Decision-level Information Fusion to Assess Threat Likelihood in Shipped Containers

Justin M. Beaver, Ryan A. Kerekes, and Jim N. Treadwell

***Abstract*—A significant challenge in the distribution of goods is assessing the potential threat that an individual shipping container poses. Due to the high volume of shipped goods, a primary concern is balancing accuracy and container scan time. The application of information fusion to the problem enables automated threat determination and the presentation of relevant data to an operator, in a decision support capacity, in order to maintain a sufficient level of processing. This paper outlines an approach to container threat assessment that combines data from multiple sources in order to reliably score the likelihood that a given container holds a threat. Fused data is also leveraged as a tool to optimize the routing of containers through a scanning system comprised of multiple data acquisition stations and providing data in multiple modes. Furthermore, we propose methods for the consolidated presentation of fused data to an operator in order to both minimize the time expended in container evaluation and maximize the accuracy of the assessment.**

***Index Terms*—Bayesian networks, Information fusion, Intelligent systems, Threat analysis**

I. Introduction

As countries are forced to account for the threats posed by the tactics of small, subversive groups operating within their borders, they are becoming more aware of the vulnerabilities in their shipping infrastructures [2]. It is desirable to have a high degree of confidence that the contents of each shipped package or container pose no threat to various personnel or resources in the freight industry, or to shipping customers. The primary barrier to the analysis of each shipped container is the considerable expense of time to inspect the contents. For example, the throughput of air cargo shipped each day would be reduced to 4% of its current volume if manual inspections of each cargo container were introduced into the processing flow [1]. In response to the contradictory priorities of both threat assessment and efficiency in container processing, it has become a high-priority need to be able to rapidly discriminate between harmful and benign packages.

This research addresses the need for a technology that can combine information from disparate data sources in order to provide a reliable threat assessment for a shipping container, and can present the fused data such that an operator can rapidly discern its threat potential. Shipped containers inherently include different modes of data that characterize their contents and provide opportunities for analysis. Textual data in the form of manifests or receipts can provide information about the expected contents of the container and other attributes such as expected weight, shipping source, and destination. Numeric data, such as the measured weight or detected radiation counts, are typically available during the processing of shipped containers and provide a basis for comparison to the text data. Image data provide views of the container after a particular imaging technology has been applied. For each of these source data modes, analysis technologies exist that can highlight those features that are of interest in containers. The goal of this research is to merge the relevant features, surfaced during data analysis, to provide an accurate threat assessment for an operator.

Section II provides a summary of the related work in this field. Section III describes in detail the methodology used to both fuse data and present that data to the operator. Section IV contains the results of implementing a simulation that demonstrates these technologies and gives an analysis of the resultant product. Section V concludes the paper..

II. Related Work

Information fusion (IF) is defined as the combination of data from disparate sources to produce an outcome that is superior to any provided by an individual source. A superior outcome typically includes an improvement in accuracy, higher confidence through complementary information, or improved performance in the presence of countermeasures [9]. Our research merges multi-modal, multi-source data in order to ascertain the presence of a threat in a shipping container. In

Manuscript received April 23, 2009. Prepared by Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6285; managed by UT-Battelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR2225. This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 for the U.S. Department of Energy. The United States Government retains and the publisher, by accepting the article for publication, acknowledges that the United States Government retains non-exclusive, paid-up, irrevocable, world-wide license to publish or reproduce the published form of this manuscript, or allow others to do so, for United States Government purposes.

J. M. Beaver is with the Applied Software Engineering Research Group at the Oak Ridge National Laboratory, Oak Ridge, TN 37831-6085 USA (phone: 865-576-0327; fax: 865-241-0337; e-mail: beaverjm@ornl.gov).

R. A. Kerekes is with the Image Science and Machine Vision Group at the Oak Ridge National Laboratory, Oak Ridge, TN 37831 USA. (e-mail: kerekesra@ornl.gov).

J. N. Treadwell is with the Applied Software Engineering Research Group at the Oak Ridge National Laboratory, Oak Ridge, TN 37831-6085 USA (e-mail: treadwelljn@ornl.gov).

this section, the relevant prior work in the fields of information fusion and container threat assessment is presented.

IF is a complex process that involves the acquisition of raw data, the transformation of that data into a suitable format, and the merging of transformed data into a composite form that highlights interesting underlying features. These coarse stages in the IF process are often referred to as the *levels* of information fusion [16]. Sensor-level fusion is the level at which relevant data is extracted from the source signal. Feature-level fusion is the combination of data to produce a composite feature vector that characterizes the object under test. Decision-level fusion is the layer that provides a projection of a future state of the object based on the feature vector provided, and is the information presented to an operator to facilitate a human decision. Related to these different levels, Dasarathy [17] characterized IF in terms of the input/output characteristics of a given fusion function: Data in-Data out, Data in-Feature out, Feature in-Feature out, Feature in-Decision out, and Decision in-Decision out. Thus, an IF architecture is simply the combination of these different types of fusion functions to produce a holistic decision support IF system.

The Joint Directors of Labs (JDL) have developed the most prominent model of information fusion. The JDL fusion model and its revisions [8] [12] [13] focus on maximizing the automation of fusion. It breaks data fusion into five levels, each of which further refines the data from the acquired state to a form that both adequately represents the entities and their environment and is actionable. Much of the literature surrounding IF focuses on the various levels of the JDL model to create and optimize algorithms that merge sensor data in a complex and dynamic space. Automated target location, identification, and tracking are central themes in this type of fusion.

Situational awareness (SA) is an extension of IF which focuses on incorporating human decision-making in the IF process. Endsley's model of SA [11] defines three levels that include Perception of the various relevant elements in the environment, Comprehension of the patterns that are recognized through analysis or evaluation, and Projection of the likely future states based on the understanding of the current state. The levels proposed in the SA model are analogous to the sensor, feature, and decision levels described in [16]. SA systems are by design semi-automated and allow for a Human in the Loop (HIL) to make decisions. The IF framework proposed in this research is likewise intended to be an HIL system; providing decision support to an operator that must analyze thousands of containers per day in a typical shipping pipeline.

The operational concepts for container processing systems are consistent with the SA model. These systems are expected to provide decision support to an operator in such a manner that maximizes accuracy and efficiency [14]. The physical analysis of shipping containers is a unique problem due to the large size of the containers, the heterogeneous nature of its contents, and the non-uniform arrangement of objects. Work has been done to address the challenges shipping containers pose to imaging systems [18] [10], or to fuse information to provide SA at container processing facilities [20]. However, little work has been done to apply IF in order to assess the threat associated with individual containers.

Sokol [19] proposed a generic framework for transforming heterogeneous data associated with shipping companies and containers into a knowledge base that that identified entities and their relationships. The work focused on the analysis of raw text to identify patterns and inconsistencies in extracted entities and relationships. However, to our knowledge, no work has been done to provide a decision-level fusion model for data associated with shipping containers in order to optimize routing through a system or produce a reliable multi-threat assessment.

III. Methodology

This section describes the technical approach to applying decision-level information fusion to the problem of container threat assessment. As a precursor to identifying threats in containers, those threats must be itemized and organized such that a series of discrete tests may provide clues to their presence. Section A describes the system and data that were considered and Section B outlines the taxonomy of threats that were addressed in this research. Section C details the methods used in constructing the probability network for threat assessment. Section D addresses the specific issue of presenting the fused data to minimize the assessment time for an operator.

A. System Architecture

This research is predicated on a multi-faceted container analysis system comprised of interrogation devices, passive detectors, and electronic access to both the container's manifest and a government program similar to the Known Shipper Database [7]. Thus, a variety of data modes are expected to be available for analysis including scanned images, sensor readings, and electronic text documents. Small-scale instances of this type of system are currently available commercially, and programs are underway to construct large-scale multi-modal container scanning and detection systems to meet the needs and interest expressed by government leaders. The thrust of this research is to provide a methodology for decision-level fusion of these data to provide a reliable container threat assessment.

Any container analysis system that incorporates multiple approaches to acquiring and analyzing data must also have an approach for merging the results of those independent analyses in order to present a consistent assessment to an operator. The information fusion system designed for this research assumes the existence of a support framework that

includes acquisition of data from a container measurement or scanning devices (Sensor-level fusion), and the analysis of the acquired data item to produce a feature vector (Feature-level fusion). Information is fused at a high level and incorporates the various feature vectors uniquely produced for each data source as depicted in Fig. 1. This architecture is based on Endsley's model of SA [11] with stages for Perception, Comprehension, and Projection. The focus of this work is the Projection stage – using extracted feature sets to predict the presence of a threat through decision-level information fusion.

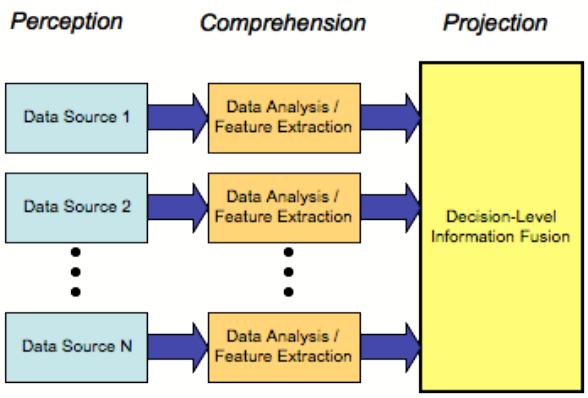

Fig. 1 Container Analysis Fusion Architecture

As a container is routed through the various interrogation and measurement stations, data becomes available and added to the body of evidence with respect to any potential threats. The *Perception* stage of the architecture is the sensor-level fusion represented by the *Data Source* blocks in Fig. 1. This stage is concerned with the acquisition of raw data in its native mode. The data at this level is the images acquired from scanning devices, the raw text of the electronic manifest, or the measurement value from the radiation detector. The acquired data is then transformed into a form suitable for fusion in the *Comprehension* stage. This stage typically involves populating a set of pre-defined features based on algorithms run against the raw data. For example, the average density of an object in an X-ray projection might be calculated and stored as a feature. Similarly, the name of a shipper might be extracted from the electronic manifest and vetted against a collection of known shippers; the result of which could be stored as a feature. The result of the *Comprehension* stage is the set of features pre-defined through the threat taxonomy (see Section B) as relevant in the threat assessment. The set of features is the input to the *Projection* stage, where decision-level fusion is implemented. It is in the *Projection* stage that this research is focused and where the threat assessment framework (see Section C) is implemented.

The decision-level fusion for shipping container processing developed in this research considers three modes of data from several different sources. Each item of data considered for this research is derived from a data source through direct measurement, text entity extraction, or image analysis. Table I describes each data item used in this research, and the data source for the item. The data items selected are intended to be representative of the types of data available for shipping container information fusion, as specified in [10].

TABLE I
AVAILABLE SHIPPING CONTAINER DATA

Data Item Description	Data Source
Container ID: The unique identifier for this container.	Shipping Manifest
Shipper Information: The name and address of the shipper.	Shipping Manifest
Destination Information: The name and address of the consignor.	Shipping Manifest
Commodity: A classification of the nature of the goods being shipped.	Shipping Manifest
Shipped Weight: The recorded weight of the container.	Shipping Manifest
Measured Weight: The weight as measured during processing.	Scales
Measured Radiation: Radiation levels detected during processing.	Radiation Portal
Measured Dimensions: The measured container dimensions.	Container Pre-processing
Raw Image: A digital image of the exterior of the container being processed.	Container Pre-processing
2-D Scanned Images: Two-dimensional images using X-ray or similar technology.	Scanning Station
3-D Scanned Image: Three-dimensional image using computed tomography (CT) or similar technology.	Scanning Station

B. *Threat Taxonomy*

This research focuses on combining data to infer the presence of specific types of materials (e.g., explosives or radiological/nuclear) inside cargo containers, placed with the intent of transporting these materials illegally or inflicting damage or injury during transport. In order to combine data successfully, an organization of threat data must be developed that enables the dissection of an overarching threat into finer-grain components, and maps those components to the features provided in the *Comprehension* phase of the fusion architecture.

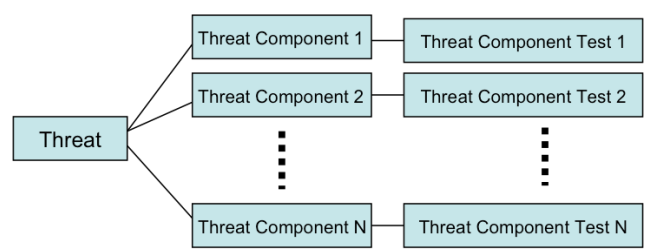

Fig. 2 Taxonomy describing threats to shipping containers.

Fig. 2 shows the abstract taxonomy that divides a threat into its compositional elements, called *threat components*, which, in the case of shipping containers, are distinct characteristics of the threat that may be acquired from a given container. The threat components represent features, or pieces of evidence, in determining the existence of a threat. The presence of one or more of these components is determined by a *threat component test*, and provides evidence towards whether the higher order threat exists. The threat component test is

typically accomplished through an appropriate data analysis or feature extraction method performed during the *Comprehension* phase.

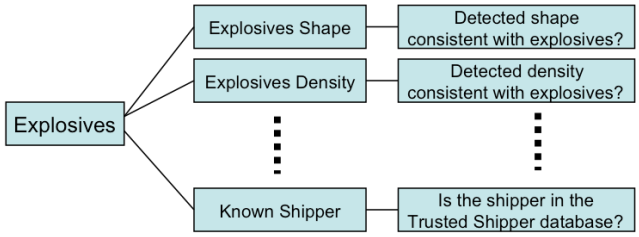

Fig. 3 Partial taxonomy of a notional explosives material threat.

Fig. 3 illustrates the application of the abstract taxonomy to a concrete example: an explosives threat. An "Explosives" threat means that the system should be focused on identifying the likelihood of explosive materials being present inside the shipping container. In order to tune the fusion framework to this specific threat, "Explosives" must be represented in the taxonomy as a collection of *threat components* that are both relevant in identifying explosive materials and also available in the set of container data (see Table I). For this example, a set of threat components associated with explosive materials would likely include features such as the shape or density of objects in the container, and whether the shipper of the container is known or trusted. Each of these components is further described in terms of the *threat component test* that distinguishes whether the component has been detected. For example, in the case of the "Explosives Shape" component, the discriminating test would be whether the image analysis software identified an object within the container that has a shape consistent with that of a commercially available explosives device.

A particular threat has physical characteristics that can be detected through signatures and observables revealed during the various physical data acquisition processes. Threat components such as shape, density, and radiation levels are examples of such characteristics. Threats also have non-physical characteristics that may be detected through acquiring more abstract attributes of the shipped container. Data items that primarily can be gleaned from the manifest, such as shipper information and commodity, fall into this category. Both the physical and non-physical characteristics of threats are treated equally in the threat taxonomy. The taxonomy structure does not attempt to convey significance of each threat component, as that is managed through the probability values developed for threat assessment.

Organizing threats in terms of their components and associated component tests allows for a flexible taxonomy. Threat components can be added, removed or modified based on the testing equipment available, the analysis environment, or the types of expected threats. In addition, this organization lends itself to driving the structure of the probability network used for threat assessment.

C. *Threat Assessment*

Determining the probability of a given threat requires combining the threat components into a mathematical framework such that the presence or absence of those components affects the likelihood that the threat exists. In addition, the probability model for the threat and its components must tolerate data that is uncertain or unavailable. For example, a practical scenario in a container analysis system is one where a container's manifest cannot be retrieved by the computer. In such a situation, it is undesirable for the system to be unable to assess the threat for that container; rather, it should carry out the analysis with minimal loss in accuracy despite the now unavailable data source.

Bayesian belief networks were selected as the mechanism for probabilistic threat assessment, and for modeling threats in terms of their components. A Bayesian belief network (BBN) is a network of nodes connected by directed arcs. Each node in the network represents a random variable in the model, and each arc signifies a cause-effect relationship between the variables. Thus, there may be several arcs leading to or from any given node, but there can be no cyclic relationships. The probability function associated with each node is the joint probability distribution of inputs to outputs. BBN node values are represented as discrete variables, and so can accommodate both subjective and objective data. They can adapt to an environment as data is processed, can infer unknown model elements based on known model elements, and perform well in the presence of uncertain or unavailable data [6].

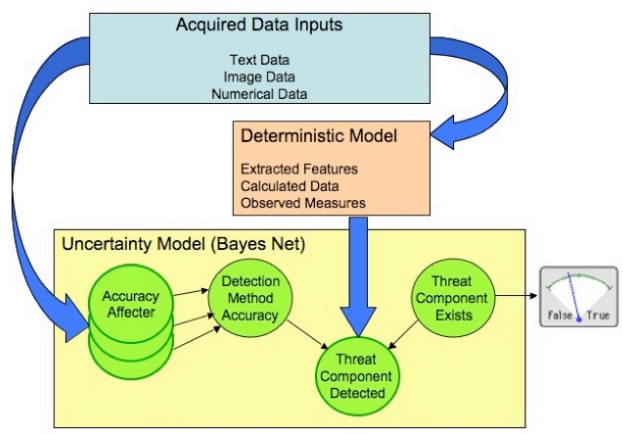

Fig. 4 Design of the Bayesian network for assessing threat components.

Fig. 4 depicts the design for determining the presence of each individual threat component. The circles represent the random variable nodes in the BBN, and the directed arrows are the arcs that depict cause-effect relationships. For each threat component, one or many detection methods may be available. Each detection method performs more reliably under some conditions and less reliably under other conditions. The BBN captures this uncertainty by accounting for the characteristics of the container that affect the accuracy of a given detection method. For example, the type of

material inside the container greatly affects the accuracy of an X-ray transmission detection method. A container packed densely with frozen foods is much more difficult to scan than a container packed sparsely with fresh flowers. Similarly, for each detection method, there are container characteristics that impact the accuracy of the test. The BBN accounts for this by using an intermediary node that summarizes the detection method's accuracy based on the given conditions.

Acquired data, in the form of raw text, images, and numerical measurements, are processed using state-of-the-practice techniques to extract features and entities, and to make the determination of whether a threat component was detected. The "Threat Component Detected" node has two states (*True*, *False*) and is the means for incorporating the results of the deterministic models into the overall model. The BBN is designed such that findings are determined for both the "Detection Method Accuracy" and "Threat Component Detected" nodes for each processed container. Once those nodes are established, the structure of the network allows for the propagation of belief to the "Threat Component Exists" node, which is also a two-state node (*True*, *False*). The output of the threat component model is a level of belief, or probability, that the given threat component actually exists based on detection result and on the factors that are affecting the detection method accuracy. This framework is applied to each threat component that has been identified for a threat, according to the taxonomy described in Section B.

The uncertainty model associated with each threat component also provides an effective means for container routing. Based on the input characteristics of the container (i.e., Accuracy Affecter nodes), detection method accuracies can be inferred. Thus, a container may be routed through the system to maximize the likelihood that a given set of detection methods will yield correct results, and not false positives or false negatives. For example, if a container analysis system is comprised of both an X-ray backscatter device and a neutron radiography device, how should an operator route the container for analysis? The probability of an accurate reading is captured by each of the detection methods' "Detection Method Accuracy" node in the uncertainty model. Thus, the model provides an automated means to route containers to the systems that will yield the most accurate results given the container's physical characteristics and scan time constraints.

Once the likelihood of each Threat Component is determined, the second tier of the BBN (see Fig. 5) combines each component to determine the likelihood that the overall threat exists. As with each threat component, the "Threat Exists" node is a two-state node (*True*, *False*) that reflects whether the system believes the threat exists based on the fusion of all of the information. In addition to a *True*/*False* value, the BBN provides a probability, or degree of confidence, that the assessment is accurate. The probability is useful in conveying to an operator the level of confidence that a particular threat exists.

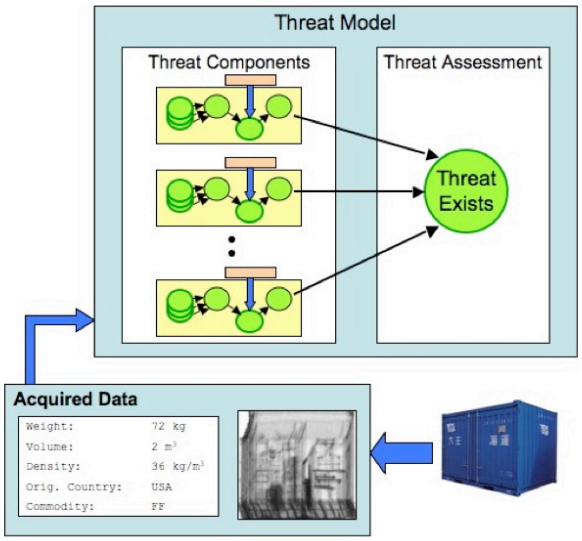

Fig. 5 Design of the Bayesian network for assessing overall threat.

The use of container threat components in our design provides flexibility in combining data elements. Consistent with the threat taxonomy, threat components are easily added to or removed from the BBN depending on the types of data sources that are available and the types of discrete tests performed on each extracted data item.

D. Visualization and Data Presentation

Visualization of threat probabilities is an important part of communicating potential threats to an end user. In cases where the threat indicator is localized (e.g., a specific region of a container), it is important to convey the location of the threat relative to the overall cargo container. From a data fusion standpoint, presenting all available relevant information in a clear, concise, and compact way is a key factor in maximally utilizing human expertise in a screening system.

We developed a simple visualization technique to illustrate the presentation of threat information to a user. This effort derives from previous work in data fusion and modeling and draws on the visualization capabilities provided by the widely used Visualization Toolkit (VTK) [4], an open-source software package developed by Kitware, Inc. The visual presentation of three-dimensional image data highlights areas of interest within the scanned container that are consistent with signatures associated with threats. In conjunction, a fading capability has been incorporated into the visualization to further distinguish objects of interest. To demonstrate this approach, we present two views of the contents of a specific container. Fig. 6 gives the user an idea of the overall content of a container densely stacked with material. The white color is used to denote objects that were not determined to be suspicious when image analysis algorithms were applied. Fig. 7 shows suspicious material (regions with high threat probability) highlighted in red, while the surrounding benign material has been faded.

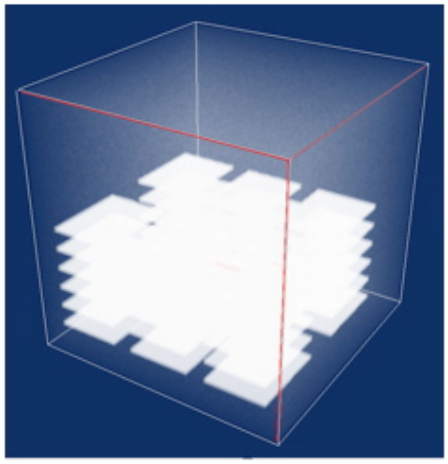

Fig. 6 3-Dimensional visualization of a shipping container.

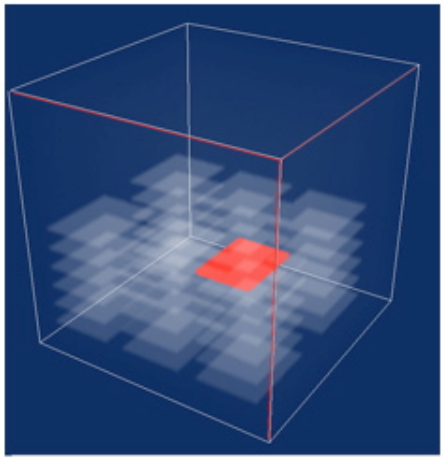

Fig. 7 Fading of characterized non-threat material.

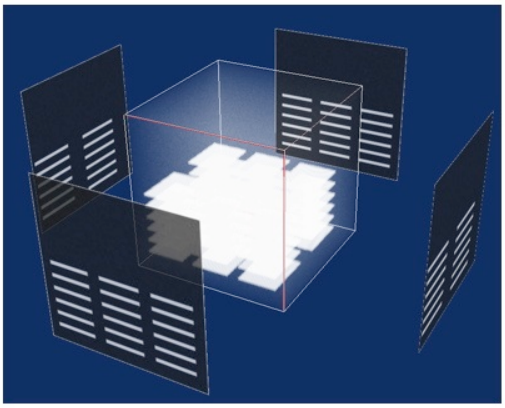

Fig. 8 Integrated visualization of volumetric and X-ray backscatter imagery.

In addition to highlighting suspicious objects/areas within a three-dimensional space, it is desirable to present multiple imaging modalities simultaneously in order to minimize assessment time for an operator, and give a positional context for all two-dimensional images acquired in the assessment process. Fig. 8 illustrates how multiple imaging modalities (e.g., backscatter and X-ray CT) may be combined into a single display for a comprehensive view of threat information. In this example, four simulated X-ray backscatter images are combined with the three-dimensional CT image presentation. The result is a visualization that gives the operator a context for the set of two-dimensional images provided, and also gives the depth and material highlighting capabilities associated with the 3-D image data.

IV. Implementation

An information fusion system for prototype container analysis was developed for this research. The system includes an operator interface that provides a view into a notional container processing system, and a back-end simulation that represents the environment and systems used for container processing. The software is written in the Java programming language and leverages the Netica libraries [3] for BBN implementation and the Visualization Toolkit (VTK) for image and volume visualization [4].

The goal of the container threat assessment system prototype is to demonstrate how fused data can be presented to an operator, and how that presentation could expedite the analysis of the threat potential each container poses. Fig. 9 shows the developed operator interface. The focus of the interface is the visualization that combines multiple imaging modalities in order to present all relevant imaging data simultaneously. The resultant image view may be rotated or zoomed using the mouse or control buttons provided on the interface. Also included is a space to present an image of the container as it was received in the shipping area. This provides a context for the operator in discerning the size and shape of the package.

Anomalies and threat assessments are elevated to the operator's attention through colorful graphics. The threat score is the probability of a given threat being present in the container, and is communicated through both a meter and a colored icon located in the southeast area of Fig. 9. The threat score icon's color maps to a 0.2 interval in the threat probability range, and is based on the Department of Homeland Security's Color-coded Threat Level System [5]. This provides the operator with an immediate visual cue of the potential for the threat to exist. In addition, the results of tests associated with container attributes are visually presented to the operator in the form of green checkmark or red 'X' icons in the Container Details panel. The icons reflect the success or failure of tests specific to a particular container detail. For example, a green check beside the measured weight of a container indicates that the results of the tests associated with the weight of the container were favorable: the measured weight is consistent with the weight recorded on the manifest, and the weight is consistent with statistical data for that commodity type. Based on the information presented, an operator chooses to clear the cargo, quarantine the cargo, or route the cargo for further processing at a downstream testing station. A decision from the operator is required for each stop a container makes in the system.

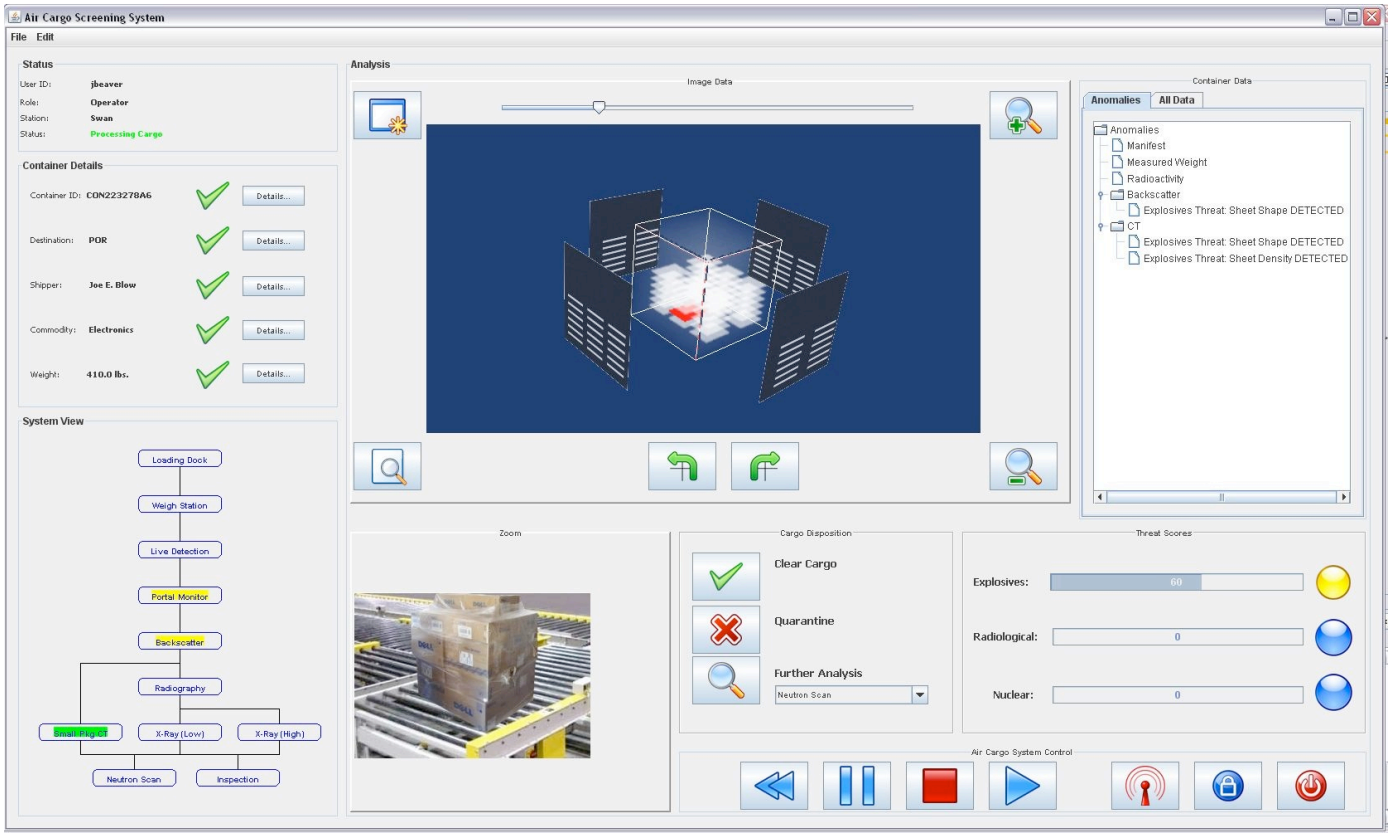

Fig. 9 Container threat assessment operator interface.

A System Viewer (located in the southwest corner of the interface) presents the system as a whole, including paths between testing stations and decision points. This gives an operator a context for the entire system, including all of the testing equipment available to consider in container routing. The presence of a container in a testing station is denoted by a yellow rectangle in the station. A green rectangle identifies the specific container for which the operator is making a decision. This view gives an operator a visual designation for the container being processed, the extent of data that has already been collected for the container, and the available options for routing the container through the system.

V. Conclusion

This research details an approach to the decision-level fusion of disparate information to produce an assessment of the presence of a threat in a shipping container. Information fusion was achieved by leveraging Bayesian belief networks for probabilistic threat assessments and the by developing a novel approach to presenting multimodal image data. A prototype system was developed to automate the information fusion and data presentation for a simulated container processing system. The operator interface for this system maximizes the use of visual cues for the automated container threat assessment in order to minimize the time required for operators to digest the quantity of information and rapidly discern an appropriate response.

The underlying Bayesian network used for threat assessment was intentionally designed such that its structure would mirror the taxonomy designed for a specific threat. It is the definition of the taxonomy, in terms of threat components and associated tests, for each threat that is critical to the implementation of this framework. The inherent consistency between the data organization and the probabilistic network allows for flexibility in terms of the taxonomy of threats. The method easily accommodates multiple instances of both threats and threat components, and can be quickly tailored to the testing equipment available in local container processing environments.

This threat assessment framework is currently designed to targets terror-oriented threats, but it is easily extended to support assessments for the presence of drugs, weapons, and other contraband provided that the threat has similarly defined components, such as shape and density characteristics. The versatile nature of this approach has prompted us to pursue applications in areas outside of shipping container threat assessment, including threat assessment for cyber security systems and for modeling social stability. Our future work for this research includes expanding it to these domains, and also validating the shipping container threat assessment model and architecture in an operational setting.

REFERENCES

[1] G. Schneider. "Terror Risk Cited for Cargo Carried on Passenger Jets; 2 Reports List Security Gaps." *The Washington Post,* June 10, 2002.

[2] B. Elias. "CRS Report for Congress: Air Cargo Security." Congressional Research Service, July 30, 2007.

[3] Norsys Software Corporation. "Netica (online)." In http://www.norysys.com, Vancouver, Canada, 2008. Norsys Software Corporation.

[4] Kitware, Inc. *The VTK User's Guide.* Kitware Inc., USA.

[5] Department of Homeland Security. "Homeland Security Advisory System (online)." http://www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm, Washington, D.C., 2008. United States of America Department of Homeland Security.

[6] S. Russell and P. Norvig. *Artificial Intelligence: A Modern Approach.* Prentice Hall, Upper Saddle Ridge, NJ, 2nd edition, 2003.

[7] Transportation Security Administration. "Known Shipper Database (online)." http://www.tsa.gov/what_we_do/layers/aircargo/database.shtm, Arlington, VA, 2008. United States of America Transportation Security Administration.

[8] Data Fusion Subpanel of the Joint Directors of Laboratories. "Data fusion lexicon." In Technical Panel for C3, 1991. United States of America Department of Defense.

[9] E.P. Blasch and S. Plano. "JDL Level 5 fusion model: user refinement issues and applications in group tracking." SPIE Vol. 4729, *Aerosense,* 2002, pp. 270-279.

[10] Stanford University Study Group, Center for International Security and Cooperation. "Detecting Nuclear Material in International Container Shipping: Criteria for Secure Systems." *Journal of Physical Security,* Vol. 1, No. 1, 2004.

[11] M. Endsley. "Toward a Theory of Situational Awareness in Dynamic Systems." *Human Factors Journal,* Vol. 37, pp. 32-64, 1996.

[12] A.N. Steinberg, C. Bowman, and F. White. "Revisions to the JDL Data Fusion Model." *NATO/IRIS Conference,* October 1998.

[13] J. Llinas, C. Bowman, G. Revora, A. Steinberg, E. Waltz, and F. White. "Revisions and extensions the JDL Data Fusion Model II." In *Proceedings of The 7th International Conference on Information Fusion,* pp. 1218-1230, 2004.

[14] B. Torell and S. Fiorillo. "Network Centric Principles and World Cargo Security." In Proceedings of *The 11th International Command and Control Research and Technology Symposium,* Cambridge, UK, September 2008.

[15] J. McGowan. "Crime and Security in U.S. Seaports." In *Cargo Clearance, Security, and Safety Panel Session, Global Intermodal Freight: State of Readiness for the 21st Century,* February 2000.

[16] L.A. Klein. *Sensor and Data Fusion: A Tool for Information Assessment and Decision Making.* SPIE Press, Bellingham, Washington, USA, 2004.

[17] B.V. Dasarathy, *Decision Fusion,* IEEE Computer Society Press, 1994.

[18] K. Kim and J. Cho. "Recognition of Identifiers from Shipping Container Images Using Fuzzy Binarization and Enhanced Fuzzy RBF Network." *Soft Computing – A Fusion of Foundations, Methodologies and Applications,* Vol. 11, Iss. 3, October 2006.

[19] L. Sokol. "Creating knowledge from heterogeneous data stove pipes." In *Proceedings of the 5th International Conference on Information Fusion,* pp. 1162-1167, 2002.

[20] B.J. Rhodes, N.A. Bomberger, M. Seibert, and A.M. Waxman. "Maritime Situation Monitoring and Awareness Using Learning Mechanisms." In *Proceedings of the Military Communications Conference, 2005.*