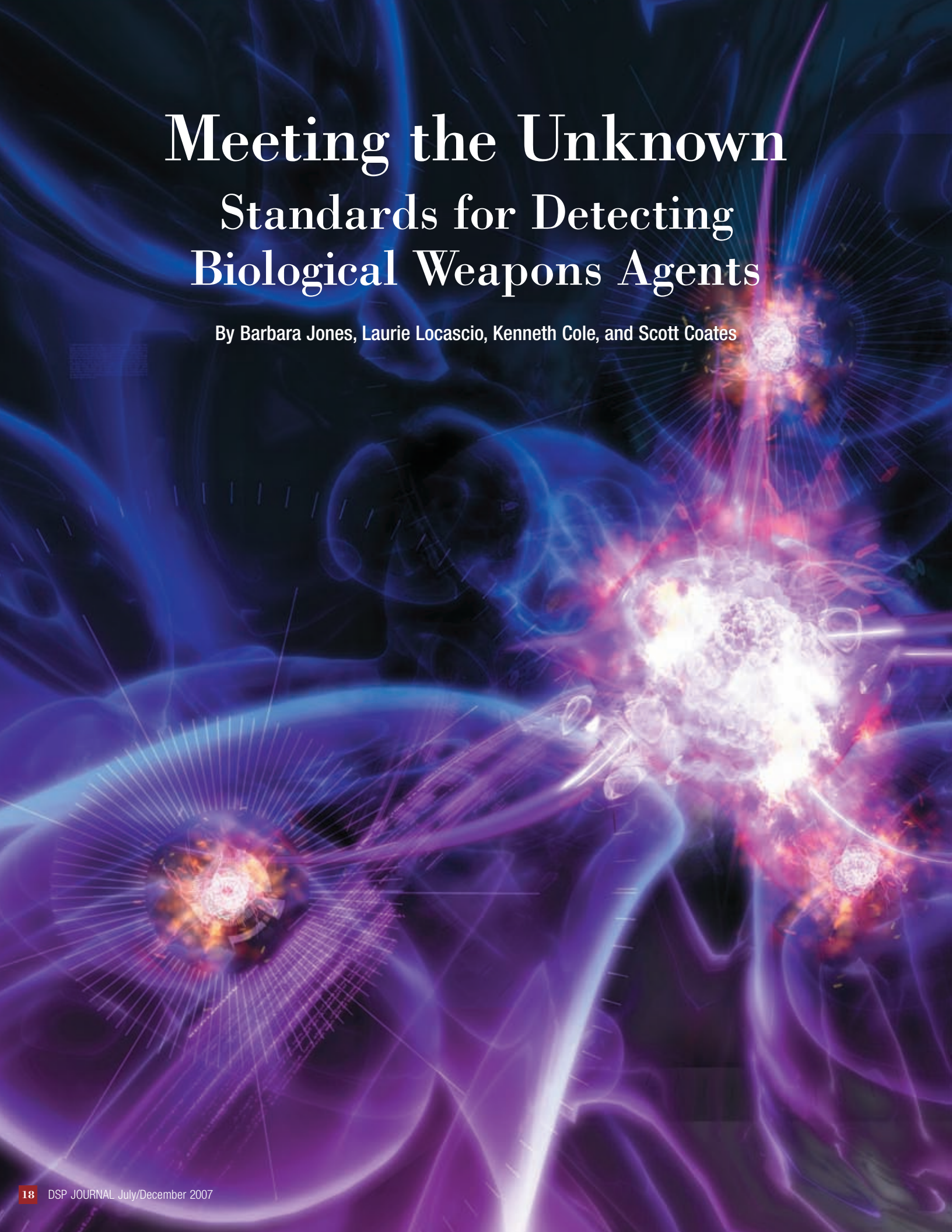
About the Author

Elaine Stewart-Craig is a special projects group leader at ECBC. In addition, she is the federal co-chair of the Detection and Decontamination Subgroup of the InterAgency Board for Equipment Standardization and Interoperability.

Meeting the Unknown

Standards for Detecting Biological Weapons Agents

By Barbara Jones, Laurie Locascio, Kenneth Cole, and Scott Coates



In its 2004 report, *Mapping the Global Future*, the National Intelligence Council acknowledged that "development in [chemical weapons] and [biological weapons] agents and the proliferation of related expertise will pose a substantial threat, particularly from terrorists." More alarmingly, it warned that "bioterrorism appears particularly suited to the smaller better-informed groups…. Terrorist use of biological agents is therefore likely and the range of options will grow."

The threat of bioterrorism is, unfortunately, one of many unknowns. The detection of biological weapons agents (BWAs) depends on proper techniques for sampling (picking the agent up from surfaces), transportation (keeping the organism alive during transport), and analysis. Standards for all aspects of BWA detection are critical to reduce the chaos and unknowns and to provide a foundation of tools that can take some of them out of the equation.

The Directorate for Science and Technology (S&T) at the Department of Homeland Security (DHS) is developing a program in biological countermeasures standards that provides a foundation for BWA detection and will continue to expand and strengthen in the areas of decontamination and monitoring. S&T's efforts include a suite of standards for sampling suspected BWAs; methods for characterizing *Bacillus anthracis* (BA) and ricin, including a measurement service for testing and calibrating equipment; validation of sampling strategies; and development of acceptance criteria for hand-held assays (HHAs) for the detection of biological agents.

Standards for Sampling

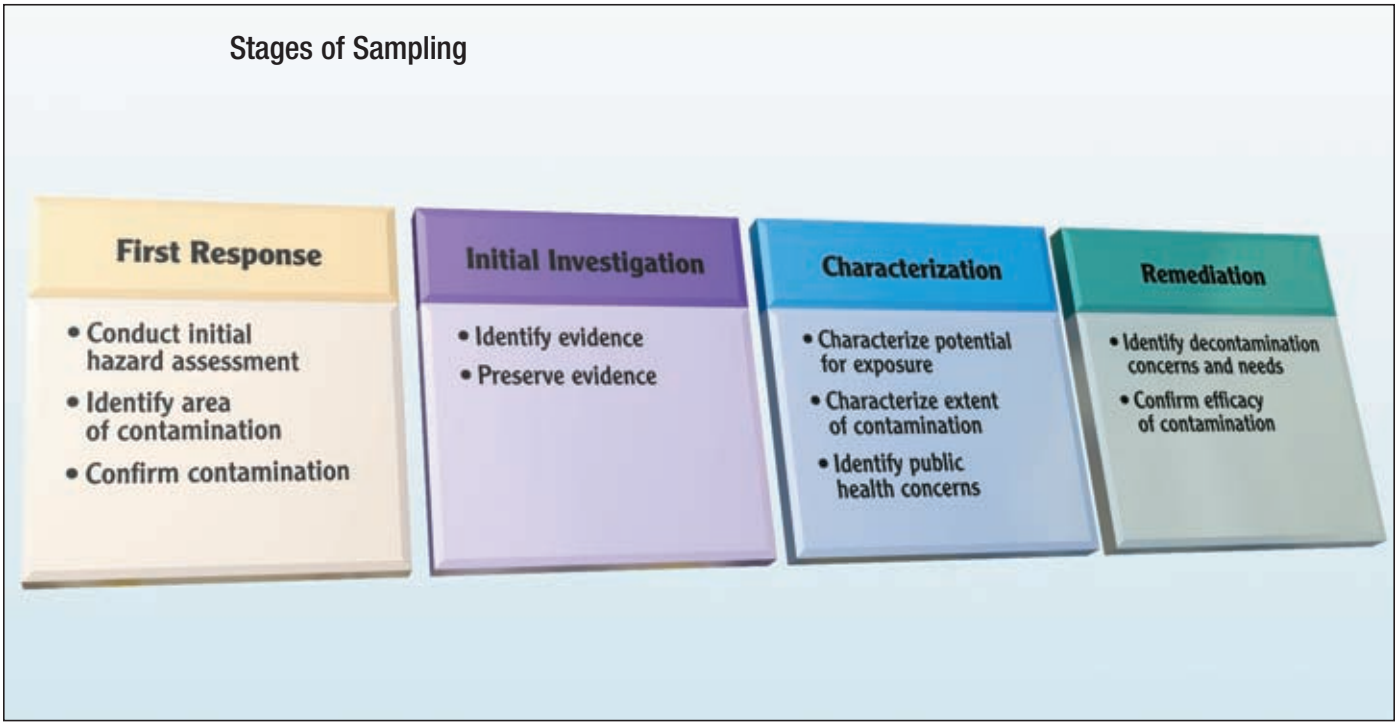
Samples from sites suspected of contamination are obtained for differing reasons. For example, samples taken for characterization or first response serve to confirm contamination, whereas samples taken after decontamination are used, in part, to clear a building for reoccupation. Standard procedures for the collection and sampling of suspected buildings and sites in the characterization phase are critical for accurate and incontrovertible analysis used in public health decisions and forensic documentation. And public health officials must have complete confidence in sample results before declaring that a building or site can be reoccupied. To provide a foundation of confidence in sampling results, DHS S&T continues to develop standards for sampling BWAs for use by first responders and others who may need to collect samples in buildings and sites suspected of contamination.

A major achievement in the area of sampling standards came in 2006 with the release of ASTM E2458, "Standard Practices for Bulk Sample Collection and Swab Sample Collection of Visible Powders Suspected of Being Biological Agents from Nonporous Surfaces." This standard was produced by a multiagency task group led

by the National Institute of Standards and Technology (NIST) and with representation from multiple federal agencies (Centers for Disease Control and Prevention, Environmental Protection Agency, Federal Bureau of Investigation, Department of Defense), the International Association of Fire Chiefs, the U.S. National Guard, and state and local public health and response agencies. E2458 was approved by the standards developing organizations, AOAC International and ASTM International, and released by ASTM within 1 year.

ASTM E2458 provides guidance on a method for collecting visible powders and on the use of residual powder for analysis with an HHA. The visible powder is first collected using a sterile laminated card and a swab, and is sealed with the card in a sterile specimen container. The residual powder can then be used for confirmatory testing using an HHA. The goal of the standard is to preserve samples for forensic evidence and public health actionable testing at a laboratory in the Laboratory Response Network while still allowing first responders to answer critical questions for local decision makers.

The collection method was rigorously validated at the U.S. Army Dugway Proving Grounds, as was the use of residual powder for HHA analysis. In the validation studies, the collection method was shown to be effective for bulk powder collection, and the residual powder was shown to be adequate for positive detection using an HHA known as the RAMP Anthrax Test. The DHS S&T has obtained an unlimited license from ASTM to allow first responders and others to download the standard free



of charge. The standard can be downloaded from www.astm.org/COMMIT/E54.htm.

Future efforts in sampling standards include standard methods for sampling both porous and nonporous surfaces and collection methods under varied environmental conditions.

Methods for Characterizing BWAs

As new technology is developed to detect and monitor biological contamination, the new instruments must be calibrated and, in some cases, assessed for their detection capabilities. To assess the detection capabilities of the instruments, the physical characteristics of the BWA analyte must be known and well documented. This is critical to allow comparisons between equipment and different lots of equipment used in detection.

To enhance measurement capabilities for BWAs, NIST has developed and published methods for characterizing the physical properties of BA spores and ricin. For example, because of their surface properties, BA spores disperse readily, making it difficult to recover samples from the environment. At the same time, those properties reflect the history of the material, providing important forensic data.

NIST also is developing protocols to provide measurement services for high-priority biological agents. Working with government and private-sector repositories to provide the analytical measurements to increase the confidence and reliability of BWA reference materials, these services will be made available to companies that make detection devices and to laboratories and personnel that are involved in the research and detection of biological threats.

Validation of Sampling Strategies

After the anthrax attacks in 2001, the Government Accountability Office (GAO) reviewed the process used for sampling a building suspected of contamination. In *Anthrax Detection: Agencies Need to Validate Sampling Activities in Order to Increase Confidence in Negative Results* (GAO-05-251), published in 2005, GAO argued the case for validated methods in all areas of sampling when contamination is suspected. One of the areas specifically addressed by the report was the need to validate whether probabilistic (random) sampling for the clearance of a building for reoccupation was needed. To assess not only this question but also the use of sampling strategies in several contamination scenarios, DHS and the Joint Program Executive Office for Chemical and Biological Weapons Detection are staging a real-world exercise using a BA simulant contamination of a mock office building. The exercise

will test sampling strategies in both overt and covert BWA dissemination scenarios and will allow the researchers to use tools such as the Visual Sampling Plan (VSP) software that was developed by the Pacific Northwest National Laboratory (PNNL) to generate probabilistic sampling site plans. In addition to the current sampling strategy methods, a Bayesian approach—an approach in which judgmental and probabilistic sampling are combined to provide a higher statistical confidence that a building or room is free from contamination—will be tested.

In addition to the real-world exercise, NIST and PNNL are working together to develop a "virtual contamination exercise" tool that will allow researchers to assess a multitude of contamination scenarios for the use of judgmental, probabilistic, and combination sampling strategies. Using an airflow and contaminant dispersal simulation software program called CONTAM, researchers at NIST can input BWA dissemination scenarios and "virtually" contaminate a building. Using the VSP software to generate probabilistic sample sites and experts to identify judgmental sampling

When contamination by BWAs is known or is suspected in a building, first responders would not be responsible for sampling that space or for making public health decisions about evacuation or treatment of occupants.

sites, researchers can predict whether contamination would be detected using current sampling methods. Using this tool, multiple building, airflow, contamination, and agent configurations can be assessed against sampling strategies. This will allow researchers to understand sampling parameters under more conditions than would be possible using real-world exercises.

The results of this testing will ultimately produce guidance on the use of judgmental and probabilistic sampling, or a combination, for the clearance of buildings for reoccupation under multiple conditions and could someday be used to prepare sampling plans for likely targets.

Acceptance Criteria for Hand-Held Assays

In the 2001 anthrax attacks using the U.S. Postal Service as a delivery route for a relatively few contaminated letters, the scale of contamination was fortunately con-

tained. A BWA attack on an urban area would be considerably less contained, and determining the extent of contamination and of decontamination efficacy after such a disaster would be a monumental undertaking. After the Hurricane Katrina disaster, a White House report, *The Federal Response to Hurricane Katrina: Lessons Learned*, concluded that the numbers of personnel trained in sampling for the Environmental Protection Agency were unable to rapidly assess the safety of the environment for reoccupation. In response to this finding, DHS has been called on to "improve the Federal government's capability to quickly gather environmental data and to provide the public and emergency responders the most accurate information available, to determine whether it is safe to operate in a disaster environment or to return after evacuation."

When contamination by BWAs is known or is suspected in a building, first responders would not be responsible for sampling that space or for making public health decisions about evacuation or treatment of occupants. Such was the case in the anthrax attacks in 2001. Because the responsibilities and actions of the first responders in such a case are well defined, it is often argued that HHAs to assess biological contamination are not necessary or needed by first responders. In fact, results from HHAs are not considered "public health actionable," thus sampling and analysis at a public health laboratory is necessary with or without rapid analysis results from an HHA.

But consider a scenario of a large-scale BWA attack. In such a scenario, it may be necessary to quickly assess large areas for contamination and quarantine or to monitor contamination in areas, considered to be "safe," that are being used for staging or reuniting families. It may be necessary to monitor hospitals for levels of contamination or to quickly identify safe areas for transportation of supplies or people. In a large-scale disaster scenario, it may not be reasonable to send samples to an overwhelmed public health laboratory and wait for results; in some cases, it will be necessary to have rapid information about contamination. In this situation, where HHAs may be the best tool for rapidly assessing the disaster environment, it is critical that the HHAs operate as advertised and that they can be relied upon for accurate results.

To provide the foundation for this need, DHS is developing criteria for the acceptance of HHAs through AOAC International. Acceptance criteria for both BA and ricin HHAs that include minimum detection levels, and minimum specificity (the ability to discriminate negative samples from true positive samples), have been developed by a consensus group that includes representatives from government, industry,

and emergency responder groups. These criteria, along with standardized evaluation study designs and instructions for standardized test materials, will be reviewed and approved by the AOAC Methods Committee on Biological Threat Agents (Committee L). These criteria will be published in the *Journal of the AOAC International* later this year and will be voluntary for the HHA manufacturers.

The Future of Bio Standards

DHS S&T will continue to strengthen the foundation that standards provide for the safety and security of the United States. Efforts to provide sampling standards will expand to include varied surfaces and contamination agents. Standards for detection of BWAs will expand to include long-range detection. Another area of concern is the threat of biological attacks on agriculture; DHS will work closely with the Department of Agriculture to develop standards for the decontamination of croplands after a BWA attack and standard methods for clearance of foods after suspected contamination. And as newer detection and monitoring technologies are developed, standards for the operation and acceptance for these technologies will also need to be addressed. These standards efforts and more will continue to provide the foundation needed by first responders, and others who are called to action in a disaster, to meet the unknown.

About the Authors

Barbara Jones is the scientific advisor for NIST's Biochemical Science Division. She serves on several federal agency task groups charged with developing standards and guidance for the detection of biological threat agents. Before joining NIST, Dr. Jones worked for many years in the areas of public health and disease prevention.

Laurie Locascio is the division chief of the Biochemical Science Division within the Chemical Science and Technology Laboratory at NIST. Dr. Locascio has published more than 90 scientific papers, and she has five issued patents and three pending patents in the fields of microfluidics and biosensors. She chairs the Division of Analytical Chemistry of the American Chemical Society.

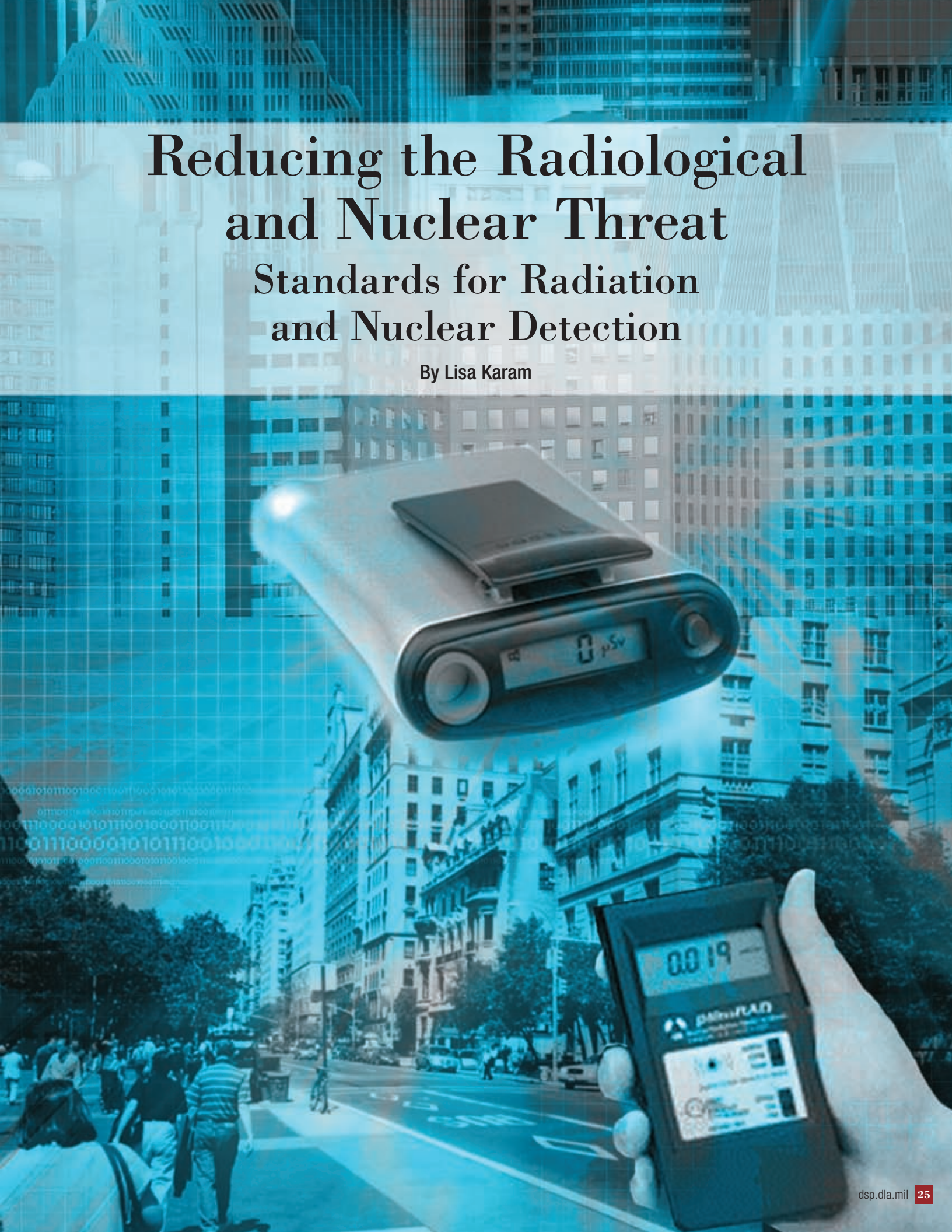
Kenneth Cole is a project leader in biodefense standards research at NIST's Biochemical Science Division. His research interests are to improve the characterization and stability of the biological reference materials used to test detection devices, environmental sampling, and remediation techniques.

Scott Coates is chief scientific officer for microbiology at AOAC International.

Reducing the Radiological and Nuclear Threat

Standards for Radiation and Nuclear Detection

By Lisa Karam



A multiyear effort to develop standards for radiation and nuclear detection for homeland security, begun in early 2002, has led to a comprehensive support system for the development, testing, and validation of effective prevention, detection, response, recovery, and forensics tools for detecting radiological and nuclear materials. The support system also provides the key measurement infrastructure to address existing and new types of radiation sensors, data analysis techniques, decontamination methods, and protective equipment.

Although the dreadful events of 9/11 fortunately did not involve radiological or nuclear devices, the potential threat from such devices has led to the inclusion in Homeland Security Presidential Directives of two scenarios, one involving radiological dispersal devices (RDDs or "dirty bombs") and the other, improvised nuclear devices (INDs). The impact of an IND incident in the United States is almost unimaginable. Even with the less directly destructive (yet perhaps more likely) use of a dirty bomb, the disruption to commerce, trade, and the way of life in the region in which the RDD incident occurred would be monumental. The subsequent resulting and perceived radioactive contamination of a large number of people in a large urban area is a recognized issue. To address that issue, security personnel (such as at ports and border crossings) and emergency responders must be properly equipped and trained to prevent, respond to, or mitigate a potential radiological or nuclear event. Only through the efficient and reliable detection of materials that could be used to bring about such events could the United States be certain to prevent the disastrous impact resulting from them.

The initial line of protection against an RDD or an IND comprises the people and groups (Coast Guard, port control, immigration, etc.) who, as part of controlling import and entry into the United States, would be the first to detect, recognize, and respond to the presence and movement of radioactive or nuclear materials via shipment, cargo, or individuals. Local law enforcement personnel, firefighters, and public health workers would join in responding to this presence, or any subsequent incident.

Anyone involved in using radiation detection instrumentation for the prevention or response to a radiological or nuclear event must have appropriate, reliable equipment and the proper training to maintain and use it, as well as the training to use the data coming from the equipment. In addition, federal, state, and local governments, which provide funds to equip responders, require assistance and guidance for purchasing detectors for a potentially wide range of radiation levels. As Figure 1 shows, instrumentation is available to detect radiation from very low (near-background level) to the highest saturation levels.

FIGURE 1. Detectors for Response and Mitigation

National standards, and their validation, for radiation and nuclear detection instrumentation performance, as used for homeland security applications, provide users with confidence that deployed technologies will perform reliably and as intended. To be effective, standards need to be developed in a collaborative environment that includes

- users (identifying needs and requirements),
- manufacturers (providing insight on current and state-of-the-art capabilities of equipment),
- researchers (suggesting potential technical improvements and evolution), and
- government entities (addressing regulatory issues and providing funding).

A major concern in tracking the movement of radiation into and throughout the United States is the sheer amount of radioactive material that is present and available. Easily transported radioactive materials are common in industry (such as Am-241, used in smoke detectors) and medicine (such as Tc-99m and Tl-201, used in cardiovascular imaging). For a period of some weeks after a nuclear medicine or imaging procedure, an individual can be radioactive enough for detection. The "specific" sources are in addition to the natural background radiation detectable by conventionally deployed radiation detectors.

The detectors at potential entry points and other areas of interest (such as sports arenas) and detectors engineered for use in a laboratory (a controlled environment) by technically trained users such as health physicists are susceptible to "nuisance" and background alarms, indicating a possible threat when none exists. In fact, until the first standards were published in 2003 and 2004, no performance standards were

Background Radiation

Background radiation comes from space ("cosmic radiation") and, on Earth, from such sources as radon in the air, building materials, and naturally occurring radioactive materials like bananas and fertilizer transported in trucks and trains. Background radiation fills the environment and provides a dose of up to 2.4 millisievert per year per person. This can be the same type of radiation as that considered to be threat level by less-sophisticated instrumentation or instruments whose parameters are set to an extremely sensitive level. (For more information, see United Nations Scientific Committee on the Effects of Atomic Radiation, UNSCEAR 2000, http://www.unscear.org/unscear/en/publications/2000_1.html.)

available to support the use of radiation detection equipment in homeland security applications for prevention, protection, response, and cleanup.

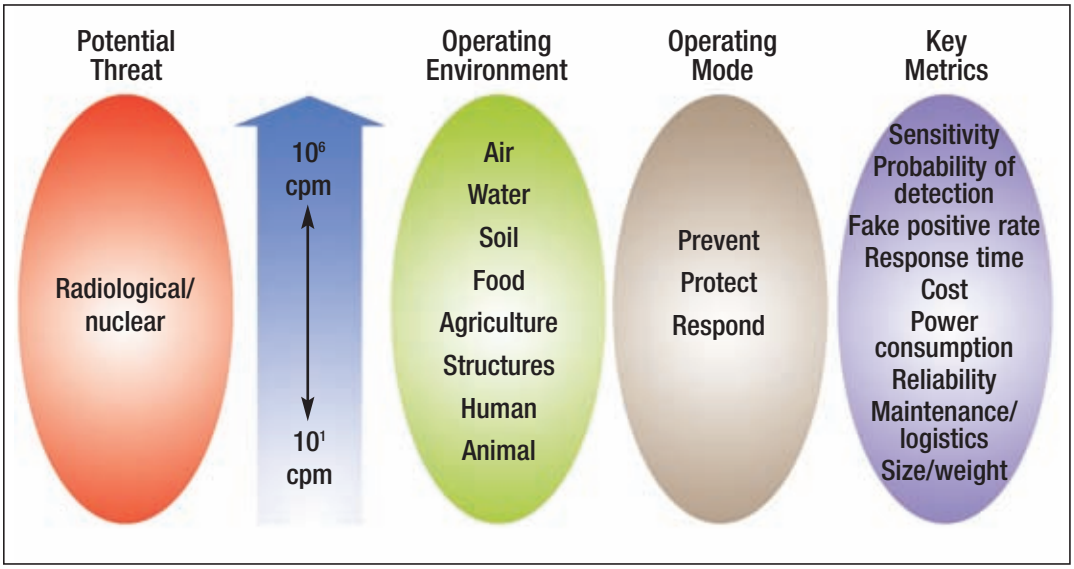
Various technical barriers (including energy resolution, sensitivity, and physical tolerances) limited the reliability of results from radiation detection instruments that were available for deployment—for the most part, instruments engineered for laboratory use—in the months immediately following the 9/11 incidents:

- Imperfect energy resolution led to misidentification of radionuclides (mistaking medical for threat sources, threat for industrial sources, and so on).
- Low sensitivity risked a low likelihood of detection, while overly sensitive instruments gave false alarms, leading to unnecessary response or a tendency to shut off the alarm system.
- Physical issues, such as the need to cool some systems and sensitivity to temperature extremes, often led to system malfunctions.

Specific issues resulting from the lack of detection instruments for homeland security applications were the dynamic range that the detectors might cover (from a single count per minute to a saturation level), the kind of operating environments (air, people, buildings), the type of operational mode (screening for prevention, personnel protection in response), and key measurement points (response time, reliability, detection probability). To address these issues, it quickly became clear that standards were needed to define the specifications for a credible mechanism by which the performance of radiation detection systems could be determined and verified. Figure 2 identifies the types of standards for detectors designed to be used in homeland security applications.

Since 2002, the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the national laboratories of the Department of Energy (DOE), instrument manufacturers, and user communities (such as first re-

FIGURE 2. Standards for Detectors: Countering the Radiological/Nuclear Threat



sponders) have been working with the Radiation Instrumentation Committee (N42) of the American National Standards Institute (ANSI) to develop a suite of performance and related standards to support reliable detection of radioactive materials for homeland security applications. The first set of standards developed, three to address portable instruments (pagers, survey meters, and radioisotope identifiers) and one for portal monitors, were for instruments that were already under consideration. Revised versions of these standards were published in December 2006.

In addition, three new standards have been published in the last year:

- *ANSI N42.42.* This standard describes minimum requirements for data formatting. A well-defined format for data is required to ensure the interoperability of instruments used in homeland security applications and to ensure the usability and reliable transmission of the data (to a central office for evaluation, for example).
- *ANSI N42.37.* This standard establishes minimum requirements and provides recommendations and guidelines for training users in basic radiation detection and proper use of radiation detection instrumentation for various homeland security applications. The standard is intended primarily for pre-event preparations; it does not cover mission-specific procedures and protocols. (Ongoing efforts are leading to the development of standards to further support first and emergency responders in the use of current equipment and to address detection performance issues of emerging technologies.)
- *ANSI N42.38.* This standard provides the criteria for the operational and performance requirements for instruments—advanced spectroscopic portal monitors—that can both detect radioactivity and identify radionuclides that may be present in or on people, vehicles, or containers.

Performance Standards for Radiation Detection Instruments

Recently Published Standards

ANSI N42.32 (revision published December 2006), "Performance Criteria for Alarming Personal Radiation Detectors for Homeland Security"

ANSI N42.33 (revision published December 2006), "Performance Criteria for Radiation Detection Instrumentation for Homeland Security"

ANSI N42.34 (revision published December 2006), "Performance Criteria for Hand-Held Instruments for the Detection and Identification of Radionuclides"

ANSI N42.35 (revision published December 2006), "Evaluation and Performance of Radiation Detection Portal Monitors for Use in Homeland Security"

ANSI N42.42 (published June 2006), "American National Standard Data Format Standard for Radiation Detectors Used for Homeland Security"

ANSI N42.37 (published December 2006), "American National Standard for Training Requirements for Homeland Security Purposes Using Radiation Detection Instrumentation for Interdiction and Prevention"

ANSI N42.38 (published January 2007), "Performance Criteria for Spectroscopy-Based Portal Monitors Used for Homeland Security"

Standards Under Development

ANSI N42.39 (draft ready for comments March 2007), neutron detection

ANSI N42.41 (draft distributed for comments March 2007), active interrogation

ANSI N42.43 (draft distributed for comments March 2007), transportable and mobile systems

ANSI N42.49 (initial draft prepared March 2007), personal electronic dose meter performance

Four standards are under development. One, N42.41, is expected to be published by the end of 2007. This standard addresses the use of a key emerging technology for detecting nuclear materials such as highly enriched uranium (HEU) that could be used in an IND or other nuclear device. These materials generally emit too little radiation to be detected by the types of instruments used for RDD and other radiations. Detecting these special nuclear materials requires active neutron interrogation, in which HEU is measured through its emission of secondary radiations subsequent to stimulation by high-energy electromagnetic radiation or by neutrons.

The instrumentation standards establish operational requirements, including detection parameters (radiation levels, radionuclides present, and so on, depending on the instrument type) and the expected electrical, mechanical, and functional performance for defined environmental conditions. All of these standards have been or are being written by committees composed of members from the user and manufacturer communities, as well as from governmental bodies with a vested interest in homeland se-

curity (DHS) and high standards of measurement (NIST). Without the time and effort put forth by those writing these standards, publication of these documents would have been impossible within the relatively short time frame required to address reliable instrument performance in radiation detection for homeland security.

Not only must standards be developed, but equipment manufacturers, testing laboratories, and other users of the standards must validate the standards and demonstrate their usefulness for currently available instrumentation. It is not unlike testing a cake recipe before it is published to ensure the expected outcome. To be certain that a standard will be usable, the criteria it defines must be known to be appropriate for the instrumentation it covers. For example, a standard that says an instrument needs to be functional after a drop of 5 meters is useful only if it is reasonable to expect the instrument to function after a 5-meter drop. To put it another way, one can make many assumptions about the validity of a standard, but manufacturers and users must have proof that those assumptions are correct before they can determine their production and acquisition plans. By putting the standards "through their paces" by testing a small sampling of instruments to the specifics contained, the standards themselves become a tool that can be used by the whole community as benchmarks for performance and guidance for procurement.

Verifying the reasonableness of a standard requires a method by which results from various test facilities can be compared. To determine the validity of the instrument performance standards (N42.32, 33, 34, 35, and 38), several DOE laboratories tested instruments using well-defined (and adhered to) testing protocols and NIST-calibrated radioactive sources. This approach was expanded to subsequent performance testing of instruments for manufacturers. (The results are available to the responder community on DHS's Responder Knowledge Base at https://www.rkb.mipt.org/.)

Standards provide homeland security personnel, early responders, health physicists, and cleanup crews with the proper equipment and training for monitoring the import, transport, or storage of radioactive and nuclear materials. This monitoring helps prevent a potential radiological/nuclear incident (and will help with managing the consequences should an incident occur). With emerging and evolving technologies for radiation and nuclear detection, the technological and measurement infrastructure, as well as new standards, for the evaluation of equipment performance must be continually developed, evaluated, and updated. New standards under development, such as ANSI N42.43 for transportable and mobile detection systems (including cranes) used for homeland security applications, will require validation as to reasonableness in advance of instrument testing for the user (and manufacturer) communities.

Standards for radiation and nuclear detection are continually evaluated and updated as technologies and capabilities evolve and, to be most effective, should be in harmony with related standards around the world. Preventing an RDD or IND event depends on cooperation among exporters and importers; the consequences of an RDD or IND would probably cross borders via radioactive fallout (not to mention political response) and may involve response from nearby countries (particularly in border regions).

Equipment and training validated against applicable standards allow effective protection against and response to radiological or nuclear events. They also support the purchase and use of equipment for safe and efficient operation, enabling laboratories and industries involved in detection and recovery efforts to respond efficiently at reasonable cost and turnaround time to minimize the potential impact on property, commerce, and health.

Standards, and the ongoing inclusion of the international community, represent the single most crucial resource for enabling instrument manufacturers, users, and government organizations to achieve interoperability in technology and a high level of confidence in results from radiation detection equipment used for homeland security.

For additional information, see the following:

- Leticia Pibida, Lisa Karam, and Michael Unterweger, "Results for Test and Evaluation of Commercially Available Survey Meters for the Department of Homeland Security, Round 2 Testing" (submitted for publication in DHS's Responder Knowledge Base, 2006)
- Leticia Pibida, Charlie Brannon, Lisa Karam, and Michael Unterweger, "Results of the Test and Evaluation of Commercially Available Radionuclide Identifiers for the Department of Homeland Security, Round 2 Testing" (submitted for publication in DHS's Responder Knowledge Base, 2006)
- Leticia Pibida, Lisa Karam, and Michael Unterweger, "Results of the Test and Evaluation of Commercially Available Portal Monitors for the Department of Homeland Security, Round 2 Testing" (submitted for publication in DHS's Responder Knowledge Base, 2006).

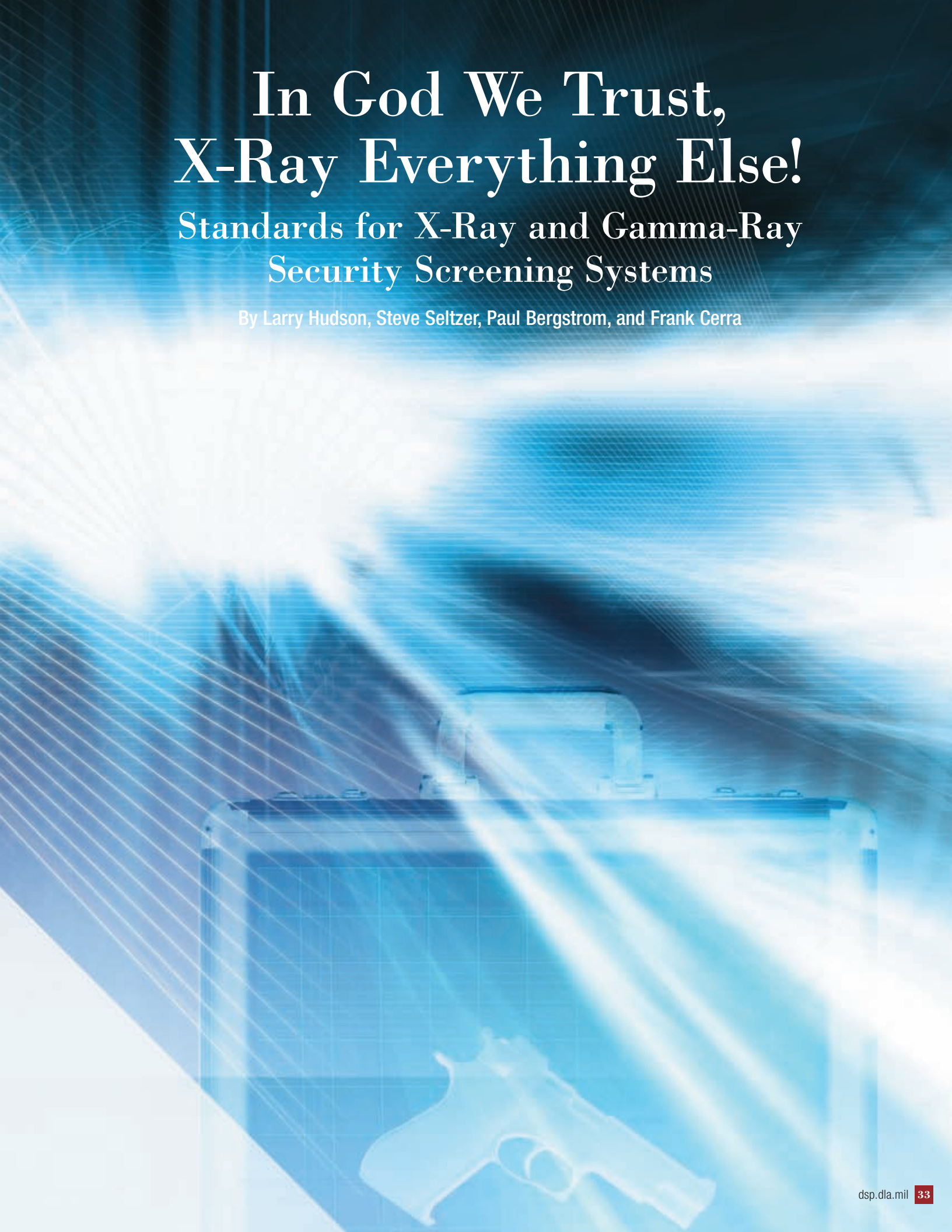
About the Author

Lisa Karam has been at NIST since 1983. As leader of the Radioactivity Group at NIST since 1998, she managed the development of standard radioactive sources and played a leading role in international interactions in radionuclide metrology. She has been the deputy chief of the Ionizing Radiation Division since March 2003 and is the division's primary liaison with the Department of Homeland Security for radiation detection and protocols and standards for radiation measurements.

In God We Trust, X-Ray Everything Else!

Standards for X-Ray and Gamma-Ray Security Screening Systems

By Larry Hudson, Steve Seltzer, Paul Bergstrom, and Frank Cerra



A suite of technical performance standards for all of the nation's security systems that screen using x-rays or gamma-rays is nearing completion. Specifically, these standards address aspects of imaging quality and radiation safety, and each specifies test artifacts, test methods, and, in some cases, required minimum performance levels. All modalities are treated: transmission and backscatter geometries as well as computed tomography (CT). The goal is to provide governmental users and industrial partners with uniform methods to compare technical aspects related to performance and standard gauges that will stimulate and quantify future technological improvements.

Since the 1920s, the National Bureau of Standards, now the National Institute of Standards and Technology (NIST), has been a world leader in promoting accurate and meaningful measurements, methods, and measurement services. Among other things, NIST develops, maintains, and disseminates the national standards for ionizing radiation and radioactivity, thereby providing credible and absolute measurement traceability for the nation's medical, industrial, environmental, defense, homeland security, energy, and radiation-protection communities. This experience and infrastructure, which includes fundamental research and radiation-transport modeling, enabled NIST to respond to rapidly emerging homeland security needs in the area of x-ray and gamma-ray security screening. In particular, efforts are nearing completion on the development of a suite of national voluntary consensus standards that span the use of x-rays and gamma rays in the screening of carried items at checkpoints, airline baggage, trucks, cargo containers, human subjects, and abandoned objects suspected of containing bulk explosives.

Funded by the Department of Homeland Security, and in alliance with the American National Standards Institute (ANSI), the development process began by recruiting working groups with representation from end users of x-ray security screening systems (primarily governmental), the manufacturers of the equipment, national research and development laboratories, and other expert stakeholders. Current best practices were considered for possible codification. Agencies and laboratories that were able to contribute key ideas because of years of extensive experience included the then Federal Aviation Administration's Transportation Security Laboratory, the Thunder Mountain Evaluation Center, the U.S. Secret Service, and U.S. Customs and Border Protection (CBP). In some cases, vendors chose to contribute proprietary in-house test methods and objects for adoption.

The Checkpoint

Nearly everyone by now recognizes the checkpoint—with its x-ray system, fed by a conveyor belt on which we place our carry-on luggage, computers, briefcases, parcels, bags, coats, and even shoes—that one must pass through to enter a secured area. Nearly 800 million passengers per year at U.S. airports pass through such checkpoints to enter the boarding area. Millions more experience checkpoints to enter secure courthouses, some schools, and sporting and entertainment venues. Although metal detectors are used to screen for possible weapons hidden

Technical Performance Standards for X-Ray and Gamma-Ray Security Screening Systems

Image Quality

ANSI N42.44, "American National Standard for the Performance of Checkpoint Cabinet X-Ray Imaging Security Systems"

ANSI N42.45, "American National Standard for Evaluating the Image Quality of X-Ray Computed Tomography Security-Screening Systems"

ANSI N42.46, "Measuring the Imaging Performance of X-Ray and Gamma-Ray Systems for Cargo and Vehicle Security Screening"

ANSI N42.47, "American National Standard for Measuring the Imaging Performance of X-Ray and Gamma-Ray Systems for Security Screening of Humans"

National Institute of Justice 0603.01, "Portable X-Ray Systems for Use in Bomb Identification and Interdiction"

Radiation Safety

ANSI N43.16, "Radiation Safety Standard for Vehicle and Cargo Security Screening Systems Using X-Ray or Gamma Radiation"

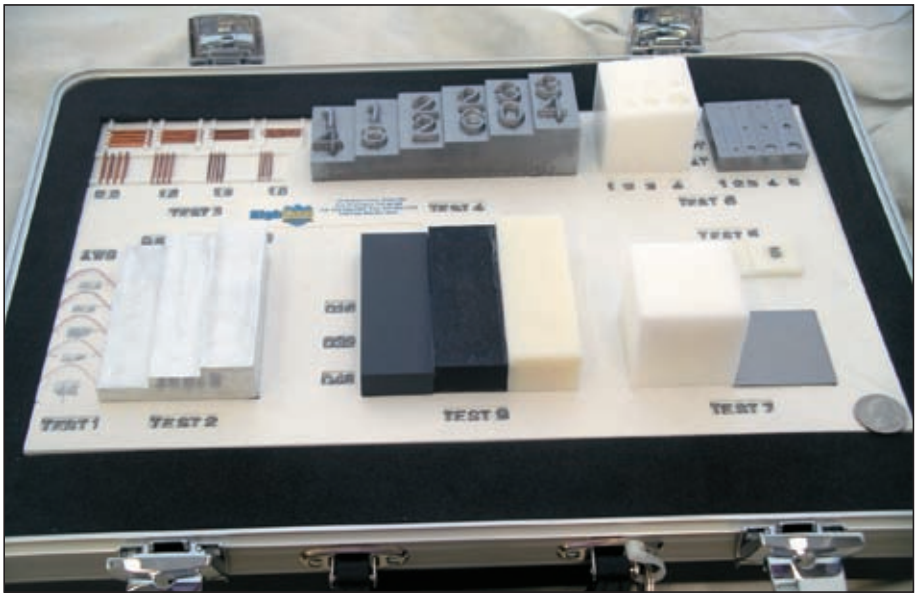
ANSI N43.17, "Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation" (revision of N43.17-2002)

on the body, the x-ray scanners are used to scan the contents of carried items without having to open containers for a time-consuming visual inspection. In addition, such equipment is often used to screen incoming parcels in mail and shipping receiving rooms.

The detection of threat and illicit material using these x-ray screening systems of course depends on the operator's ability to recognize an ever-expanding array of threat objects from an often-cluttered x-ray image filled with innocent objects. This inspection must be as quick and unintrusive as possible to minimize delays through the checkpoint and thus the associated social and economic costs.

Common sense suggests that the better the quality of the x-ray image, the better the detection performance. A new standard—Institute of Electrical and Electronics Engineers, Inc. (IEEE)/ANSI N42.44, "American National Standard for the Performance of Checkpoint Cabinet X-Ray Imaging Security Systems"—addresses detection performance. Specifically, the new standard builds upon an older standard—ASTM F792, "Standard Practice for Evaluating the Imaging Performance of Security X-Ray Systems"—and an associated test object useful in determining the resolution, penetration, and material differentiation of these systems. (See Figure 1.) The new ANSI/IEEE standard, in addition to correcting some inconsistencies in the ASTM practice, establishes minimum imaging performance requirements in each of the

FIGURE 1. ASTM F 792 Test Object



nine imaging tests associated with the ASTM test object. Through normative reference to existing standards, it also incorporates pertinent requirements for electrical and mechanical safety, electromagnetic compatibility and susceptibility, and radiation safety for these environments.

A well-defined test method and a set of minimum acceptable image-quality standards, as established in this standard, will provide value to both users and manufacturers of these x-ray imaging security systems. Buyers and prospective users of checkpoint x-ray systems will have test methods that facilitate performance comparisons among systems and will be assured of minimum acceptable imaging-performance requirements. This performance is achievable with current state-of-the-art production checkpoint x-ray systems. Manufacturers will have a better understanding of the needs, wants, and expectations of the user community and a clearer understanding of the minimum set of imaging goals. In addition, the standard can be used in acceptance tests for checking actual performance against manufacturers' test claims and for monitoring system performance over time to check for degradation that could compromise security. Some applications, such as aviation security, will no doubt require image-quality standards higher than the minimum performance established in this standard. Reporting under this standard will convey the better performance and will assure all parties of consistent and reliable performance data.

Computed Tomography

The Government Accountability Office reports that Transportation Security Administration funding related to aviation security has totaled about $20 billion since FY04. Much of this is directed toward the inspection of the some billion pieces of luggage that are checked each year in the United States for transport in the holds of commercial airliners. At present, each

undergoes inspection using the multiview CT technique, providing three-dimensional information to automated explosives-detection algorithms. (See Figure 2.)

Due to the highly sensitive nature of explosives detection in aviation security, the scope of ANSI N42.45, "American National Standard for Evaluating the Image Quality of X-Ray Computed Tomography Security-Screening Systems," is limited to test artifacts and test methods. The final test article, which is expected to be adopted by DHS's Transportation Security Laboratory for factory acceptance testing, will be composed of a novel set of x-ray phantoms designed specifically for CT security (as opposed to medical) screening. It will gauge the following image quality metrics: CT-number consistency, beam hardening and scattering, object-length accuracy and presentation, atomic number and density uniformity, CT-to-projection image registration, slice-sensitivity profile, modulation transfer function, and streak artifacts.

FIGURE 2. Reconstructed CT Image

Courtesy of Analogic Corporation

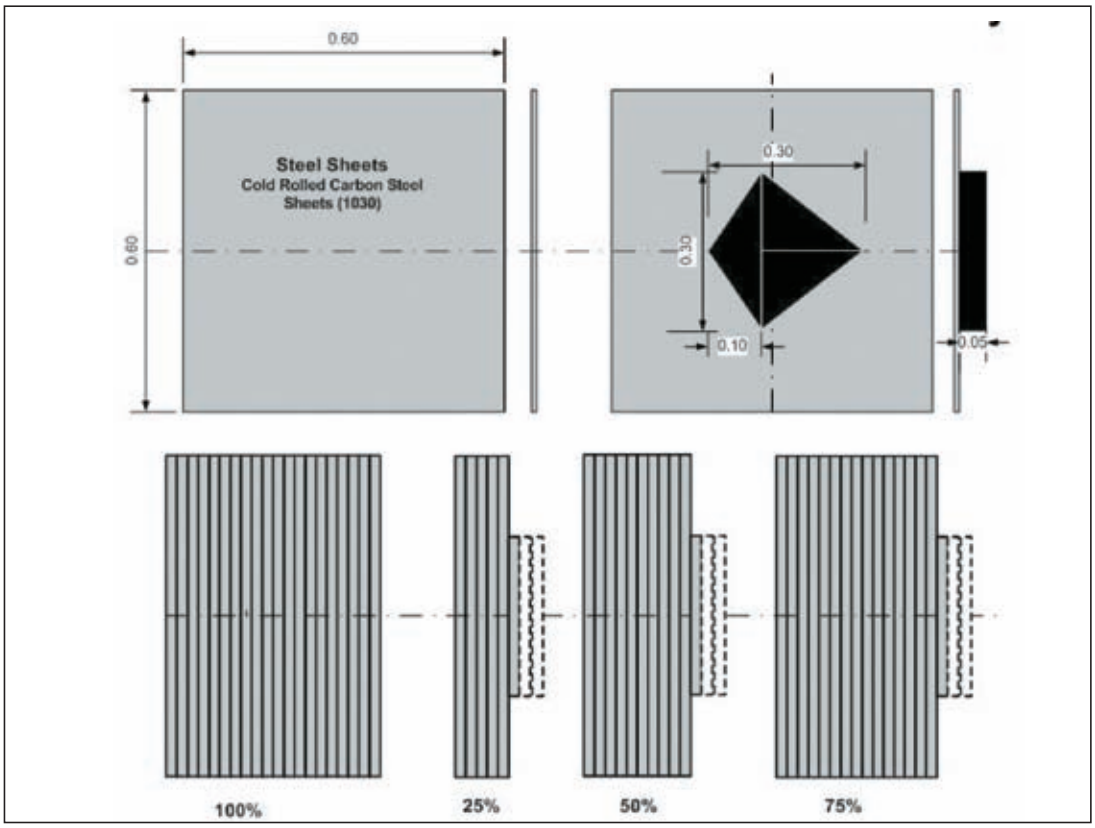
Cargo Vehicle

Daily, an average of 80,000 cargo containers arrive at the borders of the United States. About two-thirds come through seaports, while the remainder arrive by truck or by rail. A substantial number of x-ray and gamma-ray systems are already deployed at the borders to inspect some fraction of this traffic. These systems assist the officers of CBP in their attempts to interdict contraband and people illegally entering the United States. There is an increasing interest in using these systems to detect weapons of mass destruction and special nuclear material. In addition, Congress has mandated that all cargo containers entering the United States must be inspected in the future. With the need to deploy many additional inspection systems with more powerful capabilities, it is all the more important that these systems be subjected to a common test method in order to consistently compare their performance. Currently, no national standard test procedures are available for such comparisons.

ANSI/IEEE N42.46, "Measuring the Imaging Performance of X-Ray and Gamma-Ray Systems for Cargo and Vehicle Security Screening," is intended to fill this gap. This standard defines test methods for both the transmission and backscatter modes to measure the main image quality metrics of concern in imaging present-day cargo systems. These metrics are simple penetration, spatial resolution, wire detection, and contrast sensitivity. Because the purview of this standard ranges from palletized cargo to trucks and cargo containers, these methods were designed with flexibility in scaling. Given the diversity of systems and applications, no minimum level of performance is specified. Rather it is expected that the standard will provide a basis for vendors to report the capabilities of their systems in a manner that can be directly compared with other systems being considered for the same application. Figure 3 depicts a proposed test of the penetration and contrast sensitivity of a cargo-screening system. The requirement entails determining the direction of an arrow through increasing thicknesses of steel shielding.

This technical performance standard is complemented by another effort in progress, ANSI/Health Physics Society (HPS) N43.16, "Radiation Safety Standard for Vehicle and Cargo Security Screening Systems Using X-Ray or Gamma Radiation." Together, these standards will provide a solid basis for understanding and comparing the performance and safety of radiation-based cargo and vehicle security inspection systems.

FIGURE 3. Steel Penetration and Contrast Sensitivity



Body Scanners

X-ray systems are now available for screening humans, exposing them to an extremely low level of radiation. Unlike conventional metal detectors, these systems can detect non-metal as well as metal weapons. The Transportation Security Administration has begun a pilot program to test x-ray body scanners as part of their continuing effort to improve the effectiveness and efficiency of passenger screening. Other governmental institutions, such as prisons, customs, and the armed services, also have used or are considering using the body scanners. This relatively new technology has a potential for significant expansion in today's security environment.

X-ray screening of humans presents two key challenges:

- Systems must be safe and effective.
- They must afford a level of privacy appropriate for each screening situation and in line with societal standards.

To address safety and effectiveness, NIST is facilitating the development of two related standards: ANSI/IEEE N42.47, "American National Standard for Measuring the Imaging Performance of X-Ray and Gamma-Ray Systems for Security Screening of Humans," and ANSI/HPS N43.17, "Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation." The latter is a revision of N43.17-2002, which had a limited scope.

The ANSI/IEEE N42.47 standard will establish a set of imaging parameters and associated measurement methods. Minimum performance requirements will be specified for each parameter. Because of fundamental differences between the two basic technologies employed, backscatter and transmission, separate test objects will be developed for the two types of systems. (Figure 4 shows x-ray images from a backscatter body scanner, and Figure 5 shows a transmission x-ray image of a person with threat objects.) In addition to image quality requirements, N42.47 will include a complete set of performance requirements by referencing existing standards. These normative references will include provisions for electrical, mechanical, and radiological safety; electromagnetic compatibility; and electromagnetic susceptibility. This should make the standard a valuable tool for manufacturers, users, and potential buyers of the systems. Manufacturers may use the standard in the design, testing, and specification processes. For users, the standard will provide basic test methods for acceptance testing and monitoring performance degradation over time. Users may also build upon the requirements of the standard to satisfy their own special needs. Potential buyers will benefit from a uniform set of parameters for comparing available products and from a complete set of requirements to aid with purchase specifications.

The ANSI/HPS N43.17 standard provides requirements associated with radiation safety of body scanning systems. It includes dose limits and requirements for manufacturers and users of systems that employ backscatter and transmission geometries. This expanded standard will also

FIGURE 4. X-Ray Images from a Backscatter Body Scanner

Courtesy of AS&E, Billerica, MA

FIGURE 5. Transmission X-Ray Image of a Person with Threat Objects

Courtesy of SecurePath LLC

consider portals and vehicle scanners used for human screening. Transmission technology works on the same principle as digital radiography in medicine, using radiation that passes through the body to form an image. Backscatter technology uses radiation that bounces off the body to detect objects hidden under clothing and requires much lower levels of radiation (typically 30 to 100 times lower). One backscatter image requires roughly the same amount of radiation an person receives on average from natural sources every 15 minutes (or in about 1 minute of flying at high altitude).

Because of the disparity in potential dose and other safety considerations, the N43.17 standard will have two sets of requirements. The safest systems will be classified as general-use systems, following recommendations from the National Council on Radiation Protection and Measurements. Systems requiring stricter controls will be classified as limited-use systems. The standard seeks to limit the annual effective dose to an individual from all types of systems in one screening site to 0.25 microsievert. This is consistent with national and international standards of radiation protection and is a fraction of the typical annual dose from natural sources.

About the Authors

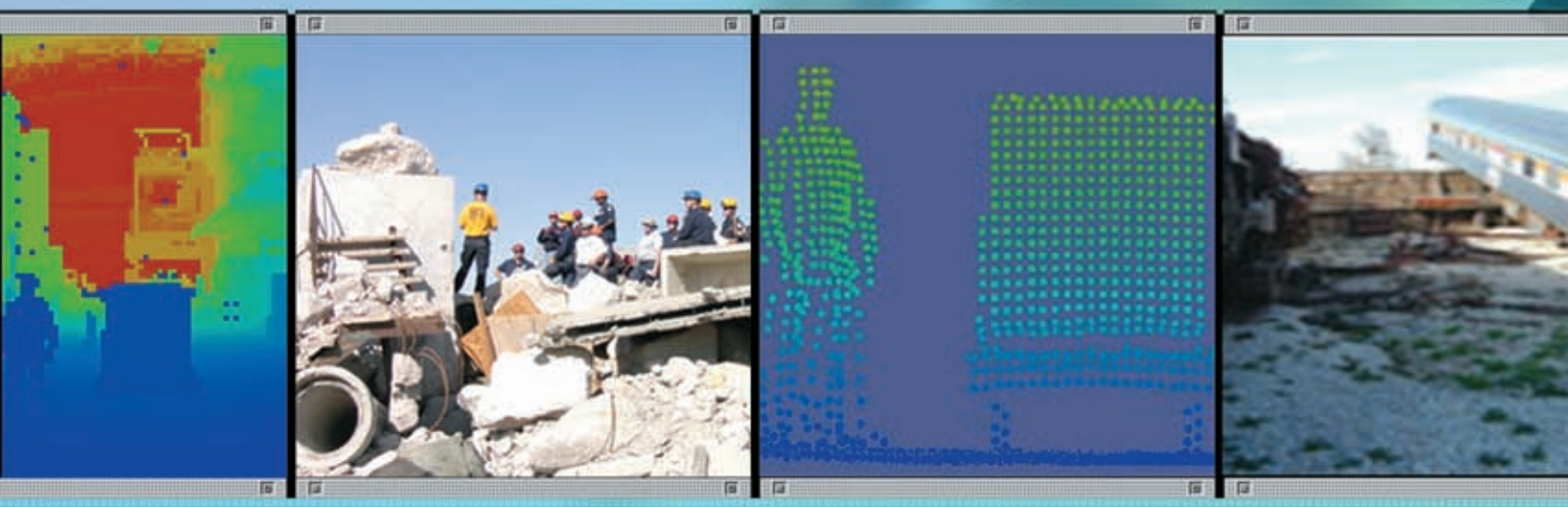
Larry Hudson has 20 years of federal service with NASA and NIST. Research interests include precision x-ray metrology, imaging, and standards; curved crystal x-ray spectroscopy; and medical, industrial, and security applications of x-ray technology. Dr. Hudson is the primary liaison for NIST to the Department of Homeland Security for bulk explosives detection and standards for x-ray and gamma-ray security screening and is the facilitator for the ANSI N42.45 and National Institute of Justice 0603.01 working groups.

Other key NIST contributors include Steve Seltzer (ANSI N42.44), Paul Bergstrom (ANSI N42.46), and Frank Cerra (ANSI N42.47 and N43.17).

Performance Standards for Urban Search and Rescue Robots

Enabling Deployment of New Tools for Responders

By Elena Messina



Some images courtesy of NIST and Robotix.

Robots hold great promise as tools that can assist responders who search collapsed buildings and other disaster sites for victims. Performance standards are needed in order to ensure that robots meet the challenging requirements of the response missions and provide the best value and utility to the responders in carrying out their difficult and dangerous jobs.

Urban search and rescue (USAR) is defined as "the strategy, tactics, and operations for locating, providing medical treatment, and extrication of entrapped victims."[1] USAR is a domain "that is a very dangerous job for human rescuers, poses an almost infinitely difficult spectrum of challenges, and yet provides an opportunity for robots to play a pivotal support role in helping to save lives."[2] However, at this time, the state of robot technology overall is not very mature, and robots are not being used within USAR missions. There is a lack of understanding of what specific roles robots can play within USAR and of how to specify and select particular robot configurations to best suit a given response organization's requirements.

Standard test methods generated from explicit requirements for USAR robots, with objective performance metrics and repeatable performance testing, will accelerate the development and deployment of mobile robotic tools for USAR responders. Noting a lack of such standards or performance metrics, the Department of Homeland Security (DHS) initiated a project in 2004 to create performance standards for USAR robots. Coordinated by the National Institute of Standards and Technology (NIST), the standards are being developed through a task group within ASTM International's Homeland Security Committee's Operational Equipment Subcommittee (E54.08). These standards address robot mobility, sensing, navigation, planning, communications, integration into operational caches, and human system interaction. Such standards will allow DHS to provide guidance to local, state, and federal homeland security organizations regarding the purchase, deployment, and use of robotic systems for USAR applications.

USAR is a multifaceted application, both in terms of the types of disasters and in the roles that responders perform. Example deployments by the federal USAR task forces, which are part of the Federal Emergency Management Agency (FEMA), include the World Trade Center collapse, Hurricane Katrina, and the California Northridge earthquake. The types of structures involved, environmental conditions, types of collapses, and hazards are very different in these examples, which are representative, but not exhaustive. A USAR operation has multiple stages, and responder teams are tasked with a variety of functions. For example, a FEMA USAR team can conduct a physical search and rescue in collapsed buildings, provide emergency medical assessments and care to trapped victims, assess and control hazards such as gas or electric service, and evaluate and stabilize damaged structures. Robots could potentially support rescue personnel in carrying out all of these functions, but each has different requirements. Initially, the standards effort is concentrating on assisting responders during the technical search phase of a response.

Just as many disciplines are required within a search and rescue team, the components within a robot are also quite diverse. A robot is a system of systems: it is built from mechanical, electrical, computer, software, sensing, and other components, each of which is complex. The disciplines involved in the various components that constitute robots are specialized enough that a different set of expertise is required to adequately study the requirements and develop the corresponding performance tests. The components have to integrate among themselves; these interactions may create additional performance requirements. To further complicate matters, the constituent

technologies and the robotics discipline are still evolving.

Performance-Based Standards Approach

The broad scope of the application domain, the breadth of technologies entailed within robotics, and the relative immaturity of robotics pose challenges to the standardization process. Challenges such as those mentioned above cannot be allowed to impede progress toward the goal of having well-understood performance goals and means of measuring whether systems meet them. We are breaking down the problem into logical, cohesive, manageable categories, and for each of these categories, producing standard test methods. The test methods objectively measure a robot's performance in a particular area. Accompanying robot deployment usage guides will help interpret test results and provide suggested performance ranges desired for different rescue operations. Ultimately, the response organization will be able to determine which robot best suits its requirements. This is similar to the way consumers select products such as cars and televisions based on published third-party test results.

Robot researchers and manufacturers benefit from the definition of test methods and target operational ranges according to type of rescue operation. These communities are fully capable of devising the technological solution to particular rescue operation needs. Hence, the USAR project's approach is to articulate performance requirements and deployment categories and to develop test methods and usage guides instead of dictating specific technical solutions or robot categories. Test methods ought to measure how effectively a responder using a robot is able to perform a task without being biased or tailored toward a particular technology.

The project began through a series of workshops hosted by NIST at which FEMA USAR team members defined the performance requirements for the robots and began itemizing the types of deployment scenarios to which the robots may be applied. Over 100 initial performance requirements were generated, along with 13 deployment categories. For each requirement, the responders defined how they would measure performance. The foundational work on requirements and deployment categories provided the organizing principles for the standards effort.

The deployment categories include ground, aerial, and aquatic, and they define the employment role, de-

One Size Does Not Fit All

Larger wide-area ground survey robot carrying small, throwable peek-bot with its manipulator. These representative robots address two of the deployment categories identified by responders. The bigger robot can cover an extended distance and insert the smaller robot into a small hole to initiate its search within a void space that would be inaccessible otherwise.

ployment method, and tradeoffs. For example, a "ground peek robot," or "peek-bot," would provide rapid audiovisual situational awareness or hazardous materials detection and could be left in place for data logging. It could be thrown into a building or a void space, or even deployed by a larger robot. Small size and expendability would be traded off for mobility and sensing range. On the other hand, non-collapsed structure, wide-area survey ground robots would be employed for long-range operations (at least a kilometer standoff distance) in uncompromised buildings and their surroundings, could provide information for site assessment and victim identification, and could stay on duty to provide continued monitoring. Ground survey robots would have greater mobility, endurance, payload capacities, and range capabilities than peek robots, but they would be larger, heavier, and likely less expendable. They may be configured in variations that include special sensors, manipulation, or breaching tools.

The ASTM task group established the following working groups: Terminology, Human-System Interaction, Mobility, Operating Environment, Communications, Sensors, Logistics, Power, and Safety. Each working group (except Terminology) is responsible for developing the test methods within its assigned area and for surveying standards for relevant work that can be leveraged. Each task group is developing standards in a series of "waves" based on the relative maturity of the requisite technologies and on the responder-articulated priority of the requirements. To further help focus the efforts of the task group, the responders have helped define which deployment categories should be given priority. Based on observing a wide range of robots representing most of the 13 deployment categories, three initial categories have been selected: ground peek robots; non-collapsed structure, wide-area survey ground robots; and aerial survey robots. The definition of these categories serves to establish the operating ranges required for the robots. For instance, the effective distance that the onboard navigation cameras must be able to see is a few meters for a peek-bot, but it is several hundreds of meters for the aerial robots.

Directed Perception Test Method

This test method addresses the responder requirement to use robotic manipulators to perform a variety of tasks in complex environments. The test artifact consists of an "alcove" formed by three sets of stacked boxes with holes. Two different alcoves are shown in the image. Inside the boxes are "targets" for different sensors. They could be such things as eye charts, heating blankets (for thermal sensors), trace explosives or stimulants, or radiation sources. The robot enters the alcove, and the operator is to clear as many holes as possible. The maximum reach and range are measured, as well as how effectively the items inside the boxes are sensed and how long the process takes. Also noted, when appropriate, is the location of "first detection" by a sensor as the robot approaches the stacks. The flooring is not flat, so as to induce additional, realistic challenges in positioning the robot and manipulator.

Correlating Test Artifacts with Mission-Relevant Objects

The visual acuity of the robot system is evaluated using standard "tumbling E" eye charts. The test method notes the smallest line that the operator can read looking at the operator control unit screen image of the robot's onboard cameras. The character sizes are correlated to the labels on hazardous materials and other types of objects that responders would look for as they perform a search, thereby bridging the gap between abstract, quantifiable, and reproducible tests and the "real world."

The developers of a test method attempt to create a set of artifacts and tasks that the robot-operator team is to perform, along with a set of metrics for measuring performance. The artifacts (also referred to as "props") are simplified abstractions of challenges that robots would have to confront in a real deployment. They are designed to be easily reproducible by other organizations at low cost.

When this article was written, test methods addressing the visual acuity and field of view of on-board cameras, cache packaging weight and volume, communications, mobility, interface usability, and sensor aiming (directed perception) were entering or already through the balloting process. An initial set of standard terms has been approved by the Homeland Security Committee, with more definitions being added as needed.

Response Robot Exercises

This standardization effort employs an iterative development approach to ensure that the performance requirements are appropriate and that the manufacturer and technology development communities are able to interact with the end users frequently. Regular response robot exercises held at USAR training sites present opportunities to dry-run testing protocols and conduct trials integrating robots into search missions. Comments from all of the stakeholders help refine and strengthen the tests. Because robots are not being used in urban search and rescue, it is essential to give the user and developer communities opportunities to experiment with deployment approaches. The events frequently generate feedback to the manufacturers and technology developers, who are able to see how their systems perform informally against the emerging performance standards.

Exercises have been held at FEMA USAR training facilities in the desert of Nevada, in Maryland, and at "Disaster City," which is in Texas. At each exercise, the local training scenarios and props have been used by responders to experiment with deploying robots, which are used to search for simulated victims that have been inserted into the different scenarios. Extensive data are captured, including video of the robots as they traverse the different environments. Example training scenarios that have been used include a freeway collapse, passenger and cargo train derailments, rubble piles, and a multistory building with a maze-like internal structure. Robots able to address most of the 13 deployment categories have participated. This has allowed responders to gain insight into what robot designs are best suited to which deployment (some can address more than one).

Simulating Disasters

A robot searches for victims in a passenger train derailment scenario at Disaster City, a FEMA urban search and rescue training facility.

Conclusion

Any new candidate technological solution must be proven useful to the responder community before it is deployed in the field. Standardized test methods generated directly from responder requirements can ensure that applicable technologies are relatively easy to use, integrate efficiently into existing infrastructure, and provide demonstrable utility to response operations. Being able to characterize the performance of a new technology under specified—yet representative—conditions, will also enable funding agencies, such as FEMA, to obtain best value in their procurements. Another benefit of having standard performance evaluations is the acceleration of the needed technology developments.

In sum, a consensus standards organization—one that includes representatives from the user communities, funding agencies, and technology developers—can produce commonly agreed-upon standard robot test methods and usage guides. Such methods and guides will enable responders to safely integrate new robotic tools into their operations.

For additional reading, see the following:

- A. Jacoff and E. Messina, "Urban Search and Rescue Robot Performance Standards: Progress Update," in *Proceedings of the 2007 SPIE Defense and Security Symposium Unmanned Systems Technology IX*, Orlando, FL, April 2007
- E. Messina and A. Jacoff, "Measuring the Performance of Urban Search and Rescue Robots," in *Proceedings of the IEEE Conference on Technologies for Homeland Security*, Woburn, MA, May 16–17, 2007
- K. Remley, G. Koepke, E. Messina, A. Jacoff, and G. Hough, "Standards Development for Wireless Communications for Urban Search and Rescue Robots," in *Proceedings of the 9th Annual International Symposium on Advanced Radio Technologies*, Boulder, CO, February 26–28, 2007.

Disclaimer

Any display of commercial products is for illustration only; it does not imply recommendation or endorsement by NIST.

[1]Federal Emergency Management Agency, *Urban Search and Rescue Response System in Federal Disaster Operations: Operations Manual*, FEMA 9356.1-PR, January 2000.

[2]J.G. Blitch, "Artificial Intelligence Technologies for Robot Assisted Urban Search and Rescue," *Expert Systems with Applications*, Vol. 11, No. 2 (1996), pp. 109–24.

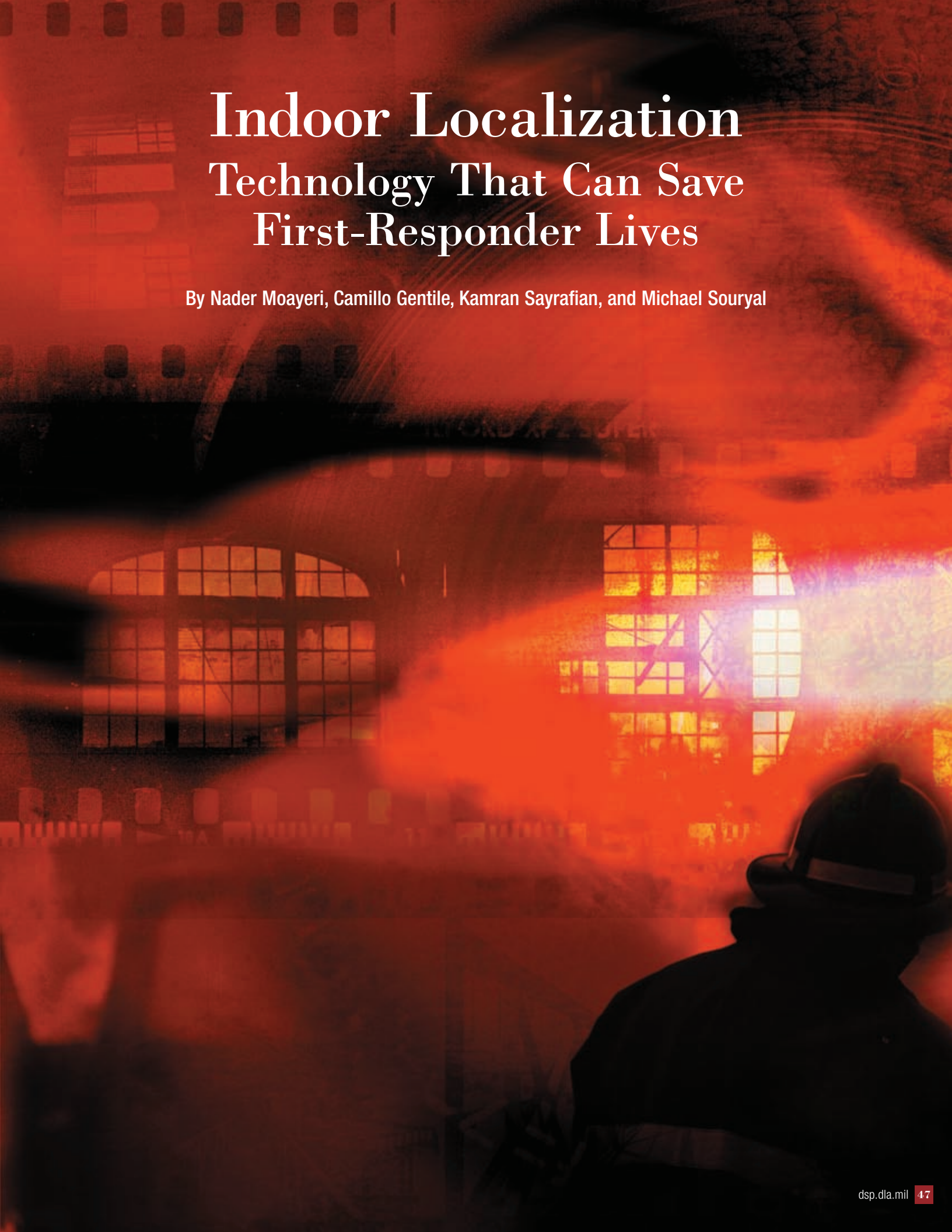
About the Author

Elena Messina is leader of the Knowledge Systems Group in the Intelligent Systems Division at the National Institute of Standards and Technology. She inaugurated and chairs the annual Performance Metrics for Intelligent Systems workshop series and has led other major related efforts, including the development of robot competitions and test arenas for RoboCup Rescue and the American Association for Artificial Intelligence. She leads the development of performance standards for robots applied to urban search and rescue and to bomb disposal.

Indoor Localization

Technology That Can Save First-Responder Lives

By Nader Moayeri, Camillo Gentile, Kamran Sayrafian, and Michael Souryal



On December 3, 1999, six firefighters lost their lives while trying to rescue some civilians and fellow firefighters in distress in an abandoned warehouse on fire in Worcester, MA. According to the official National Institute of Occupational Safety and Health incident report, all six firefighters lost their way in the thick and boiling smoke inside the building and could not get out. A report by the U.S. Fire Administration states that each year in the United States approximately 100 firefighters are killed while on duty and tens of thousands are injured.

First responders have unequivocally expressed, in various forums and documents, a strong desire for indoor localization. Indoor localization, or location tracking, provides roughly the same capability inside buildings as the global positioning system (GPS) does outdoors. It allows a positioning first responder to know his/her location and to navigate inside a building. It also provides the same information to the incident command (IC) set up outside the building, enabling the IC to make better tactical decisions and more effectively coordinate the emergency response operation. Perhaps more important, it allows the IC to launch an effective and speedy rescue operation if a first responder goes down and needs to be extracted from the building.

Over the past decade, researchers have developed a number of indoor localization techniques. However, two major obstacles must be overcome before we will see widespread use of indoor localization in emergency response operations:

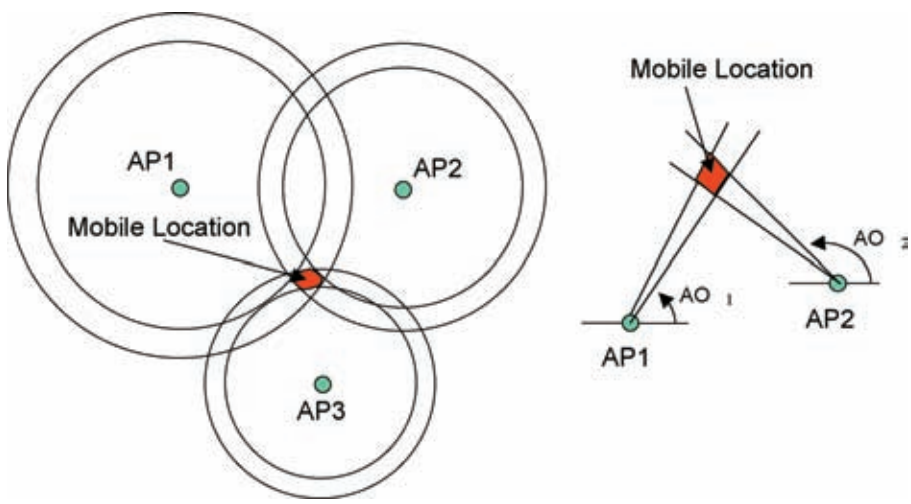
- The gap between the performance of available indoor localization techniques and the hype-induced expectations of first responders vis-à-vis localization must be closed or at least narrowed.
- Standards for indoor localization must be developed to drive down the cost of localization equipment and ensure interoperability.

One of the more promising solutions for indoor localization is based on radio frequency (RF) technology. Although GPS is a very useful technology, it does not work inside buildings, because a GPS receiver needs line-of-site (LOS) propagation paths to four GPS satellites. The indoor localization problem is much more difficult than the GPS operation due to severe signal attenuation and multipath propagation inside buildings. A severely attenuated signal may be indistinguishable from thermal noise at the receiver. We will say more about the adverse effects of multipath propagation later. It is also worthwhile to contrast indoor localization with the E911 problem, the purpose of which is to determine the location of a cell phone user making a 911 emergency call. While E911 is required to have 100-meter location accuracy 90 percent of the time, first responders wish to have indoor localization with 1-meter or preferably 1-foot accuracy. This stringent accuracy requirement is crucial because, once a first responder goes down in a burning building, rescuers have only a few minutes to rescue the first responder or he/she may perish. In addition, no good E911 solutions have been developed for high-rise buildings, because the elevation cannot be estimated in that setting.

Many indoor localization techniques rely on two basic operations, ranging and direction estimation, to determine the location of a radio-carrying mobile user:

- Ranging is the capability for a radio transceiver to estimate its distance from another transceiver based on the signal received from it. The 2D (or 3D) location of a mobile user can be estimated, through a process called triangulation, from range estimates from three (or four) transceivers, called reference nodes, at known locations (see Figure 1). A range measurement typically involves estimating the time-of-flight (TOF) for a signal to propagate from a transmitter to a receiver. The TOF can be computed by measuring the time-of-arrival (TOA) of the signal at the receiver, if the latter is synchronized with the transmitter and the transmission time is known. Another localization technique uses time-difference-of-arrival (TDOA) measurements and a process called multilateration. The TDOA is the difference between TOAs of a signal transmitted by a mobile node at two reference nodes.
- Direction estimation is the capability to estimate the direction of a transceiver emitting RF energy. The 2D (or 3D) location of a mobile user can be estimated from estimates of the direction of the mobile user at two reference nodes. Direction is specified with two angles, azimuth and elevation, in 3D and just one angle in 2D. Figure 1 shows the 2D case.

FIGURE 1. 2D Localization Based on Range and Direction Measurements with Respect to Reference Points Denoted by Green Circles



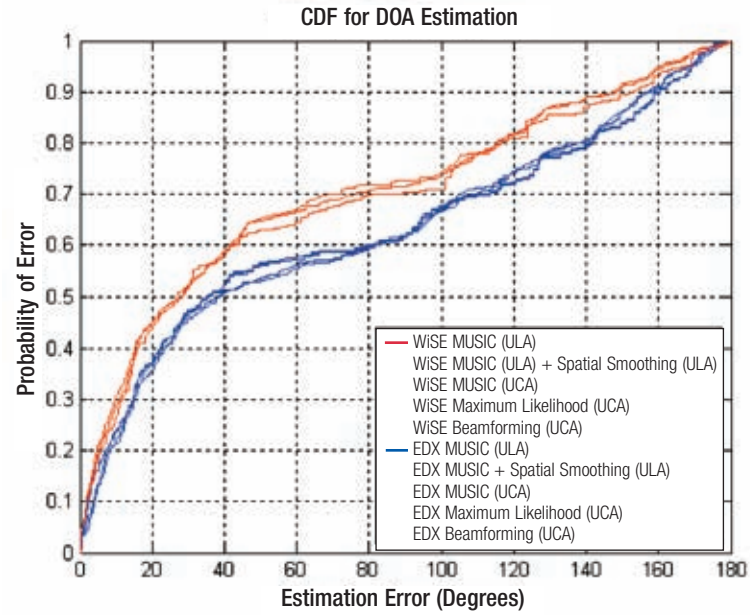
Major Indoor Localization Systems

Direction estimation techniques typically employ an antenna array to determine the direction-of-arrival (DOA) of a narrowband signal at a receiver. The antenna array consists of N elements positioned in a linear or circular fashion, separated by about a half of the wavelength of the transmitted narrowband signal. The estimation accuracy improves with increasing N. Lowering the center frequency of the narrowband signal makes it easier for it to penetrate building materials. However, a larger N or a lower frequency implies a bulkier antenna array, which

may become an issue. An emitted RF signal bounces off walls, ceilings, and other objects in a building. These reflections arrive at a receiver with various strengths and at different times, depending on the paths they take. There is also transmission through walls, ceilings, and so on, which severely attenuates the signal. Unfortunately, the direction of the strongest arrival may not be the same as the direction of the transmitter in indoor environments. Therefore, even if the direction estimation algorithm accurately estimates the direction of the strongest arrival, that would not be the relevant direction for localization purposes.

We used ray tracing to compute all the paths an RF signal would take as it travels from a transmitter to a receiver inside a building with a given floor plan and known construction material. Many other details need to be specified, which we do not list in this article. We evaluated the performance of some of the best known direction estimation algorithms in many different scenarios. Each scenario corresponds to one location pair for transmitter and receiver inside the building. Figure 2 shows the cumulative distribution function of the direction error in degrees obtained by using two ray-tracing tools. This is a negative result, because it shows that, half the time, the angle/direction error is larger than 40 degrees. We conclude that indoor localization based on direction estimation will not meet the location accuracy levels desired by first responders.

FIGURE 2. Cumulative Distribution Function (CFD) of Direction Error for Various Direction Estimation Algorithms and Two Ray-Tracing Tools (WiSE and EDX)



Ultra wideband (UWB) technology is the most promising approach for indoor ranging. In UWB ranging, a transceiver transmits a pulse lasting a few nanoseconds. Due to multipath propagation, hundreds or even thousands of delayed and scaled copies of this signal arrive at a receiver. The first arrival corresponds to the direct path—the straight line between the transmitter and the receiver. Unfortunately, the first arrival is typically not the strongest one, because walls and other objects on the direct path attenuate the signal propagation along that

path. However, as long as the first arrival can be detected and differentiated from the background noise, we would have fairly accurate ranging. If the ranging algorithm erroneously designates a later arrival, corresponding to a propagation path consisting of a number of reflections, as the first arrival, then it overestimates the true range by outputting the length of the path consisting of reflections. The algorithm can also underestimate the range if it mistakenly takes a noise or interfering signal arrival prior to the true first arrival as the first arrival. Increasing the bandwidth of the transmitted UWB signal and/or its power, using antennas with better characteristics, and increasing the receiver sensitivity are among ways of minimizing this problem and reducing the average range error. These will either increase the equipment cost or result in stronger interference to other wireless systems.

We assembled a tunable channel sounder in the 2 to 8 GHz frequency band at the National Institute of Standards and Technology (NIST) to evaluate the performance of UWB ranging (see Figure 3). A channel sounder is typically used to characterize and model RF propagation channels to enable a more judicious design of wireless communication systems. The evaluation system allowed varying the bandwidth of the UWB signal from 0.5 to 2 GHz, its center frequency from 3 to 7 GHz, and its power up to 1 watt. We used omnidirectional antennae at both the transmitter and receiver.

FIGURE 3. UWB Channel Sounder Developed at NIST

We carried out a comprehensive evaluation of ranging performance in four NIST buildings. Table 1 shows the average and maximum range error in these experiments. Excluding easier LOS scenarios in long corridors, we were able to obtain accurate non-LOS (NLOS) ranging performance up to 45 meters range in the first three buildings, with the signal penetrating up to a dozen walls. Specifically, the ranging error in these buildings averaged 1 percent, 2 percent, and 4 percent, respectively. Even though RF signals cannot penetrate metal, we were able to obtain 10 percent ranging error performance up to 15 meters range in the building that had a lot of steel in its wall material.

TABLE 1. Performance of UWB Ranging in Four NIST Buildings

Building wall material	LOS error (cm)		NLOS error (cm)		Maximum number of walls penetrated
	Average	Maximum	Average	Maximum	
Sheetrock/aluminum studs	4	10	24	41	12
Plaster/wooden studs	7	16	38	133	7
Cinder block	4	8	84	157	9
Steel	9	27	350	948	9

Recall that 3D location of a mobile user is determined through triangulation using range estimates to four reference nodes. If all the range errors are less than e, then the location error—the distance between the true location and its estimate through the triangulation process—will be a fraction of e. Therefore, a 1- to 2-meter ranging error performance at ranges of up to 45 meters satisfies first-responder requirements. We used a transmit power of 1 watt in our experiments. This level of RF energy far exceeds the UWB transmission power mask set by the Federal Communications Commission (FCC) for UWB communications. However, the FCC has apparently relaxed these limits for first-responder localization.

In principle, GPS-equipped fire trucks or police cars positioned outside a building on fire can serve as reference nodes for indoor localization based on UWB ranging. This means that the building itself does not have to have any networking infrastructure to facilitate localization. In the following paragraphs, we describe two indoor localization systems requiring that some networking equipment be installed in the building prior to the emergency: one requires the availability of a wireless fidelity (WiFi) network in the building, and the other requires the installation of passive radio-frequency identification (RFID) tags.

A WiFi-based system requires "training" of the localization system ahead of any emergency. Specifically, the received signal strength (RSS) from various WiFi access points (APs) is measured at a sufficiently dense set of points at known locations in the building, resulting in a catalog of (location, RSS vector) pairs. Then, the set of RSS values from various APs measured by a mobile user is matched to an entry in the catalog, and the location associated with that entry is declared as the mobile location. (More sophisticated variants of this approach—for example, taking the speed by which a first responder moves around—have also been developed.) Com-

pared to UWB ranging and direction estimation equipment, the localization system just described is inexpensive because it is based on readily available WiFi equipment. We developed and tested such a system and obtained a location accuracy of 1 to 3 meters, which may not be adequate for first responders. Both the need for a WiFi network in the building and offline training are drawbacks for this approach. Any significant modification, rearrangement, or introduction of new furnishings or WiFi APs in the building would make it necessary to repeat the training step.

It would be unrealistic to assume the availability of WiFi networks in all buildings, but it might be possible to mandate installation of passive RFID tags in buildings in the same way that sprinklers were added to building codes. If such tags are available and each first-responder radio is equipped with an RFID reader, then the reader would read a tag when the first responder passes by the tag. The location of the first responder can be determined by a table lookup, provided that a table of RFID tag identification numbers and their locations is constructed ahead of time and made available to first responders upon visiting the building.

Similarly, the IC can determine the first-responder location if the identification number of the RFID tag just read by the first responder is communicated to the IC. This system has two important merits:

- By populating a building with a sufficient number of RFID tags, this system can meet the indoor localization accuracy requirements of first responders.
- The prices for passive RFID tags are trending lower, and unlike smoke detectors, RFID tags do not require batteries.

The system has two drawbacks:

- RFID tags must be installed in the building prior to any emergency.
- The first responder needs to have radio connectivity with the IC and at least be able to send a few bytes every time he/she encounters an RFID tag.

We have also developed a reliable, multihop communication system for first responders at NIST that easily meets this minimal communication requirement and a lot more. More information about this RFID-assisted indoor localization system can be found in the article by Kate Remley and others elsewhere in this issue.

Even though NIST has taken major strides in characterizing and evaluating the performance of ranging, direction estimation, and localization techniques and systems through simulations (via ray tracing), as well as real measurements in various buildings, a standardized procedure is needed for evaluating localization products from various companies. This requires a national testing facility consisting of one or more buildings made of different construction materials, a number of testing scenarios, and metrics for measuring various aspects of performance and not just location accuracy.

Finally, a standard for indoor localization now exists. Task Group 4a in the Institute of Electrical and Electronics Engineers (IEEE) Working Group on Wireless Personal Area Networks (WPAN) has just completed a standard for a low-rate WPAN based on UWB technology that has ranging capability. NIST was active in this standardization process and contributed to the development of the standard. However, IEEE focused on developing technical specifications for a WPAN with ranging capability, not necessarily for emergency response operations. Therefore, localization standards that account for the specific needs of first responders are still needed. Fortunately, the National Fire Protection Association, with help from NIST, plans to develop such a standard for firefighters. Such a user-centric standard would lay out the specifications for shape and form for localization products, packaging resistance to high heat (perhaps up to several hundred degrees Celsius), water and severe shock, intrinsic safety RF energy levels, user interface, and so on. Deployment of standardized indoor localization equipment prevents proliferation of equipment based on proprietary technology and any potential interoperability problems.

Conclusions

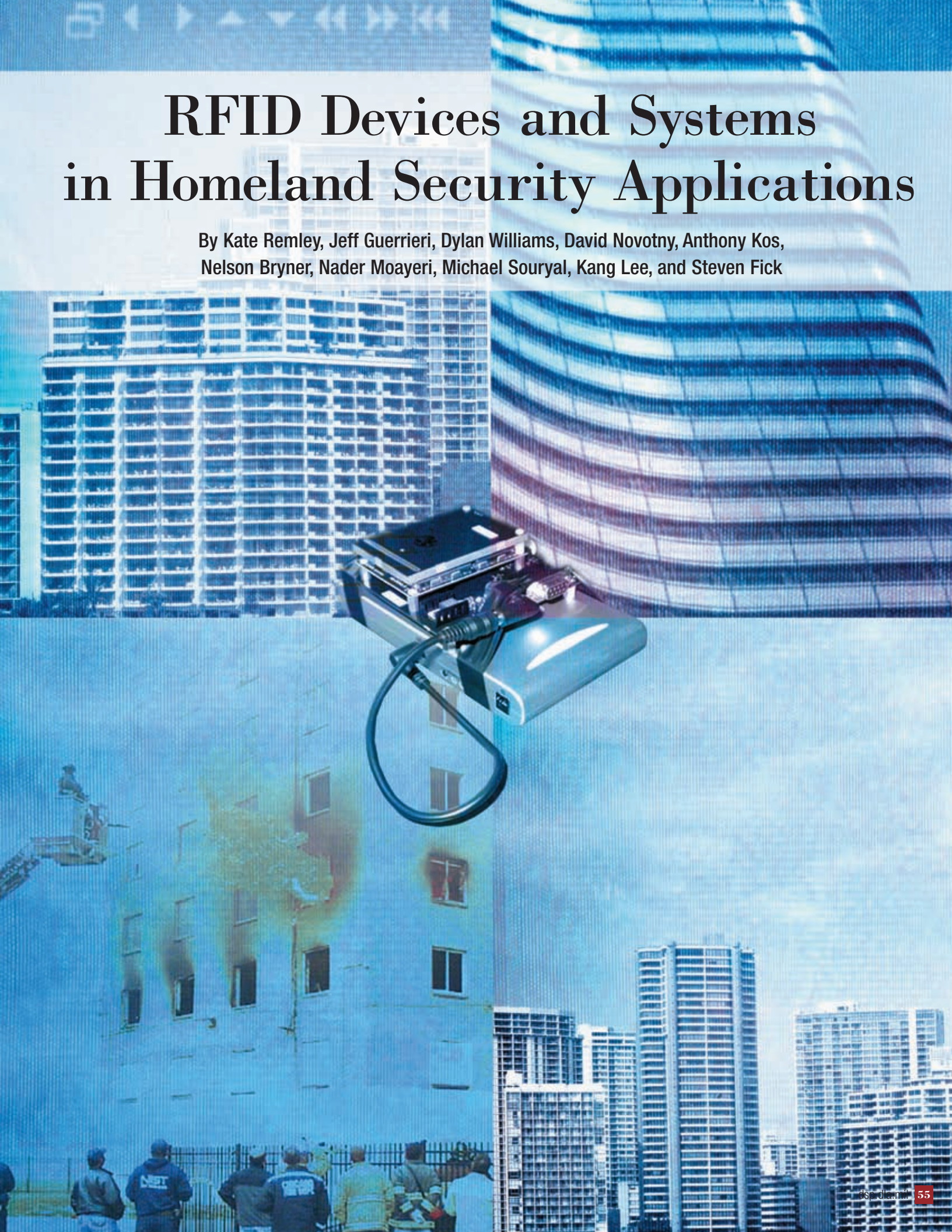
Presently first responders do not have any indoor localization capability whatsoever. They often do not even know which first responders have entered a building during an emergency, and they have to resort to calling the roll to get an idea of who might be in the building. Nevertheless, they want to have indoor localization systems that are accurate in all kinds of buildings, are inexpensive, and, preferably, are integrated with their radios and that do not rely on any networking infrastructure. At present, no single indoor localization technology or solution would meet all these requirements. However, much progress has been made in indoor localization over the past decade, and it should be possible to develop hybrid indoor localization solutions that would meet most of the requirements. For example, an RFID-assisted localization system can be integrated with a dead-reckoning system to provide a better estimate of a first responder's location when between encounters with passive RFID tags. Barometric pressure gauges can be used to provide an indication of which floor of a high-rise building a first responder is on. Similarly, it may be possible to take advantage of other technologies, such as acoustics and even infrared, along with RF technology to come up with more accurate and effective indoor localization solutions. In closing, some indoor localization capability is better than none. It is reasonable to assume that we will see various generations of indoor localization systems with improving performance over the next two decades.

About the Authors

Nader Moayeri, Camillo Gentile, Kamran Sayrafian, and Michael Souryal are researchers at the National Institute of Standards and Technology. Their research interests are in wireless communications, indoor localizations, wireless sensor networks, pervasive computing, and intelligent transportation systems. Their work focuses on testing and evaluations, measurements, standards development, and technology development.

RFID Devices and Systems in Homeland Security Applications

By Kate Remley, Jeff Guerrieri, Dylan Williams, David Novotny, Anthony Kos, Nelson Bryner, Nader Moayeri, Michael Souryal, Kang Lee, and Steven Fick



The National Institute of Standards and Technology (NIST) is carrying out numerous projects to ensure secure, reliable use of radio-frequency identification (RFID) technology in homeland security and public safety applications. This article reports on some of those projects. The projects support the Science and Technology Directorate of the Department of Homeland Security (DHS) in the development of measurement infrastructure, consensus standards, and key technologies for applications such as access control, critical asset protection at the border, and position localization for first responders.

Background

RFID technology is increasingly used in applications related to both homeland security and public safety, in part because of the ergonomic benefits and increased efficiency of remote activation, and in part because of the potential for increased security during transactions. Consensus standards that guide the design and performance verification of RFID technology have typically been developed with business or private-sector applications in mind. However, for many applications related to homeland security, a high level of security and reliability must be guaranteed. DHS must ensure that mission-critical transactions are robust. Applications include identity authentication and access control using government-wide smartcards, enhanced data exchange and position localization for first responders, and, at the border, critical asset tracking and protection such as improved container and cargo security.

To address the need for secure, reliable, and effective application of current and future RFID technology in homeland security applications, DHS has tasked NIST to develop measurement infrastructure and capabilities for RFID that will (1) ensure secure and reliable functionality through development of appropriate measurement methods, performance metrics, and testing protocols; (2) support development of key technologies to facilitate reliable use of RFID systems for homeland security and first-responder applications; and (3) support relevant standards development efforts. NIST is uniquely positioned within the federal government to help provide the technical and measurement infrastructure that will ensure secure and reliable use of RFID technology for homeland security and first-responder applications. NIST has technical expertise to provide impartial, rigorous verification of RFID component and system performance.

Results of this project are disseminated through reports and publications, as well as through direct interaction with the committees of standards developing organizations such as the following:

- Institute of Electrical and Electronics Engineers, Inc. (IEEE) 1451 (smart transducers)
- ISO/International Electrotechnical Commission (IEC) 14443 (electromagnetic and mechanical durability)
- ISO/IEC 18000 (air interface standards)
- ISO/IEC 10373-6 (test methods for proximity cards)
- National Fire Protection Association (NFPA), Committee on Electronic Safety Equipment, 1982 (personal alert safety systems) and 1221 (emergency services communications systems)
- EPCglobal/GS1.[1]

Participants in this project are involved with several of these committees. This work also supports various commercial tracking efforts, the unique identification mandated by the Department of Defense (DoD), and the e-pedigree of the Food and Drug Administration, as well as work with the NIST Federal Information Processing Standards 140-3 (security requirements for cryptographic modules) and 120 (graphical kernel system).

Project Activities

The NIST project on performance metrics and standards for RFID in homeland security applications was developed to address critical vulnerabilities and gaps in the verification and use of RFID technology in homeland security and public safety applications. Major activities are as follows:

- Electromagnetic (remote) security
- Electronic (on-chip) security
- Reliability in first-responder applications
- Technology for tracking and positioning for first-responder applications
- Standards for integrating RFID systems and sensor networks.

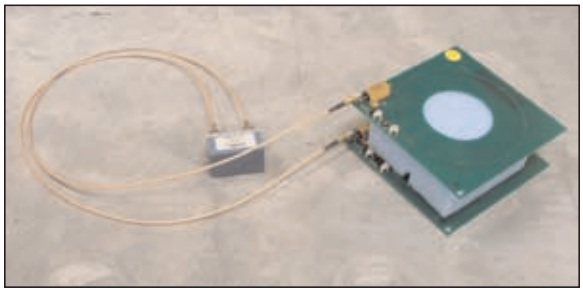
To address the vulnerabilities outlined above, five different NIST operating units are contributing. These activities are discussed in more detail below.

ELECTROMAGNETIC SECURITY

This activity was initiated in 2006 to quantify electromagnetic vulnerabilities of RFID systems and to address security concerns with respect to the wireless nature of RFID technology. This project is investigating these vulnerabilities by performing rigorous, repeatable test and evaluation of RFID systems for eavesdropping and jamming:

- *Eavesdropping.* Transactions between RFID readers and security cards used in the workplace may be remotely monitored and recorded. This project is studying the distances at which remote monitoring can occur and the equipment that is required to do so. Methods to mitigate vulnerabilities, such as shielding of the card or reader, are also being investigated.
- *Jamming.* The failure of an RFID reader to operate may be the result of technical difficulties. However, it may also be the result of intentional jamming of the system to cause chaos, or it may be the result of interference, an unintentional form of jamming. For example, at a hospital, a pharmaceutical RFID reader could be subject to interference from a high-power RF source such as that found in a Magnetic Resonance Imaging system. Using equipment such as the portable dual-loop antenna shown in Figure 1, NIST is studying power levels and signals that can jam RFID transactions and is making recommendations on ways to alleviate jamming.

FIGURE 1. Dual Loop Antenna Used for Jamming Research



ELECTRONIC (ON-CHIP) SECURITY

This multiyear project is focusing on the technology required to ensure physical chip-level security for RFID cards and tags. This includes steps necessary to protect the data, passwords, and encryption keys stored in the memory of the integrated circuits on the RFID cards and tags. The project is taking the first step toward comprehensive and open standards for RFID-based access and tracking systems in the government. Also being investigated are methods of producing and identifying counterfeit cards and tags. Figure 2 shows one method for counterfeiting: removal and duplication of an integrated-circuit chip from an RFID card. In Figure 3, the signal emitted from the RFID card is monitored for analysis of its electromagnetic signature to enable detection of a counterfeit card.

RELIABILITY IN FIRST-RESPONDER APPLICATIONS

In the future, first responders—including law enforcement personnel, firefighters, and medical personnel—may use RFID tags to locate and track team

FIGURE 2. Integrated Circuit After Removal from an RFID Card

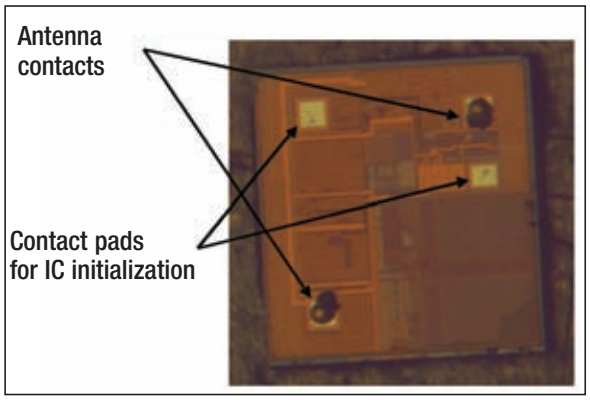


FIGURE 3. Noninvasive Counterfeit Detection Using Waveform Measurements

members, suspects, prisoners, or victims. Public safety applications such as these involve the exposure of tags to extreme environmental conditions such as high temperatures and mechanically adverse conditions. Extensive characterization of current and future materials and system reliability under both routine and adverse conditions is required to ensure desired functionality. Currently, there are no standards or test protocols for exposing RFID hardware to the high temperatures encountered by firefighters. In addition, it is not clear how well RFID-assisted position location technology would perform as a standalone stationary installation or as part of a moving or portable system. The NFPA Committee on Electronic Safety Equipment has deferred development of RFID-based device standards, citing a lack of data and testing protocols. This activity will aid in resolving this situation.

To date, this project has developed thermal and building type classifications as part of necessary performance metrics for RFID tag-based locator systems for first responders. Figure 4 shows a test fixture used to determine the exposure of an RFID tag to high thermal temperatures.

The project has also carried out laboratory tests of components of RFID systems in rough-duty and fire conditions, as well as a series of preliminary live fire experiments in a 16-story residential high-rise structure outside of Chicago, IL, as shown in Figure 5. In the future, this project will extend results of the field tests to many types of RFID systems in rough-duty and fire conditions, evaluating performance in the presence of high temperatures, water, and soot.

FIGURE 4. Test Fixture for Exposing RFID Tags to High Temperatures

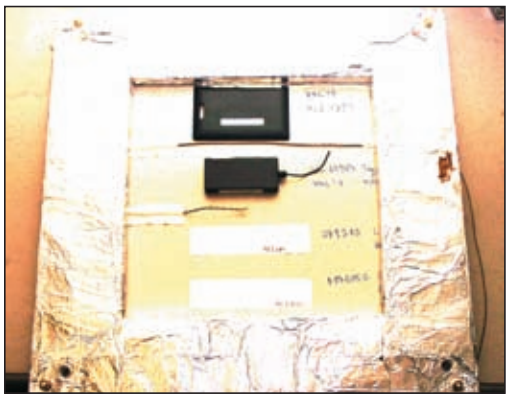


FIGURE 5. Field Tests Exposing RFID Tags to Rough-Duty Conditions at a 16-Story Building Scheduled for Demolition

TECHNOLOGY FOR TRACKING AND POSITIONING FOR FIRST-RESPONDER APPLICATIONS

This activity is examining the feasibility and performance of an indoor RFID-based wireless network for improved localization and tracking of emergency personnel. One such possibility utilizes passive RFID tags pre-installed at known locations in the building. The mobile user (for example, a first responder) is equipped with an RFID reader that continuously scans for the tags. Figure 6 shows two such prototype systems. Upon being read, tag information can be correlated with a database of tags' locations. Alternatively, location information embedded in the tag itself can be read and the user's location identified. With a wireless communications network, the positions of personnel can be relayed to a central location such as an incident command station.

FIGURE 6. Readers Modified for Use in RFID-Assisted Localization Networks

In 2006, this project studied RFID and wireless network subsystems amenable to further development and testing. Readers were integrated with a multihop ad hoc communications network for transmission of tag information to a central location. In particular, the project demonstrated transmission of IDs of passive RFID tags, deployed on each floor of an 11-story office building, over a multihop wireless ad hoc network to a laptop located on the ground floor of the building. The project has begun development of the graphical user interfaces necessary to display the position of each mobile user on portable communication devices, as well as the positions of all mobile users on the base station display.

Software is being developed to direct a first responder, in a life-threatening situation, to the nearest building exit. The project is also working to extend the range of the RFID readers. Although a reader with a 10-meter read range would not be accurate enough for meaningful position localization, a read range on the order of centimeters would force the responder to swipe the RFID card near the reader, modifying his or her behavior. This would not work either. To address this aspect, the project is developing methods to optimize the read range on the order of 1.5 meters, specifically for first-responder applications.

STANDARDS FOR INTEGRATING RFID SYSTEMS AND SENSOR NETWORKS

RFID tags can identify an asset, whereas sensors can tell the asset's condition. These two purposes are served by independent systems, but many situations require that these and other data be fused to provide mission-critical information. Therefore, this project is developing standards that will facilitate combining RFID technology and networked sensors to allow autonomous monitoring of the health and safety of first responders working in hazardous environments. Combining these technologies will greatly reduce system complexity and thus improve efficiency in communication, control, and command.

Combining the functionality of RFID tags and wireless sensor networks will expand the overall func-

tionality and capability of each of these technologies. Such systems may be applied to complex environments for applications ranging from battlefield surveillance to environment monitoring and telemetry of the health of first responders during incidents and operations.

Since 2006, this project has coordinated and held discussions with the IEEE 1451 groups on sensor standards and the ISO/IEC group concerned with the integration of sensors and RFID tags. This led to the creation of an IEEE standards development project for an IEEE 1451.7 draft standard for sensor-to-RFID tag communication.

Conclusion

Many of the expected outcomes of this project will support standards development for RFID technology in homeland security and DoD applications. The following are some examples of the outcomes of the activities described above:

- Reports on electromagnetic vulnerability of long-range RFID systems disseminated to (as appropriate) ISO/IEC 14443, ISO/IEC 18000, and ISO/IEC 10373-6
- Reports disseminated to working groups on NFPA 1982 and NFPA 1221
- Prototype integration of a dead-reckoning module into an RFID-assisted localization system disseminated to NFPA 1221
- Consensus standards development project for IEEE 1451.7 for sensor-integrated RFID systems (under way).

At the request of the DHS Science and Technology Directorate, NIST is applying a cohesive approach and improved measurement science to address the most pressing impediments to the deployment of secure and reliable RFID technologies for homeland security and first-responder applications.

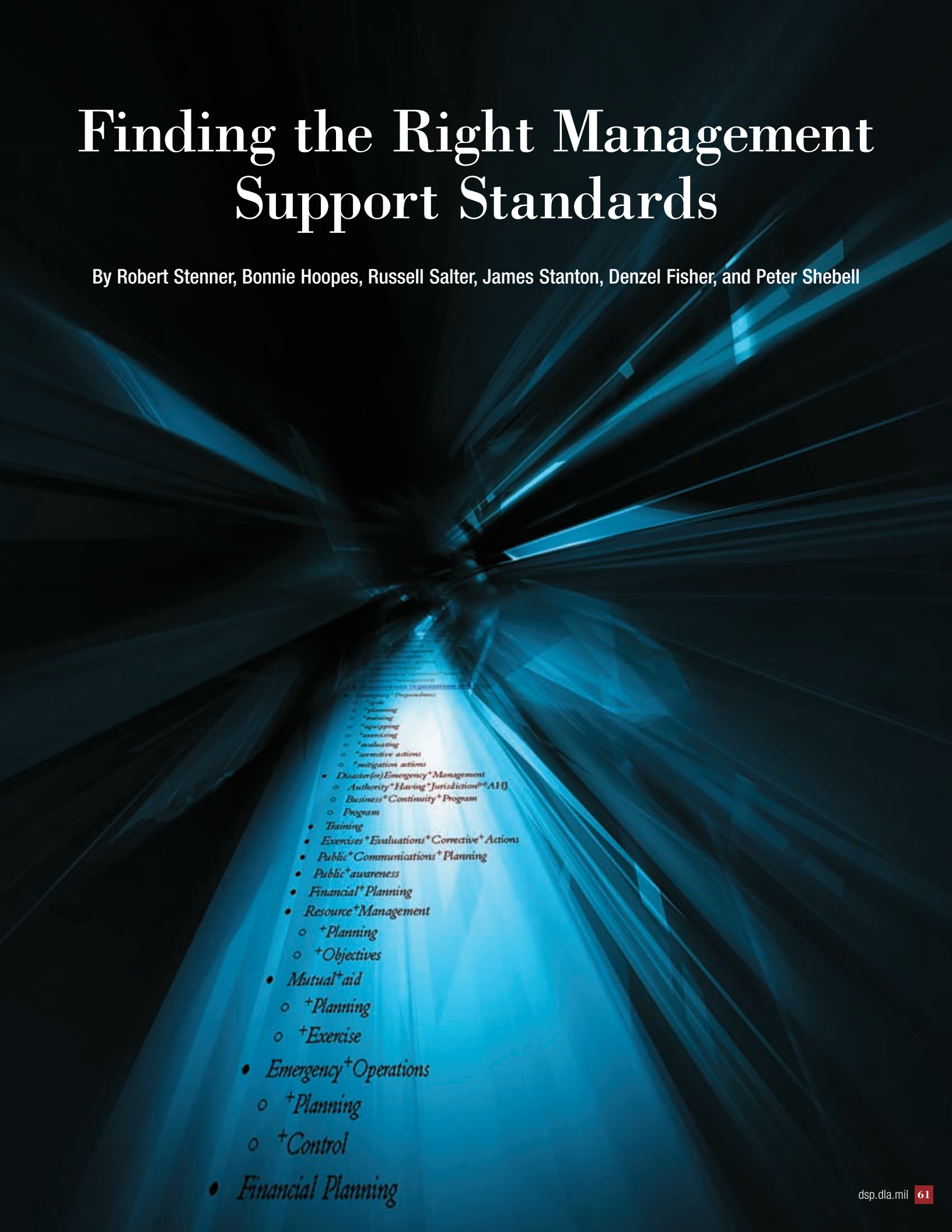
[1]EPCglobal develops industry-driven standards for the Electronic Product Code to support the use of RFID in today's fast-moving, information-rich trading networks. GS1 is an organization dedicated to the design and implementation of global standards and solutions to improve efficiency and visibility in global supply and demand chains.

About the Authors

The authors are all NIST employees. Kate Remley, Jeff Guerrieri, Dylan Williams, David Novotny, and Anthony Kos work at the Electrical and Electronics Engineering Laboratory in Boulder, CO. The remaining authors are located at NIST headquarters in Gaithersburg, MD. Nelson Bryner works at the Building and Fire Research Laboratory, Nader Moayeri and Michael Souryal work at the Information Technology Laboratory, and Kang Lee and Steven Fick work at the Manufacturing Engineering Laboratory.

Finding the Right Management Support Standards

By Robert Stenner, Bonnie Hoopes, Russell Salter, James Stanton, Denzel Fisher, and Peter Shebell



It is the responsibility of the federal government to coordinate and facilitate the creation of national systems aimed at harmonizing disparate systems utilized by state and local governments in order to better serve the public. The identification of national standards is often a logical first step in the harmonization process. This article reports on a method involving a combination of technology and subject matter experts to identify standards to support the creation of a national-level system for managing incidents.

The Challenge

The challenge was to thoroughly, consistently, and objectively review and evaluate 141 standards against a new national policy for managing incidents and to identify a subset that could serve as the foundation for a national system for managing incidents. The national policy was articulated in the Federal Emergency Management Agency document 501, *National Incident Management System*, also referred to as NIMS. The standards were quite diverse, ranging from performance standards for management systems to technical standards for equipment and professional disciplines.

The Approach

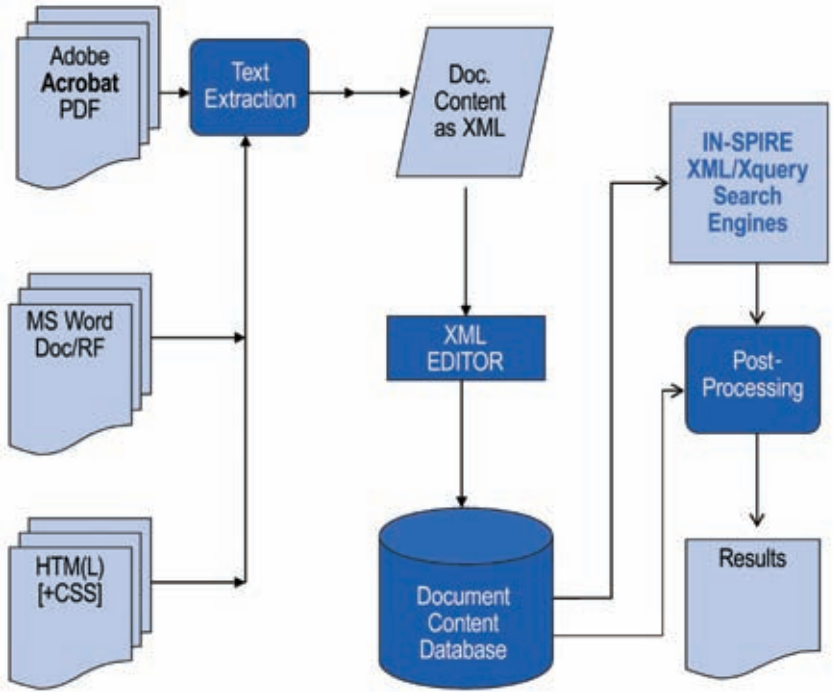
The basic approach was to use technology to assist a small technical review team with their evaluation of the standards. The technology was designed to help the review team be efficient while remaining objective, consistent, and thorough. The first step was to decompose the NIMS document into small phrases or word-strings—a series of key words, to be examined in relationship to each other, that succinctly defines the respective criteria or requirements—that would serve as search criteria, while retaining the overall structure and key content of the document. The 141 standards were converted into an electronic format and searched using an automated search tool. The output of the search tool was then used by the review team to develop a color-coded grading system to report how well each standard met specific NIMS criteria.

This approach can be applied to any subject area search for standards. The two key aspects to this approach are (1) developing precise word-string relationship criteria that adequately define the subject of the search, and (2) finding a few qualified experts who understand the subject well to serve on the technical review team.

Search Tool

The search tool was designed to consistently locate and group information based on the word-string relationships. The search tool was assembled using data mining software called IN-SPIRE[1] coupled with Extensible Markup Language (XML)[2] and Xquery[3] search engines and tools. Figure 1 shows the components of the tool used for the NIMS standards search. We used these tools because they were readily available and convenient for our use, but any convenient data mining and word-string relationship query tools should be adequate to assemble

FIGURE 1. Components of a Standards Review Tool



such a search tool. However, it will prove invaluable to include a person on the technical team who is intimately familiar with the formats and search tools selected.

We incorporated the following types of word-string relationship searches into our tool:

- *Match.* Search for text that exactly matches the search criteria, including order of words in string and form of words.
- *Fuzzy.* Search for text that exactly matches the search criteria, including order of words in string, but consider various forms of the words in the word-string (for example, monitor, monitoring, monitored).
- *Near.* Search for text containing all the words in the word-string criteria in the specific order with less than one word between them. It is case-sensitive.
- *&=.* Search for text containing all the words in the word-string criteria in any order without regard to distance between them.

These different types of word-string searches allowed us to progressively expand the search to find applicable subject areas in a standard that did not use precise or NIMS-specific language.

As previously noted, the development of precise word-string search criteria is essential for meaningful output data. The best resources for developing such criteria are requirement documents that have accurate and consistent language along with precise terminology. For example, our search used the NIMS document and the National Incident Management Compliance Assessment Support Tool (NIMCAST).[4] Figure 2 is an example of our word-string search criteria.

FIGURE 2. Examples of Word-String Criteria

NIMS Component I–Preparedness

- *Emergency+Operations+Center(or)EOC*
- *Emergency+response+nongovernmental+organization(or)NGO*
  - *+private+outreach*
- *Emergency+management*
  - *public+awareness*
  - *information+ systems*
- *Emergency+response*
  - *information+operations+security*
  - *resource+management*

I-A. Preparedness Organizations and Programs

- *Emergency+Preparedness*
  - *+cycle*
  - *+planning*
  - *+training*
  - *+equipping*
  - *+exercising*
  - *+evaluating*
  - *+corrective actions*
  - *+mitigation actions*
- *Disaster(or)Emergency+Management*
  - *Authority+Having+Jurisdiction(or)AHJ*
  - *Business+Continuity+Program*
  - *Program*
- *Training*
- *Exercises+Evaluations+Corrective+Actions*
- *Public+Communications+Planning*
- *Public+awareness*
- *Financial+Planning*
- *Resource+Management*
  - *+Planning*
  - *+Objectives*
- *Mutual+aid*
  - *+Planning*
  - *+Exercise*
- *Emergency+Operations*
  - *+Planning*
  - *+Control*
- *Financial Planning*

Legend

+ means "and" for a linked word-string that needs to be found in relationship together before tool will return a find.

(or) means the terms are exchangeable and need to be searched with the + terms using both terms as separate word relationship strings (e.g., Emergency+Operations+Center(or)EOC+resource+dispatch+tracking should be searched as Emergency+Operations+Center+resource+dispatch+tracking and as EOC+resource+dispatch+tracking).

The output from the tool was organized to facilitate the review by the technical team. Table 1 is an example of a summary output table from the NIMS standards search, and Table 2 is an example of a detailed output table from the NIMS standards search.

TABLE 1. Example Summary Output Table

	Component	Document	
		NFPA 1561	NFPA 1600
I	Preparedness		
I-A	Preparedness Organizations and Programs	3 near 4 &=	5 near 6 &=
I-B	Implement Emergency Preparedness Cycle	4 near 4 &=	3 near 4 &=
II	Communications and Information Management		
II-A	Communications and Incident Management	23 near 24 &=	6 near 7 &=
II-B	Effective Communications, Information Management and Information Sharing	4 near 4 &=	1 near 1 &=
II-C	Establishing and Maintaining a Common Operating Picture and Ensuring Accessibility and Interoperability		
II-D	Managing Interoperable Communications and Data	1 &=	

TABLE 2. Example Detailed Output Table

Comp	II-B. Effective Communications, Information Management and Information Sharing
Qu	.&= 'Incident communications' and.&= 'Incident Command common communications operating system'
Qu	.&= 'Incident communications' and.&= 'Incident Command interoperable communications'
Qu	.&= 'Emergency' and.&= 'Communications'
	NFPA 1561 •6.1 Communication Systems •6.1.1 The *communications* system shall meet the requirements of the *emergency* response agency for routine and large-scale emergencies. •6.1.4* An ESO shall provide additional radio channels for the volume of *communication*s relating to incidents with multiple tactical channels and for the complexity of multiple *emergency* incidents. •6.3 Emergency Traffic •6.3.1* The *communications* system shall provide a standard method to give priority to the transmission of *emergency* messages and notification of imminent hazards over that of routine *communications* to all levels of the incident command structure. •6.4 Telecommunicator Support •6.4.3* The incident commander shall be provided with reports of elapsed time-on-scene at *emergency* incidents in 10-minute intervals from the ESO *Communications* Center, until reports are terminated by the incident commander. •7.1 Incident Commander •7.1.9 The incident commander shall be responsible for controlling *communications* on the tactical, command, and designated *emergency* traffic channels for that incident.
Qu	.&= 'Emergency' and.&= 'Warnings'
Qu	.&= 'Public communications'
Qu	.&= 'Communication warnings'

Technical Review

Our technical review occurred in four phases:

- *Phase 1.* The team collectively defined criteria to assess the ability of each standard to meet NIMS objectives—in other words, the extent to which a specific standard, or parts of a standard, contributes to the establishment of a uniform and consistent incident management system across the nation.
- *Phase 2.* Each team member read each standard in its entirety to understand its specific content and context and to draw individual conclusions regarding the respective standard's relevance to NIMS.
- *Phase 3.* The team collectively developed a color-coded "dashboard" matrix compatible with the search tool criteria. The color-coding reflected the extent to which the standard, or parts of the standard, applied to NIMS (fully, partially, or only tangentially). Visually presenting the information enabled the team to readily understand an extremely large amount of complex information.
- *Phase 4.* The team discussed each standard, applying the criteria and developing a consensus on the applicability of the whole standard or parts of each standard to the established NIMS criteria. The team also reached a consensus on color-coding and agreed on comments to be included in the analysis.

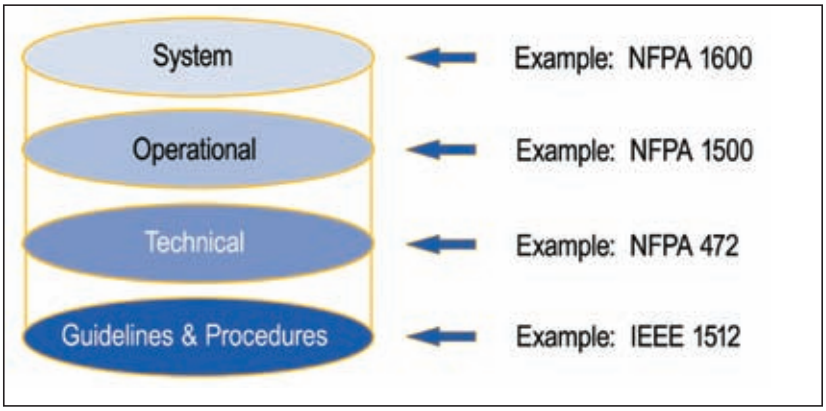
To accomplish these four technical review phases, the technical team used 12 steps:

1. Identify keywords and concepts found within NIMS component criteria.
2. Identify standards appropriate for review.
3. Apply the search tool to identify the presence and frequency of keyword relationships in each standard using criteria derivatives.
4. Develop a matrix to record the presence of keyword/phrase relationship "hits" found in the respective standard.
5. Independently read each standard to assess its applicability to NIMS.
6. Independently assess each standard.
7. Collectively review and discuss each standard using a set of consensus criteria: scope, relevance, operational application, organization level, and completeness. For standards relating to specific emergency response functions, the standard's ability to contribute to emergency management integration was substituted for the completeness criterion.
8. Produce a color-coded matrix for each standard grouped by NIMS component criteria and consensus criteria; the color-coding was assigned using the criteria of Step 7 with color assignments based on the following rules: 4 of the 5 criteria found were rated dark green, 3 of 5 rated light green, 2 of 5 rated yellow, 1 of 5 rated orange, and 0 of 5 rated red.
9. Compare the findings with the presence of keywords or concepts found by the NIMS component criteria search tool to confirm the presence or absence of specific language.

10. Capture a brief information point describing the team's rationale and conclusion.
11. Collectively review the findings to ensure consistency within the group process.
12. Place the findings into a composite matrix of all standards and all criteria, by code, with comments.

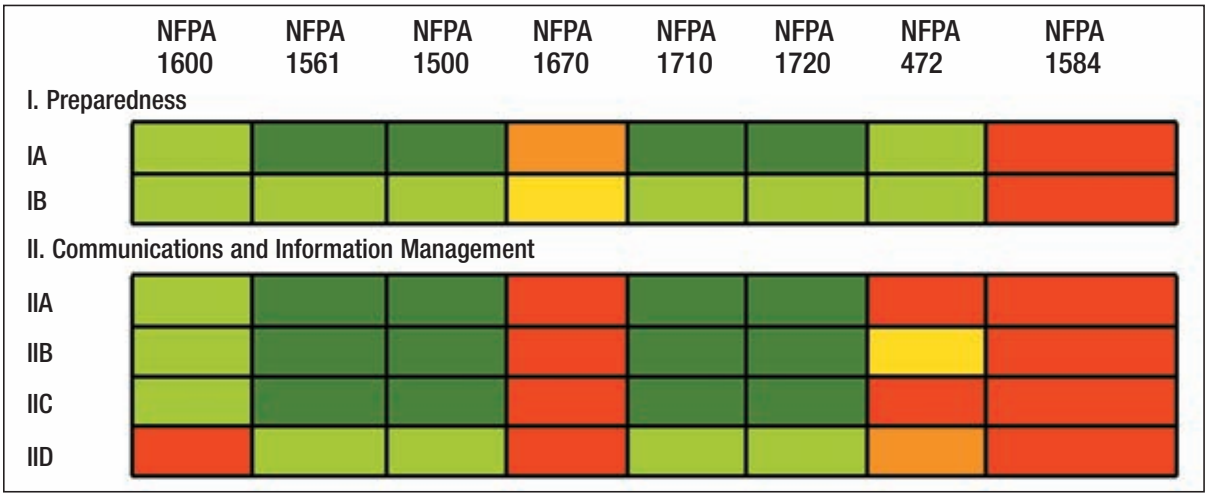
In reviewing applicable NIMS standards, the technical team found it valuable to group standards by type: system, operational, technical, or professional guidelines and procedures (tactical). Figure 3 shows the relationship of these different types of standards and provides an example of each type.

FIGURE 3. Types of Standards



The technical review produced two types of tables to display the color-coded results. The first is a dashboard table; Table 3 is an example. The color-coded gradient shows progressively how well each of the standards aligns with the specific search criteria. The progression ranges from dark green (best alignment), to light green, yellow, orange, and red (poor alignment). The other type of table displays applicable chapters or sections in a standard addressing each respective criterion and the color-coded alignment for each specific component of incident management.

TABLE 3. Example Dashboard Table



We captured the results of this analysis in a database (integrated into the tool) for future retrieval and application.

Technical Review Quality Control

The technical review of the tool-selected standards was an iterative process and frequently required the team to return to a previously reviewed standard to ascertain relationships with a particular standard being discussed. Upon reevaluating a standard, the team found it necessary to change only five previous color designations in an array of more than 680. This subsequent reevaluation process served as a quality control step for previously determined color-coding and analysis decisions. We recommend planning such a quality control reevaluation process into the technical review process to support the process and enable concurrent testing of conclusions being reached.

[1]IN-SPIRE is an information discovery tool, developed by the Pacific Northwest National Laboratory, that integrates information visualization with query and other interactive capabilities. It is designed to quickly and automatically convey the gist of large sets of unformatted text documents such as technical reports, web data, newswire feeds, and message traffic.

[2]XML is a versatile markup language, capable of labeling the information content of diverse data sources, including structured and semi-structured documents, relational databases, and object repositories.

[3]Xquery is a query language that uses the structure of XML intelligently to express queries across all kinds of data, whether physically stored in XML or simply viewed as XML.

[4]NIMCAST is a web-based self-assessment system developed by DHS's Federal Emergency Management Agency for use by state, tribal, and local departments and agencies to evaluate their incident preparedness and response capabilities. It is designed to help users determine what they need to do to comply with NIMS re-

About the Authors

Robert Stenner, a toxicologist at Pacific Northwest National Laboratory (PNNL), has more than 30 years of experience in emergency response, environmental health risk analysis, and human health impact analysis of xenobiotic agents. Dr. Stenner also chairs ASTM International E54.02 on Homeland Security Applications–Emergency Preparedness, Training, and Procedures.

Bonnie Hoopes, a technologist at PNNL, has more than 30 years of experience in web-based applications utilizing AJAX, JavaScript, PHP, Apache, XML query languages (Xquery and Xpath), open source (MySQL) and proprietary (eXist) databases, Google Earth, and Google Maps.

Russell Salter is president of Emergency Response Technology Integration Center (ERTIC), LLC. He has more than 25 years of experience in emergency management and response planning, training and exercising, most of which, was gained while directing major response programs with the Federal Emergency Management Agency.

James Stanton, a subject matter expert with ERTIC and the Maryland Emergency Operations Center, has been a leader in emergency management and preparedness at the local, regional, and national levels. He specializes in incident management and organization development to first-responder and governmental organizations.

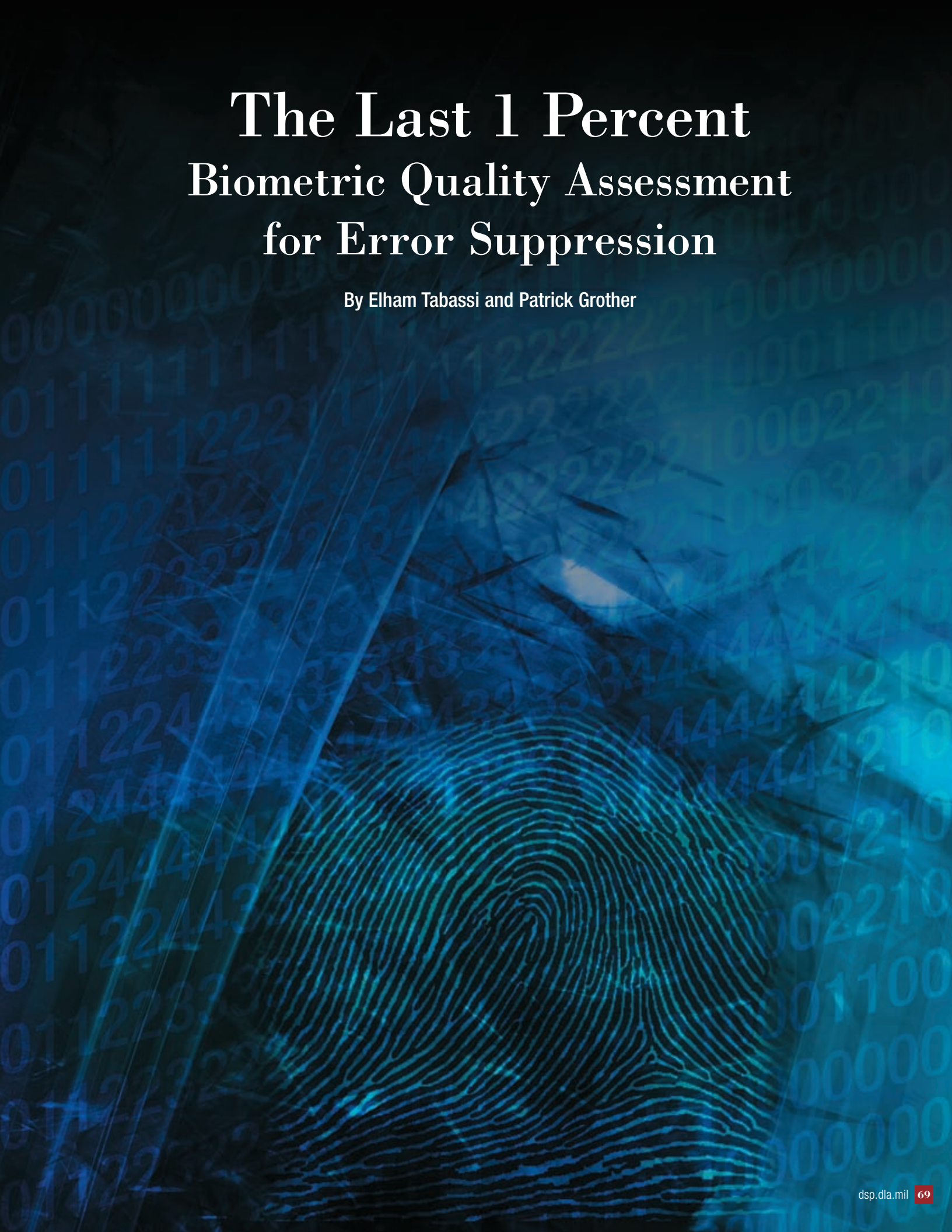
Denzel Fisher is executive vice president of ERTIC. Previously, he served 12 years in the Office of the Assistant Secretary of the Army for Installations, Logistics and Environment where he was responsible for developing and directing implementation of emergency preparedness and response policy for the Army's Chemical Demilitarization Program.

Peter Shebell is a program manager in the Office of Standards at the Department of Homeland Security. He served on detail to the National Incident Management Systems Integration Center in the Technology and Standards Branch.

The Last 1 Percent

Biometric Quality Assessment for Error Suppression

By Elham Tabassi and Patrick Grother



The performance of biometric systems depends on the quality of the acquired input samples. Accuracy of current biometric systems is high when high-quality samples are being compared.[1] However performance degrades substantially as sample quality drops. Although only a small fraction of input data are of poor quality, the bulk of recognition errors can be attributed to poor-quality samples. Poor-quality samples decrease the likelihood of a correct verification or identification, while extremely poor-quality samples might be impossible to verify or identify.

If quality can be improved, either by sensor design, by user interface design, or by standards compliance, system performance can be improved. For those aspects of quality that cannot be designed in, an ability to analyze the quality of a live sample is needed. This is useful primarily in initiating the reacquisition from a user, but also for the real-time selection of the best sample and the selective invocation of different processing methods. That is why quality measurement algorithms are increasingly deployed in operational biometric systems.

With the increase in deployment of quality algorithms, the need to standardize an interoperable way to store and exchange biometric quality scores increases. Recognizing this need, the Department of Homeland Security's (DHS's) Science and Technology Directorate initiated a program with the National Institute of Standards and Technology (NIST) to develop open-source software to compute quality scores of biometric samples (face and finger). DHS also asked NIST to develop standards that will establish an interoperable way of storing and exchanging biometric quality scores. This article gives an overview of NIST's biometric quality program.

What Is Meant by Quality?

Broadly, a sample is considered to be of good quality if it is suitable for automated matching. This viewpoint may be distinct from the human conception of quality. If, for example, an observer sees a fingerprint with clear ridges, low noise, and good contrast, then he might reasonably say it is of good quality. However, if the image contains few minutiae points then a minutiae-based matcher would underperform. Likewise, if a human judges a face image to be sharp, but a face recognition algorithm benefits from slight blurring of the image, then the human statement of quality is inappropriate. Thus, in the context of automated matching, the term "quality" should not be used to refer to the fidelity of the sample, but instead to the utility of the sample to an automated system. The assertion that performance is ultimately the most relevant goal of a biometric system implies that a quality measurement algorithm should reflect the sensitivities and failure modes of the matching algorithm. For fingerprint minutiae algorithms, this could be the ease with which minutiae are detected. For face algorithms, it might include how readily the eyes are located.

The definition of quality as a prediction of performance was first introduced by NIST when it released the NIST Fingerprint Image Quality (NFIQ) reference in August 2004. NFIQ, a fingerprint quality measurement tool, is implemented as open-source software conformant to the ISO/International Electrotechnical Commission (IEC) 9899:1999 "C" specification. It is used today in U.S. government and commercial deployments. Its key innovation is to produce a quality value from a fingerprint image that is directly predictive of expected matching performance, and it has been designed to be matcher independent. There is now international consensus in industry, academia, and government that a statement of a biometric sample's quality should be related to its recognition performance.

NFIQ, a fingerprint quality measurement tool, is implemented as open-source software conformant to the ISO/International Electrotechnical Commission (IEC) 9899:1999 "C" specification...Its key innovation is to produce a quality value from a fingerprint image that is directly predictive of expected matching performance.

Overview of NIST's Biometric Quality Program

The NIST biometric quality program has three key elements:

- Development of standards for reporting and exchanging quality scores of biometric samples
- Development of open-source software that measures the quality of finger and face image data
- Provision of technical guidance on the use of quality scores, including quality surveying for quality assurance, measuring and reporting slap quality, and quality-directed processing and fusion.

A brief description of each of these elements follows.

STANDARDS FOR QUALITY SCORES OF BIOMETRIC SAMPLES

In January 2006, the ISO/IEC subcommittee on biometrics (SC 37) initiated work on ISO/IEC 29794, a multipart standard establishing quality requirements for fingerprint (Part 4), face (Part 5), generic aspects (Part 1), and, possibly, other biometrics later. US-VISIT expressed its interest and concern in the emerging ISO/IEC 29794 activity, and the FBI expressed the need for achieving interoperability of quality scores with DHS and other government agencies.

NIST has been involved in the ISO/IEC 29794 development process. In the generic ISO quality draft (ISO/IEC 29794-1), NIST succeeded in including a requirement that quality values be indicative of recognition performance, and it has made technical contributions on the representation, storage, and exchange of quality scores. The goal is to ensure the development of an improved standard that reflects the operational needs of the U.S. government, particularly the DHS US-VISIT program, Transportation Security Administration (TSA) registered traveler program, Personal Identity Verification (PIV), and international e-Passport.

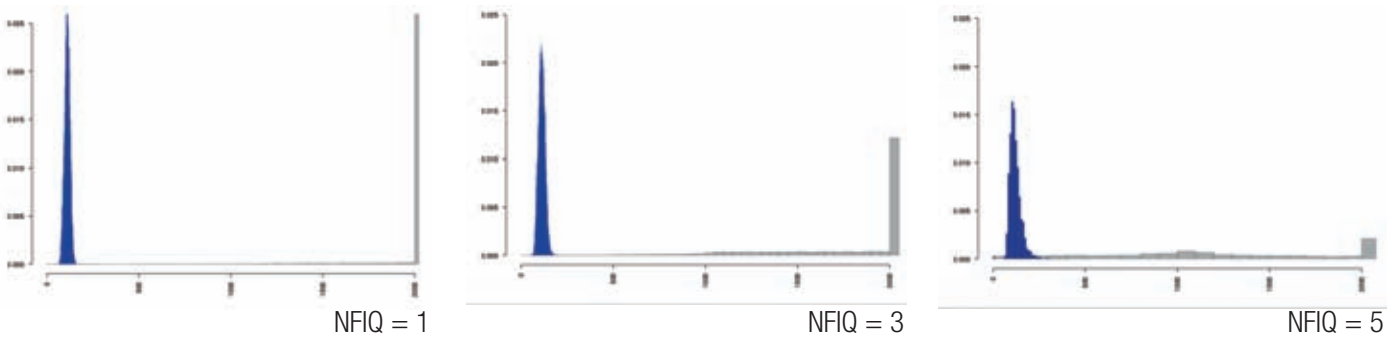
OPEN-SOURCE QUALITY MEASUREMENT SOFTWARE (FINGER AND FACE)

NIST has developed a fingerprint quality measurement algorithm specifically intended to predict performance. The method, called NFIQ, has won national and international acceptance and has become a de facto standard, and it is included in the Electronic Fingerprint Transmission Specification, which is a required standard for doing business with the FBI.

NFIQ formalizes the concept of biometric sample quality as a scalar quantity that is related monotonically to the performance of biometric matchers, under the constraint that at least two samples with their own qualities are being compared. A fingerprint sample should be of good quality if it is suitable for automated matching. That means a good-quality fingerprint has distinguishable patterns and features that allow the extraction of features, which are useful for subsequent matching of fingerprint pairs. This viewpoint may be distinct from human perception of quality. For example a fingerprint with clear ridges and good contrast might seem to be of reasonably good quality to an observer. However, if the image contains few minutiae, then a minutia-based matcher would not perform well. Therefore, NFIQ uses the term "quality" as a scalar summary of a sample that is taken to be some indicator of matchability. Technically speaking, NFIQ was developed to predict how far a genuine score would lie from its impostor distribution. Therefore, it is effective at improving false rejections while suppressing false acceptance errors. Input to NFIQ is a compressed (using wavelet scalar quantization), digitized gray-scale fingerprint image; NFIQ output is an integer between 1 and 5, where 1 is the highest quality and 5 is the lowest (unusable) quality.

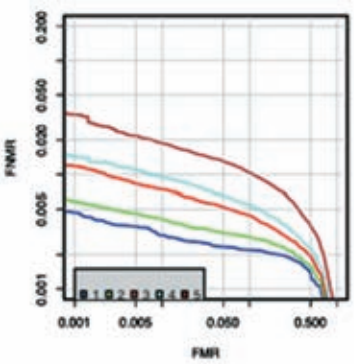
The three plots of Figure 1 show the genuine and impostor distributions for NFIQ values of 1 (excellent quality), 3 (average quality), and 5 (poor quality). The overlapping of genuine and impostor scores for the poorest NFIQ (NFIQ = 5) means higher recognition errors for that NFIQ level. In contrast, the almost complete separation of the two distributions for the best quality scores (NFIQ = 1) indicates lower recognition error.

FIGURE 1. Probability Density of Genuine Scores (in Gray) and Impostor Scores (in Blue)



As shown in Figure 2, NFIQ gives an ordered indication of performance. Five detection error tradeoff curves are generated for five levels of NFIQ. Scores of authentication samples of quality *k* and enrolled samples of quality *k* or better are used in the computation of the *k*th Receiver Operating Characteristic curve ($k = 1,\ldots,5$). This models the situation in which the enrollment samples are at least as good as the authentication samples, which is common and possible because enrollment, as a supervised activity, tends to generate samples of better quality than authentication. Figure 2 shows that the highest recognition performance is achieved for the best-quality samples (NFIQ = 1), and samples with lowest quality (NFIQ = 5) have the lowest performance. (Source code for the NFIQ algorithm is included in the NIST Biometric Image Software distribution (http://fingerprint.nist.gov/NFIS/index.html.)

FIGURE 2. Quality Ranked Detection Error Tradeoff Characteristics (five traces correspond to five NFIQ levels)



NIST has followed the same approach in developing a face quality computation technique. Development of a face quality algorithm, specifically intended to predict the utility of a face image in a matching environment, is relevant to DHS's operational needs with regard to face capture, particularly, US-VISIT's handling of watch lists and the recent use of international e-Passports.

QUALITY-DIRECTED PROCESSING

Use of quality measurement tools allows automatic quality control over biometric samples at the time of capture. If the first sample captured is of insufficient quality, it is possible to catch this in real time and request that the subject's fingerprint be retaken on the spot. Measuring quality also introduces the ability for biometric match-

ing systems to devote different levels of computing resources according to the assessed quality of the fingerprint image. Samples that are determined to be of low quality may be routed to slower, more robust matching algorithms, while the higher volume of high-quality samples may be routed to faster matching algorithms. Also, the weights for multimodal biometric fusion can be selected to allow better quality biometric samples to dominate the fusion.

NIST has been exploring the incorporation of quality scores in biometric systems. For example, NIST Interagency Report 7422 provides technical guidance on quality summarization. Quality summarization addresses the important issue of enterprise quality-assurance surveying by providing tools for combining quality scores of individual samples into one scalar representing the quality of the whole database. Such a function would support identification of, for example, defective sensors, underperforming sites, and seasonal or secular trends. Slap quality addresses the problem of how to combine quality scores of each finger (right index, right middle, …) into one scalar representing the quality of the slap fingerprints. This is relevant to DHS's operational needs with regard to US-VISIT's 10-print matching system.

In "Performance of Biometric Quality Measures," published in the April 2007 issue of *IEEE Transactions on Pattern Analysis and Machine Intelligence*, we examined methods of assessing how effective a quality algorithm is in predicting performance. This activity supports future development of quality measurement algorithms since the ability to evaluate is necessary and vital during development.

We also conducted studies on incorporating quality in multimodal biometric systems and presented "When to Fuse Two Biometrics" at the Computer Vision and Pattern Recognition conference held in New York in June 2006.

NIST held a workshop in March 2006 to identify research needs and discuss gaps in knowledge of biometric sample quality. The workshop provided a forum for experts to share their research and to discuss problems and new developments. It attracted more than 160 attendees to listen to more than 40 presentations on the world's leading technologies. NIST is planning a second workshop on quality to be held in the third quarter of 2007.

Summary

Biometric sample quality has an important role in improving the accuracy and efficiency of biometric systems during the capture process (as a control-loop variable to initiate reacquisition), in database maintenance (sample update), in enterprise-wide quality-assurance surveying, and in invocation of quality-directed processing of sam-

ples. Because of that role, quality measurement algorithms are increasingly deployed in operational systems, and biometric quality standardization is in progress. NIST is actively participating in that standardization process, with the goal of developing an improved standard that reflects the operational needs of the U.S. government, particularly DHS's US-VISIT program, TSA's registered traveler program, PIV, and the international e-Passport. NIST has developed a quality measurement tool for fingerprints, test methods to evaluate performance of quality measures, and technical guidelines on the wider use of quality measures in biometric systems, including quality summarization and quality calibration.

For more information on NIST's biometric quality program, visit http://www.itl.nist.gov/iad/894.03/quality/index.html.

[1]According to a Minutiae Interoperability Exchange Test 2004 (MINEX04) report, the best single-finger proprietary fingerprint recognition system performed at 0.0047 false non-match rate at 1 percent false match rate.

About the Authors

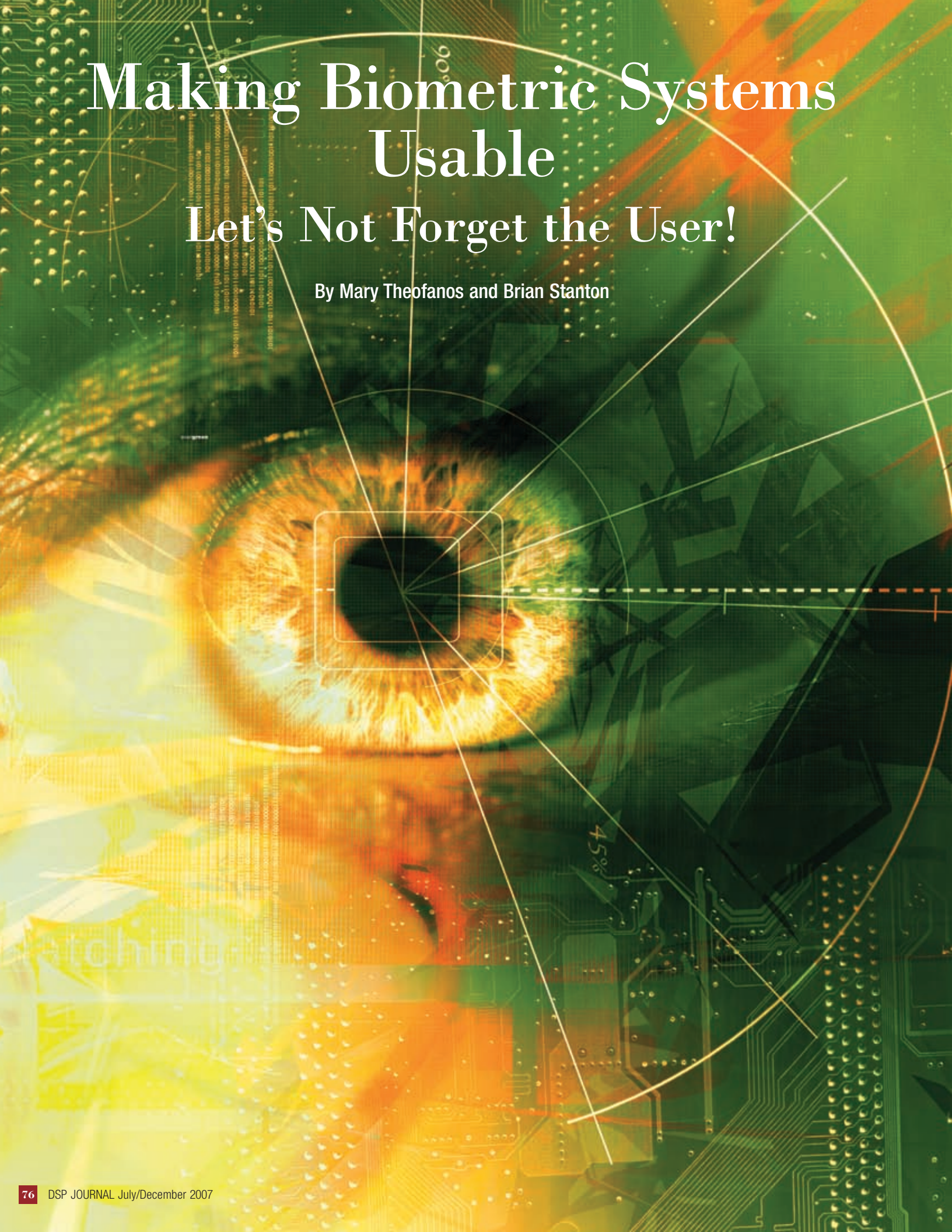
Elham Tabassi, a staff member at NIST, works on various biometric research projects, including biometric sample quality, fusion, and performance assessment. She is the principal architect of NFIQ and is involved in the development of government, U.S., and international standards for biometric sample quality, data interchange formats for biometric data, and conformance to data interchange formats.

Patrick Grother is a staff scientist at NIST, where he is responsible for biometrics testing, standards development, and analysis. He is currently involved in the development of government, U.S., and international standards for the PIV program, performance and interoperability testing, and data interchange formats for biometric data and support of fusion processes.

Making Biometric Systems Usable

Let's Not Forget the User!

By Mary Theofanos and Brian Stanton



The use of physical identifiable characteristics (biometrics) in border and transportation security has increased since 9/11. Currently, the US-VISIT program collects a right and left index fingerprint from all foreign travelers entering the United States. While deployment of biometric technologies has increased, little attention has been given to the human-computer interaction (HCI). HCI and usability guidelines are well established for desktop systems, applications, and web applications that allow developers to design systems according to HCI principles and established baselines. However, no such HCI guidelines exist for biometric systems. The Science and Technology Directorate at the Department of Homeland Security (DHS) recognized this need and initiated a program with the National Institute of Standards and Technology (NIST) to develop HCI guidelines and standards for biometric systems.

What Is Usability?

Usability is essential for a successful product. How well a system performs depends on the quality of the interaction between the user and the system. Usability provides users with the ability to quickly and easily use the system to accomplish their goals. For biometrics systems, these goals include the throughput and the quality of captured images. Thus, guidelines and standards for interactions with biometric applications will increase throughput and image quality. For developers, these guidelines provide tested techniques and approaches that result in consistent development of hardware, software, and interaction techniques that produce good-quality biometrics. For users, guidelines result in designs that help end users understand the biometrics hardware and process. This understanding decreases the time required to obtain images and improves the process for both the participant and the operator. Consider what happens if every user in the queue is confused by the interface and doesn't understand how to proceed and what to do: each user takes much longer to process than estimated, and the system may or may not acquire a decent quality image.

The goal of the DHS project is the development and testing of a set of usability guidelines for biometric systems that

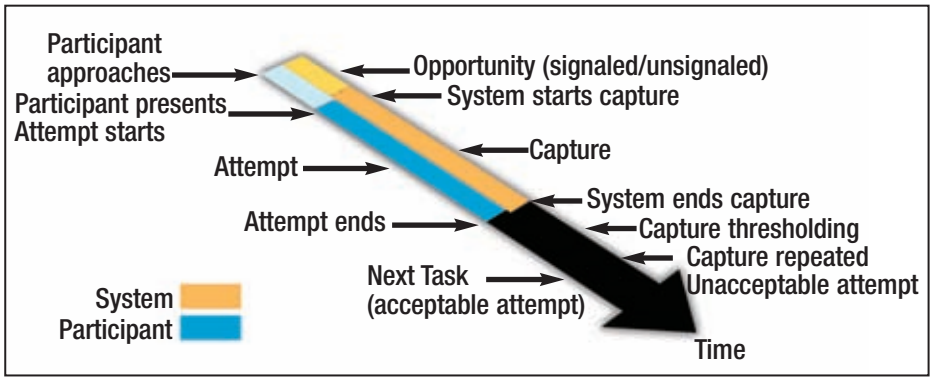
- enhance performance (efficiency and effectiveness),
- improve user satisfaction and acceptance, and
- provide consistency across biometric system user interfaces.

Current Environment

As biometric technology and applications were maturing, the focus was naturally on improving functionality and reliability through the technology. But now that biometric fingerprint technology has matured, one must examine the human factors and usability in order to gain more improvements. Figure 1 depicts the biometric capture process.

Biometric systems are going to become commonplace—to enter a country, to enter a building, to log on to a computer, or even to use a credit card. But this is a different way of doing

FIGURE 1. The Biometric Capture Process



business, and the average citizen end user is not prepared for this new approach. For example, consider the airline industry and the initial use of seatbelts. At the time, many passengers were not familiar with seatbelts and required demonstrations for use. Today, seatbelts have become commonplace; they are in every car, and most passengers are comfortable with their use and even ignore the demonstration. Many people today think they understand fingerprints from

Biometric systems are going to become commonplace—to enter a country, to enter a building, to log on to a computer, or even to use a credit card. But this is a different way of doing business, and the average citizen end user is not prepared for this new approach.

television shows. But, as is often the case, fingerprint technology is not represented accurately. It is our responsibility to communicate and teach the end user about the technology and to facilitate the transition from the unfamiliar to the familiar. This requires an understanding of the users, user behavior, and the systems' usability.

The Usability Engineering Process

ISO 9241-11:1998, "Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs)—Part 11: Guidance on Usability," makes clear that usability can be measured, and it provides an outline for how to proceed. Specifically, it is necessary to identify and understand the following:

- *Users.* Who are the users of the biometrics systems? In our environment, users include travelers (including travelers with disabilities), operators, and examiners.

FIGURE 2. The Three Usability Metrics

- *Context of use.* What is the environment, motivation, and cognitive load of the users? It is important to recognize that travelers are probably tired, a little stressed out, and carrying luggage, and they may not speak the language. All they really want to do is get out of the airport to their final destination.
- *Goals.* What are the users' goals or tasks? For instance, the operator is interested in the acquisition or capture of images. How does training impact the users' goals?

As shown in Figure 2, three usability metrics have been identified for biometric systems:

- Effectiveness—a measure of accuracy and completeness (quality)
- Efficiency—a measure of the resources expended (task time)
- User satisfaction—a measure of the degree to which the product meets the users' expectations (subjective).

Experiments at NIST have demonstrated that usability and human factors affect fingerprint performance, both the quality of the captured images and the time required to collect the images. The challenge now is to identify these significant characteristics and develop standards and guidelines that compensate for or mitigate the influence of these factors in fingerprint systems. The NIST biometrics team has identified a number of user characteristics that affect fingerprint performance. The following are examples:

- *Age, gender, height (anthropometrics).*
- *Experience.* Are you familiar with the device or the technology?
- *Ability.* Are you a person with a disability? Do you have arthritis?
- *Perception.* Are you uncomfortable with the process or the equipment? Two percent of the population has expressed concerns about the possibility of germs on the scanner. The tactile feedback from the glass and metal surface is perceived to be sticky. ATMs are usually made of hard matte textured plastic surfaces to minimize this perception.

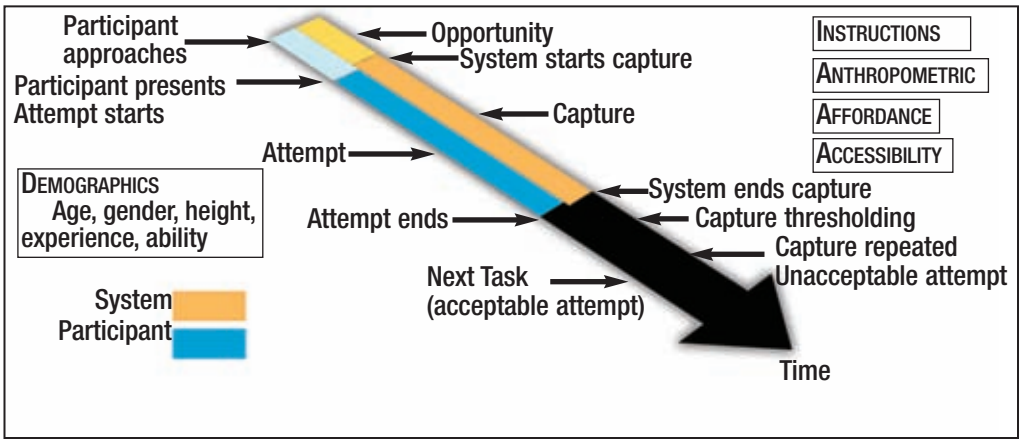
These user characteristics require that we examine factors such as the following:

- *Physical characteristics of the device.* How high is it? Does the angle of the scanner matter? What color should the platen be? Should it feel warm or cold?

- *Inherent ability of the device to relay its use.* Does the shape and configuration of the scanner convey where to place your fingers? Does the scanner indicate whether the prints have been captured?
- *Instructions and learning materials.* What form should the instructions take? Does everyone speak English?
- *Accessibility.* What about Section 508 of the Rehabilitation Act? How should the technology adapt for people with disabilities?

Figure 3 depicts the usability characteristics affecting biometrics.

FIGURE 3. Usability Characteristics Affecting Biometrics



Accomplishments

To date, NIST has completed five usability tests focusing on several of these factors:

- In the first test, NIST examined habituation or acclimatization. Does user behavior and interaction with the device over time improve or degrade user performance?
- The second study focused on anthropometrics and the height of the work surface and scanner placement. Is there a relationship between the scanner's height and the quality of captured images?
- Our third test studied the use of instructional materials. Do people perform better with oral, video, or poster instructions?
- Next, NIST conducted a study of symbols. Can we define a set of international symbols or pictograms that describe the fingerprint process? Can the symbols be independent of language and be understood by most cultures?
- The most recent study examined features for users who are significantly visually impaired. Can we define mechanisms that assist these users with locating the device, provide feedback for proper hand and finger placement, and provide an indication of the duration of the scan?

Each of these studies has resulted in a set of guidelines for use by DHS and a taxonomy of definitions for usability studies of biometric systems. In addition, the taxonomy has been sub-

mitted to the ISO/IEC subcommittee on biometrics, SC 37. The guidelines will be submitted as appropriate.

For additional information on each of the research areas and resulting guidelines, see http://zing.ncsl.nist.gov/biousa/.

Summary

Agencies using biometric systems require guidelines for the design and implementation of "usable" biometric user interfaces. Standards for testing the usability of biometric systems in operational environments are also critical for measuring biometric system performance. NIST is developing HCI guidelines and standards that identify and measure characteristics—including timing, quality, and user satisfaction—that affect user performance. The guidelines and standards will assist agencies with procuring and deploying biometric systems that are effective and efficient and improve overall system performance.

About the Authors

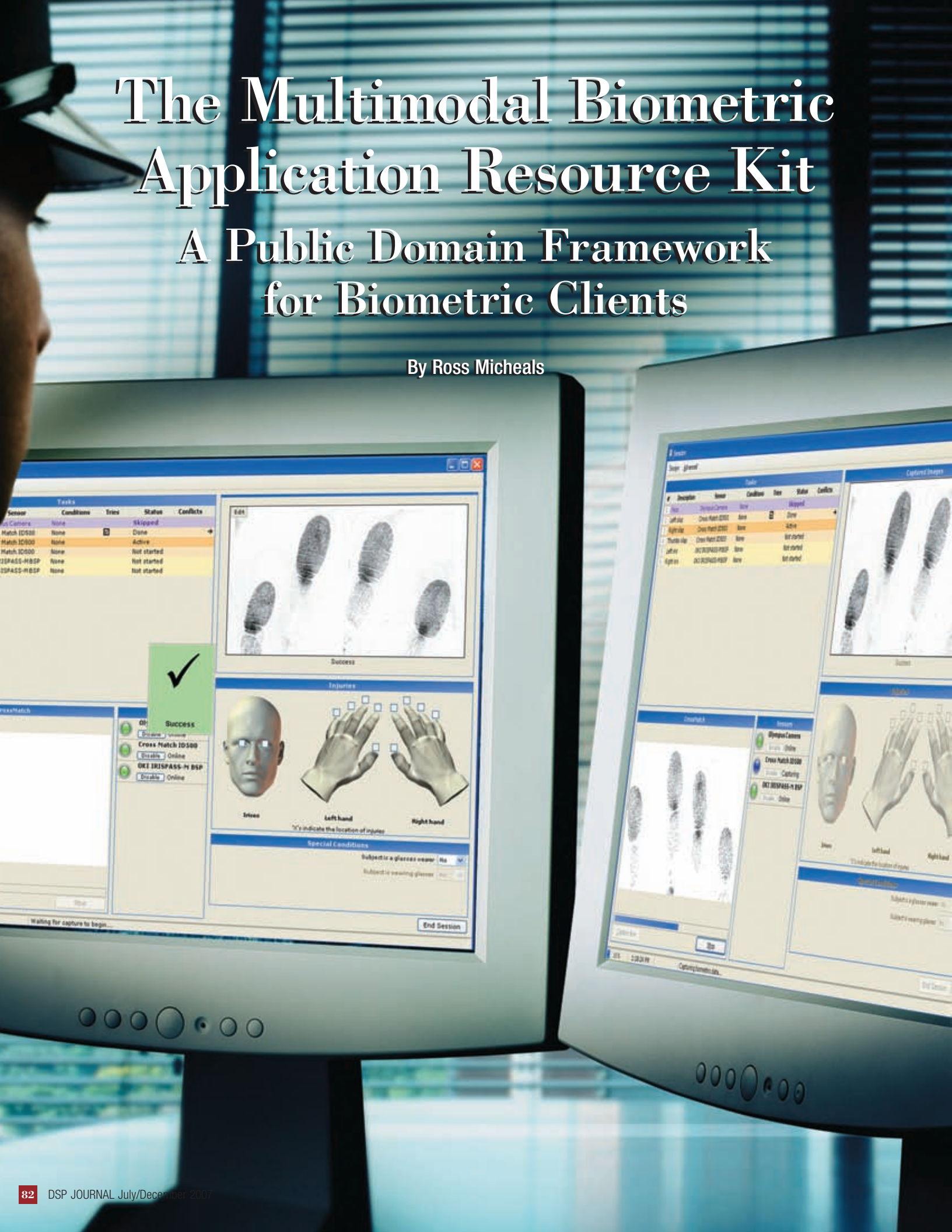
Mary Theofanos, a computer scientist in the Visualization and Usability Group at NIST, is the program manager of the Industry Usability Reporting Project, which is developing standards for usability. She is the principal architect of the Biometrics Usability Program for evaluating the human factors and usability of biometric systems and is a member of ISO/IEC JTC 1 SC 7 WG 6 and the convener of the SC 7/TC 159/SC 4 JWG.

Brian Stanton is a cognitive scientist in the Visualization and Usability Group at NIST. He works on the Industry Usability Reporting Project developing usability standards, and he investigates biometric and robotic usability. He is a member of ISO/IEC JTC 1 SC7 WG 6 and the secretariat of the SC 7/TC 159/SC 4 JWG.

The Multimodal Biometric Application Resource Kit

A Public Domain Framework for Biometric Clients

By Ross Micheals



Once used primarily by law enforcement to help identify criminals, biometric technologies increasingly are being used by government and the private sector to authenticate a person's identity, to provide security at the nation's borders, and to restrict access to secure resources—both buildings and computer networks.

Most biometric systems are "unimodal," meaning they rely on a single distinguishing physical characteristic, such as a fingerprint, for authenticating identity. But using a single feature can present problems. For example, poor illumination could make a face image unrecognizable, and dirty or damaged sensor plates could affect fingerprint equipment. A multimodal system that has several sources of information—such as fingerprint, face, and iris data—can be more flexible and reliable.

Despite efforts, most biometric system components are still not sufficiently interoperable. Organizations must either purchase a complete system or develop middleware—custom integration software—to link applications. Recognizing this gap, the National Science and Technology Council's Subcommittee on Biometrics issued the National Biometrics Challenge, which includes a call to develop middleware techniques and standards that will permit plug-and-play capabilities for biometric sensors.

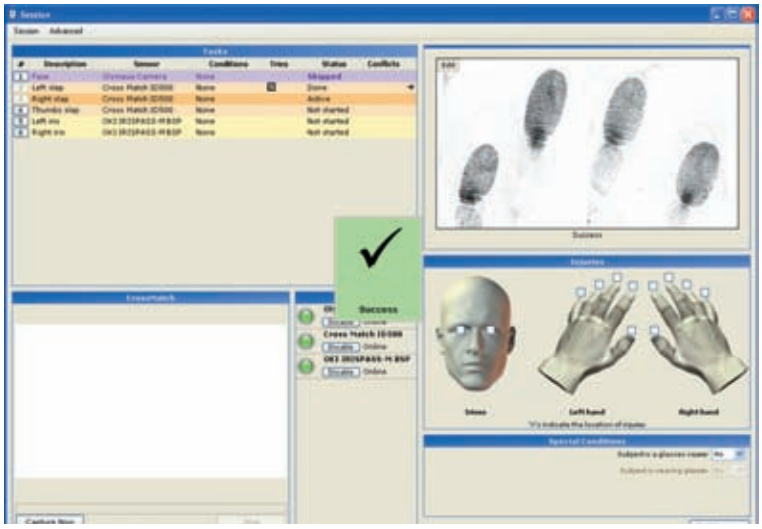
As the role of biometrics increases in organizations, stakeholders demand more capabilities from their middleware. Systems must accommodate evolving and ever-improving sensors. Workflow may need to be adapted to meet changing requirements. End users must be presented with systems having high degrees of efficiency, effectiveness, and user satisfaction.

The Multimodal Biometric Application Resource Kit, or MBARK, reduces these complexities and the costs of developing the next generation of biometric and personal identity verification applications. MBARK is public domain source code that may be leveraged to develop the next generation of biometric and personal identity verification applications. As intellectual property in the public domain, MBARK carries none of the restrictions of common open source licenses.

Three screenshots show a successful capture of fingerprints of a person's left hand—a "left slap," "polling" for fingerprints with a live preview, and handling a sensor failure.

A Brief History of MBARK

MBARK began not as a general-purpose framework, but as the "Multimodal Biometric Accuracy Research Kiosk." The Transportation Security Administration expressed a desire to have a large-scale iris image database suitable for National Institute of Standards and Technology (NIST) certification of iris recognition as a travel biometric. However, the significant fixed cost of data collection, coupled with the incremental costs of adding more sensors, suggested that overall utility could be increased by collecting multiple modalities. Given NIST's PATRIOT



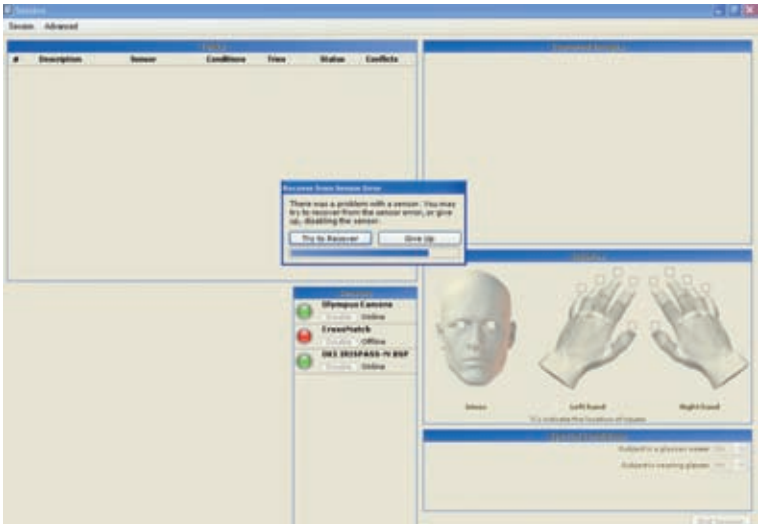
Successful capture. This screenshot shows a successful left slap. The large indicator of success fades away over a few seconds.

Polling for fingerprints with a live preview. This screenshot shows a right slap in progress. The result from the previous task, a left slap, is visible in the upper-right panel of the window.

Act mandate, the modalities were scoped to the face, fingerprint, and iris biometrics approved by the International Civil Aviation Organization (ICAO). ICAO, a specialized agency of the United Nations, "sets the standards for aviation safety, security, efficiency and regularity, as well as for aviation environmental protection, and encourages their implementation."[1]

The following timeline highlights how MBARK has been used across the federal government and within a variety of standards developing organizations:

- 2005
  - A briefing with a chief software architect for the US-VISIT program about the implementation of MBARK revealed vital missing and ambiguous requirements in the



Handling a sensor failure. This screenshot shows how MBARK prompts the operator when a sensor fails, in this case, upon initialization. MBARK will either disable the sensor or try to reset it automatically.

fingerprint scanner and client software components of US-VISIT's 10-print migration plan.

- MBARK was used to troubleshoot and discover a fix for a major bug in the Department of State's BioVisa client software.

2006

- Lessons learned in the implementation of MBARK drove contributions to a variety of standards development activities, specifically, the International Committee for Information Technology Standards M1.2 Ad Hoc Group on Tenprint Capture Using BioAPI, the Biometric Identity Assurance Services Integration Technical Committee of the Organization for the Advancement of Structured Information Standards, and the American National Standards Institute/NIST-ITL 1-2000 XML Representation Ad Hoc Working Group.
- MBARK-based guidance was submitted as a NIST contribution to *10-Print Capture Scanner and Software Requirements*, a document issued by the interagency 10-Print Capture User Group
- A custom MBARK application was developed for a large-scale usability study on the effect of instructional modality (poster, verbal, or video) on timing and errors.

2007

- MBARK is slated to serve as the implementation platform for a large-scale biometric data collection project by the FBI's Criminal Justice Information Services. As of January 2007, NIST was involved in the planning, sensor selection, and early demonstration phases. In March, a prototype data collection system was delivered to the FBI.

The Future of MBARK

The next phases of MBARK will be focused on improving technology-transfer capabilities, as well as on meeting direct stakeholder operational requirements. As stakeholders start to field MBARK-based systems, there is the critical but unglamorous work of hardening systems, integrating new technologies, and staying current with respect to the evolving operating systems and runtime environments on which MBARK depends.

Near-term goals include providing a set of code templates that vendors (or integrators) may use to incorporate new sensors into MBARK with much less effort than is required today. In addition, the MBARK workflow and system configurations need to be exposed through a variety of documentation and user-centric tools, with an end goal of developing a form of "application profile templates" for standardization.

Longer term goals include implementing capabilities to facilitate back-office communication. This includes packaging the captured data into standard industry formats, exploring client-server communications, and developing web services interfaces for service-oriented architecture applications.[2]

More information about MBARK may be found on the project website: http://mbark.nist.gov.

[1]International Civil Aviation Organization, *Annual Report of the Council*, 2005.

[2]Generally, the phrase "service-oriented architecture" (SOA) is not well defined. (Certainly its definition is much more ambiguous than other general programming paradigm terms such as "object-oriented programming." To address this gap, the OASIS Reference Model for Service Oriented Architecture (Committee Draft 1.0) defines SOA as "a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains." The document suggests that SOA is different in that "unlike Object Oriented Programming paradigms, where the focus is on packaging data with operations, the central focus of Service Oriented Architecture is the task or business function—getting something done."

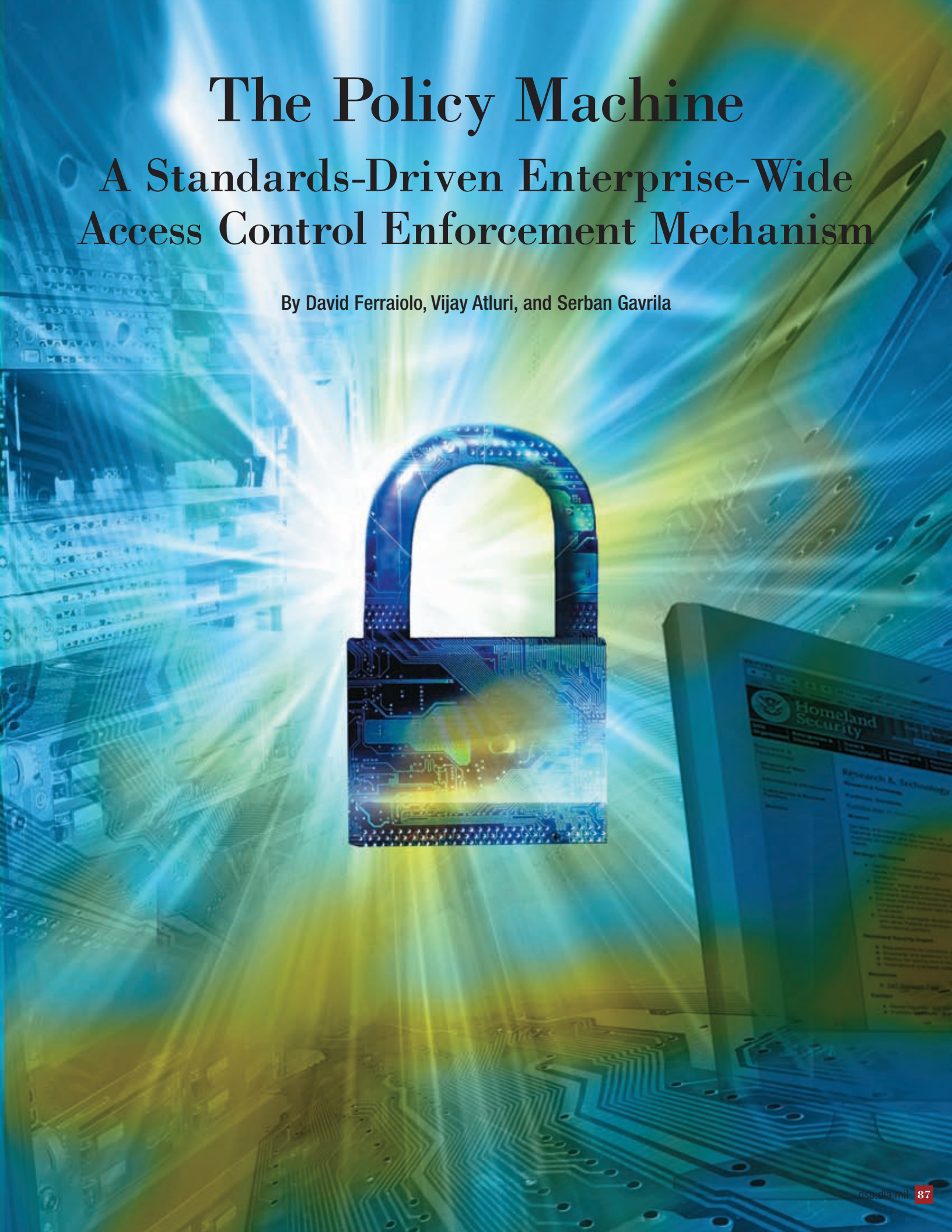
About the Author

Ross Micheals is a supervisory computer scientist at the National Institute of Standards and Technology. He leads an effort examining biometric client technologies, of which MBARK plays a key role. Dr. Micheals helped pioneer NIST's research into the usability of biometric systems; he continues to play a vital role in this research today.

The Policy Machine

A Standards-Driven Enterprise-Wide Access Control Enforcement Mechanism

By David Ferraiolo, Vijay Atluri, and Serban Gavrila



Access control facilitates controlled sharing and protection of resources in an enterprise. Although a variety of security policies are available to enforce controlled sharing and protection, current vendor product systems (VPSs) limit their implementation only to certain specific types of policies. Organizations therefore have to resort to implementing them as application code, or they simply ignore them. Also, the access control mechanism is implemented as part of the VPS and therefore is tightly coupled to the VPS. This limits the policy enforcement on a resource to the one supported by the host system. To support enterprise-wide and flexible security policies, the National Institute of Standards and Technology (NIST) has developed a standards-driven approach to the enforcement of access control that can be adopted by future VPS versions.

Access control is an indispensable part of any information sharing and protection system. In contrast to authentication, which is the process of identifying an individual user, access control or authorization is the process of controlling which users can perform which operations on which resources inside of a computer system. Access control mechanisms are responsible for defining the policies and automatically enforcing them.

Organizations may enforce many types of security policies based on their protection needs. Ensuring protection in today's access control environment requires the implementation and deployment of a multitude of access control mechanisms. These take on a variety of forms and are uniquely implemented in every VPS that creates and manages its own sessions and resources and that regulates the access requests of processes within a session to the resources. VPSs include operating systems and major systems such as a database management system or an enterprise resource planning system. Access control mechanisms can also be implemented within or as small applications (such as workflow management, time and attendance, and a corporate calendar) that run on top of a VPS but afford access control policy independent of any VPS's access control mechanism.

These heterogeneous approaches to access control raise a number of user, administrative, and policy challenges. Because the scope of control of any particular access control mechanism is limited to the resources that are stored on the VPS for which the mechanism is implemented, the user must have an administratively created account in order to access resources needed to perform his or her duties. Moreover, the user must log on to each VPS and to each application in which these resources reside and are processed. In addition to the need to create and manage multiple user accounts for each user, administrators need to specify appropriate permissions (access control data), system by system and application by application, to enable user access to data. Considering the number of users and the number of systems and applications that need to be managed in even a medium-sized organization, user account and permission administration can become costly and prone to error. Many of these user inconveniences and administrative problems are due to the failure of access control mechanisms to interoperate.

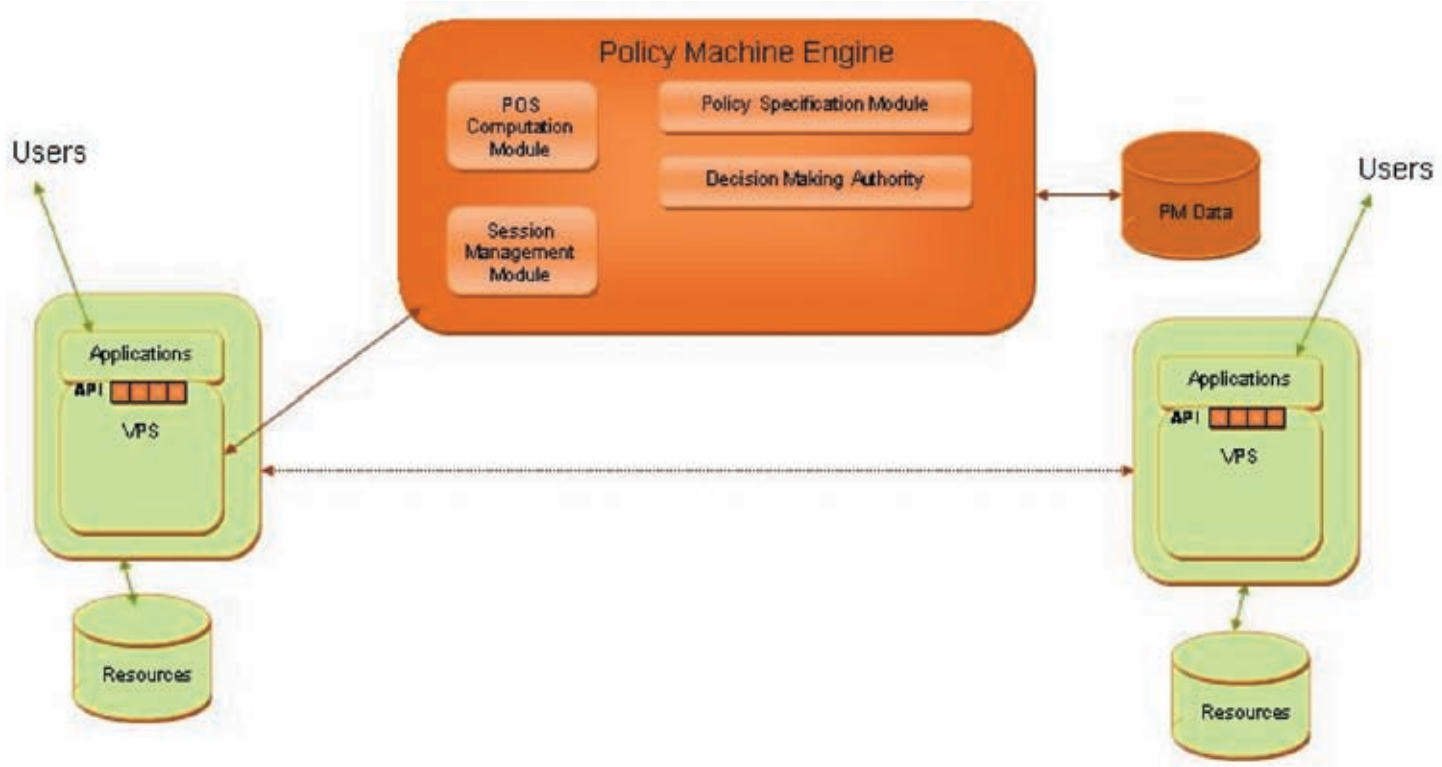
Interoperability is but one challenge with today's access control mechanisms. Another is policy enforcement. Pertaining to each organization is a unique set of access control policies that dictate the circumstances and conditions under which specific users are permitted access to specific resources. The ability of an organization to enforce its access policies directly affects its ability to execute its mission by determining the degree to which its volumes of data may be protected and shared among its user community. Whether in regard to the government's war on terror or a company's formation of a strategic partnership, the focus on sharing and protecting information is becoming increasingly acute. For instance, in response to the need to protect classified information, mechanisms exist to enforce mandatory access control (MAC) policies and to enforce need-to-know policies. In addition, in recognition of the needs of industry, role-based access control (RBAC) mechanisms enforce policies based on user functions, qualifications, and competencies, and they restrict access based on separation of duties.

Although these and other mechanisms may meet broad policy requirements within their respective user domains, specific and often ad hoc organizational requirements also need to be addressed. These requirements may, for example, pertain to controlling access based on a user's membership within an organizational entity, the inclusion of a resource within a geographical region or facility, the relative importance of data (ordinary, important, critical), or even something as esoteric as a user's affiliation to a political party. In addition, organizational policies can and often do pertain to combinations of two or more policies. For example, gaining access to a classified medical record may require the enforcement of an multilevel security policy (to prevent direct and indirect compromise of classified data), the enforcement of an RBAC policy (to ensure the user is qualified), and the enforcement of an identity-based access control policy (to protect patient privacy).

Ever since the beginning of shared computing, research programs have existed to create access control models that support specific policy objectives, often independent of any VPS. This research resulted in a rich set of formal security models that can translate organizational policy. Although each model represents a strategy for the development of an access control mechanism, the vendor community has been cautious as to the type of access control mechanisms that they bring to the marketplace. Of the numerous recognized access control policies, today's access control mechanisms are limited to the enforcement of instances of discretional access control (DAC) and simple variations of RBAC policies and, to a far lesser extent, instances of DAC and MAC policies combined. As a consequence, a number of important policies (orphan policies) lack a commercially viable VPS mechanism for their support.

In an attempt to address the above interoperability and policy enforcement problems of today's access control mechanisms, NIST, under the support of the Department of Homeland Security, has designed, specified, and developed a reference implementation for a standards-driven security policy enforcement framework, referred to as the Policy Machine (PM).

FIGURE 1. The Policy Machine



The PM is defined in terms of a standard set of configurable data abstractions, a standard set of functions, and a standardized but generic architecture. This architecture (see Figure 1) includes a standard set of policy-enforcing application program interfaces (APIs), ideally implemented within the kernel of the VPS. Also included in this architecture is the policy machine engine consisting of four modules and a set of data on which they operate:

- Through the Policy Specification Module, the PM affords the configuration of arbitrary and enterprise-specific attribute-based access control policies that, once configured, can be selectively and uniformly enforced in the protection of resources regardless of the VPS in which the resources reside.
- The Decision Making Authority in the PM is responsible for deciding whether to allow or deny access. In general, the PM architecture presumes the centralized calculation of access control decisions that are based on enterprise-specific data and local VPS enforcement based on those decisions, thus enabling the decoupling of policy configuration and access control decision making from policy enforcement.
- The Personal Object System (POS) is a logical and policy-dependent per user presentation of the currently accessible resources.
- The PM's Session Management Module creates and deletes sessions, and it attaches user attributes to the sessions.

The four modules that constitute the policy machine engine operate on the PM data. These data are managed and visualized as standardized relations by the policy specification module.

Benefits of the Policy Machine

- Flexible security policy configuration and enforcement
- Single point of user authentication
- Enterprise-wide policy enforcement
- Single administrative domain
- Combined heterogeneous policies in a single specification
- Enhanced security assurance

To be PM compliant, all a vendor needs to do is to implement a standard set of APIs that pertain to user authentication, session management, and reference mediation. In complying with the PM standard, a vendor need not make further changes to the VPS or produce multiple versions of the VPS to cater to the policy requirements of their customers. From a customer's perspective, any attribute-based access control policy can be configured, and any resource can be protected under any combination of the configured policies. Under this standard, access control policies that are currently implemented and enforced within application code can be configured and enforced by the PM and can be applied to resources perhaps in combination with other configured policies. Because the PM eliminates the need to enforce policy at the application level, it eliminates many of the vulnerabilities that are associated with implementing access control at the application level.

Similar to the notion of a programming language that enables the solving of a variety of problems using a standard set of constructs and a fixed set of computational functions, the set of standard abstractions (relations) of the PM allows organizations to configure and change any security policy. As a consequence, administrators are provided with a single scheme for administering access control data, as opposed to having to administer data VPS by VPS and application by application.

As a consequence of the architecture, the set of policies that are configured by the PM can be centrally managed and uniformly enforced within and across different types of VPSs. Although policies transcend VPSs, not all resources need to be protected under all policies. In other words, each resource may be protected under any subset of policies that are configured by the PM, regardless of the VPS on which its content is stored.

A user with permission can access a resource through any VPS that contains an application that can process the resource. A user can log on to the PM at any VPS; can be logically presented with a dynamically changing and policy-dependent set of accessible resources, regardless of where the resources are physically stored; and can access those resources under the control of a multitude of resource-specific protection policies. This eliminates the need for a

user to have a separate account on each VPS and application to which he or she requires access. Administrators do not need to manage a multitude of identities pertaining to VPSs and access control applications, nor do they need to manage multiple access control schemes.

Through the reference implementation of the PM, we can now demonstrate the configuration and enforcement of a diverse set of policies. Considering the complexity involved in manual configuration of policies, we have developed an extensive library of policies that can be imported for immediate use. We envision the emergence of VPSs that are functionally compliant with the PM as vendors learn of the PM'As advantages over the existing access control paradigm.

About the Authors

David Ferraiolo is the manager of Systems and Network Security, a group within the Computer Security Division of NIST's Information and Technology Laboratory, and is the lead for the Cyber Security Working Group in support of the Portfolio Manager for Standards in the Directorate for Science and Technology at the Department of Homeland Security. He has 23 years of experience in computer and communications security, serving both the government and private industry.

Vijay Atluri is a professor of computer information systems and a research director at the Center for Information Management, Integration and Connectivity at Rutgers University. In addition, she is a computer scientist with NIST's Information Technology Laboratory, Computer Security Division, Systems and Network Security.

Serban Gavrila has been with VDG, Inc., since 1995 and with NIST since March 2007. For NIST, he works on projects related to computer security. Those projects include development of formal specifications and implementation of enterprise-wide access control management systems, and security policy management for enterprise-issued hand-held devices.

November 13–16, 2007, Orlando, FL

DoD Maintenance Symposium and Exhibition

The DoD Maintenance Symposium and Exhibition will be held at the Rosen Shingle Creek Hotel, in Orlando, FL, on November 13-16, 2007. The theme of this symposium is Aligning Maintenance and Sustainment to Warfighter Needs. The symposium brings together government and industry representatives to exchange ideas for improving maintenance practices and procedures. It features an up-to-the-minute technical program, presentations from senior-level speakers, and a dynamic exhibit.

Participants will be able to explore the latest developments in DoD weapon systems and equipment maintenance, including military and commercial maintenance technologies, information systems, and management processes.

For more information, please go to www.sae.org/events/dod.

March 4–6, 2008, Arlington, VA

2008 DoD Standardization Conference

The Defense Standardization Program's Standardization Conference and Outstanding Achievement Awards Ceremony will be held March 4–6, 2008, at the Westin Arlington Gateway Hotel, in Arlington VA. The Westin Gateway Hotel is accessible by metro and is close to Ronald Reagan Washington National Airport, the Pentagon, and Washington, DC.

This year's event, which is being administered by SAE International, promises to be top-notch in every respect. Panels and a preliminary agenda are posted on the DSP website and on the SAE website.

For more information or to register, please go to www.sae.org/events/dsp or call 724-772-8525.

Welcome

Rear Admiral Kathleen Dussault, Supply Corps, U.S. Navy, is the Deputy Assistant Secretary of the Navy for Acquisition and Logistics Management. Along with those duties, she will also serve as the Navy Standardization Executive, replacing Nick Kunesh. Previously, Rear Adm. Dussault served as the director of Acquisition Management at the Defense Logistics Agency, Fort Belvoir, VA. We welcome her to the standardization community.

Michael Sikora has been named the new head of the Naval Air Systems Command (NAVAIR) Standardization Division. He is replacing Thomas O'Mara, who recently retired from federal service. In his new position, Mr. Sikora is responsible for managing and executing the NAVAIR Defense Standardization Program, Nomenclature Assignment, and Parts Management functions. Mr. Sikora has worked in the NAVAIR Standardization Division over the past 10 years. His most recently held position was that of NAVAIR Specification and Standardization Team Leader. Before joining the Standardization Division, Mr. Sikora was responsible for the technical planning, analysis, and coordination of instrumentation, test measurement, data acquisition, and electronic display systems required to obtain steady-state, transient, and operational performance data in the test and evaluation of gas turbine power plants and accessories at the then Naval Air Propulsion Center.

James Johnson, Army Test and Evaluation Command (ATEC), was recently appointed to the Senior Executive Service as executive director of the Developmental Test Command (DTC). In addition to his management responsibility for the command's test and technology mission and all associated resources, Mr. Johnson assumes the position of Standards Executive responsible for Lead Standardization Activity Code ENVR and Standardization Preparing Activity for numerous national and international test procedures. As the DTC executive director, he is responsible for planning, executing, and reporting on 1,700 tests supporting more than 500 weapons programs annually; directing a workforce of 7,600 employees; and ensuring the operational readiness of the Army's developmental test range infrastructure.

Farewell

Brian Simmons, ATEC, former executive director of DTC, and Army Standards Executive for DTC, was appointed director of the Army Evaluation Center (AEC). In his position as Standards Executive, Mr. Simmons was responsible for the Lead

Standardization Activity Code ENVR and Standardization Preparing Activity for numerous national and international test procedures. As AEC director, he is responsible for ensuring that senior leaders in the Army and Office of the Secretary of Defense have the essential information required before weapons and equipment are placed into the hands of our warfighters and throughout the life cycle of the system. He directs the evaluation efforts for more than 550 programs through an 800-person workforce.

Nick Kunesh has been selected to serve as special assistant for Lean Six Sigma to the Secretary of the Navy. Mr. Kunesh was selected to lead the Transformation Team Leaders, consisting of the Deputy Assistant Secretaries of the Navy, senior Navy leaders who report directly to the secretary, and the Marine Corps major subordinate and Navy echelon II commands. We wish him well in his new role, and we thank him for his service to the Defense Standardization Program.

Thomas O'Mara, head of the NAVAIR Standardization Division, retired on August 3, 2007, after 41 years of federal service. Since 1992, he has been responsible for managing and executing the NAVAIR Defense Standardization Program, Nomenclature Assignment, and Parts Management functions. It was through his stewardship that the NAVAIR Standardization Division was able to implement the DoD Acquisition Reform policy. Mr. O'Mara embraced a close relationship between military and civil aviation as he also chaired the industry-managed QPL program's Qualified Products Management Council. We wish him the best in retirement.

The Standardization Program Branch at the Defense Supply Center Richmond (DSCR) welcomes four people who have been assigned to perform Preparing Activity (PA) and Qualifying Activity (QA) functions at DSCR:

- **Travis Wood** will be the PA and the QA for the standardization documents associated with aircraft instrumentation and engine components. A mechanical engineer, Mr. Wood has been with DSCR for 4 years. He was previously with the Sustainment Engineering Branch. He also brings from the private sector a wide variety of mechanical testing and standards experience to the branch.
- **Dale Edwards** will be the PA and the QA for standardization documents associated with batteries, electrical equipment, power sources, electrical wire and cables, and electrical hardware. Mr. Edwards, a QA specialist, has been with DSCR for 23 years. He was previously with the Defense Contract Management

Agency in Springfield, NJ, the Defense Depot in Richmond, and, most recently, the Technical and Evaluation Branch at DSCR.

- **R. "Butch" Bendl** will be the temporary PA and the QA for standardization documents associated with commercial and industrial gas cylinders. Mr. Bendl assumes this role from Miguel Lopez-Oquendo, who was activated and currently is on an 18-month deployment to Iraq with the Army National Guard. Mr. Bendl, an equipment specialist, also serves as the DSCR Standardization Program Branch's Lead Standardization Activity for more than 2,600 standardization documents in 54 federal supply classes.
- **Tom Kennedy** will be the PA and the QA for standardization documents associated with measurement instruments and parachute hardware. Mr. Kennedy's duties also include implementing the Parts Management Program and managing the Critical Item Procurement Requirements Documents program. In addition, he participates on the ASTM Committee B09 on Metal Powders and Metal Powder Products.

DAU Courses—FY08

	#	Start Date	End Date	Location	DAU POC
PQM 103 Defense Specification Management	201	Oct. 9, 2007	Oct. 19, 2007	Tinker AFB, OK	256-722-1023
	001	Oct. 30, 2007	Nov. 9, 2007	DSMC, Ft. Belvoir, VA	703-805-3003
	002	April 22, 2008	May 2, 2008	Kettering, OH	888-284-4906
PQM 104 Specification Selection and Application	001	Dec. 4, 2007	Dec. 5, 2007	DSMC, Ft. Belvoir, VA	703-805-3003
	002	Sep. 16, 2008	Sep. 17, 2008	Huntsville, AL	256-722-1023

Upcoming Issues—
Call for Contributors

We are always seeking articles that relate to our themes or other standardization topics. We invite anyone involved in standardization—government employees, military personnel, industry leaders, members of academia, and others—to submit proposed articles for use in the *DSP Journal*. Please let us know if you would like to contribute.

Following are our themes for upcoming issues:

Issue	Theme
January–March 2008	Government-Industry Data Exchange Program
April–June 2008	Diminishing Manufacturing Sources and Material Shortages
July–September 2008	Defense Standardization
October–December 2008	European Union Standardization

If you have ideas for articles or want more information, contact Tim Koczanski, Editor, *DSP Journal*, J-307, Defense Standardization Program Office, 8725 John J. Kingman Road, Stop 6233, Fort Belvoir, VA 22060-6221 or e-mail DSP-Editor@dla.mil.

Our office reserves the right to modify or reject any submission as deemed appropriate. We will be glad to send out our editorial guidelines and work with any author to get his or her material shaped into an article.

DEFENSE STANDARDIZATION PROGRAM
MAKING SYSTEMS WORK TOGETHER