Fusion of Security System Data to Improve Airport Security

Committee on Assessment of Security Technologies for Transportation, National Research Council

ISBN: 0-309-10749-0, 82 pages, 8 1/2 x 11, (2007)

FUSION OF SECURITY SYSTEM DATA TO IMPROVE AIRPORT SECURITY

Committee on Assessment of Security Technologies for Transportation
National Materials Advisory Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. DTFA 03-99-C-00006 between the National Academy of Sciences and the Transportation Security Administration. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number-13: 978-0-309-10748-8
International Standard Book Number-10: 0-309-10748-2

A limited number of copies of this report are available from the National Materials Advisory Board, 500 Fifth Street, N.W., Keck WS932, Washington, DC 20001; (202) 334-3505 or (202) 334-3718; Internet, http://www.nas.edu/nmab.

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Printed in the United States of America

THE NATIONAL ACADEMIES
Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

COMMITTEE ON ASSESSMENT OF SECURITY TECHNOLOGIES FOR TRANSPORTATION

JAMES F. O'BRYON, *Chair*, The O'Bryon Group
SANDRA L. HYLAND, *Vice Chair*, Tokyo Electron Technology Center, America
CHERYL A. BITNER, Pioneer Unmanned Aerial vehicles, Inc.
DONALD E. BROWN, University of Virginia
JOHN B. DALY,[1] Consultant, Arlington, Virginia
COLIN G. DRURY, State University of New York, Buffalo
PATRICK GRIFFIN, Sandia National Laboratories
HARRY E. MARTZ, JR., Lawrence Livermore National Laboratory
RICHARD McGEE, Army Research Laboratory, Aberdeen Proving Ground (retired)
RICHARD L. ROWE, SafeView (retired)
H. BRUCE WALLACE, MMW Concepts LLC

Staff

GARY FISCHMAN, Director, National Materials Advisory Board
JAMES KILLIAN, Study Director (until June 2006)
EMILY ANN MEYER, Study Director (from November 2006)
TERI G. THOROWGOOD, Administrative Coordinator

[1] Dr. Daly passed away in April 2006.

NATIONAL MATERIALS ADVISORY BOARD

Staff

Preface

The Committee on Assessment of Security Technologies for Transportation was appointed by the National Research Council (NRC) in response to a request from the Transportation Security Administration (TSA) for a study of technologies to protect the nation's air transportation system from terrorist attacks (see Appendix B for biographical sketches of the committee members). The committee judged that the best way to provide a timely response would be to produce a series of short reports on promising technologies, focusing on specific topics of greatest interest to the sponsor. This is the fourth of four such topical reports, all of which focus on air transportation security.[1] The commit-

[1] The previous reports, also published by the National Academies Press, Washington, D.C., are *Opportunities to Improve Airport Passenger Screening with Mass Spectrometry* (2004), *Defending the U.S. Air Transportation System Against Chemical and Biological Threats* (2006), and *Assessment of Millimeter-*

tee believes that the air transportation environment provides a test case for the deployment of security technologies that might subsequently be used to protect other transportation modes as well.

This report focuses on what is commonly termed *data fusion*. The possibility of a terrorist slipping through a multilayered security system still exists, given the current configuration of security architectures across the vast majority of our nation's commercial airports. This is not to say that the technology that is being brought to bear is not useful or effective. It is effective. However, from the committee's vantage point, the various security systems and the technologies contained in them could be connected in such a way that they could extract significantly more information regarding possible threats. This could be accomplished in real time with each system operating in a more or less stand-alone mode.

Much can be learned from the Department of Defense's (DOD's) experience with data fusion, as the DOD has successful systems now deployed throughout all of its services. The process of achieving these successes, however, has been very gradual, and the initial programs were not always successful. An understanding of the successes and failures on the DOD front will allow those choosing to implement data fusion in a transportation security setting to avoid making similar mistakes.

The committee acknowledges and thanks the speakers from government and industry who took the time to share their ideas and experiences in briefings at its meetings (see Appendix C). The committee offers a special thanks to Donald Brown and Cheryl Bitner, who were the major contributors to the writing of this report. As chair of the committee through May 31, 2005, Thomas S. Hartwick also greatly assisted the work of the current committee through his participation in many of its activities. Finally, the committee acknowledges the valuable contributions to the completion of this report from Gary Fischman, director of the National Materials Advisory Board, and from NRC staff members James Killian and Teri Thorowgood.

James F. O'Bryon, *Chair*
Sandra L. Hyland, *Vice Chair*
Committee on Assessment of Security
Technologies for Transportation

Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons (2007).

Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Arnold Barnett, Massachusetts Institute of Technology,
Grace A. Clark, Lawrence Livermore National Laboratory,
Philip E. Coyle, Science Strategies,
Vijayan N. Nair, University of Michigan,
Robert L. Popp, Aptima, Inc.,
Gerald M. Powell, U.S. Army Research Laboratory,
Andrew P. Sage, George Mason University, and
James M. Tien, Rensselaer Polytechnic Institute.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Steven Berry, University of Chicago. Appointed by the National Research Council, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests solely with the authoring committee and the institution.

Contents

Figures, Tables, and Box

FIGURES

TABLES

BOX

In Memoriam

The Committee on Assessment of Security Technologies for Transportation is deeply saddened by the recent loss of one of its members. John B. Daly had a distinguished career serving our nation in a broad range of positions involving transportation security and technology. He was the worthy recipient of numerous awards and commendations for outstanding contributions to his field. John was selected to serve as a member of this committee in 2005, and he continued to serve with distinction until his illness no longer permitted his participation. He was a hardworking professional of the highest integrity and we will miss him. We dedicate this report to his memory in appreciation for his contributions.

Executive Summary

More than 1,100 bulk explosive detection systems (EDSs) and 6,000 explosive trace detection (ETD) systems have been deployed in the 438 commercial airports that service the United States. The rapid and universal deployment of these systems has resulted in minimal coordination and interface compatibility among the different systems and system manufacturers. These detection systems often stand alone, and only direct interaction by the operators enables coordination among them. Many of these multiple stand-alone inspection systems operate with undesirably high false-alarm rates, slow throughput, and excessive demands on individual operators.

In addition to EDSs and ETD systems, a large number of checkpoint and access-control systems have been deployed to prevent unauthorized entry into regulated areas of

airports. These systems use a variety of security systems, including video cameras, metal detectors, and biometrics, as well as observation by security personnel. Externally, ground-scanning radars and video cameras enable the monitoring of perimeters over large areas. Again, these access-control security systems operate primarily in stand-alone configurations. Airport security personnel currently gain situational awareness by manually combining outputs from these access-control systems.

The current widespread existence of stand-alone inspection systems and the uncoordinated operation of inspection and access-control systems leave the nation's airports and transportation network more vulnerable to a variety of potentially significant attacks than they would be if these systems were integrated. Essentially stand-alone systems are single points of failure. This means that if an attacker successfully evades discovery by a single system, that person gains access to the supposedly secure parts of the airport infrastructure.

Improving the detection and prevention of a broad range of attacks will require combining data from multiple inspection and access-control systems by means of a model which uses that input to estimate the threat level of a situation in a meaningful way. In short, being able to accomplish this task requires "data fusion." Because the concepts in this discipline are evolving, the Committee on Assessment of Security Technologies for Transportation has chosen to specify the concept definitions as used in this report; they are presented in Box ES-1.

Within the context of airport security, *data fusion* is the combination of data from multiple inspection and/or access-control systems into a single output, which can be used to make more-informed decisions. An effective data fusion system might prevent a "team bomb-making" scenario[1] by formally combining data from multiple inspection or access-control systems to indicate a higher probability for an overall alert condition.

BOX ES-1
Definitions of Concepts

- *Data sharing:* The exchange of data, possibly in different and incompatible formats, among organizations.
- *Data integration:* The assembly of data from multiple sources into a common data structure by means of a common data model.
- *Data fusion:* The combination of data from multiple sources to produce a "state estimate"—for example, the probability of a bomb in a piece of luggage.
- *Decision-data fusion:* The combination of binary decisions (e.g., yes or no) from multiple sources to produce a state estimate.
- *Parametric-data fusion:* The combination of analog measurements from multiple sources to produce a state estimate.

To enable data fusion, data sharing and data integration are required. *Data sharing,* by which data from different sources are made available to all cooperating organizations, became a concern after the attacks of September 11, 2001, when it became

[1] That is, several terrorists working in concert bring components of a bomb through a security checkpoint to be reassembled beyond the checkpoint. Singly the items are not a threat; together they are.

clear that various law enforcement and intelligence agencies had pieces of evidence about the impending attacks but none of them alone had the complete picture.[2] Data sharing is fundamentally an organizational and policy concern, with only minor technical issues relating to data latency and communications bandwidths. For example, two law enforcement agencies share data on calls for service or reported criminal incidents with an airport. The technical issues in data sharing are well understood and easily addressed in specific instances where data sharing is desired.

Data integration expands on data sharing so that data from multiple sources are placed in a common data structure, which enables their management and processing. The challenges to accomplishing data integration are technical; they concern the registration and transformation of data collected and processed in possibly different and competing frames of reference and data models. These concepts are addressed more fully in Chapter 2.

Data integration frequently is confused with data fusion. However, while data integration is necessary for data fusion, the integration alone is not sufficient to provide threat estimates. To accomplish this, the data must not only be integrated into a common data structure, but they must be combined by data fusion to produce a threat estimate. Data fusion would process the integrated data using mathematical models to provide an estimate of the threat at each point in time during the inspection and access-control processes.

As defined in this report, data fusion, unlike data integration, also provides an effective approach to reducing false alarms (false positives) while maintaining or improving the probability of detection. These improvements are obtainable with existing systems, and hence data fusion represents a cost-effective approach to the reduction of false alarms. Data fusion could enable these improvements because it takes detection and access-control systems out of their current stand-alone operational modes, providing the security personnel and the downstream systems with the data fusion results from the upstream security personnel and systems. These downstream systems and security personnel could use the information produced by data fusion to alter their inspection protocols in order to determine if an unusual occurrence was in fact a threat.

The combining of inspection and checkpoint systems made possible by data fusion means that detection thresholds could be adjusted dynamically, on a case-by-case basis, to reduce false alarms while maintaining desired detection probabilities. Automated data fusion might also remove the dependency on individual initiative and reduce the load on operators. Operators could then focus their efforts on resolving less-frequent, higher-probability alarms.

This report discusses two different data fusion models: (1) decision-data fusion (AND logic or OR logic) and (2) parametric-data fusion. Understanding the advantages and disadvantages of these models will allow technology program staff, such as those at the Transportation Security Administration (TSA), to derive the most benefit from their data fusion efforts.

Decision-data fusion merges simple binary results (e.g., “threat” or “no threat”) from individual detection and access-control systems. It is thus cheaper and easier to

[2] National Commission on Terrorist Attacks Upon the United States, T.H. Kean, Chair, and L.H. Hamilton, Vice-Chair. 2004. The 9/11 Commission Report. St. Martin’s Press, New York, August.

implement than parametric-data fusion, but it yields less robust state estimates.[3] Parametric-data fusion combines actual analog measurements (as opposed to binary results) from multiple systems and provides the most potential for improvement in the reduction of false alarms (false positives) at constant or improved probabilities of detection. However, parametric-data fusion requires very precise data integration, which costs more to implement in both time and resources than does decision-data fusion.

Finding: Decision-data (versus parametric-data) fusion does *not* necessarily allow for the greatest improvements in throughput, reduction of false alarms, or improvements in probability of detection. Most TSA data fusion efforts in current programs employ decision-data fusion.

Recommendation 1: Before implementing a data fusion approach for a specific set of security systems, the TSA should perform a formal analysis to select the specific data fusion approach that would increase the detection rate, or that would raise throughput and/or reduce false alarms while maintaining the existing detection rate.

This report reviews data fusion as a technological tool for improving air transportation security and the use of data fusion for inspection and access-control systems within airports. These airport-level mechanisms could be implemented more easily and inexpensively than could inter-airport data fusion.

Many of the technologies for data fusion within airports are already developed and understood from other applications. A focus on an airport-level implementation provides the best opportunity to develop a systems approach that can be expanded beyond individual airports as the systems mature.

The TSA is well aware of the importance of using data fusion to improve security and is funding a number of programs in this discipline. Many of the data fusion technologies under consideration by the TSA for use in air transportation security have been used by the Department of Defense (DOD). For example, the DOD has employed data fusion to improve the useful information from existing intelligence and surveillance systems. The committee review of these DOD systems has led to the following findings:

Finding: While the DOD has achieved successes in data fusion, information sharing, and networked operations, it has also had numerous unsuccessful programs in these areas. Those involved in transportation security can learn a lot from both the successes and the failures of the DOD.

Finding: Improvements can be made in security operations by effectively employing data fusion. These improvements can be accomplished with existing technologies. Experience in the DOD indicates the potential effectiveness of and benefits to security operations from applying data fusion.

Private industry has also used data fusion to improve quality and production in manufacturing. Private-industry methods include the combination of data and operator

[3] A "state estimate" is a determination of the underlying status of a system at any point in time, based on an analysis of the available data.

inputs for real-time process control. This experience provides further motivation for the TSA to develop data fusion implementation strategies.

Finding: Private industry has employed data fusion to enhance quality and to improve production and has developed data fusion infrastructure, including interface specifications and data structure, to allow the collection and analysis of information.

The Transportation Security Laboratory (TSL) of the Science and Technology Directorate of the Department of Homeland Security (DHS S&T) has current programs in data fusion covering areas such as secure network design, security system evaluation, and deployment of demonstration systems. While this list demonstrates an interest in employing data fusion technologies to improve transportation security, these efforts lack a unifying systems perspective.

Finding: The TSL of the DHS S&T has identified the need for applying data fusion and has addressed this need by implementing a number of projects at the system and checkpoint levels. However, these projects are not the output of a systems engineering analysis (which would involve formal requirements analysis and derivation) of data fusion at all levels: baggage screening, checkpoint, and access control and surveillance.

Recommendation 2: The TSA should establish a means to ensure that the following tasks and functions are carried out:

- Creation of a set of system-level data fusion requirements for checked-baggage screening, checkpoint, and access-control systems;
- Performance of a systems engineering analysis of these areas;
- Validation of these requirements against threat projections, current and projected security systems, and facility idiosyncrasies; and
- The monitoring of fundamental research in the field and adjustment of requirements where appropriate.

The threat projections against which data fusion requirements would be validated must be clearly developed so that the equipment is accurately tested against whatever it is designed to be detecting. While the TSA can improve its programs by adopting a systems approach, industry also must participate in the integration of disparate systems. Manufacturers of inspection and access-control systems have only recently begun considering the integration of data from their systems with data from other systems in order to achieve a total security system. A notable exception involves manufacturers of biometric-based access-control systems; these manufacturers have begun the systems engineering process of defining the necessary data standards for data integration. As noted earlier, data integration provides a necessary, but not sufficient, condition for data fusion, and the range of potential detection technologies must be considered when setting the standard data format.

Data fusion of access-control systems at checkpoints could link data from video cameras, metal detectors, and other access-control systems with inspection systems. Data fusion of inspection systems requires a common or standard frame of reference for

locating and identifying objects in bags. Similarly, sharing data between video cameras and metal detectors will require a standard frame of reference for locating and identifying objects on people. Further, combining bag and passenger inspection systems will require a standard frame of reference for locating and identifying people and baggage within the checkpoint and within the airport. Existing technologies can perform these functions within checkpoints, but to locate objects and people in airports will require more extensive use of video surveillance and other technologies, such as radio-frequency tagging and biometrics.

In addition to screening, the needs of airport security, or access control, require data fusion methods to enable and inform situational awareness. The components of these data fusion methods are kinematics, identity, and behavior. The kinematics component describes the motion of objects, such as people, within the airport and that of vehicles outside the airport; each object is described by a trajectory that includes state estimates for future locations. Facility data fusion requires kinematic descriptions of people, vehicles, and objects. The identity component provides classifications for all objects in the environment and includes all systems and subsystems used: this means, for example, identifying weapons and components of weapons systems. The behavior component specifies the intent and actions of the objects, giving meaning to the kinematic observations and estimates. Suspects repacking suspicious items before entering a checkpoint would be an example. Behavior should be specified to enable rapid and effective response to airport threats. Each of these components—kinematics, identity, and behavior—possesses appropriate measures of uncertainty.

Finding: Most of the detection systems now fielded in U.S. airports were built without regard for the need for data fusion or data integration among systems. Many manufacturers are attempting to create systems that not only fuse data, but also link information about passengers and baggage. However, there is little direction from the TSA with respect to the establishment of standards or requirements.

The solution to this problem of interoperability is to require manufacturers to agree to common standards and to have systems integration companies provide the integrated designs and solutions. Rather than performing this function internally, the TSA could contract with entities that have systems integration experience to develop fusion approaches and also to oversee the implementation of these efforts. Several companies and institutions possess the required competencies, including much experience with DOD developmental programs of similar complexity.

Recommendation 3: The TSA should work (that is, contract) with the leading integrators and manufacturers to form a representative working body and require it to develop initial strategies and standards for the integration of airport security, checkpoints, checked-baggage screening, and access control, including legacy systems.

Human operators are much better than automated systems at detecting hard-to-specify but salient events. Computer-based systems without human oversight are better at detecting easy-to-specify events, such as the presence of a substance with a particular density or atomic number. The advantage of providing human inputs into a data fusion

system is that the human operators and the automated inspection and access-control systems exercise their respective and complementary strengths and so allow greater potential for the detection of terrorist events. The requirement to provide input into a fusion system is unlikely to distract operators from their other tasks, as the need to provide human input would likely be quite a rare event. In fact, many of the human tasks in security require vigilance that can actually be enhanced by the addition of a subsidiary task.

Finding: Data fusion would enhance security system effectiveness if it were to combine inputs from security personnel with data from detection systems into a unified situational awareness system.

Recommendation 4: The TSA should develop formal data-entry mechanisms for security personnel that will enable the combination of human observational data with security system data. These mechanisms should be designed so as to maintain performance on existing tasks.

The implementation of data fusion does not come without risks. The TSA can significantly reduce these risks by implementing data fusion deployments in stages. Rather than simultaneously attempting to incorporate data fusion into all inspection and access-control systems, a staged approach would select a subset of these systems for fusion. Once data fusion was accomplished in one subset, the next phase would involve the next subset of systems selected for fusion. This process would proceed until data fusion had been incorporated into all inspection and access-control systems in an airport.

Finding: The implementation of data fusion based only on laboratory testing is a high-risk strategy. Operational testing conducted as a subset of certification testing is required to ensure data fusion system effectiveness.

Recommendation 5: The TSA should implement any data fusion systems through a series of staged deployments at an operational testbed as designated by the TSA and/or at selected airports. The experience from these early staging events can then be incorporated and used in the data fusion systems rolled out in later implementations.

1

Introduction

The U.S. air transportation system is an attractive target for terrorists because of the potential that attacks on it will cause immediate harm and anxiety to large numbers of people, as well as cause massive economic disruption to the United States and the world. The system is vulnerable owing to its mission to provide service to people with a minimum of intrusion on privacy and with minimal disruption of access. The detection and mitigation of attacks on air transportation are made more difficult by the transient nature of the passengers' movement through airports and the fact that it is common for passengers to be carrying several bags, making it relatively easy to conceal threat mater-

ials. The use of commercial airliners as weapons in the September 11, 2001, attacks on the Pentagon and the World Trade Center has also broadened concepts of what constitutes a threat to U.S. assets in general and to the air transportation system in particular.

Based on terrorist attacks to date involving the hijacking and bombing of aircraft, current threat-detection measures concentrate on detecting weapons or explosives. In the future, such attacks could also involve the use of toxic chemicals, chemical and biological warfare agents, or even radiological and nuclear materials.[1]

The government agency charged with responsibility for the implementation of technology for countering such threats is the Transportation Security Administration (TSA). The TSA, and the Federal Aviation Administration before it, have invested extensively in the development and deployment of technological and procedural systems designed to protect the traveling public. In support of this mission, the TSA has tasked the National Research Council (NRC) with assessing a variety of technological opportunities for protecting the U.S. transportation system, with a focus on the air transportation system.

STATEMENT OF TASK

In order to perform the assessment requested by the TSA, the NRC created the Committee on Assessment of Security Technologies for Transportation, under the National Materials Advisory Board. The committee's statement of task is as follows:

> This study will explore opportunities for technology to address national needs for transportation security. While the primary role of the committee is to respond to the government's request for assessments in particular applications, the committee may offer advice on specific matters as required. The committee will: (1) identify potential applications for technology in transportation security with a focus on likely threats; (2) evaluate technology approaches to threat detection, effect mitigation, and consequence management; and (3) assess the need for research, development, and deployment to enable implementation of new security technologies. These tasks will be done in the context of current, near-term, and long-term requirements.
>
> The committee will perform the following specific tasks:
>
> 1. Identify potential applications for technology in transportation security with a focus on likely threats derived from threat analyses that drive security system requirements. Review security system developments structured to meet the changing threat environment. Assess government and commercial industry plans designed to address these threats.
>
> 2. Evaluate technology approaches to threat detection, effect mitigation, and consequence management. Delineate the benefits of the insertion of new technologies into existing security systems. Evaluate the trade-offs

[1] The President's Homeland Security Department Proposal, available at http://www.whitehouse.gov/deptofhomeland/bill/index.html, accessed April 22, 2007; National Research Council. 2002. Making the Nation Safer: The Role of Science and Technology in Countering Terrorism, National Academy Press, Washington, D.C.

between effectiveness and cost, including the cost of changing the security system architectures.

3. Assess the need for research, development, and deployment to enable implementation of new security technologies. Review and assess the potential benefit of existing and advanced detection technologies, including scanning technologies, sensing technologies, and the use of computer modeling and databases. Review and assess emerging approaches to effect mitigation and consequence management.

COMMITTEE APPROACH

An overarching goal of this committee has been to provide timely reports that meet the TSA's priorities for defeating terrorist threats. The committee judged that this could best be done by issuing a series of short reports on chosen technology applications. In consultation with the TSA, the committee selected four topics for study and produced four reports (all published by the National Academies Press, Washington, D.C.), of which this report is the fourth:

1. *Opportunities to Improve Airport Passenger Screening with Mass Spectrometry* (2004),
2. *Defending the U.S. Air Transportation System Against Chemical and Biological Threats* (2006),
3. *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons* (2007), and
4. *Fusion of Security System Data to Improve Airport Security* (2007).

Taken together, the four reports will satisfy the first part of the statement of task—an identification of applications for technology in transportation security. Independently, each report addresses a particular technology focus and identifies additional research needs.

By mutual agreement between the committee and the sponsor, the broad focus on "transportation security" in the statement of task was narrowed to the "threat of attacks on the air transportation system." While the defensive measures and technologies discussed here may not have application to all transportation modes (e.g., containerized ships, bridges, highway tunnels, subways, and others), the committee believes that the air transportation security arena provides a relatively well controlled testbed for gaining experience with defensive strategies that could be adapted to other, more-complex, less-controlled transportation spaces—for example, bus terminals, train stations, cruise ships, and cargo terminals—with appropriate modifications.

BACKGROUND

The security of the U.S. commercial aviation system has been a concern since the 1970s when hijacking became a serious problem. A number of aviation security programs have been implemented. However, weaknesses continue to exist. These weaknesses were observed and exploited by terrorists on September 11, 2001, enabling them to hijack four commercial aircraft, with tragic results. Terrorists and persons of like mind can be expected to continue to examine the nation's transportation security operations, both overtly and covertly, to find weaknesses to exploit.[2]

While all modes of transportation are security concerns, aviation security remains a priority. With hundreds of commercial airports, thousands of commercial aircraft, tens of thousands of daily flights, and millions of passengers using the system daily, providing security to the nation's commercial aviation system is a daunting task. Figure 1-1 illustrates some of the threat vectors that may exist in the nation's largest airports.

As can be seen in Figure 1-1, there are multiple points of vulnerability in and around an airport. Protection of each of these points generates a large body of data. Integrating the data collected in a manner that allows a better picture of potential threats could substantially strengthen airport security.

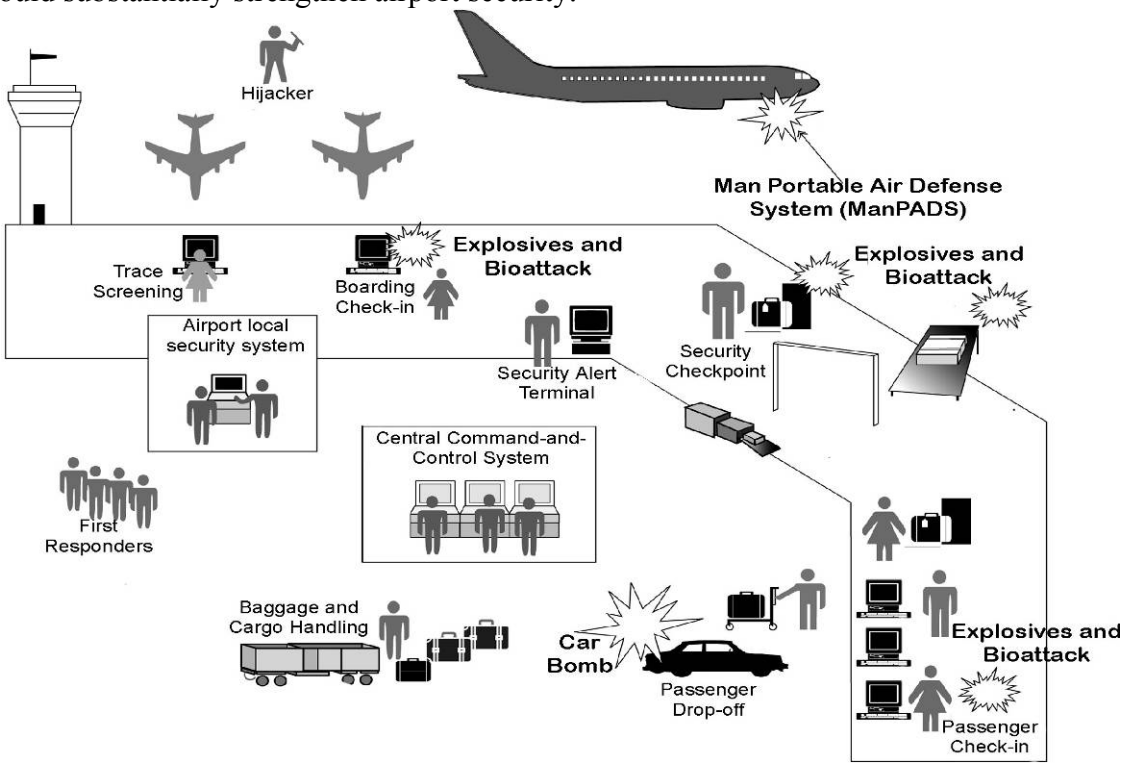

FIGURE 1-1 Generic airport diagram showing various airport spaces and some likely sites for attacks. Data fusion would allow for the coordination of input data from each of these potential threat vectors.

[2] *Al Qaeda Training Manual.* Available at http://www.usdoj.gov/ag/trainingmanual.htm. Accessed April 22, 2007.

On November 19, 2001, President George W. Bush signed into law the Aviation and Transportation Security Act (ATSA) (Public Law 107-71), which mandated the federalization of passenger and baggage screening at more than 438 commercial airports in the United States by November 19, 2002, and the screening of all checked baggage using explosive detection systems (EDSs). On March 1, 2003, the TSA was transferred from the Department of Transportation to the newly created Department of Homeland Security, as required by the Homeland Security Act of 2002 (Public Law 107-296).

Virtually all of the nation's aviation security responsibilities are with the TSA. They include the conducting of passenger and baggage screening and the overseeing of security measures for airports, commercial aircraft, air cargo, and general aviation. These programs of the TSA are intended to form a layered system that maximizes the security of passengers, aircraft, and other elements of the aviation infrastructure.

The TSA has undertaken several programs to measure and improve the performance of checkpoint and checked-baggage operators in detecting threat objects. In July 2003, the TSA completed a study of the performance of its passenger and carry-on luggage-screening system, which identified numerous performance deficiencies, such as inadequate staffing, poor training of screeners, and poor supervision of operators. These deficiencies were the result of a lack of skills and knowledge, low motivation, an ineffective work environment, and wrong or missing incentives. The TSA is taking steps to remedy these deficiencies. Although it is making progress in its checked-baggage screening operations, it continues to face operational and funding challenges in screening all checked and carry-on baggage using EDSs, as mandated by the ATSA.[3]

SHORTCOMINGS OF EXISTING SYSTEMS

The United States has 438 airports that service commercial aviation and has deployed more than 1,100 bulk EDSs and 6,000 explosive trace detection systems manufactured by a number of different companies. The overarching requirements to deploy these systems universally and rapidly have understandably led to little coordination and interface compatibility among the different systems and the system manufacturers. As a result, the present situation is that detection systems operate largely as stand-alone systems, and only operator interaction enables coordination among these systems. Many of these multiple stand-alone detection systems operate with undesirably high false-alarm rates, slow throughput, and excessive demands on individual operators.

Deterring many likely attack scenarios will require the coordinated operation of the detection systems within the airports to prevent attempted attacks from succeeding. Consider, for example, a team of terrorists whose objective is to place an explosive device on an airplane. By separating out elements of the device, each member of the team may be able to get through security screening individually. Once through, they can assemble their device. An effective data fusion system might prevent this scenario by merging data from multiple systems to indicate an overall alert condition, thereby turning data into information.

---

[3] Government Accountability Office. 2004. Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts. GAO-04-592T. General Accounting Office, Washington, D.C., March 30. Available at http://www.gao.gov/cgi-bin/getrpt?GAO-04-592T. Accessed April 22, 2007.

Data fusion also provides the most effective approach to reducing false alarms while simultaneously maintaining or improving the probability of detection. This improvement is possible because data fusion should enable the combination of different security system modalities to discriminate explosives from ordinary passenger items.

Data fusion is also essential for facility security. In the area of access control, data fusion is considered critical to the deployment of biometric systems. At the airport level, there is a major need to integrate and fuse data from multiple, facility-monitoring security systems. Without this fusion, the airports are vulnerable to a variety of attack vectors. For example, some airports have security systems in their heating, ventilation, and air conditioning systems to detect the presence of chemical or biological agents; however, these security systems are not linked to video, motion, or radar security systems to provide situational awareness in the presence of an attack. It is thus difficult for airport security personnel there to direct an effective response to such an attack.

SCOPE OF THE REPORT

The scope of this report was derived from the expressed needs of the TSA. During briefings to the committee, the Transportation Security Laboratory identified the following three reasons for pursuing data fusion and integration in transportation security: (1) to improve or maintain detection accuracy while decreasing false alarms, (2) to reduce the footprint at airports from new in-line systems, and (3) to reduce staffing requirements by automating information processes.

The current approach to most threat detection consists of multiple stand-alone detection systems, some with unacceptably high rates of false alarms and slow through-put. These individual systems also impose high demands on individual operators. Any integration or fusion of data takes place at the initiative of individual operators and security personnel. As is illustrated in Chapter 2, standardized data integration and automated fusion systems should remove the dependency of these systems on individual initiative and reduce the load on operators. Operators could then focus their efforts on resolving higher-probability alarms.

The current security technologies include x-ray radiography and computed tomography (CT), trace detectors, and metal detectors. Human observations are also made but are not formally incorporated into or used by any of these security methods. Further, all decisions by current security schemes are binary, and there is no method for the fusion of partial results that, taken together, would suggest a threat.

For example, a CT operator scanning a passenger's bag may not signal an alarm but may be close to the alarm threshold; at the same time, a TSA security agent may notice suspicious behavior by the owner of the bag. There is currently no way to put these two partial pieces of evidence together to suggest the advisability of a more complete search. As another example, the x-ray radiography image of passenger X's carry-on bags may indicate a threat, but the physical search reveals nothing in the carry-on bags; a checked bag belonging to passenger X may also alarm, but the fact that two alarms have been raised for the same traveler will not be known.

New technologies proposed for introduction at airports include biometrics, mass spectrometry, x-ray diffraction, x-ray backscatter, millimeter-wave (MMW) and terahertz

(THz) imaging,[4] nuclear quadrapole resonance, and Secure Flight (a program to rapidly identify passengers who are unlikely to present a threat). In addition, the committee anticipates further improvements to existing technologies. However, at this point, little effort (other than biometrics) has been focused on integrating either existing or future technologies. At the time of this writing the committee is not aware of any attempts to develop standards for data integration of existing or new technologies.

For the nation to make progress in improving the security of all transportation systems, the TSA will need to make more effective use of its security systems and its security system data-processing mechanisms. This report focuses on exactly this area—how the TSA and airport security personnel can better utilize existing security systems (humans and machines contributing to the security information flow) through the fusion of data—and it provides the foundation for the more effective use of existing and future security systems that will enable significant improvements in the transportation security environment.

In order to provide the most timely and easily implemented recommendations to the TSA, the scope of this report is limited to near-term objectives and does not address a number of important ancillary questions. In particular, it does not address the integration and sharing of data above the airport level. That is, it does not address regional or national data integration or fusion among airports and among different security organizations. These important questions will require additional study. As any regional or national approach to integration or fusion will require the implementation of the recommendations in this report at the airport level, the approach recommended here is a necessary first step for later regional and national integration and fusion initiatives.

STRUCTURE OF THE REPORT

The committee met several times with the study's sponsor, the TSA, and with input from the TSA, it developed the following objectives for this report:

1. Describe the air transportation data fusion problem from the elemental system level to the airport level,
2. Discuss current projects to address data fusion, and
3. Provide recommendations for improving security and data utilization through data fusion.

The report is structured to follow these objectives, with Chapter 2 serving as a foundation on issues related to data fusion in an airport security model and providing an overview of current projects in this realm (projects of the Department of Defense and private industry). Chapter 3 contains the majority of the committee's scientific analysis, with a summary of the TSA data fusion projects. Recommendations for moving forward are presented in Chapter 4.

[4] For more information on MMW and THz technologies, see National Research Council. 2007. *Assessment of Millimeter-Wave and Terahertz Technology for Detection and Identification of Concealed Explosives and Weapons*, The National Academies Press, Washington, D.C.

The committee expects that this report will have an audience beyond those in the TSA, including those in academia, equipment manufacturers, airport security personnel, and policy makers. The report is thus intended to be accessible to a variety of readers.

2

Data Fusion for Security Operations

WHAT IS DATA FUSION?

Data fusion for security operations is a state-estimation process based on data from multiple security systems or data sources.[1] The states of greatest relevance to security are the threat levels (from, e.g., a bomb in baggage), although a larger set of

[1] The results and definitions in this chapter derive from D.E. Brown. 2006. Data Fusion for Air Transportation Security, Technical Report 2006-3, Department of Systems and Information Engineering, University of Virginia, Charlottesville, February 14.

states could be envisaged (such as the potential for an outside attack). The goal of data fusion is to increase the accuracy of the estimate.

Modern data fusion systems can involve prodigious amounts of information that must be rapidly extracted from data sources, processed, and transferred. The data sources may involve computer systems on the ground; systems on moving conveyors, vehicles, or aircraft; systems on specific sensors; and even from systems in space. The large quantities of information produced by such systems may need to be processed rapidly to be effect-tive. For transportation security, in some cases, this processing must be done in real time, sometimes in very short periods and across many interfaces. Also, the way in which information is generated is important. Proving the validity of algorithmically driven results versus that of analytically created results, and doing so in real time, is a formid-able objective.

Some transportation security data fusion systems may involve information extracted from hundreds of thousands of files or records, the processing of results, and the selection and then the transfer of the proper information. And yet the developer may propose fielding such systems never having tested the extraction and transfer of more than a few files, and never having carried out the whole process end to end in real time. Also, unique simulators and emulators may need to be designed and built to exercise these systems in a realistic way during development. This work can require dozens of contractors and suppliers all working together as a team with clear, effective, and open communication.

Data fusion may have a significant impact on the performance of a system (see Figure 2-1). Even multiple looks with the same security system can provide improve-ments in metrics such as probability of detection. As Figure 2-1 illustrates, combining multiple security systems can frequently overcome the ambiguity present in many situations and defeat attempts at deception.

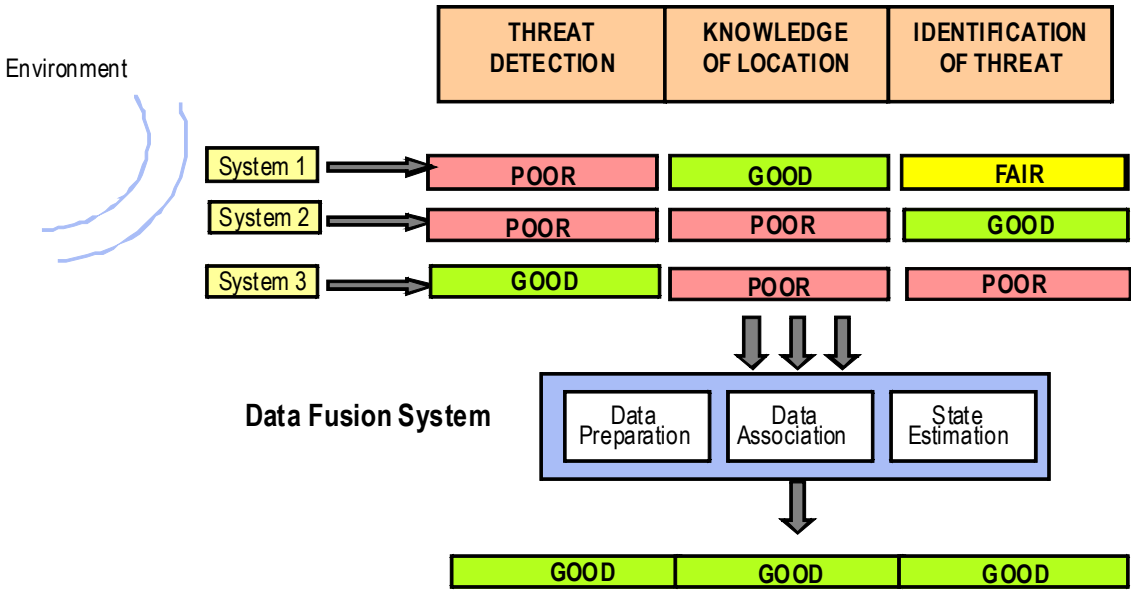

FIGURE 2-1 Data fusion overview. The fusion of data from multiple systems can improve the results from any individual system.

Data fusion will most likely be incorporated both within security systems and as a separate fusion component implemented apart from individual security systems. Better performance (as measured by increased probability of detection and decreased probability of false alarm) can sometimes be achieved through parametric-data fusion—that is, the combining of data at the signal level rather than fusion at the decision level.

This report examines the issue of data fusion from the perspective of the actual security systems: baggage screening, checkpoints, and access control. To facilitate this discussion, the next section describes the steps in data fusion.

STEPS IN DATA FUSION

Typically, data fusion consists of three steps: data preparation, data association, and estimation or prediction.

Data preparation means putting the data into a form that will enable fusion. One of the most important components of the preparation step for fusion is data registration. The data, which come from different sources, must have a common registration—that is, the data must be converted to the same view angles and spatial and temporal resolutions. For example, if a security system, such as baggage screening, detects a likely explosive in a bag, the location of the likely explosive needs to be conveyed to the secondary security system (e.g., hand searching the bag) in order to direct the search; but for this to happen properly, the two security systems must have a common registration coordinate system or their data cannot be combined. This registration involves both spatial and temporal resolution because change can occur in both bags and passengers (i.e., both can move, and bag contents can shift), and there needs to be allowance for change if fusion is to be done effectively.

In addition to registration, the data preparation step also requires formally defining confidence intervals for data produced by each security system or source. No security system is perfect in its reporting, but it is not enough simply to recognize this fact. Effective fusion requires that data be quantified. The fusion of results from two security systems has the potential to reduce the errors associated with each individual security system. However, to understand and exploit that reduction, it is necessary to know the amount of variance in data as an input to fusion. With this knowledge, the fused output should have a quantified error rate that is less than that of any of the individual security systems.

Other parts of data preparation include data cleaning and normalization. Cleaning removes obvious errors from the data. Normalization puts the data on common scales of measurement.

The second step in fusion, *data association*, looks for data that are linked. In baggage screening, this means looking for multiple security system results showing the presence of an explosive. For example, at check-in, a service agent might input observations of a passenger's suspicious activity. Those results, associated with suspicious baggage-screening results, can be used to estimate the likelihood of terrorist activity by that particular passenger. Association provides hypotheses about linkages in the available data; typically, multiple hypotheses result from this processing step. Hence, algorithms for data association are computationally expensive and inexact, which means that one can

only approximate the most likely linkages in the data. Data fusion cannot avoid or completely eliminate false positives or negatives.

The last step in fusion is *estimation or prediction*. Once data are associated, they might be used to estimate a current state or situation and to predict a future state: a common estimation or prediction problem in transportation security is that of estimating or predicting the probability that an object is an explosive. Another use might be to estimate the probability that an area or object is the target for an attack. Methods for estimating rely on parametric statistical modeling and have been advanced by developments in mixed-effects modeling.

COMPARISON OF DECISION-DATA FUSION AND PARAMETRIC-DATA FUSION

Data fusion is most easily, and typically, accomplished by taking the decision outputs from each security system and combining them into one global decision. While simple to implement, this approach, called decision-data fusion, has several shortcomings. An alternative approach combines the data from multiple sources and uses these data together to produce a state estimate. This approach, which the committee calls parametric-data fusion, has the potential to improve system performance, but it requires more extensive registration, normalization, cleaning, and error parameterization than does decision-data fusion. In this section, the committee discusses the performance characteristics of parametric-data fusion for transportation security, as compared with the simpler decision-data fusion method.

To illustrate decision- and parametric-data fusion, the committee discusses two hypothetical explosives-detection security systems whose outputs can be correlated. The committee has not made any assumptions about the applicability of these notional examples to current security systems or existing technology, and it has not performed a detailed statistical analysis of the issues. Security System 1 reports integer values between 2 and 13 with an average of 4, and each value is converted into a probability of detection (PD) that is conditional on the data. Security System 2 reports real values between −11.7 and 72.8 with an average of 14.0. Figure 2-2 shows the response histograms and a response profile for each security system for a test set of size 31 with 12 detectable targets. Over this data set, the security systems have a correlation coefficient of −.009. These data are simulated and do not represent the response histograms or response profiles of any known security systems.

The graphs in Figure 2-2 show the marginal distributions for the response from each hypothetical security system and are not conditioned on the presence or absence of a simulated explosive. Figure 2-3 shows the density of each security system response conditioned on the presence of a simulated explosive. These plots show that neither security system alone would be completely effective in detecting the presence of the simulated explosives over a range of test cases.

These security systems can be operated in one of five modes: with each one operating individually without fusion, by connecting the systems' decision outputs (decision-data fusion) with AND or OR logic, or by combining their responses to produce a single fused probability using parametric-data fusion. The discussion below explains

each of these modes and provides the associated receiver operating characteristic (ROC) curves for comparisons.

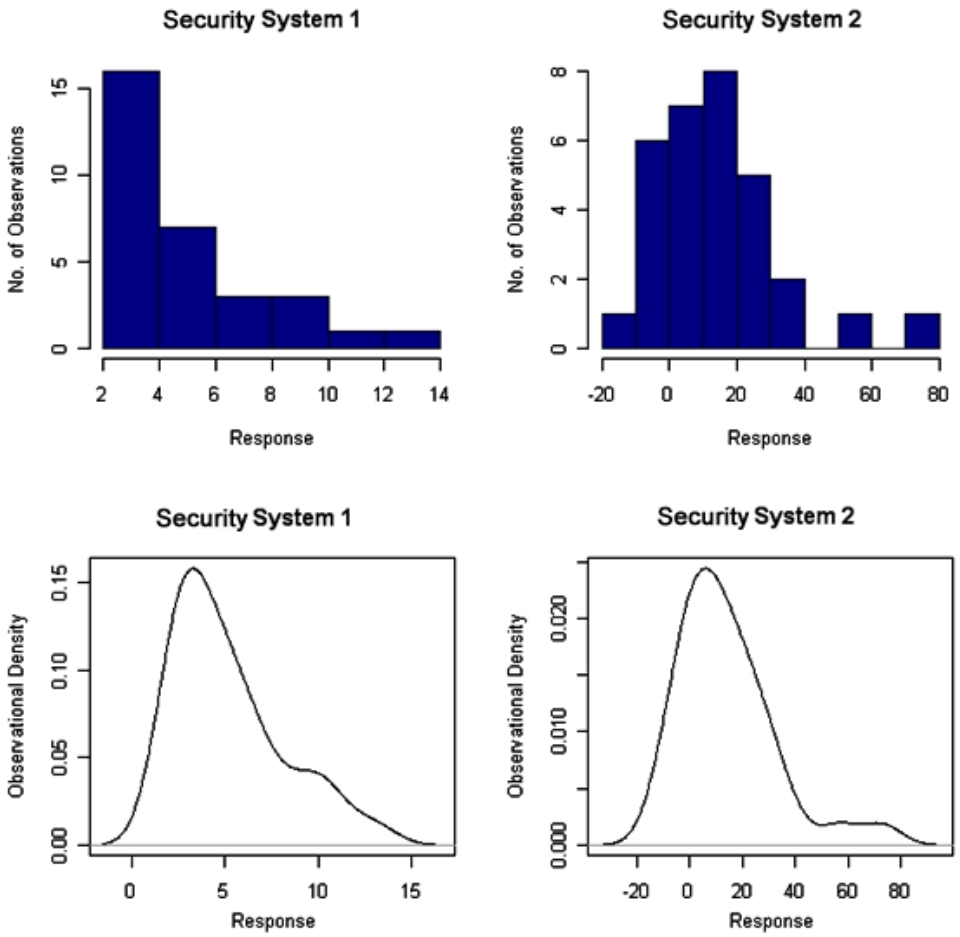

FIGURE 2-2 Notional individual security system response histograms (top) and response profiles (bottom) for the test sample—Security System 1 and Security System 2.

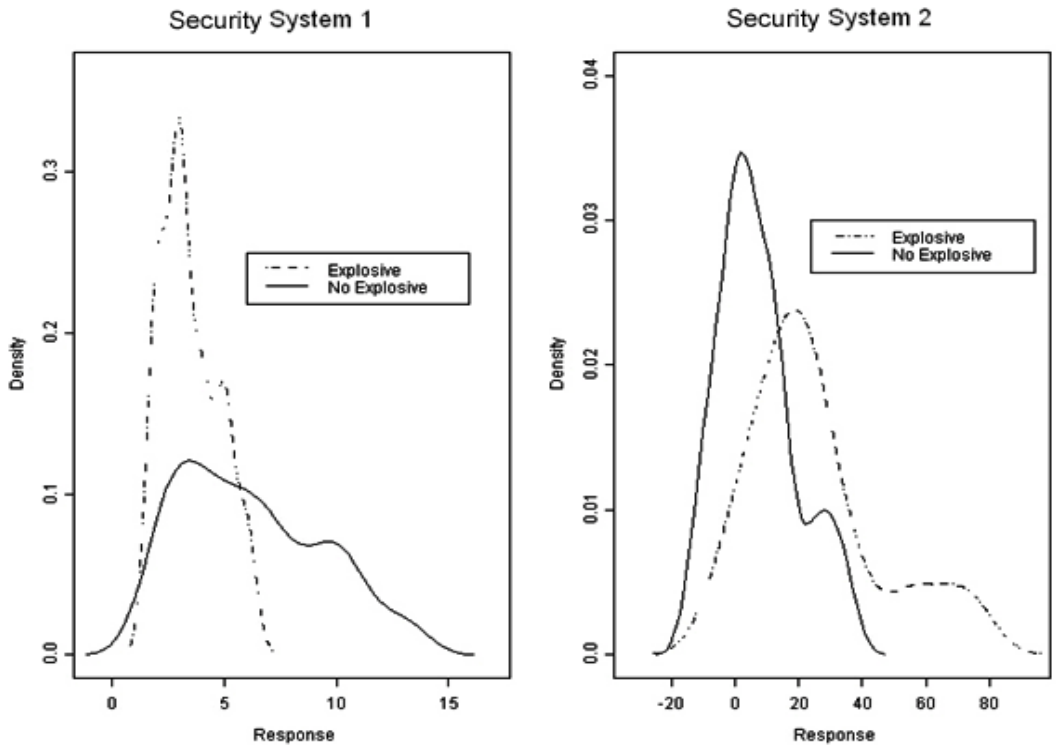

FIGURE 2-3 Conditional response profiles for each notional individual security system.

Individual Security Systems with No Fusion

The individual security system mode first uses a single security system to produce a response based on the sample input object; this response is then converted into a detection decision. The block diagram in Figure 2-4 shows this mode of operation. The decision function is normally part of the security system. This function is separated out in the diagram, since it will be important to an understanding of the modes of operating multiple security systems. The output from the process is a detection decision with an associated PD.

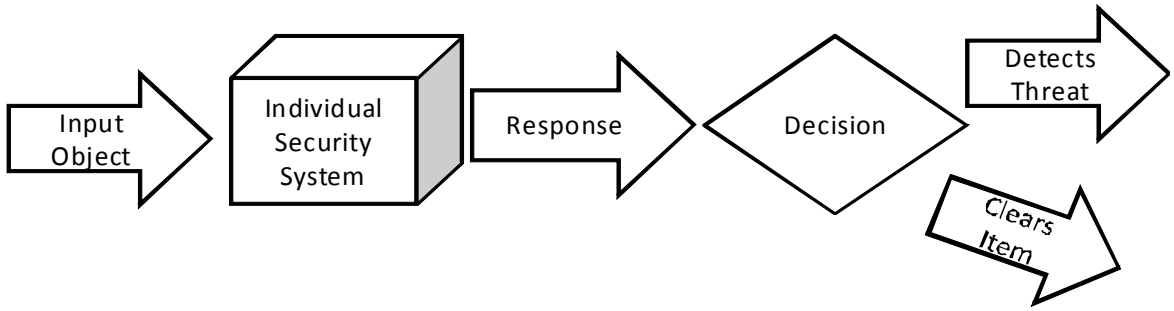

FIGURE 2-4 Individual security system operational mode with no data fusion.

Security system manufacturers can set the threshold for detection; the threshold results in a probability for true positives (sensitivity) and false positives (specificity).

Typically, the operating characteristics of security systems against these two measures are plotted as ROC curves. The ROC curves for the security systems in this example are shown in Figure 2-5. The dashed line indicates how a system that randomly makes a detection decision would perform, while the solid line indicates the performance of the sample system. Clearly both of these sensors do better than randomly making a decision.

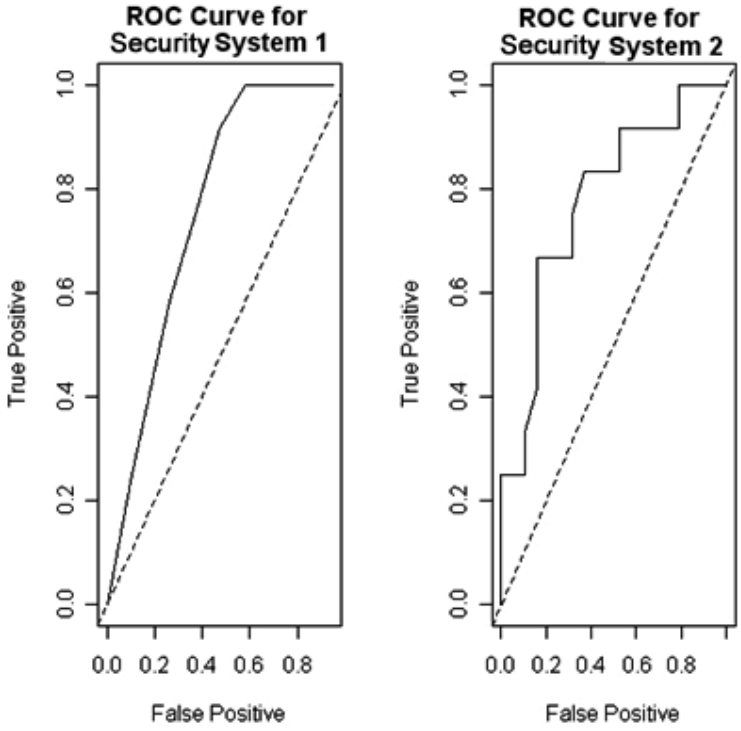

FIGURE 2-5 Receiver operating characteristic (ROC) curves for each security system—Security System 1 and Security System 2—for the test sample. Solid line: performance of the sample system; dashed line: performance of a system that randomly makes a detection decision.

An alternative way of looking at these data would be in a Bayes table (Figure 2-6), where the results of the tests are examined for true detections, missed detections, false positives, and true negatives, as shown.

	Threat Seen	**No Threat Seen**
Threat Present	True Detection	Missed Detection
No Threat	False Positive	True Negative

FIGURE 2-6 Example of a Bayes table for examining test results.

While the differences are subtle, it is important to distinguish between a false negative and a missed detection. A false negative means that a threat item has been inappropriately identified as a nonthreat, whereas a missed detection means that the threat item has not been seen.

Decision-Data Fusion with AND or OR Logic

One of the simplest ways to combine more than one security system in support of decision making is through AND or OR logic. This decision-data fusion approach allows the operator to use the security systems as manufactured and to change out security systems as needed for maintenance or replacement.

AND logic is illustrated in Figure 2-7. The input object is processed first by Security System 1; if this security system detects a threat, the input object is passed to Security System 2. If the second system also detects a threat, it will signal an alert. If the second system does not detect a threat, the item is cleared.

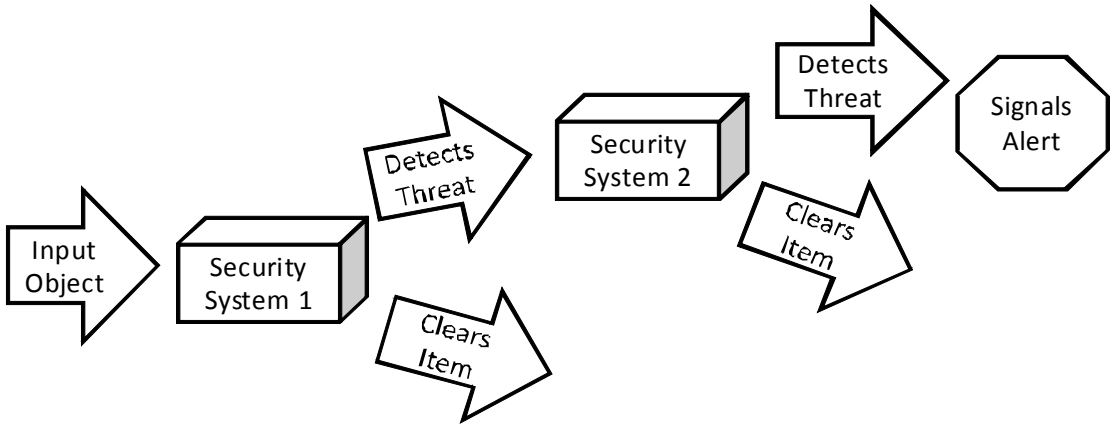

FIGURE 2-7 Decision-data fusion with AND logic.

This approach is designed to reduce the number of false positives. The ROC curve in Figure 2-8 supports this expectation for the committee's example data. For a false positive rate, called a false-alarm rate (FAR)[2] of 0.2, or 20 percent, the combined security systems with decision-data fusion with AND logic have a true positive rate of almost 0.8; when each operating in a stand-alone mode the two security systems, 1 and 2, experienced true positive rates of 0.45 and 0.67, respectively.

[2] The FAR derives from putting the data (actual known cases) through the systems and then counting the number of times alerts were signaled on cases that were not threats. False negatives, where a threat item is inappropriately identified as a nonthreat, are calculated similarly.

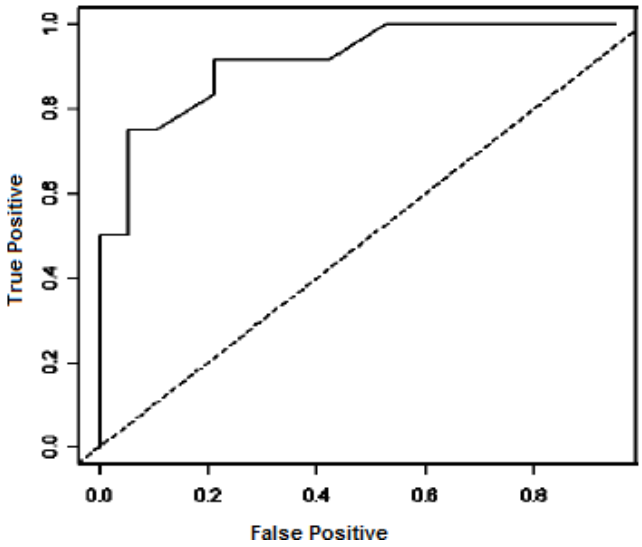

FIGURE 2-8 Receiver operating characteristic (ROC) curve for the AND decision-data fusion for the combination of two notional security systems (solid line). The dashed line represents chance performance.

OR decision-data fusion logic simply combines the security systems so that detection by either security system will cause an alert, and it takes both security systems to clear an input object. The block diagram for this approach is shown in Figure 2-9, and the ROC curve based on the example data and security systems is shown in Figure 2-10. Notice that with the false positives—the FAR—limited to a notional value of 0.2, the OR decision approach does worse than each individual security system. The resulting probability of detection for OR decision-data fusion is 0.42, whereas for Security System 1 it is 0.45 and for Security System 2 it is 0.67. The OR decision-data fusion logic works to decrease the FAR, but at the cost of increased missed detections. This example shows that simply assuming that a decision-data fusion approach will improve performance is not always correct. Before implementing fusion, the Transportation Security Administration (TSA) should perform the necessary analysis to ensure that the correct approach is selected.

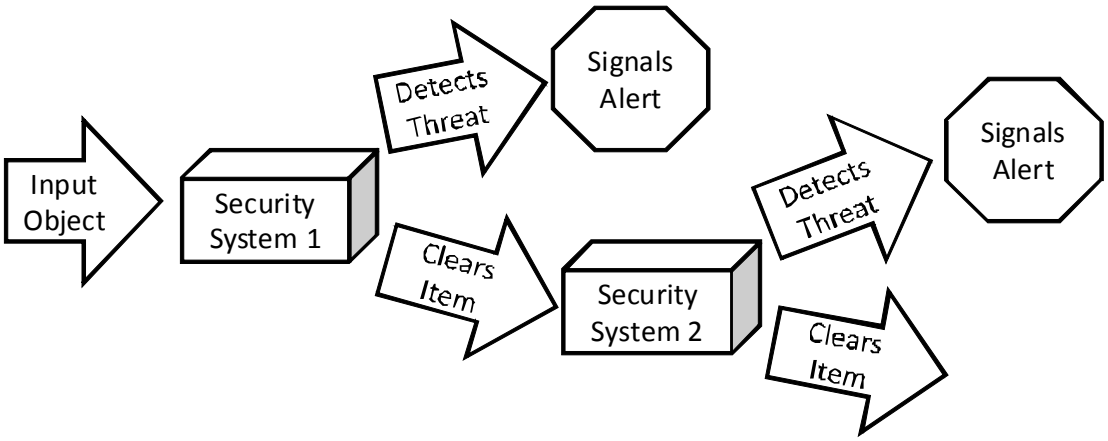

FIGURE 2-9 Combining security systems with OR decision-data fusion logic.

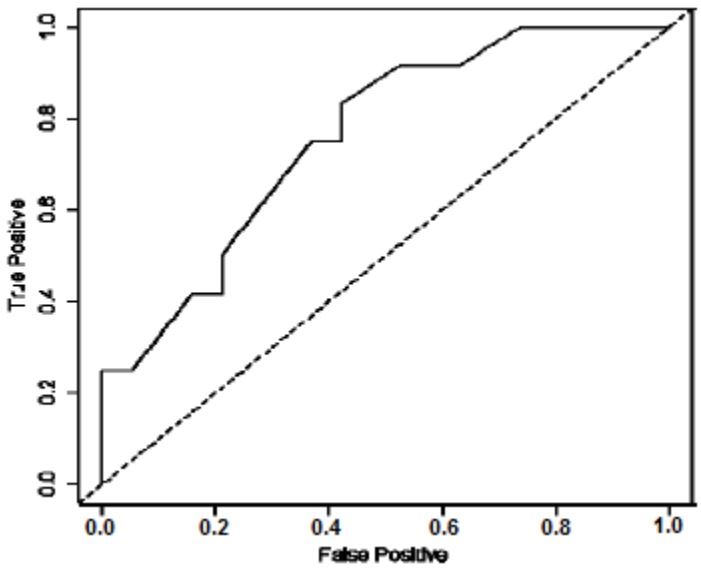

FIGURE 2-10 Receiver operating characteristic (ROC) curve for the OR decision-data fusion for the combination of two notional security systems (solid line). The dashed line represents chance performance.

Parametric-Data Fusion of Security Systems

As Figure 2-4 shows, each security system produces a response and a detection decision. It is important to note that parametric-data security system fusion combines responses from each security system rather than combining their detection decisions as would data fusion based on AND or OR logic. The parametric-data fusion process is illustrated in Figure 2-11. The input object is processed in some sequence by both security systems, but their response values are combined in a joint estimate of the probability of detection (correct classification).

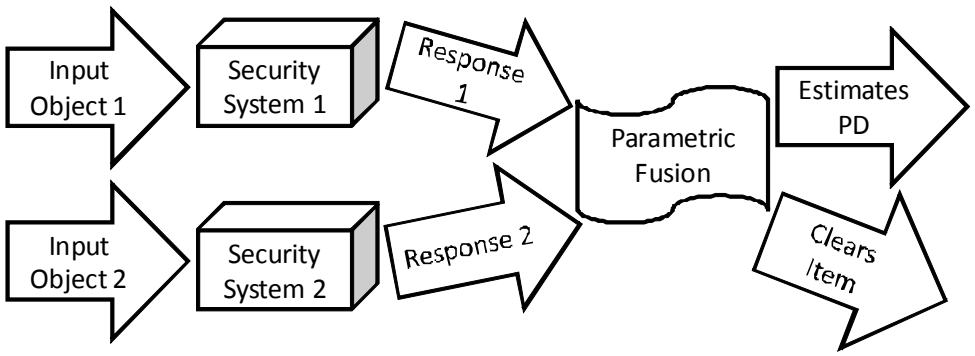

FIGURE 2-11 Parametric-data fusion response values from two notional security systems. NOTE: PD, probability of detection.

As shown in the ROC curves in Figure 2-12, parametric-data fusion provides better results than the other models in trading off true positives versus false positives in the ROC curves. Figure 2-12 shows that the fusion of the two security systems for the

example data results in false positive rates of less than 0.2 and true positive rates of better than 0.8. By comparison, neither the AND combination logic (Figure 2-8) nor the OR combination logic (Figure 2-10) could achieve a 0.8 true positive rate without accepting something more than 0.2 in the rate for false positives. In general, parametric-data fusion produces better results than decision-data fusion over a large range of values.

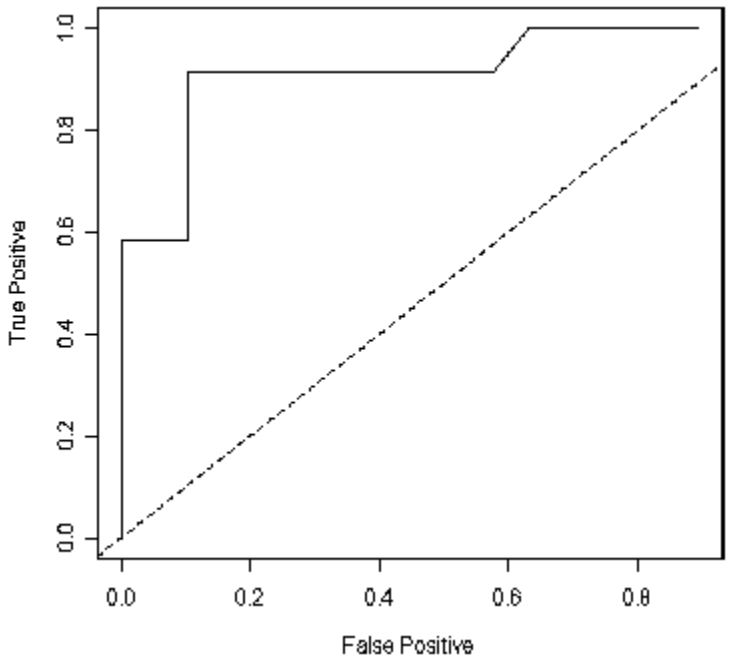

FIGURE 2-12 Receiver operating characteristic (ROC) curve for the parametric-data fusion for the combination of two notional security systems (solid line). The dashed line represents chance performance.

The results of all the different fusion alternatives for this example are summarized in Figure 2-13, which shows all ROC curves on a single plot, and in Table 2-1. In the committee's example, data fusion itself improves the performance of single security systems. However, the extent of the improvement depends on the *type of fusion* employed. Here, the AND logic for decision-data fusion provides more significant improvement than the OR logic does. OR decision-data fusion actually does worse over large portions of the error surface than does Security System 2 by itself. Parametric-data fusion provides the best performance over significant, but not all, regions of the error surface. When compared with AND decision-data fusion, parametric-data fusion provides improvements in the probability of detection, with only slight degradation in false positives.

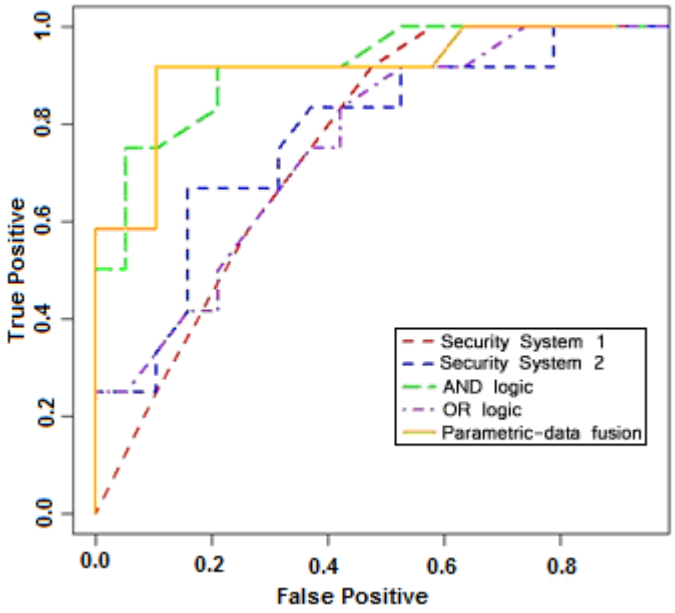

FIGURE 2-13 Receiver operating characteristic (ROC) curves for different modes of operation: individual security systems without fusion, systems' decision outputs combined with AND and OR logic, and systems' responses combined with parametric-data fusion.

These data are also shown in Table 2-1. Column 2 of this table shows the probability of detection of each mode of operation at a fixed FAR of 0.20. Column 3 shows the minimal FAR achieved when the probability of detection is set to the values shown in column 2. Thus, it can be seen that parametric-data fusion provides a 10 percent improvement in the probability of detection over AND decision-data fusion when the FAR is set to 0.20. For these systems, the OR decision-data fusion approach makes things worse by reducing the probability of detection at the FAR of 0.20.

TABLE 2-1 Summary of Fusion Results for Different Modes of Operation for the Two Example Security Systems

Mode of Operation	PD (FAR = 0.20)	Minimum Observed FAR
Security System 1 alone	0.45	0.20
Security System 2 alone	0.67	0.16
AND logic decision-data fusion	0.83	0.20
OR logic decision-data fusion	0.42	0.16
Parametric-data fusion	0.92	0.11

NOTE: PD, probability of detection; FAR, false-alarm rate.

The foregoing is just a simple example of how fusion may be used, and these results apply to the notional security systems used for this data set. Increasing the complexity and changing the performance of the security systems would change the resulting ROC curves. In particular, the AND decision-data fusion approach does not always dominate the OR decision-data fusion approach. Nor is parametric-data fusion always dominant over most of the error surface.

Figures 2-14 and 2-15 show ROC curves for the same two notional security systems but with random permutations (e.g., Gaussian noise) added to their measurements. Notice that in Figure 2-15, the OR decision-data fusion approach dominates the AND. These results indicate that before implementing a fusion approach, the outputs from the security systems need to be analyzed to ensure that the most appropriate fusion approach is adopted.

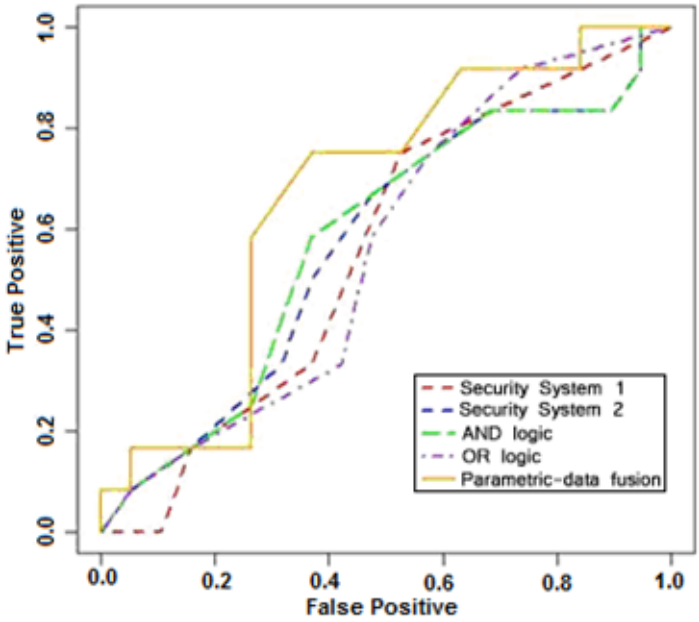

FIGURE 2-14 Receiver operating characteristic (ROC) curves for random permutations of security system measurements in different modes of operation: individual security systems without fusion, systems' decision outputs combined with AND and OR logic, and systems' responses combined with parametric-data fusion.

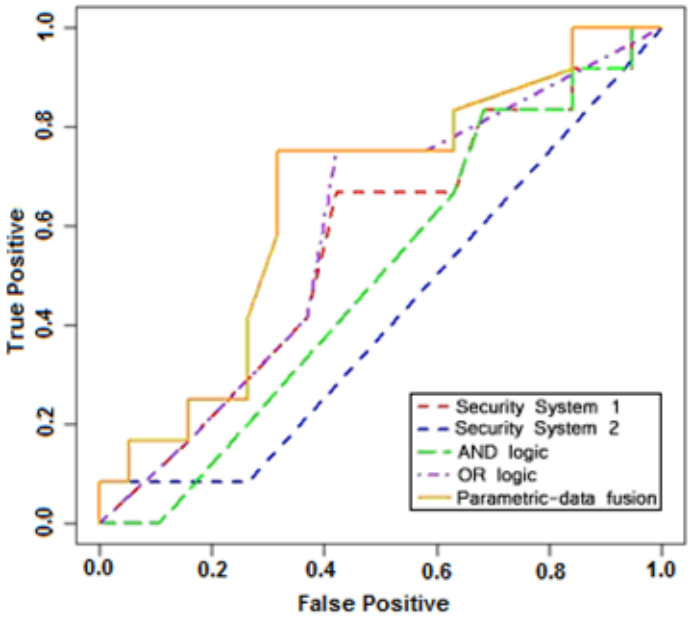

FIGURE 2-15 Receiver operating characteristic (ROC) curves for random permutations of security system measurements in different modes of operation: individual security systems without fusion, systems' decision outputs combined with AND and OR logic, and systems' responses combined with parametric-data fusion.

There are also cost considerations that must be addressed in the implementation of a security system data fusion solution. In particular, the increased requirements for data preparation with parametric-data fusion approaches are minimized with decision-data fusion. In addition, software maintenance and hence life-cycle costs are lower for decision-data fusion than for parametric-data fusion.

Finding: Decision-data (versus parametric-data) fusion does *not* necessarily allow for the greatest improvements in throughput, reduction of false alarms, or improvements in probability of detection. Most TSA data fusion efforts in current programs employ decision-data fusion.

Recommendation 1: Before implementing a data fusion approach for a specific set of security systems, the TSA should perform a formal analysis to select the specific data fusion approach that would increase the detection rate, or that would raise throughput and/or reduce false alarms while maintaining the existing detection rate.

3

Current Data Fusion Endeavors

This chapter first provides illustrative examples of the successful use of data fusion by the Department of Defense (DOD) and private industry that may be analogous to the use of data fusion for transportation security. It then summarizes current data integration and data fusion projects initiated in this area by the Transportation Security Laboratory (TSL) of the Science and Technology Directorate of the Department of Homeland Security (DHS S&T). By examining the successes and failures of the DOD and others and building on the current research, the Transportation Security

Administration (TSA) has a strong foundation for expanding its use of data fusion by employing a more focused, systems engineering approach.

DEPARTMENT OF DEFENSE INITIATIVES

Within the DOD, data fusion endeavors have concentrated on the development of tracking algorithms based on multiple input sources and on the development of automatic target recognition (ATR). For example, Beugnon and colleagues[1] used a two-security-system fusion model and developed adaptive algorithms for the prediction of vehicle tracking in the presence of security system noise. In the field of ATR, the DOD research, development, testing, and evaluation (RDT&E) budget justification explains that "ATR systems improve the capabilities of our armed forces by enabling them to make better use of the information provided by such military sensor systems as radar, laser, infrared, hyperspectral, identification friend or foe, and electronic signal measurement."[2]

As the DOD moves toward greater use of data fusion, reports of specific applications have begun to appear in the technical press, although typically these reports lack quantitative data. Over a decade ago, *Aviation Week and Space Technology* reported the use of a synthesized picture of a battlefield in a laboratory simulation of Joint Surveillance and Target Attack Radar System (JSTARS) and Airborne Warning and Control System (AWACS) operations, using software developed by Mitre Corporation.[3] That report indicated that time-integrated displays were "very powerful in terms of showing the operator what is going on." Even earlier, the U.S. Navy had deployed data fusion systems on the Aegis cruiser that linked the SPY-1 radar system with all radars on ships within a battle group. This data fusion provides commanders with early warning and target tracking capabilities to detect, identify, and engage both surface and air targets effectively. Similarly, *Aviation Week and Space Technology* described the use of data fusion in network-centric warfare using the Network Centric Collaborative Technology (NCCT) project. The aim of this project was to obtain large improvements in data quality at the cost of only 10 to 25 percent of the cost of a major sensor upgrade. This article quotes information from the NCCT project as follows:

> One of the system's features is a "goldmine algorithm" that was developed to correlate what might be two or three equivocal or fleeting contacts if taken individually. But cross-references often can offer a solid target location. With conventional, single-location intelligence systems, up to 90 percent of contacts go unreported because they are considered unreliable. Moreover, the algorithm cuts false alarms almost to zero.[4]

---

[1] C. Beugnon, T. Singh, J. Llinas, and R.K. Saha. 2000. Adaptive track fusion in a multisensor environment. Pp. 24-31 in Vol. 1, Proceedings of the Third International Conference on Information Fusion, July 10-13.

[2] RDT&E Budget Item Justification Sheet. February 2004. Available at http://www.dod.gov/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/OSD_BA3/L-30603232D8Z_ATR__R-2(co)_R-2a__Feb_2004.pdf. Accessed January 26, 2007.

[3] D. Hughes. 1994. Air Force explores data fusion for Joint STARS. Aviation Week and Space Technology, March 7.

[4] D.A. Fulghum. 2002. It takes a network to beat a network. Aviation Week and Space Technology, November 11:28.

The Limited Operational Capability Europe and the successor program, the All Source Analysis System (ASAS), have provided Army commanders with up-to-date fused awareness of the battle space. Brown and colleagues[5] describe a formal process that was used to evaluate the effectiveness of the ASAS as a fusion system. While this was an early system, the later deployments of the ASAS in both Gulf wars have demonstrated its operational effectiveness.

However, the ASAS can also be used to illustrate the difficulties of a data fusion program. The developers of this system initially struggled with the goal of automatically bringing situational awareness to military commanders from all available intelligence data. This goal proved much too challenging, given the current state of understanding in areas such as estimation theory, machine learning, and statistical decision theory. The ASAS has now been successfully deployed and, as mentioned above, used in two Gulf wars by relaxing the automation requirements to incorporate human-directed and informed processes for data fusion.

The U.S. Navy has a Bayesian data reduction algorithm to help with data flow in a network-centric environment. The algorithm works as a "data fusion engine" and can be an "integral part of network centric warfare."[6]

Another naval example is the Sensor System Improvement Program for the Navy's EP-3 Aries II, developed to give a "fused tactical picture of the battlespace." This had operational testing in September 2004, with more than 16 missions accumulating 128 flight hours, resulting in a "significant improvement in capability over previous versions."[7]

During the past several years, the U.S. Army has been conducting a science and technology program currently entitled Advanced Research Solutions—Fused Intelligence with Speed and Trust (ARES-FIST) to develop advanced technologies providing automated support for responding to commanders' priority intelligence requirements. The ARES-FIST program is illuminating sources of complexity in this problem domain, developing software technologies and prototype applications to advance the state of the art on problem characteristics in data fusion requiring research. It is also developing technologically mature software applications to provide incremental, yet substantial performance gains in areas such as the rapid identification of critical reports and indicators that analysts need to answer priority intelligence requirements and that commanders need to make decisions and take actions (actionable intelligence). The program is also developing software support to intelligently guide the collection of the information most needed to answer critical intelligence requirements.

Military systems have also explicitly considered the human decision maker operating on the output from a data fusion system. To move to higher levels of fusion, it must be possible to provide a realistic estimate of current and future status and even to estimate the intent of an entity (e.g., a vehicle) within the battle space. This capability has

---

[5] D.E. Brown, C.L. Pittard, and A.R. Spillane. 1992. ASSET: A simulation test bed for evaluating data association algorithms, Computers and Operations Research, 19(6):479-493.

[6] F. Donovan. 2004. Navy develops algorithm technology to sort through net centric data flow. Aerospace Daily and Defense Report, June 24.

[7] GlobalSecurity. 2004. Available at http://www.globalsecurity.org/intell/systems/ep-3-ssip.htm. Accessed January 26, 2007.

become known as aided adversarial decision making.[8] How the human can best be interfaced to such fused data systems has been studied empirically.[9]

ATR provides similar capabilities—specifically: "Improved ATR will enable our forces to handle an ever increasing load of sensory information in the complex situations encountered in the military missions of the future. ATR capabilities are becoming essential to the warfighter, as the services pursue 'network-centric' concepts for exploiting sensory imagery and information acquired through large arrays of sensors at all echelons."[10]

There has also been considerable investment in the problem of tracking potentially hostile aircraft. The problem has involved fusing data from multiple radars on multiple targets. Details of such work can be found in Bar-Shalom and Li, in Blackman, and in Kameda and colleagues.[11]

A nonmilitary application is described by Rogova and colleagues in their report on the use of data fusion algorithms for improved traffic flow for crisis management.[12] This work assigns network states based on multisource data as a demonstration of decision-level fusion. The network states could range from "normal flow" to "severe congestion" and could be characterized on the basis of the fusion of data from inputs such as the detection of individual vehicles, queues, traffic counts, or traffic types.

The Department of Homeland Security can learn from the experiences of the DOD and U.S. allies that have institutionalized an active, layered defense predicated on sophisticated command-and-control intelligence systems. "To respond quickly to rising threats, the United States requires timely and actionable intelligence. Improved human intelligence collection, improved intelligence integration and fusion, improved analysis of terrorist threats and targets, and improved technical collection against potential chemical, biological, radiological, nuclear, and explosive weapons are all critical in this regard."[13]

This success of these principles is described by Assistant Secretary of Defense Benjamin Riley as follows:

> In Afghanistan, U.S. forces found and hit moving targets in minutes by sharing information. In Iraq, national intelligence moved in minutes to a B-1 Bomber that

---

[8] J. Llinas, C. Drury, W. Bialas, and A.C. Chen. 1998. Studies and Analyses of Vulnerabilities in Aided Adversarial Decision Making. AFRL-HE-WPTR-1998-0099. Dayton, Ohio, Air Force Research Laboratory.

[9] Ann M. Bisantz, James Llinas, Younho Seong, Richard Finger, and Jiun-Yin Jian. 2000. Empirical Investigations of Trust-Related System Vulnerabilities in Aided, Adversarial Decision Making. Report for the Center for Multi-source Information Fusion. Department of Industrial Engineering, State University of New York at Buffalo, Amherst, N.Y. January.

[10] RDT&E Budget Item Justification Sheet. February 2004. Available at http://www.dod.gov/comptroller/defbudget/fy2005/budget_justification/pdfs/rdtande/OSD_BA3/L-30603232D8Z_ATR__R-2(co)_R-2a__Feb_2004.pdf. Accessed January 26, 2007.

[11] Y. Bar-Shalom and X-R. Li. 1995. Multitarget-Multisensor Tracking, Principles and Techniques, YBS Publishing; S.A. Blackman. 1986. Multiple Target Tracking with Radar Applications, Artech House, Norwood, Mass.; H. Kameda, S. Tsujimichi, and Y. Kosuge. 2002. Target tracking using range rate measurements under dense environments, Electronics and Communications in Japan, Part 1, Communications 85(3):19-29.

[12] G.L. Rogova, P.D. Scott, and C. Lollett. 2005. Higher level fusion for post-disaster casualty mitigation operations. Paper presented at 8th International Conference on Information Fusion, July 25-28.

[13] Department of Defense. 2005. Strategy for Homeland Defense and Civil Support, June, p. 11.

> hit the meeting place of senior Iraqis. The military proved adept at developing tactical knowledge in information-constrained operations. Now consider this: most state and local agencies that would initially respond to a terrorist attack in the United States do not have compatible abilities to cull knowledge from the resulting flow of on-scene information.[14]

Overall, the experience of the DOD with data fusion has been one of gradual learning, with successful systems now deployed throughout all of the services. In most cases the initial versions of these systems did not meet expectations or specifications; however, the development, testing, and deployment of these initial attempts informed the later developments of the successful systems. These experiences have motivated the recommendations by this committee for the establishment of a data fusion authority to provide oversight to systems development, for a formal systems engineering approach of the data fusion processes, and for realistic operational testing and feedback from this testing to systems development.

Finding: While the DOD has achieved successes in data fusion, information sharing, and networked operations, it has also had numerous unsuccessful programs in these areas. Those involved in transportation security can learn a lot from both the successes and the failures of the DOD.

Finding: Improvements can be made in security operations by effectively employing data fusion. These improvements can be accomplished with existing technologies. Experience in the DOD indicates the potential effectiveness of and benefits to security operations from applying data fusion.

RESEARCH AND PRIVATE-INDUSTRY INITIATIVES

Private industry uses data fusion to increase production, decrease costs, and minimize the need for operator attention during manufacturing activities. Data fusion can be integrated at many different process steps and in a variety of ways, depending on a company's needs.

An example of data fusion needs in private industry can be drawn from the manufacture of computer chips. This manufacturing activity requires more than 200 individual process steps, each of which must be controlled within a well-characterized range to produce a profitable yield of usable chips.

For many years, the data from each individual step—for example, regarding film thickness and line width—were monitored individually, even though it was well understood that interaction between the individual steps could compensate for errors in processing. Using straightforward data integration, wafer lots could be tracked as they moved from the beginning of the manufacturing line to final testing. Recently,

[14] Benjamin Riley, Assistant Secretary of Defense. 2003. Information Sharing in Homeland Security and Homeland Defense: How the Department of Defense Is Helping. Department of Defense, Washington, D.C. September, p. 1.

manufacturers have moved toward fusing the data from individual steps and using mathematical models to predict the final yield. Instead of a "pass/fail" for a process step, the actual measurement value is recorded, and the target "window" for each subsequent step is adjusted to maximize the final yield.

As the ability to fuse data improves with the increased networking of tools in the manufacturing facility, industry is moving away from measuring a physical dimension on a processed wafer; it is moving toward monitoring voltages and impedances on the processing tool during the actual wafer processing, using the same mathematical modeling approach to predict the final yield. In addition to saving measurement and operator time, understanding which process steps have the largest impact on reducing yield allows the manufacturer to focus resources on improving those critical process steps.

This increasing amount of data fusion and the move to monitoring more fundamental parameters are possible because semiconductor manufacturers agreed on interface protocols and made the providing of these interfaces a requirement to the sale of manufacturing equipment. No equipment vendor could survive without being able to support all of the common equipment interface protocols. This "system-level" view by the manufacturers has led to the ability to control a complex manufacturing facility centrally, focusing resources on the biggest yield detractors and decreasing the number of operators required to run a semiconductor manufacturing facility.

Research conducted at the Center for Embedded Network Sensing of the University of California at Los Angeles has focused on the development of shared databases that allow multiple users and systems to share, manage, and search continuous data streams.[15] While there is no formal decision-making process based on these combined data, the data can inform other commercial, industrial, and security efforts.

Finding: Private industry has employed data fusion to enhance quality and to improve production and has developed data fusion infrastructure, including interface specifications and data structure, to allow the collection and analysis of information.

TRANSPORTATION SECURITY INITIATIVES

The TSL has been involved in a number of projects that might inform the design, implementation, and use of data fusion for transportation security. Table 3-1 summarizes these projects and categorizes them by type: infrastructure for data fusion, data integration, or data fusion. Infrastructure projects look at communications, data modeling, database resources, and techniques for data fusion and data integration. Data integration projects have been focused on centrally locating data from multiple sources. The central location could be the terminal for security personnel or a data store. Finally, data fusion projects have considered the combination of data from multiple sources for threat estimates.

[15] G. Chen, N. Yau, M.H. Hansen, and D. Estrin. 2007. Sharing Sensor Network Data. Available at http://research.cens.ucla.edu/pls/portal/url/item/2B2EEE5C176148E8E0406180528D260E. Accessed March 8, 2007.

Perimeter Surveillance

The Secure Perimeter Awareness Network (SPAN) program combines multiple detection systems designed to provide early warning and alerts for unauthorized access. Essentially, the program takes advantage of the Airport Security Detection Equipment radar to detect unauthorized entry and combines the data from this radar with data from optical and infrared camera security systems. When deployed near facilities close to water, it could also incorporate data from underwater detection systems. The SPAN is to be deployed in Kennedy International Airport in New York City.

A related program, the Seattle Airport Project, has as its objective the fusion of ground surveillance radar and intelligent video into a single track for intrusion detection

TABLE 3-1 Data Fusion Projects of the Transportation Security Administration

Data Fusion Project	Description	Project Type
Command, Control, Communications, Computation, and Intelligence Laboratory	Conduct secure network design, development, implementation, and engineering activities to support an evolving architecture for networking of sensors	Infrastructure for data fusion[a]
EWR/JAXPORT Vehicle Tracking System, Florida	Consists of facility and deployment of a vehicle tracking system in an airport/seaport RF-rich environment to evaluate functional and operational benefits. As of 10/07, this project was suspended due to lack of funding.	Infrastructure for data fusion
Fusion of Sensors and Systems	Evaluate an architecture and design of existing and new commercial-off-the-shelf sensors for perimeter security and stakeholder data distribution. As of 10/07, this project was suspended due to lack of funding but established a test bed being used by Galveston and the Coast Guard.	Infrastructure for data fusion
Cargo Aircraft Motion Detection/Tracking	Demonstrate an integrated motion-detection/camera system on a static aircraft capable of detecting human motion. As of 10/07, the ground portion of this project has been completed. However, the airborne project is ongoing.	Data integration
Smart Container	Adapt Vehicle Access Communicator (VAC) Tracking Unit for use on containers. As of 10/07, this project has been integrated into the EWR/JAXPORT Vehicle Tracking system.	Infrastructure for data fusion
C3 Checkpoint Podium—PHX	Integrate cameras, TRXs, WMDs, ETDs to local C3 Command Center at checkpoint	Data integration
C3 Checkpoint Podium/RFID Integration—DIA	Develop same basic capability as PHX—except selectee carry-on RFID. As of 10/07, this project has been merged with the C3 Checkpoint Podium—PHX	Data integration
Cargo Information Action Center	Consists of virtual network to collect/distribute "Columbia/Snake River stakeholders" data	Infrastructure for data fusion
SUB-DAX Fusion	Fuse sensors in subterranean environments (rail, light rail, vehicular traffic, tunnels)	Data fusion
Ship Commerce Integrity	Fusion of software and models into ship routing/rerouting tool	Data fusion

NOTE: EWR/JAXPORT, early warning radar/Jacksonville Port Authority, Florida; RF, radio frequency; RFID, Radio Frequency Identification; C3, Command, Control, and Communication; PHX, Phoenix Sky Harbor International Airport, Arizona; TRX, transaction; WMD, weapon of mass destruction; ETD, explosive trace detection; DIA, Denver International Airport, Colorado, SUB-DAX, Subterranean and DAX Technology.

[a] Design provides the basic infrastructure to support future decision and parametric-data fusion.

and identification. An older TSL project, Fusion of Security Systems, employs existing radar technology to provide perimeter defense. The Seattle Airport Project intends to fuse the radar data with data from video systems.

The TSL has also developed projects to explore other security approaches for the airport perimeter and aircraft on the ground. The early warning radar/Jacksonville Port Authority Vehicle Tracking System program in Florida will fuse Global Positioning System and radio-frequency identification data to track vehicles for perimeter defense.

The Cargo Aircraft Motion Detection/Tracking program is designed to demonstrate an integrated motion-detection/camera system on a static aircraft. The motion detection will direct slewing of camera systems. These projects demonstrate an interest in the use of data fusion to improve perimeter security. Again, they lack a systems approach to their development and common data structures for the extant security systems that would provide the foundation for significant improvements through data fusion.

Access-Control Systems

An example of a TSL initiative to improve airport access control through data fusion is the Airport Access Control Pilot Program. It is designed to provide access control at intended entry points by integrating data from biometric systems with data from the legacy access-control systems. The goal of this fusion approach is to stop intruders and to provide adequate access control at doorways.

The TSA has funded another fusion demonstration project in the access-control area: US Access. This registered-traveler program was created to enable frequent travelers between Dulles International Airport in the Washington, D.C., area and Heathrow Airport in London to go quickly through airport security and immigration control. It will use two fingerprints in an OR logic and fuse them with face recognition in an AND logic. However, the TSL will be allowed to postprocess the data with more advanced fusion logic. In addition, the National Biometrics Security Project will provide data on 10 fingerprints, 9 facial poses, and both irises for 10,000 people. The combination of data obtained through normal business practices plus the additional data should allow for experiments with fusion as a means to enable improved access control; the project has the potential to reduce the burdens of transportation security.

Need for a Comprehensive Strategy

While the projects described in Table 3-1 provide useful information and results in particular locations, the committee has seen no obvious attempt to develop a comprehensive strategy for the use of data fusion to improve transportation security. Each project is essentially a stand-alone attempt to build localized infrastructure or to share information. There has been no obvious attempt to plan or implement these projects to achieve the most effective use of data fusion at all levels.

Finding: The TSL of the DHS S&T has identified the need for applying data fusion and has addressed this need by implementing a number of projects at the system and

checkpoint levels. However, these projects are not the output of a systems engineering analysis (which would involve formal requirements analysis and derivation) of data fusion at all levels: baggage screening, checkpoint, and access control and surveillance.

Chapter 4 discusses ways to better implement the projects and other opportunities for data fusion.

4

Opportunities for Data Fusion

With an understanding of the potential capabilities provided by data fusion, it is now possible to describe the opportunities for data fusion within transportation security. Of particular interest are approaches that yield the most improvements quickly and inexpensively.

The Department of Defense (DOD) is experienced in networked operations. All local, state, and federal responders need to be on the same level of situational awareness. Situational awareness improves efficiency by determining where and when to apply critical resources. Information sharing has application at both the local level and the

national level. At the local level (taking an airport as an example), information sharing between local police, safety, and transportation security authorities might provide a more comprehensive view of the expanse of a threat, combining actions as they are occurring in varying regions of the airport. The ability to fuse the "combined" local data at the national level may reveal patterns of threats not otherwise seen when the events are viewed only in isolation. Multiple events planned in combination serve to confuse and paralyze those reacting to an attack.

For the Transportation Security Administration (TSA) to move from the recognition of data fusion as a key technology for transportation security to having an effective plan for implementing data fusion solutions requires a systems approach. This approach would provide the programmatic basis for integrating security systems for checkpoints, checked-baggage screening, and access control. Key outputs from this systems approach that will enable the successful implementation of data fusion are the following:

1. A set of data standards (e.g., Extensible Markup Language [XML]) for the integration of data from security systems and security personnel;
2. A path for the growth and migration of passenger pre-screening as an input to data fusion;
3. Reference frames for exchanging locational data at all levels from within bags to within airports;
4. Standards for the identification of explosives, hazardous materials, and items that appear as hazardous but are not;
5. Common measures of uncertainty for all data inputs and validated error rates from security systems;
6. Data structures for radio-frequency (RF) tagging and other object identification and marking;
7. Ontologies for potential threat objects, systems, subsystems, and scenarios in baggage screening, checkpoints, and airports that enable the linking of alerts, observations, and historical data and provide for dynamic threat assessment;
8. Data structures for airport and airport perimeter kinematics with a particular focus on trajectories;
9. Visualization methods that enable distributed situational awareness and assessment;
10. Standardized data structures for access control, including biometrics; and
11. Standardized data interfaces for access control with facility security.

Every year many hundreds of research papers that explore new developments and approaches in data fusion are published. While most of these do not directly address issues in transportation security, it is important for the TSA to be aware of these research results. Where appropriate, it may be possible to apply these research results to fuse data in transportation security settings.

Recommendation 2: The TSA should establish a means to ensure that the following tasks and functions are carried out:

- Creation of a set of system-level data fusion requirements for the checked-baggage screening, checkpoint, and access-control systems;
- Performance of a systems engineering analysis of these areas;
- Validation of these requirements against threat projections, current and projected security systems, and facility idiosyncrasies; and
- The monitoring of fundamental research in the field and adjustment of requirements where appropriate.

Data fusion offers the potential for improvements in baggage screening, checkpoint operations, and access control. In baggage screening, data fusion provides a cost-effective approach to using existing technologies to reduce false alarms (false positives) while maintaining or possibly improving the probabilities of detection. Data fusion for checkpoint operations can also improve the detection of suspicious activities and objects while not increasing waiting or processing times. For airport access control, data fusion can provide an effective approach for integrating biometrics to allow entry only to authorized personnel. It also offers a promising method for effectively employing existing sensors, such as radar and video surveillance cameras, to protect the perimeters of airports. All of these processes are described in greater detail in the sections that follow.

Experimental work done at the Phoenix Sky Harbor International Airport in Arizona illustrates how data fusion can impact security screening. At this airport, magnetometers, computed tomography (CT) scans, trace-explosives detection, and video surveillance were linked; their outputs were viewable at a central security station. At the time of the committee's visit, this design was implemented for one set of security checkpoints in one terminal. Rather than simply displaying the data from these devices, their results could be routed through a data fusion system. In doing so, an alert from a magnetometer could be fused with data from a CT scan to provide a more rapid assessment of the potential threat. These data could also be combined with human assessments of passengers provided by the screeners. The fusion of these assessments with the results obtained from the inspection devices could increase the detection probabilities and/or reduce false alarms.

OPPORTUNITIES IN BAGGAGE SCREENING

Data fusion may have a direct positive impact in baggage screening through the combination of results from different screening systems. Each system is designed to identify explosive materials. Candidates for fusion include x-rays, pulsed fast neutron analysis (PFNA), and nuclear quadrupole resonance (NQR) (see Figure 4-1 for their locations on the electromagnetic spectrum). X-ray interactions with matter at the energies used for the detection of explosives (50 to 1,000 kiloelectronvolts [keV]) occur by photoelectric absorption and scatter.

Sources of Data

X-ray diffraction technologies with energies in the 30 keV to 80 keV range have the interactions with matter that are mainly diffraction plus photoelectric absorption. Diffraction measures the atomic lattice spacing of crystalline materials or the local arrangement of atoms in a chemical compound that can be used as a specific measure of a range of compounds. Neutron interactions with matter include inelastic scattering and generate gamma rays that are related to the elemental makeup of the material. Quadrupole resonance, however, measures the interaction of electromagnetic radiation effects that are related to the local environment of the nuclear spin. Thus, all of these technologies measure radiation or particles, and by their interactions with matter, they are used to infer, to identify, or to specify the actual materials present within luggage.

Advantages

Fusing data from the technologies described above has advantages over using data from just one technology. Some vendors are currently exploring a two-level bag-screening process that involves a high-throughput projection x-ray system that screens all bags and directs any bag with objects matching a broad threat profile to a more sensitive CT-based system. There are other possible combinations; the committee explores some of them in the subsection below, entitled "Notional Model."

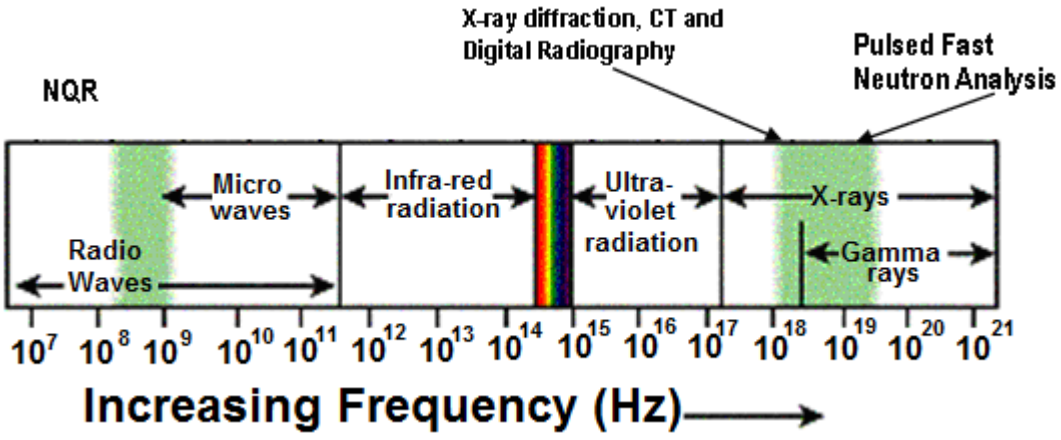

FIGURE 4-1 Notional diagram showing the various radiation and particle interactions with matter that are used for the detection of explosives material. NOTE: NQR, nuclear quadrupole resonance; CT, computerized tomography. For the pulsed fast neutron analysis to which the committee is referring, the gamma rays are detected.

Coupling x-ray CT explosive detection system (EDS) technology with other technologies most likely will provide the biggest reduction in the false-alarm rate in the near term. However, this reduction may come at a substantial penalty in system cost,

throughput rate, and airport footprint. For example, coupling an x-ray CT EDS machine with an alarm resolution system based on NQR[1] and pulsed fast neutron analysis would assist in resolving false alarms, but it would also increase the space needed. A sample baggage-flow diagram for the coupling of these technologies is shown in Figure 4-2.

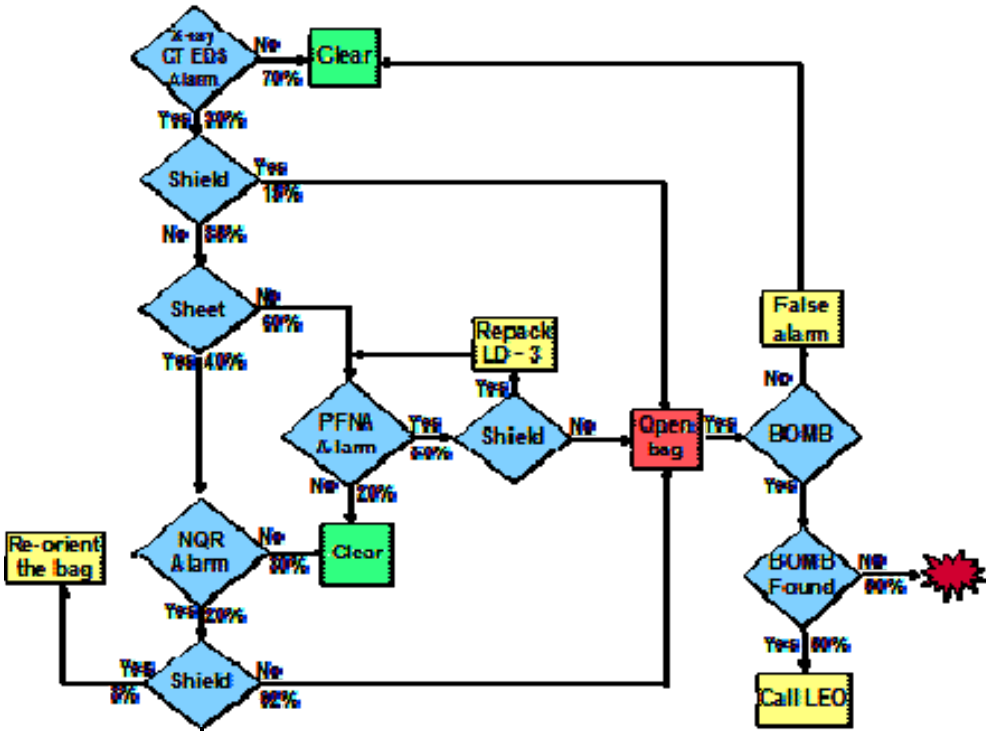

FIGURE 4-2 Notional flow diagram illustrating one way in which an explosive detection system (EDS) could be coupled to two existing alarm-resolving systems, nuclear quadrupole resonance (NQR), and pulsed fast neutron analysis (PFNA). The percentages by the various logic flow paths represent nominal "notional" probabilities that may be encountered in operational scenarios. NOTE: LEO, law enforcement officer; CT, computerized tomography.

Several technologies could be selected to help reduce machine false alarms in the x-ray CT EDSs. In Figure 4-2, the committee has depicted NQR and PFNA, since they both have some good performance parameters validated by testing conducted at the TSL.[2] Other possible data fusion candidates include coherent x-ray scattering (CXRS) and pulsed fast neutron transmission spectroscopy (PFNTS). One issue with CXRS is that there are little to no reported TSA performance data. Good TSA-conducted test data exist for PFNTS, but the current status and/or availability of the PFNTS prototypes is not clear.

[1] This has also been referred to as quadrupole resonance.

[2] T.J. Rayner. 1995. Nuclear Quadrupole Resonance System for Explosive Detection, Phase 1 Final Report, DOT/FAA/CT-FR95, U.S. Department of Transportation, Washington, D.C.; Air Cargo PFNA Test and Status Report. 2001. Ancore Corporation, South Melbourne, Victoria, Australia, January; Curtis Bell and Derry Green. 2001. Pulsed Fast Neutron Analysis (PFNA) October 2000 Test Overview, Presentation to NRC Panel on Assessment of the Practicality of Pulsed Fast Neutron Analysis for Aviation Security, January 29.

Directed trace-explosive detection may not be the best candidate for alarm resolution. Even if one uses directed trace sampling on an alarmed item, there is no quantified metric for the probability that one may miss collecting any explosive contamination on the outside of the item or for the probability that there is a lack of contamination on the outside of the item when an explosive is present inside. In either case, one could conceivably clear the item that contains an improvised explosive device or a bomb. While directed trace-explosive detection is a good technology to raise an alarm, it has significant risks if used to clear an alarm raised earlier in the inspection process. Furthermore, there is evidence that the manual inspection process is not always accurate, and it has had difficulty in identifying an alarmed item within a bag, a prerequisite for a successful directed trace alarm resolution.

Notional Model

In implementing the process depicted in Figure 4-2, every step up to opening the bag can be automated. First, a bag is scanned by one of the x-ray CT explosive detection systems, and it either signals an alarm or does not. Since x-ray CT is the only current technology that meets the EDS detection criterion and has reasonable throughput, it is clearly the only potential technology for first-stage alarm detection at this time. The committee has selected a notional probability of alarms for airport baggage as 30 percent, based on field-test data.[3] Any non-alarmed bag is cleared to go onto the airplane, while an alarmed bag is held for further investigation.

The diagram in Figure 4-2 includes three causes for alarm—shield alarms, sheet alarms, and bulk explosive alarms. Each is treated separately. For shield alarms, the only solution at this time is to open the bag. This is because one cannot clearly preclude the potential of a sheet explosive, and an x-ray shield alarm will result in a shield alarm for many potential sheet alarm technologies (NQR or CXRS).

For sheet alarms, NQR is a likely candidate alarm-resolution technology for further inspection—it has a high probability of detection for the explosive materials present in explosive sheet materials and a low probability of false alarm. If subsequent scanning by NQR produces a shield alarm, it has been shown that a simple reorientation of the bag within the system may eliminate the shield alarm. If this is not the case, the bag must be opened.

Bulk explosive alarms could be resolved using the PFNA technology. Since PFNA was initially developed for the detection of explosives in cargo containers, it can inspect several bags at a time. The scenario shown in Figure 4-2 assumes that the bulk explosive CT EDS alarms are packed into an LD-3[4] container for inspection by PFNA. If PFNA results in a shield alarm or "opaque volume," the LD-3 should be repacked in a less dense configuration and rescanned.

In this scenario, all unresolved alarmed bags must eventually be opened. Opening a bag and finding the alarmed item, whether a real bomb or not, has been found to be surprisingly difficult. For example, when an image of a potential threat (the alarm) is

[3] EDS Reporter: A Monthly Report on a Sample of Explosive Detection Systems. 2002. Security Technology Deployment Office, Washington, D.C., August.

[4] The LD-3 is the most common type of unit load device for transporting cargo by air; it measures 79"W × 60.4"D × 64"H.

shown on the EDS screen, the ability of the screener to follow through and actually find that same threat and remove it is low.

Individual protocols may vary depending on the needs and resources of each airport. In the protocol established by the committee, however, once a bag gets to the "open bag" stage, it is wise to have a law enforcement officer present. Furthermore, opening a bag would be hazardous if a bomb inside the bag has been set to detonate when the bag is opened. A fusion system that reduced false alarms would ensure that the person opening the bag would have a higher proportion of bags to search that did contain true threats, as increasing the probability that an item contains a true signal will likely increase the probability that an operator will detect that signal.

OPPORTUNITIES FOR PRE-SCREENING OF PASSENGERS

The integration of the many public and federal agency databases into the passenger security screening system is critical in inhibiting the terrorist from entry onto the aircraft. This "pre-screening" of passengers allows the remaining security system components to focus the necessary resources downstream in the screening process. For instance, if the passenger pre-screening system were capable of assigning a threat "score" to an individual at the point of initial screening, the system could, at that point, deny further airport access (high score) or recommend further screening (elevated score) with a variety of screening methods next in the process.

Sources of Data

Many attempts have been made to pre-screen passengers on the basis of criteria other than random selection. These various schemes have had limited success owing, for example, to concerns over the privacy rights of the passengers. The lack of depth in the passenger pre-screening system, however, can put tremendous strain on the remaining components of the security system. At these junctures, the system still depends on the "human in the loop" to discover a threat, although few TSA efforts have been made to link observed behavior patterns through the entry of such behavior patterns into a centralized database.

Also of note is the use of so-called psychological screening of passengers through simple questioning by police, ticket agents, security agents, and others, as practiced by El Al Israel Airlines. At least one company is already offering the technology necessary to fuse check-in data to EDS sensitivity,[5] and the Israeli government is said to have used it and collected data on its performance. The TSL has identified this approach as a promising one in its strategic plan.

At least two of the computed tomography systems (GE/InVision and L3) in place today can be commanded in real time to dynamically increase or decrease the sensitivity of the scan. By encoding the results of the Secure Flight passenger pre-screening (see below) onto checked-baggage tags, the bags of passengers with high threat scores could

[5] See Y. Margalit. 2007. Fusion Frenzy. Available at http://www.secprodonline.com/articles/41853/. Accessed March 8, 2007.

automatically be subjected to a higher sensitivity screening, while those with low scores could go through a streamlined process. Since the number of passengers selected for additional screening is expected to be low, the increased false-alarm rate associated with this higher sensitivity should not be a great hindrance to system throughput.

Alternatively, several approaches have been attempted in order to identify passengers who are unlikely to present a threat to the aircraft. Two recent examples of which the committee is aware are the Registered Traveler program and Secure Flight. Registered Traveler allows a limited set of frequent fliers to provide specific data to the TSA. Secure Flight employs information already extant in the air carriers' databases to rapidly identify passengers who are unlikely to present a threat.

Privacy Issues

While senior officials in the Department of Homeland Security and the TSA remain committed to the concept of using existing database information to pre-screen passengers, political considerations and operational issues have stymied even operational testing, much less implementation of expanded passenger pre-screening. The TSA does hope to test the consolidated TSA-operated "watch list" portion of the successor to the computer-assisted passenger pre-screening system, Secure Flight, this year.

The "right to privacy" was not recognized in U.S. courts until 1890, following an article in the *Harvard Law Review* by Samuel D. Warren and Louis Brandeis that reviewed previous tort claims based on the public disclosure of private facts.[6] New York State enacted a statute[7] that codified this implied right. A separate aspect of this general right to privacy is the intrusion on seclusion or solitude through such means as wiretapping or high-powered binoculars. However, in all cases, it has been recognized that an individual's expectation of privacy must be reasonable and that the right can be surrendered. In the realm of airline security, most legal scholars regard an individual's choice to fly as tacit consent to the screening procedures used, provided that adequate notice of the screening is provided.

Any individual airport security system collects and analyzes data about passengers (baggage screening, behavioral observations, passengers passing through metal detectors, and so on), which may present a trivial invasion of privacy. However, the aggregation of these data within a single system may provide more detail than most passengers would be comfortable with and may raise questions about the trade-off between personal freedoms and security.

In *Whalen v. Roe* (1977), the Supreme Court addresses this issue as follows:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our armed forces and the enforcement of criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and

[6] John Wade, Victor Schwartz, Kathryn Kelly, and David F. Partlett. 1994. Prosser Wade and Schwartz's Cases and Materials on Torts (9th ed.). Foundation Press, Westbury, New York.

[7] New York Civil Rights Law, §§ 50-51.

> potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions. We simply hold that this [electronic] record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment. [8]

These issues have been raised in previous reports of the National Research Council—most notably, *Airline Passenger Security Screening: New Technologies and Implementation Issues*, which noted: "Limitations on the [deployment of new] technology will . . . be imposed as a result of passenger intolerance for invasion of privacy, delays, or discomfort."[9]

OPPORTUNITIES IN CHECKPOINT SCREENING

Checkpoints at the majority of airports today consist of stand-alone systems that have no reporting capability, either among other systems in the airport or to higher levels. Thus, there is no capability to combine or fuse the data obtained through checkpoint screening to gain the advantages of orthogonal measurements or warnings in determining whether security concern exists. Generally, the screening done at airport checkpoints occurs in two ways: through the screening of people and the screening of carry-on objects.

Sources of Data

Technologies currently being tested and piloted for deployment into the checkpoint environment have greater detection capabilities than those of earlier technologies. However, even these newer technologies are independent systems that neither interact with one another nor report to higher levels for data analysis.

Making any connection of alarms or threats between items in carry-on baggage or items on the person is done by the human operator and requires the operator to independently match the person and the hand-carried object.

Screening of Carry-on Objects and Passengers (Technology Deployed Today)

The following technologies are those used to screen carry-on baggage in U.S. airports today:

---

[8] *Whalen v. Roe,* 429 U.S. 589 (1977).

[9] National Research Council. 1996. Airline Passenger Security Screening: New Technologies and Implementation Issues. National Academy Press, Washington, D.C.

- *X-ray:* X-ray radiography systems continue to be the primary method for detecting objects of concern in carry-on baggage. These systems provide the operator with a projected image of the bag and of objects inside, which he or she must independently interpret. With the exception of CXRS, there is no elemental analysis for explosives. Shielding (metal blocking the view of items behind the shields) can be an issue. X-ray radiography systems as currently deployed are most useful for the detection of weapons.
- *Trace-explosives detection:* Ion mobility spectrum systems are used for trace-explosive detection either randomly or if the x-ray examination has led checkpoint personnel to question an item that might be inside a carry-on bag. Trace detection is typically accomplished by collecting a sample from the surface of the carry-on bag and placing the sample in a trace-detection machine that analyzes the sample for any explosive residue. These systems are good for identifying most explosives.
- *Visual inspection:* Operators visually inspect bags and search them for potential threat objects.

The following technology is used to screen passengers boarding planes in U.S. airports today:

- *Metal detectors:* The primary screening of passengers is accomplished by requiring the passenger to walk through a metal detector. The variable-sensitivity system provides an audible alarm and visible red light if metal objects are detected. If a portal's metal detector signals an alarm, the person is normally taken to an adjoining area for further screening with a handheld metal-detection wand.

None of the preceding carry-on baggage or passenger screening systems are linked in any way. Further, information regarding the results of the screening is not communicated to a higher level. Alarm responses are discrete events and are not integrated with other security information.

Screening of Carry-on Objects and Passengers (New Technologies)

New technologies, including differing levels of test and pilot programs in the United States, are being introduced into aviation checkpoints around the world. Highlights of the new technologies include the following:

- *CT-based hand-carried systems:* X-ray CT machines traditionally used in the checked-baggage areas at airports have been downsized for use at check-points. These systems provide attenuation-specific analysis, along with the capability by means of imaging, for analysis by security personnel after a machine alarm has occurred. The systems can also be operated remotely, allowing for higher throughput and reduced operating costs. These systems have potential computer capabilities for performing pattern recognition, and they have the capability to communicate with higher-level systems.

- *Advanced technology:* X-ray systems that acquire multiple views, dual energy, and/or x-ray backscatter images.

Among the technologies being tested for screening passengers are the following:

- *Trace portals:* Similar in concept to trace-explosive detection systems, the trace portal system works by having the passenger walk into a portal where air jets blow onto the passenger to try to dislodge any explosive residue. Any residue is then analyzed for chemical specificity. These systems can be operated remotely.
- *Whole-body imaging systems:* Three basic kinds of technologies are used in imaging the human body: active millimeter wave, passive millimeter wave, and backscatter x-ray. All of these systems create some type of image of the person through their clothing to display threat images or information to an operator for analysis. These systems can be operated remotely and also have extensive computer capability for integration.
- *Biometrics:* Biometric systems of all types should be useful in the future, assuming that trusted-traveler programs are approved; in such programs, identity verification is important in determining the amount of screening that the person will receive.

Current Systems

Newer screening systems for airports are designed as system building blocks, providing the potential to integrate security systems. For example, metal detectors are being integrated with an optical imaging system—as with a zone metal detector scanning the area from the knee to the floor and being fused with the whole-body photograph system. Although much more computer-based and capable of communicating large amounts of data, these systems are not being integrated into a system hierarchy but rather are being integrated piecemeal to replace or add capability to existing methods of operation.

Pilot programs, such as the General Electric Checkpoint of the Future at San Francisco International Airport, are being developed in an effort to integrate multiple technologies into a single "checkpoint system."

Other changes that could have profound impact on checkpoint operations are also worth discussion. One is the concept of the privatization of the checkpoint operation, whereby commercial companies would be responsible for equipment selection and information sharing. The second is a rebirth of trusted-traveler programs, with private companies providing memberships to people who agree to various levels of pre-screening, including background checks and biometrics or other types of recognition programs. While these "trusted" travelers have the potential to be threats, the likelihood is reduced, and such programs are currently the only method of verifying people in these areas.

Private companies are moving rapidly to prepare these new technologies for deployment to checkpoints, but there appears to be little guidance regarding what will be approved for operations, who will regulate them, or how they will be regulated.

OPPORTUNITIES FOR FUSION OF AIRPORT PERIMETER SURVEILLANCE SYSTEMS

Airport security includes perimeter surveillance systems designed to detect intruders at a distance, such as ground surveillance radars. It also includes access-control systems designed to prevent unauthorized entry into buildings (see the following section). All of these aspects of airport security may benefit from data fusion. Data fusion for perimeter surveillance would combine the multiple detection systems designed to provide early warning and alerts regarding unauthorized access.

OPPORTUNITIES FOR FUSION OF AIRPORT ACCESS-CONTROL SYSTEMS

As with other technologies, access control might also be improved with the deployment of data fusion of multiple biometric devices. The airport security application of biometrics for access control requires a level of technical performance that is difficult to obtain with a single biometric device. Much research has been conducted over the past two decades regarding the uniqueness of body features, and as a result, the methods of employing biometric algorithms have matured. The use of multiple biometric measurements from independent biometric sensors typically improves technical performance and reduces risk—including an improved level of performance where not all biometric measurements are available, so that decisions can be made from any number of biometric measurements within an overall policy on accept/reject thresholds.[10]

Sources of Data

From a theoretical point of view, biometric processes can be combined to give a guaranteed improvement in performance over that of individual biometric devices. Any number of suitably characterized biometric processes can have their decision scores combined in such a way that the multibiometric combination is guaranteed (on average) to be no worse than the best of the individual biometric devices. The key is to correctly identify the method that will combine these matching scores reliably and maximize the improvement in performance.[11]

Current Systems

The TSA is well aware of efforts to promote the standardization of biometric data fusion. Efforts are under way to publish a technical report from the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) considering all levels of fusion, including the following: decision level (every biometric

[10] International Organization for Standards. 2007. Text of Working Draft Technical Report 24722 on Multi-Modal and Other Multi-Biometric Fusion, ISO/IEC JTC 1/SC 37 N1271, p. v.

[11] International Organization for Standards. 2007. Text of Working Draft Technical Report 24722 on Multi-Modal and Other Multi-Biometric Fusion, ISO/IEC JTC 1/SC 37 N1271, p. 11.

process generates a Boolean result), score level (every biometric process generates either a match score or multiple scores that are fused into a single score), feature level (every biometric process generates features that are then fused into a single set or vector), and sample level (every biometric process results in a collection of samples that are fused into a single sample). The ISO/IEC report also considers multibiometric systems for different scenarios, including verification, positive identification, and negative identification.[12]

If the airport access control biometric data fusion projects planned by the TSA follow the guidelines as outlined in the ISO/IEC biometric fusion technical report, the Transportation Security Laboratory (TSL) would benefit from this formal systems engineering approach and could serve as a good example to other TSA programs.

The committee's review of the opportunities for employing data fusion for current airport operations led to the following finding and recommendation:

Finding: Most of the detection systems now fielded in U.S. airports were built without regard for the need for data fusion or data integration among systems. Many manufacturers are attempting to create systems that not only fuse data, but also link information about passengers and baggage. However, there is little direction from the TSA with respect to the establishment of standards or requirements.

Recommendation 3: The TSA should work (that is, contract) with the leading integrators and manufacturers to form a representative working body and require it to develop initial strategies and standards for the integration of airport security, checkpoints, checked-baggage screening, and access control, including legacy systems.

HUMAN SENSORS

Not all data used in data fusion need to come from instruments. In the DOD applications, data also come from human intelligence and may be fused successfully with instrumentation data. An example of the use of human intelligence is the apprehension of Ahmed Ressam in a car carrying explosives to bomb Los Angeles International Airport for the so-called millennium plot. He was stopped by a border guard at Port Angeles, Washington:

> Upon noticing that he appeared nervous, customs officers inspected him more closely and asked for further identification. Ressam panicked and attempted to flee. Customs officials then found nitroglycerin and four timing devices concealed in a spare tire well of his automobile.[13]

Another example is the methods reportedly used by Israeli security forces and now widely used to train Western law enforcement agencies. These methods attempt to stop terrorists before they can act by targeting "the bomber not the bomb."

---

[12] International Organization for Standards. 2007. Text of Working Draft Technical Report 24722 on Multi-Modal and Other Multi-Biometric Fusion, ISO/IEC JTC 1/SC 37 N1271.

[13] "Ahmed Ressam." Available at http://en.wikipedia.org/wiki/Ahmed_Ressam. Accessed March 12, 2007.

For both of the above approaches there are well-documented reports of success in individual incidents, but sparse data exist on the traditional measures of probability of detection and probability of false alarm. However, a data source such as a human observer can contribute to overall systems effectiveness if the source is (1) better than a chance level of hits and false alarms and (2) correctly fused with other data from independent, preferably orthogonal, sources.

Human observation could be fused with instrument data by, for example, providing a number of observers, even security personnel performing other tasks, with the ability to raise concerns about a passenger by entering a code into the system where it could be processed for fusion. For example, the checkpoint person assisting passengers through the metal detector (or its replacement) might observe unusual behavior (such as holding one's hands over a body part) or abnormal nervousness about the security process. Entering these observed data into a fusion system might not itself trigger an alarm, but it could do so if combined with other subcritical data. The passenger might have been "almost" selected by the Secure Flight system or his or her checked bag might have alarmed but then been cleared. None of these events alone would cause an alarm, but a suitable fusion system would be able to combine the data leading to a fusion alarm without a high penalty in false alarms.

In terms of the allocation of function, humans are much better than automated systems at detecting hard-to-specify but salient events. Computer-based systems without human oversight are better at detecting easy-to-specify events, such as the presence of a substance with a particular density or an atomic number in a particular shape. The advantage of providing human intelligence inputs into a data fusion system is that both humans and instruments play to their respective and complementary strengths so as to allow greater potential for the detection of terrorist events. Adding data input tasks to the existing tasks of security personnel must be done carefully. As with all changes involving human operators, careful task analysis and human-computer interaction design are required to ensure that performance on all tasks, old and new, is achieved at the highest level.

A human-based fusion system would need to consider how to display to the human decision maker the importance of each source of data: a machine-based fusion system would need to parse text input to allow fusion. As with any other input into a data fusion system, human inputs need to meet data registration and data integrity requirements. Chapter 2 defines these further as spatial and temporal registration, plus confidence intervals to indicate data uncertainty. The design of either human or machine-based fusion systems is not simple, but any such fusion system will perform better given valid input from human sensors.

Finding: Data fusion would enhance security system effectiveness if it were to combine inputs from security personnel with data from detection systems into a unified situational awareness system.

Recommendation 4: The TSA should develop formal data-entry mechanisms for security personnel that will enable the combination of human observational data with security system data. These mechanisms should be designed so as to maintain performance on existing tasks.

AIRPORT-WIDE DATA FUSION MODELS

In addition to the fusion of data within each airport security system, data fusion can occur on an airport-wide level, as illustrated in Figure 4-3. In this model of data fusion, each piece of data is fed to the next level of screening in order to ensure that security personnel have the best idea of an individual's or an item's threat potential for the entire time that the individual or item is present at the airport and, in some cases, even prior to arrival on airport grounds.

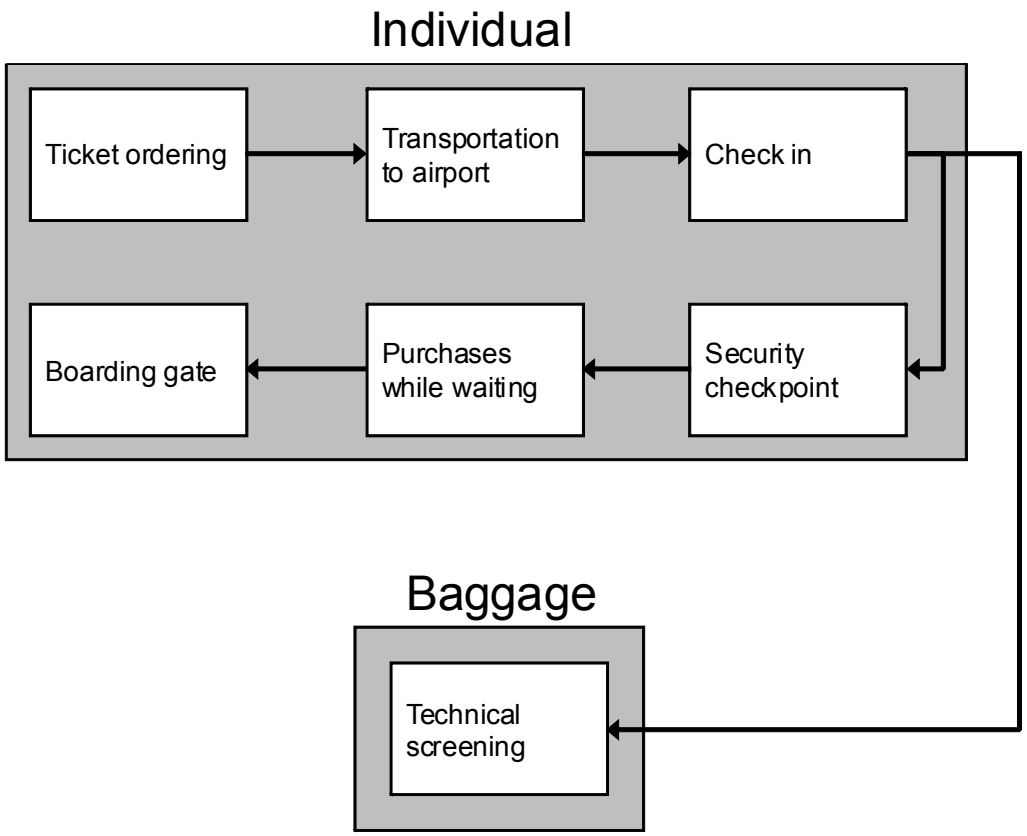

FIGURE 4-3 Data can be fed to later checkpoints to achieve an airport-wide model of data fusion.

IMPLEMENTATION CONSIDERATIONS

As discussed in Chapter 2, poorly implemented data fusion will provide no significant improvements. For example, a simple decision-data fusion system using OR logic actually performed worse than the individual security systems. As discussed in Chapter 3, there are many examples of failed attempts at data fusion. Many of these failures resulted from an attempt to directly export systems from laboratory testing into

field use. To alleviate these problems, the committee recommends the use of a systems engineering approach to implement data fusion projects more effectively.

Finding: The implementation of data fusion based only on laboratory testing is a high-risk strategy. Operational testing conducted as a subset of certification testing is required to ensure data fusion system effectiveness.

In addition to a systems engineering approach to data fusion, the successful use of this technology in transportation security will require a modular approach. An approach to maximizing the probability of success from data fusion implementations is to use a staged deployment strategy. The TSA has not yet been required by Congress to formally establish an operational testing program analogous to that required of the DOD and the military departments. This approach would implement fusion through a series of staged fusion modules. For example, the opportunities in checked-baggage screening could be modularized through the combination of data from an x-ray CT EDS with an alarm-resolution system based on nuclear quadrupole resonance and pulsed fast neutron analysis, discussed in detail earlier in this chapter. This could be implemented through a series of staged deployments in an operational testbed as designated by the TSA and/or at selected airports and tested, calibrated, and improved before broader deployment is attempted. In the same fashion, checkpoint systems fusing trace, magnetometer, video, and human observations could be implemented, tested, calibrated, and improved in single airports before broader deployments.

Recommendation 5: The TSA should implement any data fusion systems through a series of staged deployments at an operational testbed as designated by the TSA and/or at selected airports. The experience from these early staging events can then be incorporated and used in the data fusion systems rolled out in later implementations.

Appendixes

Appendix A

Acronyms

ARES-FIST	Advanced Research Solutions—Fused Intelligence with Speed and Trust
ASAS	All Source Analysis System
ATR	automatic target recognition
ATSA	Aviation and Transportation Security Act
AWACS	Airborne Warning and Control System

CT	computerized tomography
CXRS	coherent x-ray scattering
DOD	Department of Defense
DHS S&T	Department of Homeland Security Science and Technology Directorate
EDS	explosive detection system
ETD	explosive trace detection
EWR/JAXPORT	early warning radar/Jacksonville Port Authority
FAR	false-alarm rate
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
JSTARS	Joint Surveillance and Target Attack Radar System
MMW	millimeter wave
NCCT	Network Centric Collaborative Technology
NQR	nuclear quadrupole resonance
NRC	National Research Council
PD	probability of detection
PETN	pentaerythritol tetranitrate (explosive)
PFNA	pulsed fast neutron analysis
PFNTS	pulsed fast neutron transmission spectroscopy
RDT&E	research, development, testing, and evaluation
RF	radio frequency
ROC	receiver operating characteristic
SPAN	Secure Perimeter Awareness Network
STDO	Security Technology Development Office
THz	Terahertz
TSA	Transportation Security Administration
TSL	Transportation Security Laboratory
XML	Extensible Mark-up Language

Appendix B

Biographies of the Committee Members

James F. O'Bryon, *Chair,* served as deputy assistant secretary of defense until his retirement in 2001. During his 15 years in the Pentagon, he served under seven secretaries of defense, as director, Live Fire Testing, and deputy director, Operational Test and Evaluation. Mr. O'Bryon also worked in various positions within the Office of the Director of Defense Research and Engineering in the Office of the Undersecretary of Defense for Acquisition and Technology, overseeing and directing test and evaluation activities for the secretary of defense. These activities included the examination of the test plan adequacy; test execution; and vulnerability, lethality, and survivability of the

nation's major defense systems and the application of tactics and doctrine to these issues. He has testified before various committees of the U.S. Congress on defense and homeland security issues as well as drafted reports from the secretary of defense on system survivability, vulnerability, and lethality. He has served on more than a dozen committees addressing such issues as directed energy, ozone-depleting compounds, and modeling and simulation. His degrees are from the King's College, George Washington University, and the Massachusetts Institute of Technology. He has also served for nearly 20 years as a mathematician, ballistician, and weapon systems analyst at the Ballistics Research Laboratory and the Army's Materiel Systems Analysis activity. He currently works as an independent defense consultant for several government entities, not-for-profit organizations, and defense industries and serves as president of The O'Bryon Group.

Sandra L. Hyland, *Vice Chair,* is the Etching System group manager, Tokyo Electron (TEL) Technology Center, America, responsible for TEL's etch process development at the Albany Nanotechnology Center at the State University of New York at Albany. She supports oxide and low-k film etch for integrated development projects for TEL and IBM, as well as for other members of the Nanotechnology Center. Dr. Hyland was formerly East Coast manager for TEL Etch Systems, analyzing technology trends and customer data to determine hardware and process needs for manufacturing current and next-generation computer chips, including both capability and cost-reduction considerations. She had previously been an integration engineer for IBM's radiation-hardened computer chip manufacturing facility and managed a processing facility for the Jet Propulsion Laboratory to assess various materials for their potential as solar-cell substrates. Dr. Hyland was also a staff officer for the National Research Council's (NRC's) National Materials Advisory Board, where she managed committees on aviation security and the design of U.S. paper money. She has a Ph.D. in materials science from Cornell University and an M.S. and a B.S. in electrical engineering from Rutgers, the State University of New Jersey, and Rensselaer Polytechnic Institute, respectively.

Cheryl A. Bitner is vice president of programs for Pioneer Unmanned Aerial Vehicles, Inc., a joint venture of AAI Corporation. She has served as program director for electronic warfare trainers, maintenance trainers, gunnery system trainers, and on-board (embedded) trainers at AAI Corporation and as director of AAI quality systems. She has more than 21 years of industry experience in providing training and simulation products for both government and commercial customers, and has a strong background in cost- and schedule-control techniques. Her responsibilities include ensuring positive program performance, strategic planning, and personnel management and development. Ms. Bitner is a certified project management professional, a certified quality manager, a certified software quality engineer, and a member of the National Training and Simulation Association. She has published a cost-and-benefit analysis of piloting and navigational team trainers and contributed to the *AAI Training Systems Newsletter*. Ms. Bitner completed the advanced program management course at the Defense Systems Management College in 1989 and holds an M.S. in engineering science and a B.S. in computer science from Loyola College.

Donald E. Brown is chair of the Department of Systems Engineering of the University of Virginia. His research focuses on data fusion and simulation optimization with applications to intelligence, security, logistics, and transportation. He has developed

decision-support systems for several U.S. intelligence agencies and was previously an intelligence operations officer for the U.S. Army. Dr. Brown is coeditor of *Operations Research and Artificial Intelligence: The Integration of Problem Solving Strategies* and *Intelligent Scheduling Systems* and is an associate editor for the journal *International Abstracts in Operations Research*. He has been president, vice president, and secretary of the Systems, Man, and Cybernetics Society of the Institute of Electrical and Electronics Engineers. He is past chair of the Technical Section on Artificial Intelligence of the Institute for Operations Research and Management Science and was awarded that society's Outstanding Service Award.

Colin G. Drury is a professor of industrial engineering at the State University of New York, Buffalo, and executive director of the Center for Industrial Effectiveness, where he has worked extensively in the integration of ergonomics/human factors into company operations. His efforts have resulted in increased competitiveness and job growth for regional industry and two National Association of Management and Technical Assistance Centers' Project of the Year awards. Since 1990, Dr. Drury has headed a team applying human factors to the inspection and maintenance of civil aircraft, with the goal being error reduction. He performed a study for the Air Transport Association evaluating the Federal Aviation Administration's modular bomb set and the use of this bomb set in training and testing security screeners. Dr. Drury is a fellow of the Human Factors and Ergonomics Society, the Institute of Industrial Engineers, and the Ergonomics Society. In 1981, he was awarded the Bartlett Medal by the Ergonomics Society, and in 1992 the Paul Fitts Award by the Human Factors and Ergonomics Society. He has a Ph.D. in production engineering from Birmingham University, specializing in work design and ergonomics. Dr. Drury served on the NRC Panel on Assessment of Technologies Deployed to Improve Aviation Security.

Patrick Griffin is a senior member of the technical staff at Sandia National Laboratories and was chair of the NRC Panel on Assessment of the Practicality of Pulsed Fast Neutron Analysis for Aviation Security. At Sandia National Laboratories, Dr. Griffin performs research in the areas of radiation modeling and simulation, neutron effects testing, radiation dosimetry, and radiation damage to materials. He is active in the standardization community and is the current chair of the American Society of Testing and Materials Subcommittee E10.05 on Nuclear Radiation Metrology.

Harry E. Martz, Jr., is the director for the Center for Nondestructive Characterization (CNDC) and leader of the measurement technologies focus area at the Lawrence Livermore National Laboratory. Dr. Martz has an extensive background in the use of computed tomography and x-ray radiography (technologies commonly used in explosives detection) to perform nondestructive evaluation. His current projects include the research of nondestructive characterization systems for detecting improvised explosive devices and radiation/nuclear threats as well as nonintrusive characterization techniques as a three-dimensional imaging tool to better understand material properties and perform inspection of components and assemblies, and generation of finite-element models from characterization data. Dr. Martz has served on several NRC committees and panels dealing with the general topic of aviation security. In addition, he chaired the NRC Panel on Technical Regulation of Explosives Detection Systems.

Richard McGee is a retired electronics engineer with 35 years at the Ballistic/Army Research Laboratory (ARL), Aberdeen Proving Ground, Maryland. He is

currently working part time as a senior scientist contractor at ARL. Mr. McGee is an experienced researcher with extensive expertise in millimeter-wave, infrared, radiometry, radar, smart munitions, and sensor-based systems engineering and integration. He possesses solid understanding of the procedures and tasks required to transfer technology from the research laboratory to the field. Mr. McGee has conducted field experiments to characterize near-Earth propagation of millimeter waves (10 mm to 1 mm wavelength) in turbid and tactically hostile environments. He has designed, fabricated, and field-tested smart munitions sensors as well as instrumentation to measure millimeter radiometric and radar signatures of red and blue combat vehicles and various terrains. Other projects in which he has been involved are microwave and millimeter-wave holography and the development of multispectral fusion target recognition algorithms and synthetic aperture radar and inverse synthetic aperture radar high-resolution instrumentation.

Richard L. Rowe is retired chief executive officer of MCMS, Inc., a $550 million electronics contract manufacturing company. His experience includes sensor technologies applied to aviation security, and his expertise includes new technologies in optics and radio frequency, electronic sensors, and switch products. He has more than 20 years of experience in the electronic sensors and switch products industry. Prior to his work in the electronics industry, Mr. Rowe was with the U.S. Army for 6 years. He has a master's degree in engineering administration from The George Washington University, Washington, D.C., and a bachelor's degree in engineering and applied sciences from the U.S. Military Academy, West Point, New York. He has served on the boards of various electronics firms and was awarded the Honeywell Lund Award (a major leadership award) in 1987.

H. Bruce Wallace is president of MMW Concepts LLC, a firm that he established to provide consultative expertise. He retired as a Department of the Army civilian employee most recently acting as deputy and director of the Weapons and Materials Research Directorate of the Army Research Laboratory. Previous to that, he spent 7 years as chief of the radio frequency (RF) and Electronics Division, where he was responsible for the Army's basic and applied research in RF technologies. His primary area of research involved investigation of the application of millimeter-wave techniques to weapons systems. This included studies in electronic components, atmospheric and near-Earth propagation, active and passive system designs, and high-resolution polarimetric imaging. Key outcomes from his work were the development of the Sense and Destroy Armor millimeter-wave system; the Army's High Resolution Radar Imaging facility, which provides state-of-the-art imaging on ground platforms; and the Multifunction Radio Frequency System, which has become a key electronic component in the Army's Future Combat Systems. He is author of more than 60 government and open-literature publications. Mr. Wallace has served on multiple Department of Defense and North Atlantic Treaty Organization panels as chair or Army lead and as lead investigator on several trade studies of Department of Defense radar systems and capabilities. He was a member of two NASA review panels providing technical and managerial review of basic research programs and a member of the independent review team examining the performance of the Phoenix Mars landing radar. He is a fellow of the Institute of Electrical and Electronics Engineers Geosciences and Remote Sensing Society.

Appendix C

Selected Presentations on Data Fusion

The following is a list of speakers who made presentations related to the topic of this fourth report of the Committee on Assessment of Security Technologies for Transportation. Other presentations given at information-gathering meetings of this committee informed its deliberations for earlier reports and are thus not included in this appendix.

October 15-16, 2002

Data Fusion
Donald Brown, University of Virginia

Data Integration
Hans Miller, Computer Assisted Passenger Pre-Screening II

December 12-13, 2002

Quantum/InVision Plan to Integrate Quadrupole Resonance/Computerized Tomography
Tam Rayner, Quantum/InVision

March 20-21, 2003

Data Fusion to Reduce False Alarm Rates
Ron Krauss, Transportation Security Laboratory

False Alarm Reduction
David Schafer, Analogic

December 12-13, 2003

TSA Science and Technology Deployment
Rodger Dickey, TSA

TSA Command, Control, Communications, Computing and Intelligence, Fusion of Sensors and Systems, and Radio Frequency Identification
Anthony Cerino, TSA

TSA Information Systems Enterprise Architecture
Christopher Allen, TSA

October 6-7, 2004

False Alarm Rate Reduction
Matthew Merzbacher, InVision Technologies

Data Fusion
John H. Huey

May 24-25, 2005

TSA Perspective on Data Fusion
Anthony Cerino, TSA

TSA Chief Technical Officer Comments
Clifford Wilke, TSA