Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems

Stanford Study Group[1]
Center for International Security And Cooperation
Stanford University

Abstract

This article grew out of a week-long study in August 2002 to assist ongoing efforts inside and outside the government to remedy some vulnerabilities of the international shipping system on which US and a great deal of world prosperity depend. The study's objective was to identify the most important research initiatives and the major policy issues that need to be addressed in order to improve security of imports using shipping containers, particularly against the importation of nuclear materials and weapons, while maintaining an open trading system. To be effective, a system to detect nuclear weapons or special nuclear material before they reach U.S. ports must be international in scope and reach. It must also be economically acceptable both in terms of total cost and with respect to how these costs are allocated; degrade gracefully when subjected to attack; produce actionable intelligence in a timely manner; treat false alarms realistically; be adaptable to a variety of local physical and political conditions; be auditable, secure yet accessible to the needed foreign and domestic security agencies, and have clear lines of oversight and responsibility. Finally, the system should be flexible enough to allow for regular updates as users and operators gain experience and system performance is reviewed. This study identified a sample technical approach that is feasible technically and operationally and involves components already in the early deployment stage. The approach involves container certification; monitoring at ports of embarkation, debarkation, and continuously during shipment and storage; and continuous data fusion. Specific recommendations regarding system characteristics made by the study include rigorous testing during deployment and in the field, international coordination of standards and protocols, careful analysis of the system for compatibility with pertinent governmental policies and business and labor agreements, and early provision for forward-looking research and development.

I. Introduction

This paper presents the results of a summer study conducted at Stanford University that examined how existing technology and resources can be applied most effectively to prevent the transport, by means of international commercial shipping, of illicit nuclear materials for use in terrorist activities.[2] The focus of this effort was on the detection of nuclear weapons and special nuclear materials (SNM), as well as detecting forms of radioactive material that could be used in other types of terrorist attacks, including radiological dispersal devices ("dirty bombs").[3] Issues associated with the illicit transport and import of chemical and biological weapons agents for use in

[1] Members of the study group were: Sam Chiu, Sid Drell, Bill Dunlop, Steve Flynn, Zack Haldeman, John Harvey, Tom Karzas, Michael Levi, Howard Lowdermilk, Michael May, Rob Nelson, Vic Orphan, Pief Panofsky, Tonya Putnam, Phil Stroud, and Dean Wilkening. Michael May, Tonya Putnam, and Dean Wilkening took responsibility for drafting this article.

[2] During the week of August 18-23, 2002, the Center for International Security And Cooperation (CISAC) of the Institute for International Studies (IIS) at Stanford University hosted a set of four summer studies sponsored by The John D. and Catherine T. MacArthur Foundation. The Container Security Study was one of these studies. It brought together physicists, engineers, and social scientists with experience on issues that included nuclear detection and radiography, port and container security, systems engineering, and international relations.

[3] Special nuclear materials, hereafter referred to as SNM, are the fissile materials essential to make nuclear weapons, plutonium and highly enriched uranium (HEU). Procuring them is generally agreed to constitute the major technical impediment to making nuclear weapons. Aside from a few state-to-state and state-sanctioned and monitored arrangements, there is no licit international trade in SNM or, obviously, nuclear weapons.

terrorist activity, while extremely important and in many ways more difficult to deal with, are not considered here.

The objective of this study was to assist ongoing efforts inside the government and in the private sector to remedy obvious security vulnerabilities in the international maritime shipping system. This system as it exists today has been designed for speed and efficiency—not security. A nuclear terrorist act against a major port would have extremely grave economic, political, and human consequences that would extend far beyond the port or country of attack, and could temporarily paralyze the international trading system.

An effective system for detection of nuclear weapons or SNM before they reach U.S. ports must be international in its scope and reach. Some sharing of information and technology with foreign governments and personnel will be, therefore, unavoidable to ensure needed coordination and cooperation. However, care should be taken to ensure that potential terrorists are not, at the same time, aided in their efforts to introduce illicit nuclear weapons or materials into international trade. With this caution in mind, this report omits detailed discussion of all government functions, equipment or security practices of a sensitive nature.[4]

The system of international maritime shipping handled approximately 230 million twenty-foot equivalent container units (TEU) in 2000, of which 31 million TEU (17 million actual container boxes) came through North American ports.[5] Shipping containers account for 95% of U.S. import-export cargo tonnage. Under normal conditions, the system of international maritime transport depends on the ability to maintain a steady flow of container traffic through the world's major ports. Efforts to achieve a secure system must not threaten the economic viability of the network and, by extension, the system of global trade.

Clearly, preventing the importation of materiel for nuclear terrorism involves activities that go beyond container security. Consequently, container security should be viewed in the context of an overall security architecture for preventing, disrupting, deterring, and protecting against terrorism. A comprehensive analysis of the threats posed by international terrorism requires consideration of both the operational capabilities of the organizations that pose a threat—including attention to recruiting, training, financing, command, control and communications, attack planning, mobility, and weapons acquisition, production, handling, and delivery—as well as our own security weaknesses that can be exploited. Terrorists intent upon smuggling nuclear weapons or materials into the territory of the United States or one of its allies have a number of delivery modes from which to choose. Among them are maritime shipping, airplanes (not just commercial airliners), trucks, trains, buses, private cars, and possibly even cross-border foot traffic. Among the maritime delivery modes are commercial shipping containers, other material taken aboard container vessels (e.g., supplies, equipment, luggage, fuel, etc.), non-containerized freighters, tankers, cruise ships, fishing boats, ferries, and private pleasure boats. Thus, shipping containers are only one means for transporting an assembled nuclear weapon or special nuclear material (SNM) across international borders, albeit an obvious and particularly important one given the economic impact associated with disrupting the international maritime shipping industry.

---

[4] This study was conducted at an unclassified level and drew exclusively upon information available in the public domain. As a rule, the sample technical approach described in this report incorporates commercial equipment and technologies currently available. However, in a few cases the approach recommends equipment that has not yet been developed for use in the commercial sector, but which is within the range of existing technical expertise.

[5] Testimony of Paul F. Richardson, President of Paul F. Richardson Associates, Inc., on behalf of the United States Maritime Alliance, The Pacific Maritime Association, and the National Association of Waterfront Employers before the Subcommittee on Coast Guard and Maritime Transportation, United States House of Representatives, On Funding for Seaport (Intermodal Cargo) Security, Washington, D.C., March 14, 2002; and *Drewry Container Market Quarterly*, Drewry Shipping Consultants, March 2001 as reproduced in http://www.p-and-o.com/results/Presentations/02Overview.pdf.

Unfortunately, the short duration of this study precluded an analysis of the overall security architecture and detailed consideration of these other transport methods.[6] The conclusions and recommendations of this study follow from an informal estimate of how the system of international commercial maritime traffic would figure into a comprehensive risk assessment. However, a comprehensive risk assessment should be conducted both to verify this estimate, and to ensure effective resource allocation of within an overall strategy for US homeland security. The resources in question are not only financial but also include opportunity costs associated with dedicating personnel and diplomatic efforts to enhance the security of maritime shipping, as opposed to other aspects of the international terrorist threat.

For example, a comprehensive risk assessment might conclude that, after allocating resources to fix the most urgent security vulnerabilities, it would be more cost-effective to deal with terrorism by attacking the problem as close to the source as possible. This would imply that a higher priority should be placed on US and foreign intelligence to identify and monitor groups likely to attempt to acquire nuclear weapons and SNM for terrorist purposes, thus allowing states to preempt terrorist operations. Similarly, efforts to reduce and secure existing stockpiles of nuclear weapons and SNM, especially in Russia, and to eliminate illegal trade in dangerous radioactive sources may be a key element in a comprehensive strategy for preventing acts of nuclear terrorism. In this regard, the Nunn-Lugar Cooperative Threat Reduction program would continue to be essential. Domestic and international programs for controlling and securing SNM and radioactive sources, such as those managed by the Nuclear Regulatory Commission (NRC) in the United States, the US Department of Energy, and the International Atomic Energy Agency (IAEA) internationally would also be important.

In addition, a security assessment that attempts to fully account for the costs of enhancing the security of international container traffic in the context of other threats and vulnerabilities should also factor in counter-balancing, non-terrorism-related benefits. For example, criminal activities are common in the realm of international container shipping. Private shippers, insurers, and governments routinely attempt to minimize theft, customs violations, and the flow of illegal narcotics and other contraband. Some of the technologies and equipment recommended here as components in a "systems approach" to detect the transport of illicit nuclear materials have been developed and marketed commercially for these purposes. Shippers and port or terminal operators already are adopting, with or without government support, several elements of a nascent security system.[7] Examples include installations of radiographic imaging and passive radiation detection equipment at Dover and Portsmouth in the United Kingdom, radiographic imaging equipment at ports in Singapore, and installations for scanning cross-border rail and truck traffic on both sides of the U.S. border with Canada and Mexico. Much of this equipment could be integrated into an overall security system to detect illicit international trade in radioactive and special nuclear materials with minimal additional impact on the flow of container traffic.

However, measures adopted voluntarily by commercial operators are, in general, not adequate to the task of ensuring reliable detection of smuggled nuclear weapons and special nuclear materials (SNM). First, a different selection and configuration of sensors would be required to detect nuclear weapons and SNM, as opposed to more common forms of commercial contraband such as drugs. Second, and more important from a systems perspective, the permissible failure rate for

[6] The suggested system for detection of nuclear materials in shipping containers could be adapted with some effort to international commercial truck, rail, airplane, and other maritime transport modes. Clearly, each of these modes has features that differ in potentially important ways from maritime shipping, but the group did not have time to investigate those differences in any detail.

[7] To date these investments have been made mainly for the purpose of interdicting drugs, reducing pilferage and other criminal activities.

commercial inspection systems falls short of a tolerable threshold for security—some losses due to crime are accepted as part of "the cost of doing business." By contrast, the consequences of even a single breach of security involving a nuclear weapon could be catastrophic. Therefore, a more sophisticated strategy is required to fulfill the objective of preventing incidents of nuclear terrorism on U.S. territory.

Nevertheless, every effort should be made to integrate any security system against nuclear smuggling with efforts to provide commercial security. A government-sponsored counter-nuclear effort could benefit from commercial investments in security, while commercial security interests could benefit from the surveillance added by government-sponsored efforts.

A significant proportion of the total volume of international shipping passes through very large "super-ports." Roughly 25% of all container handling worldwide is performed at the five busiest container ports—Hong Kong, Singapore, Pusan, Kaoshiung, and Rotterdam.[8] Steps to detect illicit nuclear materials at these and other "choke points" in the international system of maritime shipping should be a focus of early efforts. Similarly, a large fraction of the shipping destined for the United States enters through a relatively small number of ports. Much of the transportation, terminal operation, insurance and re-insurance business is similarly concentrated. This level of concentration does not eliminate the need to secure the many smaller installations that could provide vulnerable entry points, but it makes it possible to begin testing equipment and system approaches in a few major locations with a realistic expectation that practices adopted at those sites may, with suitable inducements and economies of scale, spread to cover the rest of the industry.

No single technology can detect illicit nuclear weapons and materials with 100 percent reliability. Consequently, a security-oriented approach to container inspection should be structured as a "layered defense," incorporating a number of independent detection opportunities along the supply chain. System design, and continued system monitoring is as important as appropriate equipment and practices, given that all static systems and technologies are vulnerable to eventual evasion by a sophisticated enemy. Attention to minimizing overall system vulnerabilities—including those arising from human operators—is important. Care should be taken in overall system design and maintenance not to introduce new vulnerabilities as existing weak points are addressed. To achieve those ends, the system should be continuously tested by means of "red-team" exercises that probe for vulnerabilities because, unlike other forms of contraband and theft, there will be relatively few if any real-world experiences with nuclear weapon smuggling to draw upon, although the number of smuggling incidents involving radioactive sources is somewhat larger.

One program for installing and testing new equipment and new ideas, Operation Safe Commerce, has received congressional approval and funding, and is in the early stages of implementation at three major U.S. ports.[9] Operation Safe Commerce is a voluntary partnership between private companies, commercial carriers, terminal operators, and local U.S. agencies to develop and test procedures, equipment, and information systems to improve the security of the maritime shipping system.[10] The program permits government and commercial entities to install experimental systems and equipment, and to conduct trials of new technologies, information

[8] None of the five largest ports are located in the United States. However, if the port facilities at Long Beach and Los Angeles are considered together, then they are third in the ranking.

[9] The ports of Los Angeles-Long Beach, Seattle-Tacoma, and New York-New Jersey have been designated as testing sites, together with companion ports outside the United States—Hong Kong and Singapore for the west coast ports, and the port of Rotterdam for New York-New Jersey.

[10] Three different types of players will be eligible to run test-bed experiments at these designated ports: (1) groups that win contracts from the $28 million dollars in federally appropriated funds; (2) commercial entities that have developed technologies for port security and which hope to earn endorsements for their products; and (3) scientists and technicians from government laboratories who want to test newly developed equipment and technologies.

systems, and procedures, with minimum disruption to port activities.[11] The Stanford Container Security study group strongly recommends ensured funding for Operation Safe Commerce and similar projects that incorporate a systems approach to maritime and port security, and which also contain specific provisions for collecting needed data, and developing and testing new technologies for improving maritime and port security.[12] The recommendations made in this report are intended to be compatible with this and other test-bed projects.

More generally, three major categories of challenges are associated with improving the security of international commercial shipping networks and port facilities:

1. Technical challenges: Equipment and system design, and research management;
2. Economic challenges: Anticipating the costs of required technical and human investments, and determining which entities will bear those costs; and
3. Institutional challenges: Overcoming domestic and international impediments to securing cooperation from various market participants, interest groups, and nation-states.

Of these, economic problems appear to be paramount. However, concerns surrounding sovereignty over ports and inspection facilities, labor agreements, and other underlying political constraints will be far from simple to overcome. Commercial equipment is currently available that can remotely scan closed containers to determine, with a reasonable degree of confidence, whether they contain many types of nuclear or radiological materials. However, it has yet to be determined whether more discriminating methods of interrogation, which tend to be more expensive and time consuming, will be adopted at large ports, not to mention many smaller port facilities. To be readily embraced by system participants, the costs of achieving a secure system will have to be small relative to shipping costs (a few percent of the cost of the goods shipped), unless significant government subsidies are made available to alleviate the financial burden. Deciding how to spread these costs fairly, and in such a way as to maximize incentives for compliance among legitimate market participants, will be a critical component in reducing opportunities for maritime transport to be used either as a conduit for or a target of nuclear terrorism.

Fortunately, improvements in container security will produce economic and social benefits that will accrue to partner governments and market participants. As already noted, integrating existing and prospective systems for commercial security and security against nuclear terrorism can substantially reduce the overall cost of the system. Moreover, benefits from reducing theft, contraband (e.g. drugs, trafficking in humans, small arms, etc.) and other forms of illegal activity suggests that the cost of improving security for container traffic need not be charged primarily to defense against nuclear terrorism since other public goods will benefit.

A number of more specific problems were also identified within the three general categories mentioned above. They include challenges associated with:

[11] Constructing a Secure Trade Corridor: A Proposed Multilateral Public/Private Partnership, by Dr. Stephen E. Flynn, Senior Fellow, Council on Foreign Relations, p. 4.

[12] One such program is the Container Security Initiative run by the US Department of Commerce (see http://www.customs.gov/news/ctpat/index.htm).

- Development of internationally acceptable standards for certification of "trusted" shippers, together with methods for monitoring the continued integrity of those arrangements;
- Specification of an optimal combination of types of external scanners and detectors at ports of embarkation;
- Devising cost-effective technologies for assuring container integrity after inspection, including technology to communicate to monitors when a breach occurs;
- Designing technologies and systems to assess the presence of dangerous nuclear material under realistic conditions;
- Overcoming difficulties associated with inspecting the contents of tightly packed containers, and bulk goods;
- Identification of suitable locales and procedures for handling suspect containers entering or approaching a U.S. border;
- Developing a system for reliable communication, control, and data fusion in the monitoring of container traffic, including coordination with the intelligence community;
- Advancing effective international agreements for safeguarding the international trading system from the consequences of illicit trafficking in nuclear weapons and SNM.

This report attempts to provide at least preliminary solutions to these issues—particularly as they relate to maritime shipping of dangerous nuclear materials, with priority given to nuclear weapons and special nuclear materials.

III. Objective and Scope of Report

Objectives

- Develop an example of a technical "systems approach" to detecting nuclear weapons, special nuclear weapons material (SNM), and other radioactive material, in internationally shipped containers, that is feasible within the economic and political constraints of the international trading system;
- Lay out key criteria, features and cautions for a layered system reaching as far "upstream" in the chain of custody as needed to guarantee the security of the container contents; and
- Identify legislative and executive branch initiatives that will be helpful for the short term and within a longer time horizon, while also highlighting steps likely to prove counterproductive.

The objectives of the Container Security study were to:

Audience

The intended audience for this report includes policy makers, staff and researchers in the executive and legislative branches involved in designing and implementing the U.S. approach to preventing catastrophic terrorism against, or by means of, the system of international maritime shipping. More narrowly, the observations and recommendations contained in this report are directed toward groups carrying out Operation Safe Commerce, the U.S. Customs' Container Security Initiative, and other dedicated testing and evaluation programs.

Focus and Context of Study

Measures to improve the security of shipping containers and the international system of maritime transport make sense only as part of a more comprehensive strategy for protecting the

United States against nuclear and radiological terrorism. Such a strategy should include (but need not be limited to) the following four elements:

1. To prevent unauthorized acquisition of nuclear weapons, SNM, and radiological materials;
2. To deter at a system-wide level attempts to use these types of weapons if prevention fails;
3. To develop the means to detect and interdict illicit nuclear and radiological materials, i.e., defend the United States, if deterrence fails; and
4. To prepare for, and be able to respond effectively to the use of nuclear and radiological weapons against US targets.

The study group focused its efforts on detection and interdiction of dangerous nuclear materials in the system of maritime container shipping, with particular emphasis on nuclear weapons and SNM.

The emphasis on nuclear weapons and SNM was motivated by two considerations. First, a terrorist attack using a smuggled nuclear weapon, or an improvised nuclear device using illicitly acquired SNM, presents a far more dire, although less likely, threat than a non-nuclear terrorist attack using more common radioactive materials. Second, some types of SNM pose particularly challenging detection problems due to their comparatively low levels of radioactivity. With this caveat, the content of this report is in substantial measure applicable to broader efforts to detect many types of illicitly shipped dangerous radioactive materials.

The focus on maritime shipping was prompted by the observation that groups seeking to acquire a nuclear weapon or illicit SNM are more likely to conduct those activities overseas than inside the United States, where nuclear weapons and SNM are tightly controlled. Without appropriate safeguards, commercial shipping containers are an obvious mode for covert delivery of dangerous contraband, including heavy, bulky objects, such as fully assembled nuclear devices, or heavily shielded radioactive sources. Sufficient effort should be placed on improving container security to make this delivery mode relatively unattractive to any terrorist group that has managed to procure an assembled nuclear device, or SNM. A layered system offering opportunities to detect such a weapon *before* it enters a U.S. port would increase the security not just of the United States, but also of the international maritime commerce system, against the global disruption that detonation of a nuclear weapon in any major port would cause. In addition, a system for detecting smuggled nuclear weapons and SNM may also succeed in intercepting illicit radioactive materials contained in an RDD. Finally, such a system should be integrated into an overall architecture for protecting the United States form any form of nuclear and radiological terrorism, regardless of delivery mode.

Threat Scenarios and Overall Priorities

The following three threat scenarios underlie the analysis undertaken in this study:

1. Importation of an assembled nuclear weapon that could be detonated in a U.S. port, or at some inland point of transit;
2. Importation of SNM for assembly into a nuclear weapon within the United States.
3. Explosion of a radiological dispersal device (RDD) in a commercial port in order shut down port operations and jam international maritime traffic. [13]

[13] The group did not consider scenarios involving the importation of high explosives alone (a common ingredient for assembled nuclear weapons and RDDs), which involves very different control measures.

The study group concluded that preventing importation of an assembled nuclear weapon should receive the highest priority. Although this scenario is the least likely of the three *a priori*, the catastrophic nature of the consequences that would follow if carried out successfully warrant significant preventive efforts. Preventing the importation of SNM is a slightly lower priority because, even though it could lead to an outcome comparable to the importation of an assembled nuclear device, illegally transported special nuclear materials cannot be used immediately in an attack. The requirement for assembly within the United States offers further opportunities for law enforcement agencies inside the United States to detect and prevent a planned attack.[14]

The third threat scenario, illicit importation of an assembled RDD or radiological materials for use in a radiological dispersal devise (RDD), would have less catastrophic consequences if successfully carried out than either of the two scenarios just described. At the same time, detection of illicit radiological materials poses a different type of challenge to any screening system. In contrast to the close governmental and IAEA monitoring of all *legitimate* international transport of nuclear weapons and SNM, there is a significant legitimate international commercial trade in radioactive sources, and in products containing radioactive materials and components.[15] Therefore, the development of security systems capable of distinguishing quickly and efficiently legitimate from illicit radioactive cargo—possibly even within a single shipping container—constitutes a key technical design challenge. Meeting this challenge will be essential to avoiding unnecessary delays for legitimate shipments and for minimizing costly false alarm rates.

IV. Desirable System Characteristics

In this section, we suggest some universal criteria for evaluating the effectiveness of a security system designed to prevent nuclear terrorist attacks. Implications for system testing and deployment are likewise discussed where appropriate. We also note the desirability, when framing legislation and regulations, of distinguishing between short-term measures that may be needed to meet immediate problems, and more long-term steps toward an effective, robust, and affordable system that only experience can provide. We return to the latter topic later.

Cost Effectiveness

Estimates of the overall cost for the design and implementation of a security architecture for detecting illicit trafficking of nuclear materials must take into account both 'direct' and 'indirect' costs. Direct costs include equipment, real estate and operating costs over a specified system lifetime ("life-cycle cost"). Indirect costs include those associated with likely shipping delays caused by the security measures, or costs generated by widespread reorganization of contracting and insurance arrangements under a new set of rules.[16]

Direct and indirect system costs will be offset by expected savings in the form of more accurate shipping manifests, reduced theft, spoilage, and other sources of loss, to yield the "net system cost." As noted above, to be feasible from an economic perspective, the net system cost should not exceed a small fraction of the overall shipping costs, or, alternatively, a very small fraction of the value of the goods shipped. The final step in this process entails comparing the net system cost to the total expected social benefits of the system. The most important metric is the benefit from preventing, or reducing the likelihood of, a catastrophic terrorist event, although

[14] Unfortunately, a quantitative risk assessment of these threat scenarios was not possible due to data limitations.

[15] It follows that the guiding assumption in designing a system to prevent a nuclear terrorist attack on U.S. territory—that nuclear weapons and SNM are more easily acquired abroad—is less robust with regard to these types of radioactive materials.

[16] Note that each component of the system design is likely to entail a range of choices that require trade offs.

reduced contraband (e.g., drugs, small arms, and trafficking in humans) is clearly another social benefit.

The relative cost-effectiveness of different security systems must also be considered. Because some systems will be more effective than others in detecting specific forms of contraband, the outcome of this analysis depends in part upon the goals and requirements of the system in question. This is an issue of policy choice—not a technical issue. At the technical level, any proposed security architecture should be tested on a prototype basis during development to collect information on actual equipment costs and reliability, operating costs (i.e., personnel costs and shipping delays), and the false alarm rates experienced at each stage of inspection under normal operating conditions. Only then will it be possible to make informed comparisons between different systems and configurations.

Realistic Cost Allocation

The international trading system is comprised of manufacturers, port authorities, terminal operators, transportation companies (both local and international), security companies, together with local and national governments and participating agencies (e.g., customs and immigration), and consumers. The cost of any security system will be allocated among these various actors. If the net security system cost is small (a few percent of shipping costs, or a few tenths of a percent of the value of the goods shipped), it may, in many cases, be possible to pass those costs on to the consumer without noticeable effect. However, as the net costs of security increase relative to shipping costs this option may become exhausted, and the political and economic dilemmas of deciding where in the system those costs will be absorbed will become more difficult to resolve. For example, commercial shipping companies already operate within a very narrow margin of profitability, which means that they are unlikely to be able to absorb the costs of the proposed security system. How cost allocation issues are decided can have an effect on the effectiveness of system operations. For example, the greater the financial burden placed upon commercial operators, the greater their incentives to attempt to circumvent any system for detecting nuclear or radiological materials in order to obtain a competitive advantage. Again, time and limitations of expertise among members of the study group precluded a detailed evaluation of these issues.

Market forces can be expected to provide some parts of the needed response. For example, most of the passive and active scanning equipment in the system proposed in the next section is being produced commercially, albeit in many cases using technologies developed in partnership with government laboratories. Various firms have begun marketing technologies for intermittent or near-real-time tracking of the location and condition of individual containers**.** Bonded, private firms are likely to appear both in the United States and abroad to provide verification of container contents for "certified shipper" programs. In other areas, such as the construction and operation of an integrated international data network, it is unlikely (and indeed possibly undesirable) that private commercial operators would fulfill this requirement.

At the broadest level, ensuring that the system of international container traffic is secure against use by terrorists should be viewed as a public good and, therefore, appropriate for government action and support– particularly for countries that stand to lose a great deal from the disruption of the international trading system. Indeed, there are strong incentives for governments to cooperate with, if not subsidize, enhanced security measures, assuming they share a similar view of the threat. Even if they don't place nuclear terrorism as high on the list of threats as the US government, the public good of reduced contraband may provide a strong incentive to participate. Cooperative arrangements incorporating standards that are acceptable internationally will have to be established to identify shippers and ports that fail to adhere to specified security measures, and to establish procedures for managing such situations as they arise.

Robustness

Any proposed security architecture should be designed to degrade gracefully if performance at any level is compromised. Systems must be scrutinized for potential common-mode failures, *i.e.*, failures at one level that affect system performance at multiple levels simultaneously, thereby degrading system performance unexpectedly and often drastically. For example, large databases are subject to illicit intrusion. They should have smaller, local backups. The same is true of detection and communication equipment. Since every system component can be expected to fail at some time, efficient levels of redundancy, together with monitoring by human operators, are important to a robust system design. To ensure that security systems maintain a high level of robustness under many types of conditions, they should be subjected to mock attacks (i.e., "red teaming"), both simulated and actual field exercises.

To the greatest possible degree, the system should be designed to capitalize on existing alignments of incentives that favor compliance, and to identify those areas that will require greater degrees of monitoring and a more heavy-handed approach. In some cases, market discipline itself may provide adequate incentive—perhaps with some government subsidization—for industry actors to adopt and adhere to preferred security practices. In other contexts, the alignment of incentives may be achieved with targeted inducements—for example, faster processing of containers that meet "certified shipper" criteria. In still other areas, the threat of official sanctions—such as the loss of privileges to ship to U.S. ports—may be required to elicit desired responses.

Finally, any security system should be designed with enough flexibility to permit incorporation of new equipment and procedures during and after initial design and implementation. This feature is essential, since neither the threats posed by terrorist groups, nor the technology available to deal with those threats will remain static. At the same time, it is important to ensure that new vulnerabilities are not introduced in the course of attempting to eliminate existing vulnerabilities. Therefore, modifications to the system architecture should be undertaken with a view to their likely effect on the entire system.

Production of "Actionable Intelligence"

Another criterion of effective system design is that alarms in the system must be "actionable"—they must occur at points where the triggering containers can be identified, diverted from the regular flow, and handled appropriately. For example, hard intelligence information that a nuclear or radiological weapon has been loaded onto a ship headed for the United States in the current maritime security system is not at present "actionable" because there is no way to identify and track down the specific ship or container, or to know when or where it is scheduled to arrive. For instance, the container in question could be transferred to another ship at an intermediate port without the knowledge of US authorities. A US President facing this situation would have to invoke burdensome ad hoc inspections at all US ports of debarkation for an indefinite period of time to guarantee that the weapon does not arrive, thus substantially disrupting global trade.

By contrast, portal monitoring and improved tracking procedures under a future security system could detect the presence of the weapon before it is loaded onto a ship, thus allowing the appropriate authorities to take effective action. This includes, for example, tracking suspect ships and containers after they depart the port of embarkation for interdiction before they enter US territorial waters. In short, intelligence improvements in the international system of maritime transport should be geared toward producing alarms that are triggered at points in the system that will permit action that is both effective, and minimally disruptive to the system as a whole.

Realistic Assessment and Treatment of False Alarms

Under the proposed systems-approach to container security, when radioactivity is detected at any stage in the scanning and sensing process, further investigation is triggered to determine if illicit

nuclear or radiological material is present. False alarms (also called 'false positives' or 'Type II errors') are events that occur when personnel at one level of the security system erroneously believe that illicit nuclear material has been detected based on sensor responses or other information. The problem of false positives in the detection of radioactivity among commercial shipped goods is complicated by the widespread presence of background radiation, which in some cases mimics radiation from SNM, as well as the legitimate trade in materials with traceable radioactive signatures.

The number of false positives generated by a security system is an important factor in overall system cost. In general, adding layers to the inspection process can reduce the false alarm rate—particularly layers that attempt to detect nuclear material via different physical signatures. However, increasing system complexity also increases costs. As a suspect container advances to higher levels of scrutiny, more sophisticated imaging and sensing equipment is required, as well as more time to collect data, and additional expertise to interpret it reliably.

Determination of an acceptable overall system false alarm rate for detection of a nuclear weapon in a shipping container is both an economic question and a policy judgment.[17] However, the number should almost certainly be small—perhaps on the order of one or at most a few such events per year (at least in the beginning) somewhere within the international shipping system. Because the economic and political consequences associated with the highest level of response are quite serious, incentives will be very strong to ensure that false alarms are kept to an absolute minimum. False alarms at lower levels in the system can be tolerated more frequently, up to a point.

Another concern is the effect that false alarm rates and thresholds may have on the human components of the system. If the false alarm rate is determined to be too high at some stage of the process, operators may be tempted to modify or circumvent procedures or sensors that are perceived to be unreliable, thereby undermining the integrity of the entire system. Therefore, before a security system is deployed, it is critical to collect data to determine actual false alarm rates at various levels of the system under normal operating conditions. In addition, care should be taken to ensure that when alarms do occur using recommended procedures, that operator compliance with system procedures is not discouraged.

Compatibility With Existing Systems

To be effective, a container security system must be able to function in multiple contexts. It must be adaptable to variety of local conditions, including variance in the organization and physical layout of port operations, education and training levels of personnel, cultural habits, financial arrangements, and contracts governing shipping and delivery. In few if any contexts will it be feasible to construct a comprehensive security system from the ground up. Rather, components of the system will have to be implemented incrementally, particularly in major ports, to permit continuity of operations.

Adoption and implementation of many of the recommended technologies, such as X ray and gamma imagers, may be achieved relatively quickly, given their dual use in detecting contraband and reducing economic losses. However, many port facilities have extreme space constraints for increasing the number of scanning facilities and diversion areas, and this may limit how quickly adaptations can be achieved. Other aspects of the proposed system, such as certified shipping programs, and various types of data collection, can be initiated on a small scale, with the objective of eventually linking and standardizing the overall system using international "best practices."

[17] The lower immediate risks from contraband SNM imply that even high-level false positives pose a less serious problem than with assembled nuclear devices.

Political Feasibility

The sample layered security system presented in this document is designed to push the risk of a nuclear terrorist attack as far as possible from U.S. shores.[18] To achieve this goal, the system will have to serve the security needs not only of the United States, but those of all major participating countries—who will also wish to minimize their own risk becoming targets of nuclear terrorism. The particular form that the required international coordination and cooperation should take—be it an international convention, a series of bilateral agreements, or a formal international organization modeled on the IAEA—was not discussed in detail by the study group.

Any proposed security system must be acceptable domestically within major participating countries. Where local architectures and practices are a source of concern for security, international standards need to be clearly spelled out, and resources and expertise made available to help correct the problem. In the United States, among the debates that should be anticipated are those from unions regarding new labor practices at ports, resource allocation issues, and turf fighting between various federal agencies with responsibility for international commerce and counter-terrorism. Another traditionally sticky issue will involve determining rules and practices regarding the sharing of technology and potentially sensitive intelligence with foreign personnel.

Clear Lines of Oversight and Responsibility

As with any complex international security system, establishing clear lines of oversight and responsibility will require considerable coordination, time and effort. Above all, to prevent the lines of oversight and responsibility from becoming confused by bureaucratic compromises will require continued attention from the governments involved. The US government will have a major oversight role, in view of the US position as the world's largest importer, exporter, and possibly most likely terrorist target. Given that the US Department of Homeland Security has just been created, it is impossible to go into meaningful detail on this issue. However, it is very important that it be raised.

Auditability

Another important feature of system design is the question of who will audit overall system performance, and the performance of its component functions. Clearly, auditing requirements will differ considerably from container loading at certified shippers, to operation and maintenance of sensing equipment in foreign and domestic ports or on board cargo ships, to the integration and interpretation of collected data. In some cases, such as the handling of data, these functions are likely to be highly centralized. Other elements of the system, such as on-site monitoring and verification of container contents, have an unavoidably de-centralized character.

Auditing protocols and procedures will require tailoring to local conditions in individual countries to ensure compliance with internationally agreed standards. For example, certified shippers may be required to have security personnel to inspect goods before loading, two-man rules for sensitive inspections, standard equipment for monitoring radioactive emissions, standards for tags and seals, or controlled access areas for goods prior to loading. Standard training for security personnel and subsequent monitoring of a company's performance must also be agreed upon. The latter could be done through a central data repository that collects information about international shipping activities, but it would also require periodic onsite inspections to ensure these data are accurate.

Standards for detection equipment performance and maintenance must be set internationally to avoid incompatible detection capabilities at different ports. The calibration and proper functioning of this equipment must be periodically checked onsite by authorized personnel, possibly

[18] This is a common goal for most strategies aimed at securing international commerce. See Stephen Flynn, op. cit.

from an international team. The output of sensing equipment at port facilities and shipboard may also be remotely monitored using a central data repository. Red team exercises and surprise inspections that test the functioning of the security system at a facility are also possible, although these can be quite intrusive and, therefore, will be possible only with the cooperation of local governments and private companies.

V. Sample Technical Approach

In this section, we present an example of a technical "systems approach" to securing maritime container imports against SNM and other radioactive materials. Organizationally, the approach is separated into operations to be performed during the stages of transport illustrated in Figures 1 and 2. These operations can be usefully grouped into four site-specific stages or 'clusters', and one continuous system-wide function:

- Certification of the packing of individual containers;
- Security procedures at the port of embarkation;
- Continued monitoring after a containers have been loaded onto a ship and during transit;
- Security procedures at the port of debarkation;
- Continuous collection and fusion of data regarding the movement of individual shipments of goods in a computer system designed to fail gracefully under physical or cyber attack on some of its components.

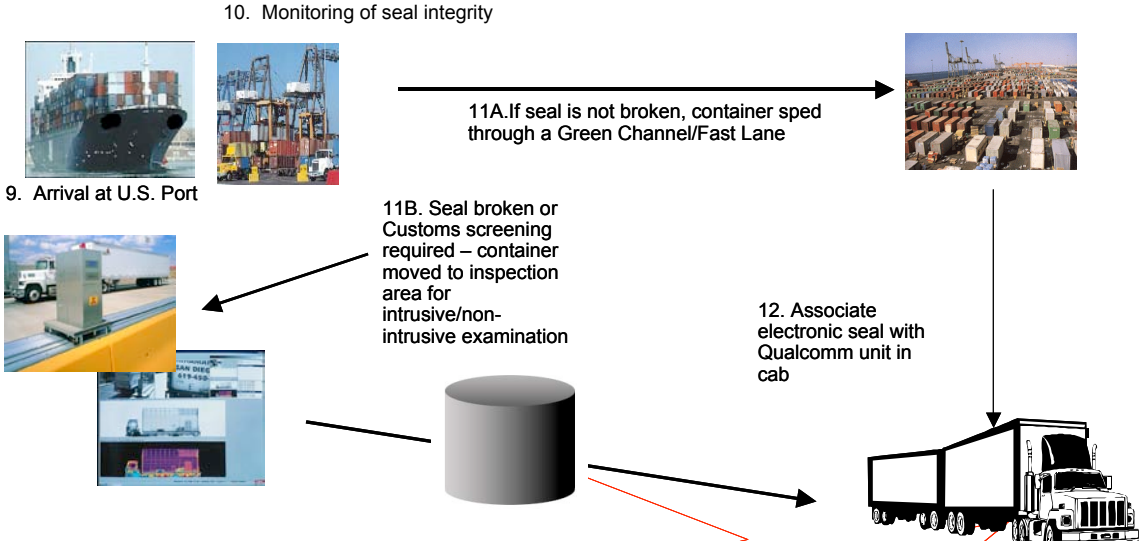

Figure 1: Cargo Flow And Monitoring At Ports Of Embarkation

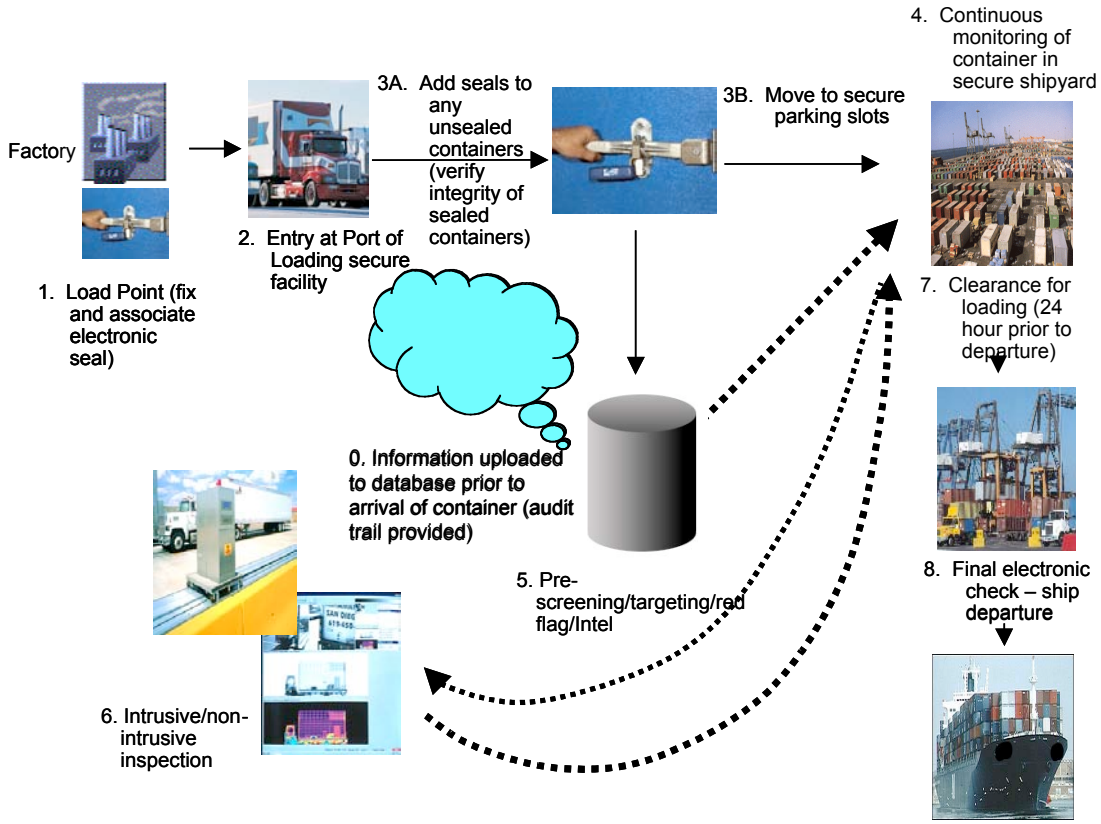

Figure 2: Cargo Flow And Monitoring At Ports Of Debarkation

We have been as specific as possible regarding the technologies to be utilized at each stage of the system. However, this report should in no way be construed as an endorsement of any particular manufacturer of commercial equipment. The purpose of this sample system is to show how a system can, with adequate and continuing monitoring, testing, and adjustment, be designed to meet the requirements outlined in the previous section. Time and experience will undoubtedly produce better systems.

Container Certification

The first stage of this process involves controls on the packing, sealing and storage of intermodal shipping containers until they are transported to the maritime port of embarkation (MPOE). Occasions for security lapses abound in the early stages of container transport, particularly in storage areas, where both time and opportunity to enter the containers can be plentiful. Where possible, security measures should be undertaken *before* individual containers reach choke points in the system where delay is costly or unacceptable.

As a rule, containers are filled either at the point of manufacture, or on the premises of freight consolidators. The standard practice is to close the container using a simple, inexpensive lock (unless the contents have some special value). Once locked, containers are seldom re-opened or inspected by officials. Instead, reliance is placed on information in the cargo manifest. The contents of individual containers are weight-limited, which means that there is often empty volume in the container where additional, non-declared cargo could be placed.

A system designed to prevent importation of dangerous nuclear material must begin by separating, to the maximum extent possible, "suspect" and "non-suspect" cargo and containers. Potentially relevant considerations include, the type of material involved, its point(s) of origin, and whether a trusted auditor has overseen the packing of the container. Wherever possible, the establishment of "certified shipper" programs is recommended as a first layer of security. Auditing by bonded, private companies whose business success depends on reliability is suggested, but government officials must be able to perform checks and audits of their own.[19] In most cases, this type of certification will be less expensive than wide use of more technologically sophisticated methods of verifying contents after the container is sealed.[20] The following are elements of our sample technical approach at certified shipper sites:

1. Manufacturers and consolidators adhering to security standards are established as certified shippers.
2. The shippers load containers using secure procedures and "certify" container contents.
3. Certified shippers must be audited regularly to ensure that accepted procedures are followed; existing pre-shipment inspection companies have the infrastructure to implement the audit process in the near term.

Once a container is inspected and certified, it is important to verify that its contents have not been altered or tampered with. The study group recommends development of a small, multi-purpose security device to be affixed to each individual shipping container. This electronic seal-tag, geo-locator, radiometric sensor, and communication device would:

- Add intrusion and radiation detection capability to existing devices;
- Monitor the position and security of the container throughout transfer;
- Be subject to theft, damage, and maintenance requirements; and
- Probably piggyback on increasingly adopted commercial tracking systems.

The proposed device would combine the functions of an electronic seal-tag that incorporates a small intrusion detector, a geo-locator, nuclear sensors, and a communication device. One must realize that "perfect" seals do not exist. All seals can be broken in time and protocols for seal inspection foiled. Therefore, any system for seal monitoring must include visual inspection in addition to automatic monitoring of seal integrity to minimize the chance that a container breach will go unnoticed. The geo-locator envisioned is not a complete GPS system, but would enable a central controller to determine the container location. The nuclear sensor would be passive, and would augment sensors operative at ports, and during shipboard transit.

The device should be designed and placed within the container so as to minimize opportunities for, and maximize detection of, theft and sabotage, including diversion and tampering during transport to the port of embarkation, as well as during any temporary storage period. It should never leave the container except for maintenance by approved personnel. In our judgment, the technology required is well within the state of the art, at a cost of between $100 and $200 per device. To give this figure some perspective, the cost of a single shipping container is approximately

[19] The procedures to be followed by certified shippers need to be negotiated and approved by all parties, and will differ in detail according to contexts and materials. For instance, an automobile shipper is likely to take steps to certify his shipment that differ from a shipper of clothing or refrigerated goods.

[20] Relative costs will depend on relative labor as well as relative equipment costs. Inspection of closed containers may be automated and thus require more expensive equipment but lower labor costs than inspection of contents during filling containers.

$8,000. Aside from the nuclear sensor, which is relatively cheap, all other elements of the device will have independent commercial value.[21]

Ports of Embarkation

Under current practices, individual shipping containers, with the possible exception of those packed with highly perishable cargo, often spend time waiting either at the point of origin, at way stations in the exporting country, or at the port of embarkation. Depending upon the port and the operators, waiting containers may or may not be kept in a monitored, guarded area. Under the proposed system, waiting time will be used to conduct a battery of differentiated screenings to detect undeclared nuclear and radiological materials. The three-tiered detection system suggested for ports of embarkation would include:

1. Gamma and neutron portal monitoring for all containers (designed to detect weapons-grade plutonium, weapons-grade uranium, and RDD materials);
2. Gamma radiography (e.g., VACIS) or X ray radiography for all non-certified containers, all certified containers that alarm portal nuclear monitors, and a certain percentage (yet to be specified) of certified containers that do not alarm portal monitors as a random check;
3. Isotope identifiers (handheld gamma spectroscopy) for passive inspection of high-density "suspect" regions in VACIS image; and
4. Active interrogation (e.g., PELAN-14 MeV neutron activation and thermal imaging) designed to identify shielded highly-enriched uranium for the small percentage of containers showing high-density anomalies.

At ports of embarkation, all containers destined for transport to the United States, or to other cooperating countries that join the system, will be subjected to passive gamma and neutron radiation monitoring before being loaded onto a ship (Stage 1). Such systems are already in place at some ports, as Figure 3 illustrates for the ports of Portsmouth and Dover in the United Kingdom.

Figure 3: Passive Gamma And Neutron Radiation Monitoring

All containers from which radioactivity has been detected will be subjected to a second inspection (Stage 2) involving active radiographic imaging with X rays or gamma rays.[22] An example

[21] As with all system elements, the recommended procedures and equipment characteristics, e.g., the false positive and false negative rates, must be ascertained during the test-bed programs.

of such an imaging system (the "VACIS" system built by SAIC) is shown in Figure 4. The left side of the boom arching over the containers in the figure houses a low-level gamma source while the right side contains two rows of sodium iodine detectors for imaging. An example of the radiographic image created by such imaging systems is shown in Figure 5, where the upper image illustrates a car being carried inside a truck and the lower image illustrates the same configuration with several dark objects clearly visible representing C-4 simulants.

Figure 4: Radiographic Imaging Devices

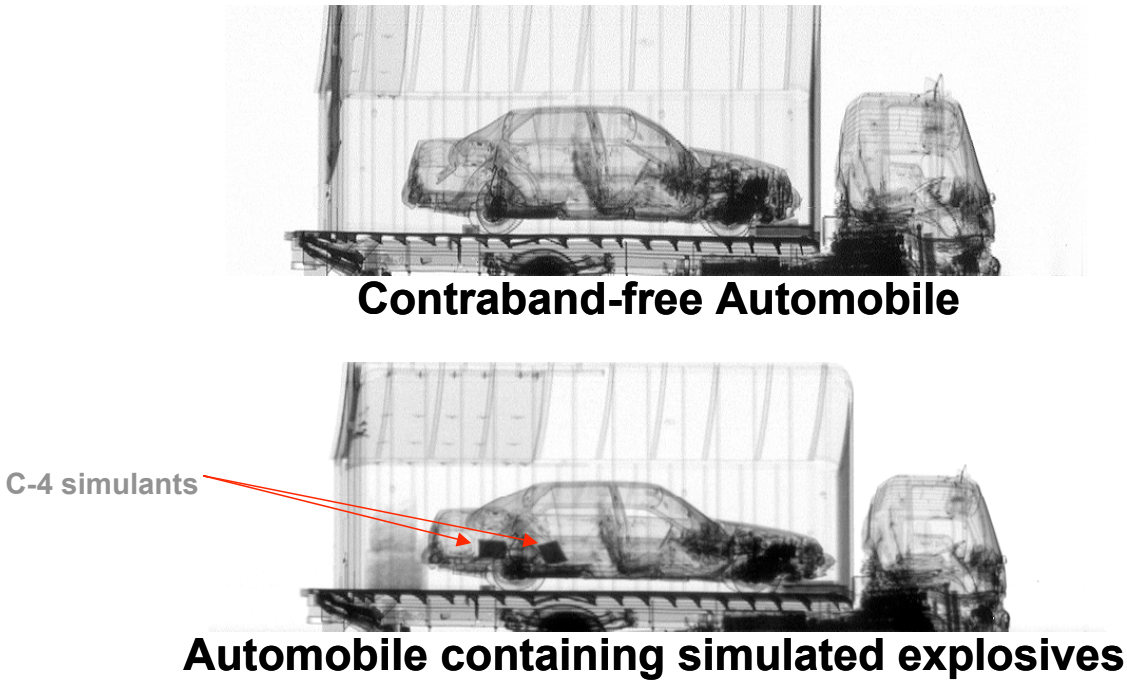

Figure 5: Example Of Radiographic Images

[22] Heavy shielding can be detected using gamma- or X ray radiography—an active measure that irradiates the contents of a closed container with a minimal dose (around 5 μrad—a minute fraction of the daily background dose of radiation received by humans).

The small percentage of containers that continue to be suspicious following stage 2 inspection will advance to a third stage in which more time-consuming and intrusive inspection of the container is conducted. For example, the container could be examined with a pulsed neutron source (see Figure 6) to look for the delayed gamma rays or neutrons associated with fissile materials, or the container could be opened, and the contents scanned for the presence of fissile material with a hand-held gamma ray spectrometer (see Figure 7). Or, a thermal imaging device could be used to detect the heat signature associated with an assembled nuclear device.[23] If, after a container passes through the entire system, security personnel still believe contraband nuclear material is present, higher authorities would be contacted. If a weapon is suspected, special Nuclear Emergency Search Teams (NEST) will be called in to locate, verify and disarm the weapon. During this process, the affected port will in all likelihood cease to operate, and precautionary evacuations of the surrounding areas may be appropriate.

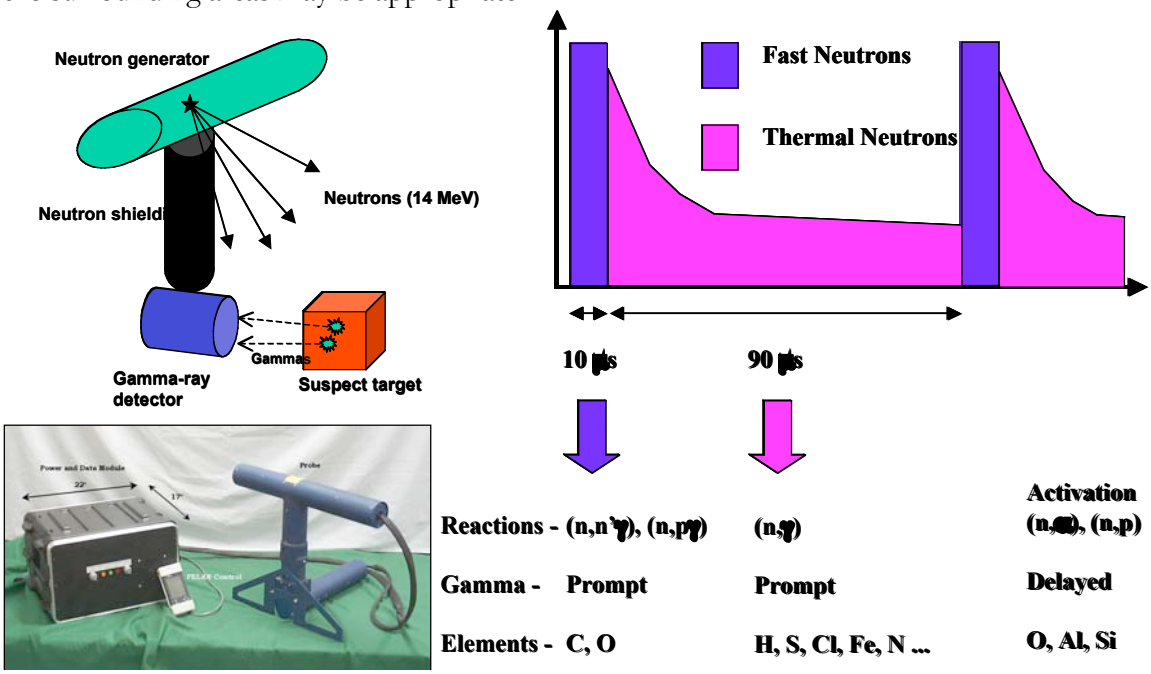

Figure 6: Pulsed Neutron Source To Detect Fissile Material

The proposed layering of technologies is intended to provide a comprehensive screening of container traffic with minimal delays imposed upon the vast bulk of containers passing through the system. Once radioactivity is detected, the system faces the problem of determining quickly and accurately whether its source is legitimate (and only legitimate) cargo. For example, ceramic materials and certain organic compounds emit detectable levels of radioactivity, and lead or other heavy metals will mimic the appearance of shielding on a gamma-ray or X ray scan. Unfortunately, it is not commercially practicable at present to subject the entire volume of international container traffic to the full battery of scanning and imaging technologies at the port of embarkation. Increasing the technical sophistication of scanning equipment brings higher equipment costs, and greater time

[23] There was some difference of opinion among members of the group with respect to the wisdom of allowing port officials to open suspect shipping containers in order to conduct gamma spectrometry and thermal imaging. The possibility of booby-traps or automatic detonation devices suggested, to some members, that only specially trained Nuclear Emergency Search Teams should ever open a container that is suspected of holding a nuclear device.

delays for measurements and interpretation.[24] Certifying shippers helps reduce the inspection load at all but the relatively rapid and cheap stage 1 inspection level. In addition, reliable information collected on individual containers as they advance through the system is important for targeting suspect containers apart from the results of the stage 1 passive radioactive measurements.[25] The layered inspection approach suggested here applies the more time consuming and costly inspections in stages 2 and 3 only to suspect containers tagged in the preceding stage.

- **Detects nuclear and radiological weapons**
- **Provides automatic detection and identification of over 30 radionuclides**
- **Eliminates need for periodic calibration**
- **Lightweight--less than 2 pounds**
- **Uses efficient gamma-ray detector (CsI with photodiode) which minimizes acquisition time**
- **Operates in survey and analysis (expert and non-expert) modes**

Figure 7: Handheld Gamma Radiation Spectrometer

How foolproof the proposed combination will be can only be determined by actual testing with "red teams" attempting to introduce various dangerous nuclear materials, simulated weapons, or their equivalents. The emphasis at this stage should be the detection of assembled nuclear weapons. Once a weapon is loaded onto a ship destined for a U.S. port, it could be detonated before inspection at the port of entry. Again, rates for both Type I errors (false negatives) and Type II errors (false positives) are important to testing system performance. Various combinations of equipment and staffing need to be tested for reliability and efficiency, and these results quantified by test-bed programs.

Transit

Once loaded, containers typically remain on the ship during transit to the United States, although some off-loading and reloading may occur at intermediate ports of call. In addition, some shuffling may occur to make room for other containers destined for earlier off-loading. From the point at which a container is loaded onto the ship, and throughout transit to the United States, operational priorities shift to conducting additional spot-checks using external sensors to detect radioactivity from container contents, monitoring location, detecting intrusion, further sensing nuclear radiation, and communicating information to a data fusion and control center.

The time needed for a container ship to cross an ocean should be viewed as an opportunity to include another stage of detection procedures. However, it was noted that the stacking of containers in tight blocks on board transport ships during loading might limit the ability of ship-mounted detectors to identify and pinpoint suspicious cargo. The group did not evaluate the dimensions of this difficulty quantitatively.

[24] Modern radiography, via fixed installations costing a few million dollars each, permits an accurate measurement of density differences, but at the cost of some minutes delay for interpretation. Of course, one installation could be teamed with several interpreters, but this would cause labor costs to rise.

[25] Tighter inspection and tracking procedures are already in place for high value and some time-sensitive shipments.

The multipurpose tamper-detection and radiometric monitoring device described above, and recommended for installation in each container will continue to fulfill the same functions aboard ship as during land transport. The long integration time during transit will improve the ability of the nuclear sensor component of the device to detect low-level radiation signatures. It is possible, for example, that small quantities of SNM that may have escaped detection at the port of embarkation could be detected during ocean transit. Appendix A details the relevant technical considerations. We have not made a quantitative estimate of the cost associated with the required sensors, nor have we analyzed the effect of the environment (shocks during loading and unloading, temperature fluctuations, etc.) on sensor performance.

Ports of Debarkation

At the U.S. port of debarkation, the proposed procedures for handling off-loaded containers will differ somewhat from those at port of embarkation. Although many of the same technologies are suggested, they will need to be applied in different configurations, and with somewhat different parameters and objectives. At the port of entry a more detailed inspection of suspect shipments is possible, since delays at this stage will not have the potential to affect thousands of non-suspect containers, as may be the case at the port of embarkation. Accordingly, more emphasis may be given to the detection of SNM (a tougher target than assembled nuclear weapons) at the port of debarkation.

In addition, information regarding the tracking and handling of individual containers will be available at the port of debarkation. This allows for more precise pinpointing of suspect cargo, including questionable shipments of radiological materials. The system will bring together data from the port of embarkation, the shipper (certified or not), the seal/tracking/radiation sensor device described above, the shipping manifest, and other intelligence sources. As with the POEs, our sample technical approach would require that all containers pass through nuclear portal monitors, that non-alarming containers are spot-checked by radiography and/or cleared to exit port, and that all alarming containers are inspected by radiography, and suspect anomalies are scanned with an isotope identifier and interrogated with active neutron interrogation.

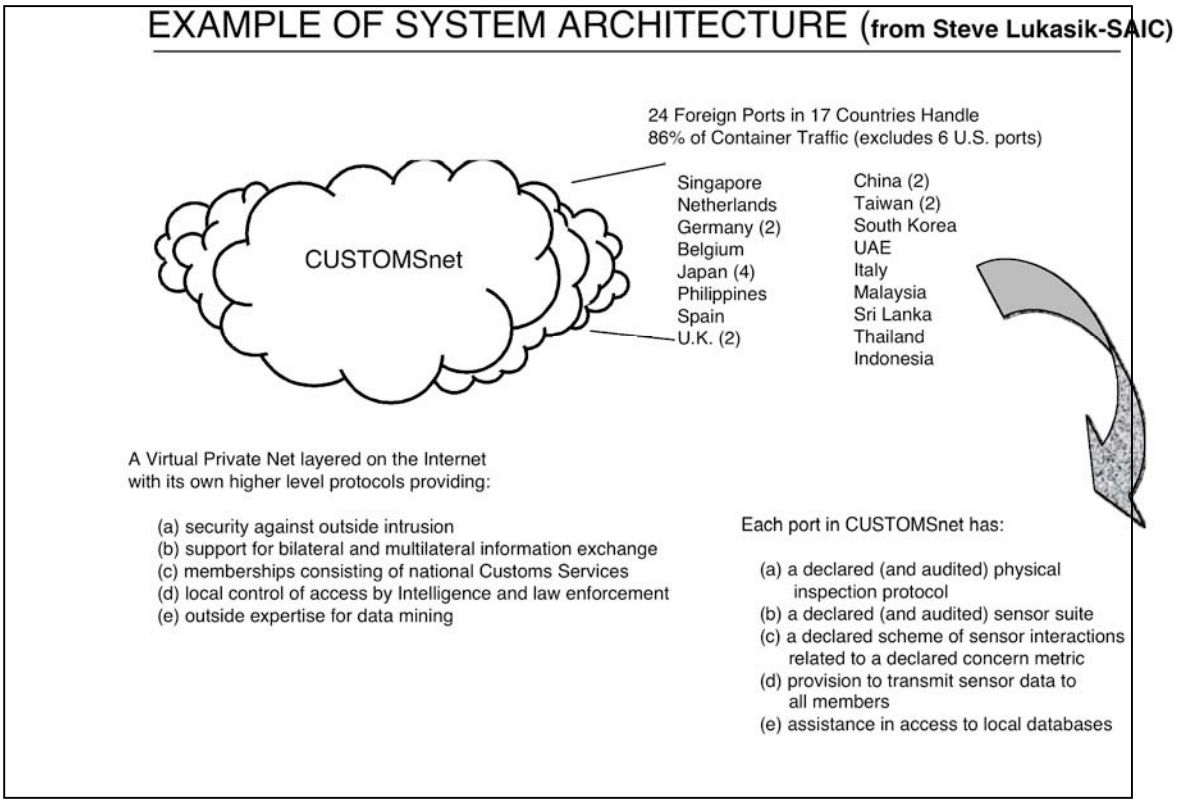

Figure 8: A Possible System Architecture For Data Fusion

Continuous Information Monitoring and Data Fusion

An information and data fusion system is an essential component of a comprehensive container security system. Only through continual operation and monitoring can suspect shipments be reliably identified, proper action taken, and system faults identified and corrected. One possible system architecture devised by Steve Lukasik is shown in Figure 8.

The data system would incorporate and fuse information from multiple human and technical sources, including:

- Sensor information (radiation levels, radiographs, etc.) wherever taken;
- Readouts from intrusion sensors and records of alarms;
- Cargo manifests;
- Inspection information;
- Information about original loading point, travel routes (verified to the extent possible by logs from the multi-function device attached to the container);
- Relevant intelligence information about shippers, other shipping agents, ports and countries involved; and
- Information gathered by human agents about deviations from normal shipping or other patterns.

Other desirable system features include compatible data storage for all categories of information, coupled with some level of real-time analysis incorporating data mining algorithms that will highlight problematic features of any particular container, and promptly retrievable archiving.

The goal of the information and data fusion component of the system is to help decision-makers in the United States pinpoint suspect containers, and, in extreme cases, to decide whether particular container ships should be prevented from entering U.S. territorial waters. Once established, the system will permit American officials to delay or detour suspect shipments, if such action is required. Finally, for the information produced by the system to be relevant, there must be appropriate connectivity to groups that may be expected to take action on the basis of the information gathered such as the Coast Guard, the Customs Service, the FBI, and others.

Again, only experience can demonstrate the full range of characteristics that will be required of an information system. Whatever information system is originally selected should remain highly adaptable throughout the testing and early deployment period, and should be reviewed regularly thereafter.

VI. Desirable Government Initiatives

Lead Government Technical Integrator

The federal government needs a lead technical integrator to coordinate nuclear container security initiatives. Depending on the final structure of the Department of Homeland Security, either it or the NNSA will be best equipped to assume this role. The leader should draw on related agencies, particularly the Defense Threat Reduction Agency and the Office of the White House Science Advisor. The leader should also participate in all interagency working groups addressing container security, at a high level. In addition to technical integration, this agency will fund analyses of the economic impact of various security architectures, including the conditions under which direct government subsidies become justified.

Technology Development Grants

Funds should be allocated for research and development of technologies for radiation detection, tamper detection, X ray and gamma-ray imaging, and information integration. Funds should be made available to applicants from academia, the national laboratories, and industry, and should be awarded by the new DHS in consultation with the Departments of Transportation, Commerce, and Energy. These grants should focus on exploring new technologies, lowering the cost of currently available technologies, and technology transfer.

Incentives for Cooperation between R&D, Test Beds, and Pilot Projects

Integrating technologies into the port environment will be essential. Close cooperation between R&D leaders and available pilot projects and test beds will ensure technologies are tested in realistic conditions during all stages of development. To encourage this, funds should be appropriated for the NNSA, DTRA, and other appropriate departments and agencies, to be used exclusively for expenses related to cooperation with test bed and pilot project facilities. Similarly, the US Customs Service, Coast Guard, and other appropriate departments and agencies, should receive funds to be used exclusively for expenses related to cooperation with groups developing nuclear security technologies.

International Standards for Container Inspection, Securing, Certification, Transport Monitoring, Data Handling and Storage, and Communication Systems

International standards will be essential for the effective functioning of a comprehensive container security system. Institutional participants should include:

- International Organization for Standardization (ISO), the standards bridge between public and private sectors;

- International Maritime Organization (IMO), the UN agency responsible for improving maritime safety and for technical cooperation; and
- International Atomic Energy Agency (IAEA), which should be the lead technical participant in the system.

The U.S. Government should give a single organization responsibility for surveying ongoing international efforts in this area, and for initiating negotiations as early as possible to establish appropriate standards and to develop protocols for authoritative action in the above areas, or in any other area needed for secure shipping.

International Test Bed

The US government should commit funds, in cooperation with other governments and entities, to establish an international test bed for nuclear container security. While pilot projects at individual foreign ports are important, an integrated test be will be essential in troubleshooting proposed systems and technologies and in training workers.

VII. Conclusions and Recommendations

The goal of the system outlined in this report is to improve international supply chain security from the point of containerization to the final port of debarkation within the United States, with minimal interference with flows of legitimate international commerce. Our study of these issues reached the following conclusions:

1. Rigorous testing of any candidate system is essential and should be continued during deployment and in the field.
2. The robustness of the system should be reviewed against the near-certainty that important elements would fail, either during normal operation or due to attack. The objective should be to ensure that elements of the system degrade "gracefully," and not in ways that significantly impair the overall performance of the system. In particular, data systems should be reviewed for their degradation characteristics against intrusion and under various forms of electronic attack.
3. Each element of the system should be designed to generate "actionable intelligence." The technical aspects of this challenge must be considered in tandem with potential economic, legal and political implications of diverting suspect containers from normal traffic or, in extreme situations, halting traffic altogether. Barriers to coordination among the agencies involved, both within the U.S. government and across national boundaries, should not be ignored or minimized.
4. International agreements to coordinate standards and to develop protocols for authoritative action will be essential. A suitable institution with membership that includes the majority of trading states should follow the testing programs and prepare options for such agreements.
5. Plans for system implementation at specific ports should be analyzed for their likely effects on labor agreements, business contracts, insurance liability, etc. Labor disputes resulting in port stoppages should be analyzed for their effects on global flows of goods, and for their wider economic impact. In this regard, insight could be gleaned from an analysis of the economic impact of the 11-day shutdown of 29 ports on the west coast of the United States due to a labor dispute during September and October 2002.
6. Longer-term research and development objectives should be identified and budgeted for, even though deployment of a security system to improve security in the short term is possible using available technologies and equipment. Forward-looking research and

development should be carried out under the supervision of an agency tasked with evolving a comprehensive transportation security system and should not be fragmented according to specific modes of transportation.

Appendix A: Analyzing System Performance With A Simple Queuing Model

This appendix describes a simple queuing system to model the flow of cargo containers through two sequential detection stations (with possibly multiple parallel detection machines at each station). The model can be used to examine the impact of parametric changes on system performance. The following metrics will be computed from the model:

- Time required to inspect a ship-load of containers
- Equipment utilization
- System bottleneck: the probability that certain equipment is idle because of congestion

Modeling environment:

The inspection system at a port is assumed to consist of two layers: a passive neutron or gamma ray detection system (stage 1) and an active X ray or gamma ray radiographic imaging system (stage 2). Containers come in two types: those from certified shippers and those from other shippers. The criteria for a container to earn a "certified" label are discussed in the main body of this report. All containers pass through stage 1. All non-certified containers also pass through the stage 2 inspection, along with any certified container that does not pass the passive detection layer according to some pre-specified selection criteria. Of the certified containers that pass stage 1, a randomly selected fraction are also imaged in stage 2. Containers subject to stage 2 scanning will proceed to an available radiographic machine. If no radiographic machine is available, the container will wait in a holding area. If the holding area is full, the container stays at its current location (meaning that a passive neutron/gamma detection machine will remain idle). The scan time at stage 2 depends on container label and the result of stage 1 examination but is generally around 5-10 minutes. The detection time for stage 1 inspection is on the order of 10 seconds. After completion of stage 2 scanning, the container will exit from our system (our model boundary). Additional search/examination after stage 2 is outside the scope of this simple model. It is assumed that an alert will be issued and other procedures will be followed should the test results warrant it.

Input parameters:

Physical parameters:

n: the number of containers to be examined
N(pd): the number of passive detection machines available at stage 1
N(rs): the number of radiographic scanner available at stage 2
K: the holding capacity immediately before stage 2 stations

Design (or soft) parameters:

F(c): fraction of containers that are certified
PC(pass): probability that a certified container passes stage 1 test
PN(pass): probability that a non-certified container passes stage 1 test
FE(c): % of certified containers (passing stage 1 test) exempted from stage 2 scanning
FE(n): % of non-certified containers (passing stage 1 test) exempted from stage 2 scanning
(The notional container screening system discussed in this report assumes FE(n) is zero)

Processing time parameters: processing time at various stages will depend on container status (certified or not, passing or failing stage 1 test). Longer processing time may be desired if a container fails stage 1 test and/or that it is non-certified.

T1: processing time for each container at stage 1
T2(c-p): stage 2 processing time for a certified container passing stage 1 test
T2(c-f): stage 2 processing time for a certified container failing stage 1 test

T2(n-p): stage 2 processing time for a non-certified container passing stage 1 test
T2(n-f): stage 2 processing time for a non-certified container failing stage 1 test

What is the model?

A queuing model requires three input elements:

1. The arrival process: how often and how random are the arrivals of "customers" (containers) to the queuing system;
2. The service process: how many "servers" (detection/scanning machines) are available, how long is the processing time to "serve" each customer"; and
3. The service discipline/configuration: how are customers "selected" to be served, how many holding spaces are configured if all servers are busy.

The situation we are considering does not suggest itself as a "ready-made" queuing system: all the n containers are immediately available to be examined, thus making the arrival process a bit tricky to model.

Modeling the "arrival" process:

We model the "output" from stage 1 as the arrival process feeding into stage 2, which will derive its randomness (of inter-arrival time) from the variability of the service process at stage 1. Some of the containers leaving stage 1 will exit the system (those which are exempted from stage 2 examination), which will modify (reducing) the "arrival" rate into stage 2. The numbers of machines at stage 1 will also determine the "output" from stage 1, thus the arrival rate into stage 2.

The service process:

The service time can be determined from (1) the percentage of containers of different classifications (certified or not, pass/fail from stage 1), and (2) the service time specified from system design for different classifications.

The service configuration:

The number of holding spaces in front of stage 2. More holding spaces will reduce the probability that stage 1 machine(s) is blocked from working (container completing stage 1 examination cannot leave).

The computation:

With the above specifications, we model our queuing system (very crudely to provide rule-of-thumb insight) as a simple M/M/a/b queuing model. The first two specifications (M/M) assume a Markovian model for both the arrival as well as service processes (Poisson arrivals and exponential service time), which we recognize as a simplifying assumption. The parameter "a" specifies the number of scanners at stage 2, while "b" represents the number of holding spaces. A simple spreadsheet model is constructed to compute the probability that the system is in various "states." In this simple model, a state is defined as the number of containers at stage 2, those being scanned plus those waiting in the holding area. Once the probabilities are computed, we can compute the metrics as specified earlier.

First order sensitivity considerations:

Table A1 provides qualitative impact of system metrics (columns) when we change the value of system parameters (rows). A "plus" sign in the matrix indicates that an increase in the system parameter will result in an increase in the corresponding metric. A "minus" sign indicates the opposite effect. The exact magnitude of the change depends on the preset values of the other system parameters.

Table A1: Qualitative Model Response Matrix

	Processing time for all containers	Utilization of stage 2 machines	Blocking probability when all stage 2 machines are busy
# of containers	+	+	+
# of stage 1 machines	-	+	+
# of stage 2 machines	-	-	-
Holding capacity	-	+	-
Certified containers %	-	-	-
Prob (C-containers pass stage 1)	-	-	-
Prob(NC-containers pass stage 1)	-	-	-
% of C-P containers exempted	-	-	-
% of NC-P containers exempted	-	-	-
T1: stage 1 time	+	-	-
T2(C-P): stage 2 time	+	+	+
T2(C-F): stage 2 time	+	+	+
T2(NC-P): stage 2 time	+	+	+
T2(NC-F): stage 2 time	+	+	+

Container classification: C: Certified, NC: Non-Certified, P: Passing stage 1, F: Failing stage 1

Other considerations

There are two types of false alarms:

- False positive: a container is declared a "fail" after stage 2, but that it is a false alarm. False positive creates major disruption in port operation. The exact degree of disruption depends on the designed response, which is outside the scope of this appendix. Such disruption imposes economic cost as well as psychological harm. It may also induce indifferences when the next alert arrives. Therefore, it is desirable to reduce the frequency of its occurrence.
- False negative: a container passes all inspection to leave the system when, in fact, it contains materials we intend to detect. The cost of such event is obvious. Thus, we should minimize the probability of such occurrences.

We can decrease the occurrence probability of these undesirable events by increasing the processing time at both stages. More careful and deliberate attention at both detection/scanning stages provides better discrimination between the presence and absence of the materials we intend to detect. However, increasing container inspection time at the two stages will contribute to the increase in overall processing time of a shipload of containers, as indicated in the table above. Table A2 provides a sample strategy to maintain an acceptable level of false alarms while keeping the processing time of a container ship constant. This will obviously result in additional cost in equipment: a tradeoff to be made in the overall system design process. A "plus" entry means an increase in the associate system parameter.

Test Bed:

In order to understand the relationship between false alarm and processing time, we need extensive testing to collect reliable and robust statistical data: how to design an optimal test procedure (minimizing alarm rates with a constant inspection time) and how to determine test sensitivity level to declare whether a container passes or fails inspection. Obviously, a decision to pass or fail a container entails a tradeoff between false positive and false negative event occurrences. A stringent pass criterion will decrease the likelihood of false negative events while increase that for false positive events. A more lax pass criterion will have the reverse effect. Therefore, a careful

tradeoff analysis will need to be performed. Our main report contains a discussion of the need for rigorous experimentation.

Table A2: A Sample Strategy To Minimize False Alarms

	Lowering the level of false alarms while keeping in check system processing time
No. of stage 1 machines	+
No. of stage 2 machines	+
Holding capacity	+
% of C-P containers exempted	-
% of N containers exempted	-
T1: stage 1 time	+
T2(C-P): stage 2 time	+
T2(C-F): stage 2 time	+
T2(N-P): stage 2 time	+
T2(N-F): stage 2 time	+

Container classification: C=Certified, N=Non-certified, P=Passing stage 1, F=Failing stage 1

Optimization:

An interactive optimization approach can be designed to consider and balance the tradeoff amongst various system metrics in the search for a set of optimal system parameters. The tradeoff has to be made between cost, time and false alarm rates. We suggest an interactive optimization platform so that a decision-maker can make intelligent tradeoff when the help of computerized decision support system. Such a decision support system will also allow for the evolutionary design of the monitoring system when new technology emerges or when new tradeoff has to be made. An interactive decision support system also allows an individual port to set its own criteria or to react to emergency situation (e.g., when new intelligence information indicates a high likelihood of smuggled radioactive contraband materials). Another use of an interactive optimization system is to evaluate the impact of policy changes: how desirable is it to increase the percentage of certified shippers? A well-designed system should allow sensitivity analysis of a combination of external as well as internal factors.

Full-scale analysis:

A more detailed and accurate analytical model is needed to examine the interaction of all the system parameters with greater fidelity. Another approach is the development of a full-blown simulation model to follow the flows of containers through the detection system. Such an effort is under way at the Los Alamos National Laboratory. In the mean time, analytical modeling should provide valuable insight and guidelines as we move towards the evolutionary design of such an inspection system.

Conclusion

We have created a simple queuing model to examine the first order impact of various system metrics when the system parameters are changed. The value of this simple model is to identify critical elements of the system to be isolated for more in-depth examination. More detailed system modeling and analysis is essential in the design of a real inspection system.