SECURE CARGO CONTAINER AND SUPPLY CHAIN MANAGEMENT BASED ON REAL-TIME END-TO-END VISIBILITY AND INTRUSION MONITORING

AVANTE International Technology, Inc.
70 Washington Road, Princeton Junction, New Jersey 08550, USA
www.avantetech.com

The Challenge of Supply Chain

"Needle-in-a-haystack" is a frequently and deeply felt syndrome challenging security professionals trying to isolate specific problem containers from the 21,000 containers arriving daily at US ports and the millions arriving worldwide yearly.

Disruption of shipping and trade caused by potential weapons of mass destruction (WMD) using containers as a Trojan horse is one scenario that hounds all experts in custom and homeland security.

Many solutions based on smart locks and seals have been examined and extensively tested since 9/11 [1,2,3,4,5,6,7,8,9]. Most of the current proposed solutions focus on the electronic lock, seal and gasket sensor on the container door. They do not address the problem of intrusion through other surfaces of the container not touching the lock and seal or gasket or the contents stuffed inside the containers [10,11,12].

Table 1 (below) is a list of the basic challenges and the desired solutions.

TABLE 1: SUPPLY CHAIN SECURITY CHALLENGES

Challenges	Solutions
1. Impossible to inspect all of the containers or even 10%.	▪ Monitor, track and trace every container from stuffing, loading, transit, rerouting, and disposition. Use secured stuffing sites only. ▪ Incorporate an automatic real-time locating and monitoring system for every container. ▪ Maintain real-time visibility and monitoring of all containers and supply chain including any tampering after sealing. ▪ Ability to detect any intrusion inside the container during all phases of transport from factories to shelves.
2. No way to know if tampering occurs during transit and too late to prevent loss upon arrival at unloading port.	▪ Real-time reporting of any exception and incidence to destination custom and port authorities for deterrent action before arrival. ▪ Smart seals incorporating an active tag on the outside of the container or incorporated as part of the outside container seal. [5,6,7,8] The problem is that such smart seal solutions are only effective if intrusion is through the lock or seal. Reporting of exceptions or problems is not real-time. ▪ Sensors for radioactive, chemical and biological destructive agents integrated inside the container. But problems are not noted until arrival at the unloading port. ▪ Effective solutions will detect intrusion inside the container by any means and through any surface in real-time.
3. Cannot be sure whether any contents may contain weapons of mass destruction (WMD)	▪ Ideally secured stuffing locations are used for containers. ▪ Place monitoring RFID devices integrated with radioactive, chemical and biological sensors inside the container upon sealing. ▪ Monitor any tampering and activities inside containers with RFID-sensors during transit from starting point to the container loading port. Open the seal and retrieve sensors to verify the safety of items inside containers. . Replace sensors and place lower cost RFID devices inside the containers before loading onto an international carrier. ▪ Suitable public independent monitoring agencies can be linked and used as the clearinghouse of all monitored data to solve the last three out of four core elements of the "Container Security Initiative (CSI)": o Using intelligence and automated information to identity and target high-risks containers; o *Pre-screening those containers identified as high-risk, at the port of departure, before they arrive at U.S. ports;* o *Using detection technology to quickly pre-screen high-risk containers; and* o *Using smarter, tamper evident containers.*

Considerations for an Effective Intrusion Detection Solution

A "smart box or smart container", foretelling the presence of WMD inside a container, is a dream solution. Almost all the proposed solutions for smart containers are based on securing the locking mechanism by monitoring tampering (usually by breakage) of part of the RFID seal. Some monitor the tie-string of the seal while others measure the breakage of the lock-pin or other integral parts of the seal. GE (with partnership of Allset) monitors the changes of pressure on the gasket on the door seal [5].

The proposed solution assumes that intruders will get inside the container to take valuables or place WMD by getting in through the door. By tampering with the door lock seal or the gasket pressure, the intrusion will be detected.

However, as pointed out by many seasoned professionals [9,10,11,12], *"Seals and e-seals detect tampering with a seal, but not container intrusion—despite some manufacturers' marketing claims"* [13]. Monitoring the door seal is only meaningful if the intruder comes in through the front door. It will serve no useful function if intrusion is made through other surfaces of the container by cutting through the steel panel.

Experts in the field want a solution that places monitoring devices inside the container capable of detecting actual intrusion through any surface by any means.

The following table lists some possible physical means to achieve internal detection and possible defeating mechanisms. A new approach to manage this complex problem is also proposed.

TABLE 2: POSSIBLE INTERNAL CONTAINER INTRUSION MONITORING MECHANISMS AND RELATED PROBLEMS

MECHANISM	BENEFITS & SHORT-COMINGS	POSSIBLE DEFEATING MEANS
1. Light	▪ Relative low cost sensor. ▪ Need mechanism to transmit the message of intrusion.	▪ Intruder can use IR or perform intrusion without light.
2. Air Pressure	▪ Relative low cost sensor. ▪ Need mechanism to transmit the message of intrusion.	▪ Pressure can be monitored and compensated relatively easily.
3. Sound	▪ Relative low cost sensor. ▪ Need mechanism to transmit the message of intrusion.	▪ Too many possible noises that can induce false alarms.
4. CO2 or other gases	▪ Relative low cost sensor. ▪ Need mechanism to transmit the message of intrusion.	▪ Intruder can use self-contained breathing device.
5. EMI leakage	▪ May use the active RFID tag itself to transmit signal. ▪ Need outside monitoring device.	▪ Single emitter may have substantial difference in vibration during transit to give false positives.
6. AVANTE ZONER™ method	▪ Use two or more active RFID ZONER™ tags. ▪ Each ZONER™ transmits signals at several discrete power levels. ▪ Use differential signal levels to distinguish sealed and open (or ajar) state. ▪ ZONER™ tags are placed inside container at random positions. ▪ Use outside RELAYER™ network.	▪ Redundant tags to minimize false alarm (both false positives and false negatives). ▪ Use quantitative measure of combined signals to further minimize false alarms. ▪ Almost impossible to defeat even by insiders.

AVANTE developed the patent-pending method of using individual ZONER™ tags each emitting its own discrete power signal. A planned network of RELAYER™ devices is used to provide automatic monitoring and real-time intrusion reporting. The testing done so far is extremely effective with inherent usage costs lower than all other proposed current solutions. Actual intrusion monitoring into the container is now possible. With suitable tracking and monitoring infrastructure, a secure supply chain with end-to-end visibility can be achieved with equitable costs per container. These costs should be inclusive of hardware and the costs of distribution, management and monitoring services. Efficiencies achieved through use of RFID tagging are estimated at $400-$1600 per container which easily absorbs the costs associated with tagging the container [14, 15].

Finding out intrusion or tampering at the unloading port is much too late!

Most earlier e-seal proposals focused on ascertaining whether containers arriving at US ports had been tampered with or had intrusion through the access door of the container. The monitoring network and readers are positioned at unloading ports such as Tacoma Seaport. Not only is this monitoring possibly not effective, it is also too late.

Figure 1A: Discovering intrusion into containers at the unloading port may be too late!

Figure 1B: Discovering intrusion and tampering inside containers at borders is much too late!

Figure 1 (above) is an illustration of how some of the earlier e-seals were checked [3]. Since items are checked at a border or a container port, discovery of tampering or any malicious materials, such as weapons of mass destruction, will be much too late.

An effective solution should give the ability to inspect any exception or potential tampering in international waters or other locations that will minimize potential destruction or damages [16]. Such solutions will require the ability to provide real-time reporting from monitoring systems as the tampering or intrusion happens. The destination custom and port authorities will have the option to inspect the container and ship away from the seaport. If the carrier is trustworthy, the captain and security staff may be asked to inspect and report their findings that possibly include a video feed for monitoring purposes.

End-to-end monitoring helps minimize risks

Most plans for securing the supply chain include the use of secure stuffing locations that are monitored by trusted agents and US custom staff.

Stuffing and monitoring the contents being placed into containers coming to the US is one of the best approaches. However, the security monitoring of inland transport is the single weakest link in the end-to-end process. Using ZONER™ RFID tags equipped with optional radioactive-chemical-biological sensors placed inside the container, along with an exterior mounted monitoring RELAYER™, creates a cost effective solution providing end-to–end tracking and monitoring after container stuffing.

Figure 2 (below) is a solution that may be used for containers during the inland transit from domestic or foreign stuffing sites or factories.

Figure 2: A single RELAYER™ (with internal time clock) placed outside the container monitors access into the sealed container. Redundant ZONER™ devices with optional integrated sensors are used to monitor radioactivity and chemicals inside the sealed container during the inland transit to the port terminal. The devices and the data from the sensor-integrated ZONER™ are extracted upon arrival at the departure port. After a final check, Standard ZONER™ devices are placed inside the container and sealed by terminal management and departing port authorities.

The ability to sort out containers stuffed with WMD before loading onto an ocean carrier represents a major cost effective step in securing the supply chain. The side benefit is the ability to minimize the stolen goods or possible smuggling activities.

End-to-end visibility and security management of the containerized supply chain should cover all phases of container movements:

After ascertaining the stuffing and inland transporting of the containers, continual tracking and monitoring of the containers based on various operational and storage stations must still be vigilantly maintained. Figure 3 illustrates a cost effective way to monitor both stuffed and empty containers while parked inside a container yard or loading terminal.

Figure 3: RELAYER™ ad hoc RF network installed around the yard communicates to the monitoring station all quiescent signals from redundant ZONER™ devices placed inside each container. Tampering and exceptions are reported in real-time to local or destination custom authorities and others with need-to-know. Detailed data is also stored by an Independent Monitoring Agency.

A ship sailing to United States may pass through and stop at as many as 17 ports before arrival. Intrusion could occur while at sea or during stops at other ports. Representing a cost effective solution, Figure 4 below is an illustration of using ZONER™ RFID placed inside the container along with the RELAYER™ monitoring network.

Figure 4: RELAYER™ ad hoc RF network onboard communicates to the monitoring station all quiescent signals from redundant ZONER™ devices placed inside each container. Tampering and exceptions are reported in real-time to destination custom authorities and others with need-to-know. Detailed data is also stored by an Independent Monitoring Agency.

Container Real-Time Locating and Monitoring (RTLM) System- AVANTE CONTAINER-TRAKKER™ Solution

The following is an outline and description of CONTAINER-TRAKKER™ container and supply chain security management system with 100% end-to-end visibility:

1. A set of RFID ZONER™ tags that transmit messages from inside the container. The receipt of a number of specific multiple discrete signals (using AVANTE patent-pending cyclic multiple signal power technology) positively identifies tampering into the container after it has been sealed. The differential signal levels rather than perfect on/off signals minimize tampering related false alarms. Built-in redundancy also helps to prevent false positive and insider tampering.
2. An ad hoc RF RELAYER™ network is used to relay messages from the container ZONER™ devices during both normal and tamper evident conditions. Normal condition and status reports of both the ZONER™ and RELAYER™ network are made periodically. Exceptions and tampering trigger immediate reporting to the proper authorities in real-time.
3. A monitoring and communication computer is housed in a sealed, hardened tamper proof box. This sealed monitoring data and communication “GREEN BOX” is installed by a third party agency to provide true independent reporting and monitoring services.
4. The “GREEN BOX” includes the following sub-systems:
    - A redundant processor and non-volatile memory.
    - A GPS location reporting system.
    - A satellite or other suitable communication means.
    - An optional, multi-channel video digital recording device. Video feeds to destination authorities and independent monitoring agencies are made when possible.
5. A trusted organization, “Public Independent Monitoring Agency (PIMA)”, is chartered to provide the services of receiving all data from the end-to-end visibility process. AVANTE proposes PIMA as a network of companies certified by the World Trade Organization located in the partnering countries.

   The cost for such monitoring services would be paid in part from the fixed container fees paid by shippers.

A cost effective method to foretell the WMD inside the container and the ability to detect intrusion is only the beginning of any security solution. For a secure supply chain management, the system must achieve all four aspects in the Secure Container Initiatives (See TABLE 1). The flow illustration in Figure 5 (below) lists the issues and processes that must be resolved to ensure international supply chain security. A secure supply chain cannot be achieved without technology including detailed process monitoring managed by trained organizations and people among the partnering countries.

Figure 5: A pictorial representation of a secure supply chain management system with 100% end-to-end visibility of containers that are individually monitored and tracked in real-time.

Product Source Security Issues:
- Who shipped the products?
- What are the products?
- Who loaded the products?
- Who checked and sealed the container?

Inland In-Transit Transportation Security Issues:
- Who transported the products?
- Any stop over and other routing issues?
- Any in-transit tampering?

CONTENT AND INLAND IN-TRANSIT MONITORING:
- Integrate the use of chemical, biological and radioactive sensors with AVANTE RFID-ZONER™ inside seals.
- Use external RELAYER™ with internal time clock to monitor any in-transit tampering.
- Record and report all results from sensors during inland transit.
- Manage exceptions and problems.
- At the port, replace sensors with new set of ZONER™ devices sealed under terminal management.
- A third party "Public Independent Monitoring Agency" (PIMA) should be placed in charge of issuing and monitoring all devices and certification.

Terminal and Storage Management Issues:
- Holding area security
- Holding period
- Any consolidation?
- Who checked and sealed the container?
- Any tampering?

Terminal Loading Security Issues:
- Who performs the final check?
- Is container lock or seal used?

TERMINAL AND PORT MONITORING:
- Install RELAYER™ monitoring network and other infrastructure to cover all storage and layover areas.
- Lock and position one or more redundant AVANTE RFID-ZONER™ inside container.
- Monitor and record periodic status reports on the discrete signals received from ZONER™ devices.
- An exterior mounted ZONER™ is used to communicate with the RELAYER™ network collecting data from inside ZONER™ using the highest power discrete signal. Optional integration with chemical, biological, radioactive, and other sensors is possible.
- System gives real-time automatic reports of any unauthorized access or tampering.
- System provides official departure notice to initiate the monitoring system.

International In-Transit Security Issues:
- Any unauthorized accesses to containers?
- Any tampering during transit?

Stop Over Security Issues:
- Any unauthorized accesses to containers?
- Any tampering?

IN-TRANSIT MONITORING:
- Install RELAYER™ monitoring network and other infrastructure to cover all ship deck storage areas.
- Install sealed monitoring "GREEN BOX™" along with appropriate communication devices.
- Report quiescent signals from all ZONER™ devices placed inside every container and the status of RELAYER™ network.
- Real-time and automatic reporting of any unauthorized access or tampering of any container (by monitoring appropriate differential signal strength levels of ZONER™ devices when they are opened or closed) to destination custom and port authorities.

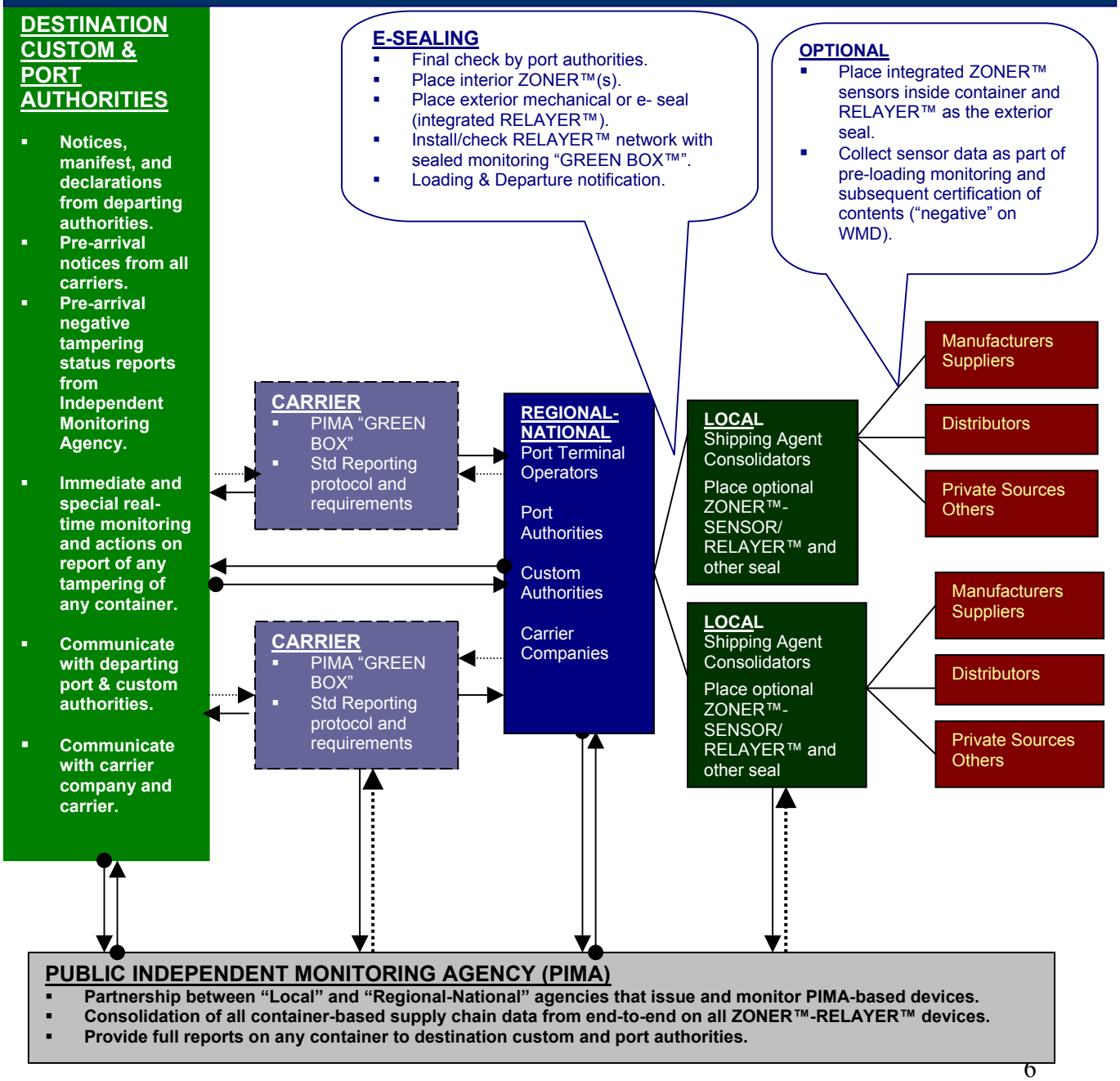
A solution for container and supply chain security and visibility must include a functional real-time monitoring infrastructure and services network

Chris Koch, President of the World Shipping Council once said about the e-seal "smart box" project, *"This is a shipper-applied device. Customs will do the reading of the device. I don't think these particular containers will receive expedited treatment."* (Journal of Commerce Online, November 19, 2003)

The "smart container" solution should not be just the placement of e-seal devices on container doors. The solution must include trusted agents in deploying and placing devices and then monitoring the processes and data from end-to-end. A suitable workflow representing the solution is shown in Figure 6 (below).

A network of trusted monitoring clearing houses of the supply chain data must be established. Also a network of trusted local agents is required to distribute and properly install the monitoring ZONER™ and RELAYER™ devices.

FIGURE 6: Functional Flow-Chart of the Proposed CONTAINER-TRAKKER™ Container Real-Time Locating-Monitoring System and Services



Real-Time Locating & Monitoring (RTLM) Container and Supply Chain Services

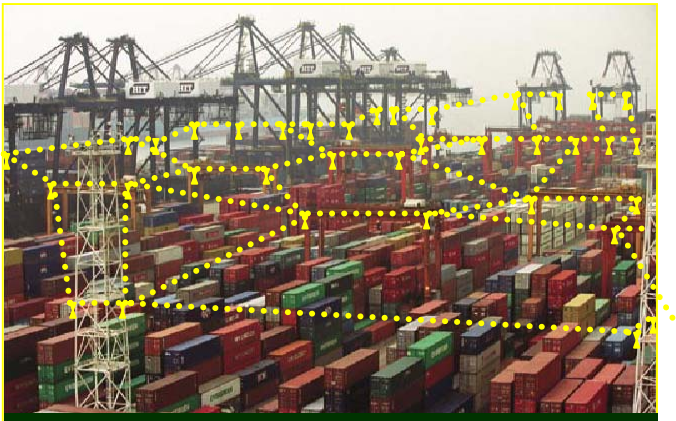
While technology may be the building block of a cost effective solution, securing the world trade and supply chain is a complex integration of technologies, effective processes, and execution by trained people. The technology of “smart box” or “smart container” must be coupled with end-to-end monitoring and tracking systems and services to provide visibility and security.

A full solution as depicted in Figure 6 is best met with partnerships between government agencies and existing terminal operators and supply logistic management companies. The following is some of the proposed functions of this system.

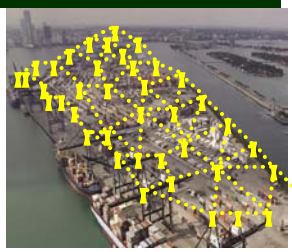
1. 100 percent, 24/7 real-time monitoring and reporting of all access to containers after sealing from departing ports.
2. All status and exception reports are made independently of onboard and operational staff.
3. Exception and tampering reports are made in real-time. Normal status reports are made periodically as scheduled.
4. Reports of exception and tampering are made in accordance to the following harm-benefit protocol:
   - First to the destination port and custom authorities.
   - The same reports are sent to the Public Independent Monitoring Agency (PIMA) as the information clearing- house.
   - The destination authorities will manage any exception events and communicate with the departing authorities and onboard security staff. No direct reporting of events will be made to the onboard and departing authorities unless authorized by the destination authorities or, by mutual or international agreement.
5. The monitoring devices inside the containers, the message-relaying network onboard the carrier, and the communication network are installed and monitored independently by a third party independent agency.
6. AVANTE Container CONTAINER-TRAKKER™ services include self-diagnostic reporting along with system event and periodic reporting.
7. Additional real-time video feed triggered by tampering is an available option.
8. All systems are built-in with redundancy to prevent false reporting.
9. This end-to-end container visibility provides security equivalent to 100% inspection of all containers.

Figure 7 below is an illustration of RELAYER™ network placed at a port terminal, truck terminal, container port or distribution center for stuffing containers.

FIGURE 7



- RELAYER™ ad hoc RF network installed around the yard communicates to the monitoring station all quiescent signals from redundant ZONER™ devices placed inside each container.
- Tampering and exceptions are reported in real-time to local or destination custom authorities and others with need-to-know. Detailed data is also stored by an Independent Monitoring Agency.



- Factory, distribution center or warehouse facilities staff load containers.
- Shipping agent seals with ZONER™ (may be optionally integrated with sensor devices for high risk situations).
- Those containers with integrated sensors are inspected at the port terminal and replaced with standard ZONER™ devices and mechanical seals.

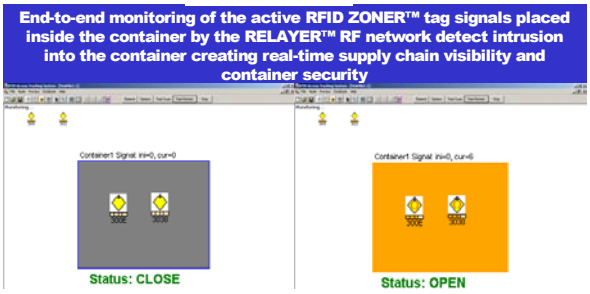
Managing false alarm in e-seal

One of the problems preventing the e-seal technology from gaining faster acceptance is the rate of false alarms. Opinions differ but a false alarm rate from 1% to 0.01% seems to be acceptable. AVANTE believes the false positives must be kept below 0.1%. This can be achieved through the use of two or more active tags emitting at combined 8-10 discrete signal levels.

While the use of quantitative signal differential is effective even for a single ZONER RFID tag, any vibration may distort the door seal to cause a fluctuation of power signals being received by the monitoring RELAYER™. The use of two active tags provides an additional safety factor in avoiding false alarms caused by any fluctuation.

Figure 8 is a representation of user interface in testing the discrete signals received by outside monitoring network.

Figure 8



Conclusion

Container and supply chain security is an urgent concern for the international community. A temporary shut down of US ports would have a chilling effect on economies all around the world. E-seal security capabilities on lock and seal cannot address intrusion through anything other than the container door and certainly not through any of the containers' other surfaces.

A special ZONER™ RFID technology that allows quantitative measurement of multiple discrete power signals has been developed by AVANTE. Tags are placed inside the container to monitor intrusion on any surface of the container, not just the door.

A real-time end-to-end tracking and monitoring system solution based on patented RFID sensor technology is presented to provide for secure supply chain management. The long-sought solution of "smart box or smart container", endorsed by custom authorities, can be achieved without the excessive false positives that plague traditional e-seal technology.

The cost of implementing the "smart container" initiatives can be paid for by the $400-$1600 cost savings achieved by shippers and their partners resulting from supply chain efficiencies and loss prevention.

REFERENCES

1. "Electronic Cargo Seals: Context, Technologies, And Marketplace", Michael Wolfe, July 12, 2002 (Prepared for ITS Joint Program Office, Federal Highway Administration, and USDOT).
2. "Report on Electronic Container Seal Technologies (Task 2)", Chel Stromgren, August 23, 2002. (Funded by the Center for Commercial Deployment of Transportation Technologies at Cal State, Long Beach)
3. "Part 1: Electronic Container Seals Evaluation", Mark Jensen, December 2002 (Sponsored by USDOT ITS Joint Program Office, Office of Intermodalism, FHWA Office of Freight Management and Operations)
4. "Securing the Supply Chain: Container Security and Sea Trial Demonstration Results", RAE Systems, Jan. 2005
5. "GE Uses RFID to Secure Cargo", Jonathan Collins, *RFID Journal*, January 12, 2005.
6. "High-Tech Container Solutions, www.frontlinetoday.com
7. "Mesh Radio Network Performance in Cargo Container", *Sensors* March 2005
8. "Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors; GAO-03-770, July 2003 Report to Congressional Requests
9. "Security: Improving the Security of the Global Sea-Container Shipping System", Maarten van de Voort, Kevin A. O'Brien with Adnam Rahman and Lorenzo Valeri, 2003 Rand.
10. "The Limitations of the Current Cargo Container Targeting", March 31, 2004, Written Testimony by Stephen Flynn, Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, US House of Representative.
11. "Operation Safe Commerce Phase III", US DHS RFP, Due February 18, 2005.
12. "In-Transit Container Security Enhancement", World Shipping Council, International Mass Retail Association, The National Industrial Transportation League, September 9, 2003.
13. *"It is important to recognize that e-seals are not necessarily a solution to containerized cargo security concerns."* As a report by the Vulnerability Assessment Team at Los Alamos National Laboratory states. "High-tech electronic seals are not automatically better than simple mechanical seals, and are often worse." *"Tampering-Indicating Seals: Practices, Problems and Standards",* by Roger G Johnston, Ph.D., Vulnerability Assessment Team. Los Alamos National Laboratory, Los Alamos, New Mexico. Prepared for the World Customs Organization Task Force on Security and Trade Facilitation February 2003 Meeting, Page 1.
14. *"Smart" Container Success Will Depend on Government Mandates",* Feb 1, 2005, Frontline Solutions.
15. *"Frequently Asked Questions, Attachment A (End of this article)*
16. "COMPARATIVE ELECTRONIC CONTAINER SEAL TECHNOLOGIES AND PROCESS" Attachment B (End of this article).

ATTACHMENT A

FREQUENTY ASKED QUESTIONS (FAQ)

1. How does the "Real-Time Locating and Monitoring" system of CONTAINER-TRAKKER™ work?
   - One (preferably two) or more AVANTE active RFID tags (ZONER™) are placed and sealed inside each cargo container.
   - Each ZONER™ emits an identified burst of ID signals at several discrete and different power levels every one to three seconds.
   - If the door of the container is open, all of the several signals at different power levels of the ZONER™ are "heard" by the outside network of RFID readers (RELAYER™). When the door is closed, only some (if any) of the signals will be "heard" by the ad hoc RF RELAYER™ network in the quiescent state.
   - Acts of tampering are immediately reported to the destination port and custom authorities. If a video-monitoring infrastructure is incorporated, tampering can trigger direct camera feed to the proper port and custom authorities.
   - A carrier with tampered container(s) may be inspected before arriving at its destination port to prevent any potential mass destruction or other losses.

2. How much will it cost to install a RELAYER™ network for a ship that holds 3000 containers?
   - A reasonable estimate is to place a RF RELAYER™ ("router") every 40-meters in a square grid.
   - Even for the largest carrier, there may not be a need of more than 30 RELAYER™ devices to form the network of readers.
   - Each RELAYER™ router devices costs in the range of $238 ($168 for larger volume applications) each. To cover the entire carrier, the RELAYER™ network cost could be less than $6,000.
   - The data and communication center requirements are in the sealed, secure "GREEN BOX". The total cost to equip the largest of ships is estimated to be less than $10,000.
   - In comparison to the traditional "fixed position readers" system for e-seal technologies, there is a cost advantage of 10 or more in using RF RELAYER™ network.

3. How much will it cost to install a RELAYER™ real-time locating and monitoring network for a port terminal yard of 2.5 square miles (4 square kilometers)?
   - A reasonable estimate is a RELAYER™ ("router") every 30 to 50 meters in a square grid, or 2500 RELAYER router devices to form a comprehensive network.
   - Each of the 2500 RELAYER™ router devices costs about $168 ($238 for smaller volume applications).
   - To cover the yard of 2.5 square miles costs $420,000.
   - Additional requirements are computer hardware and software. AVANTE estimates the cost for covering a facility of this size at less than $1,000,000.

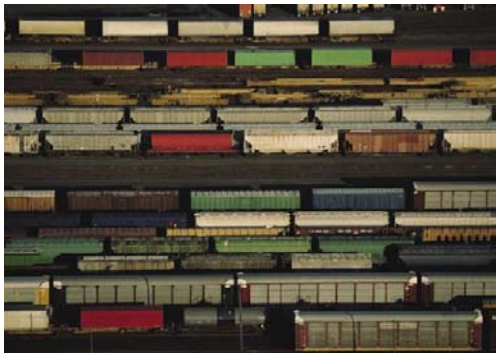
4. How much will it cost to use the ZONER™ device in a single trip for a container?
   - The cost for each ZONER™ with sensor may cost in the range of $100-$300 depending upon the hazards being monitored. The sensors can be re-used as many as 100 times with some replacement of sensor components and battery.
   - There is a cost for the service provided by the PUBLIC INDEPENDENT MONITORING AGENCY (PIMA).
   - The overall cost for a standard container should be less than $30 per container trip. The cost for those higher-risk containers requiring pre-loading sensor monitoring service may cost as much as $50 per container trip.

5. What are the benefits of the “Real-Time Locating and Monitoring” system of CONTAINER-TRAKKER™?
   - Real-time reporting to destination custom and port authorities of any tampering inside containers.
   - Public Independent Monitoring Agency (PIMA) as data clearing house for all tagged containers.
   - Effective 100% inspection of all containers.
   - Reduced theft and inventory shrinkage.
   - 24/7 real-time container and supply-chain visibility.
   - End-to-end automatic container chain-of-custody tracking.

6. What are the advantages that distinguish the AVANTE CONTAINER-TRAKKER™ solution versus that of the “smart container” using other “e-seal”?
   - All of the current e-seal technologies place seals on the outside rendering them susceptible to “smart” insider tampering.
   - Outside and single e-seal technologies are more susceptible to false alarms.
   - The detection of tampering is made after the containers have arrived at the destination port and en route to their final destination points.
   - Two or more redundant ZONER™ devices placed inside the container are inherently more robust against tampering, even against insiders.
   - The redundancy helps minimize false alarms of the monitoring system.
   - The use of a low cost ad hoc “Real-Time Locating and Monitoring” network is the first to include both onboard carrier and all port terminals and storage yards monitoring to provide real end-to-end secured visibility.

7. How fast can one place the ZONER™ devices in the container?
   - ZONER™ devices are equipped with self-attaching magnetic holders that can be placed in random positions anywhere inside the container.
   - Different removable attachment methods can be used for aluminum or other containers.
   - More permanent attachment methods can also be used.
   - The same mechanical lock-and-seal can be used outside for additional security.
   - An optional ZONER™ can be “permanently” attached to the outside of each container to provide for supply-chain visibility at negligible costs. By locating the outside ZONER™ in close proximity to the inside ZONER™ device, data can be relayed or “routed” from the inside integrated sensors to report on radioactive, biological, chemical, temperature, moisture, impact, and other activities.
   - Other e-seal solutions require specialized installation training. They also require changes from the current workflow protocol. ZONER™ is equipped with self-attaching magnets for ease of placement. The same mechanical seal is recommended on the outside with training as required.

8. Can the “ZONER™” devices and “RELAYER” network be used for train containers or other containers that may be non-metallic?
   - AVANTE specialty shielded ZONER™ devices can be placed in insulating containers and achieve excellent results.
   - Each device is positioned on the container door so that the shield will be open when the door is open. Redundant devices are recommended and placed in several different positions to prevent false alarms or insider tampering.



9. What are the patent positions of AVANTE on the solution proposed for real-time supply chain visibility and security management (CONTAINER-TRAKKER™)?

The ZONER™ and RELAYER™ active tag technology and application are covered by several AVANTE pending US patents. End-to-end supply chain visibility and security management is covered by US patent 6,883,710 ("Article Tracking System and Method") by AVANTE with priority date of October 2000. The following are some of the important claims:

Claim 57: **A system for tracking article at a plurality of stations,** wherein a smart tag is associated with the article, comprising:
a plurality of stations at which an operation is performed, each said station comprising: a smart tag reader for transmitting and/or receiving information-bearing signals in a smart tag format via said antenna in the detection region proximate said station; and
a processor for storing in a database at least information contained in the received information-bearing signals, and for providing information that is included in the transmitted information-bearing signals;
at least one smart tag associated with an article, said smart tag including an electronic memory and an antenna coupled to the electronic memory for transmitting and/or receiving information-bearing signals in the smart tag format, wherein the information-bearing signals represent information to be stored in the electronic memory and/or represent information produced from the electronic memory;
whereby **information is communicated between the electronic memory of the smart tag and the processor database of a particular station via the smart tag reader** thereof when the smart tag is in the detection region of that particular station;
a computer processor including a database for receiving information from the processor database of at least one of the plurality of stations and for providing a database record of the information represented thereby; and
communication means for communicating information between the database of said station and the database of said computer processor, whereby **the respective database of said station processor and of said computer processor are linked by said communication means** for providing and receiving information therebetween.

Claim 58: The system of claim 57 wherein the information contained in the information-bearing signals is **representative of one or more of the identity of the smart tag, the identity of the article,** a model number, a serial number, information of interests to the proprietor or operator of the system or method, a type number, a name or nomenclature, material and/or component information, order or contract number, and such information relating to the article, **information relating to the container carrying the article** and/or information relating to apparatus into which the article will be incorporated, **the identity of the station, the operation performed at the station, an operator associated with the station, a measurement made at the station, access information, inventory information**, loyalty information, personnel time and attendance, a date, and time.

Claim 60: The system of claim 57: wherein information processed by the computer processor includes at least application specific data and a relational check number representative of the application specific data; and/or wherein information processed by the station processor includes at least application specific data and a relational check number representative of the application specific data; and/or **wherein information stored in the electronic memory of the smart tag includes at least application specific data and a relational check number representative of the application data.**

Claim 64: The system of claim 57 wherein said communication means further comprises one or more of wire, cable, fiber, **radio or RF transmission**, a local area network (LAN), a wide area network (WAN), **the Internet**, and a combination thereof.

Claim 67: The system of claim 57 wherein the smart tag is either attached to the article or is **attached to a container** for containing the article.

Claim 70: The system of claim 57 wherein the operation performed at ones of the plurality of stations includes at least one of a manufacturing operation, processing, testing, inspecting, operation timing, productivity monitoring, work and/or time recording, an inventory operation, a quality control operation, personnel time and attendance recording, access control, **a shipping operation, a receiving operation, a storage operation**, a display operation, a sales operation, a loyalty program, a buying operation, a wholesale operation and a retail operation.

Claim 71: The system of claim 57 wherein at least ones of said plurality of stations are disposed in one of a warehouse, a manufacturing facility, a processing facility, a display, a storage bin, entrance and exit gates, an access way, **a vehicle, an airplane, a ship, a train, a truck, a container, a storage container, a transport container**, a store, and a display facility.

ATTACHMENT B

COMPARATIVE ELECTRONIC CONTAINER SEAL TECHNOLOGIES AND PROCESSES

Manufacturer Vendor	e-Logicity[1]	Hi-G-Tek[1]	Savi[1]	All Set[1] (GE)	**AVANTE** International Technology, Inc.
Device & Technology	Active RF Tag @ 433 MHz	Active RF Tag @ 915 MHz	Active RF Tag @ 433 MHz	Active RF Tag @ 2.4 GHz	Active RF Tag **@ 433 MHz** (optional 868-915 MHz and 2.4 GHz versions.)
All e-seals can or adapt to transmit: (1) Seal ID, (2) Container ID, (3) Optional Reader ID and data, (4) Time stamp, (5) Manifest, (6) Encryption, and (7) data log from integrated sensors.					
Range (Max.)	21 meter	30-80 meter	>100 meter	30-80 meter	>100 meter
Data Capacity	Some for container ID	2kB	8kB Typical (Expandable)	5kB	**32kB Typical**
Container Sealing Mechanism	Traditional exterior e-Seal	Traditional exterior e-Seal	Traditional exterior e-Seal	Interior e-Seal	Interior ZONER™ devices + Exterior RELAYER™ Network **[2]**
Tamper Self-Detection Means	Change in resistance on cutting of bolt. Resistivity differs among bolts.	Impedance change in 48 parallel wires. Random connections.	Change in magnetic flux through steel bolt (Hall effect)	Door gasket pressure sensor	Differential closed-open RFID signals from among 4 or more - power level bursts. Redundant units to improve security and eliminate false alarms.
Tamper Resistant Weakness	Exposed outside and easier to bypass.	Exposed outside and easier to bypass.	Exposed outside and easier to bypass.	More difficult but still susceptible to tampering.	No conceivable means to bypass detection.
Re-Useable?	Yes. With replacement part.	Yes. With replacement part.	Yes. Except replacement bolt.	Yes. With replacement part.	Yes. Other than battery, no part needs to be replaced or added.
Cost of e-seal	$25	$160/$110	$69/$21	Not available.	Target of $50 or less per trip (including monitoring services)
Cost of Reader	Not available. Fixed position.	$500/$550. Fixed position.	$1770/$2495. Fixed position.	Not available. Fixed position.	$168/$238 per router device depending on volume.
Battery Life	3-10 Yrs	3-10 Yrs	3-10 Yrs	3-10 Yrs	**Engineered for 5 years usage** (Option for 10 years available)
Ease of Use	Minutes to install.	Minutes to install.	Minutes to install.	Minutes to install.	Seconds to place ZONER™ devices with self-attaching magnet at positions inside and near the container door.
Real-Time Monitoring to Report Tampering?	May be adapted for monitoring. Needs costly infrastructure.	May be adapted for monitoring. Needs costly infrastructure.	May be adapted for monitoring. Needs costly infrastructure.	May be adapted for monitoring using Bluetooth lite.	Real-time reporting of any tampering via RF RELAYER™ network and IMA-managed "GREEN BOX" communication system.
Locating of Tampered Container?	Not provided for or planned.	Not provided for or planned.	Not provided for or planned.	Not provided for or planned.	The same real-time monitoring RELAYER™ RF network is also a real-time locating system.

[1] Data extracted from July 11, 2003 Phase 1 Final Report on "Container Seal Technologies and Processes" by SAIC (Contract # N66001-02-D-0039-0001)

[2] (Incorporated several patented and patent-pending RFID technologies and applications of AVANTE International Technology, Inc.) One (preferably two) or more of AVANTE active RFID tags (ZONER™) are placed and sealed inside the container. Each ZONER™ has a self-attaching magnet or other attaching means. Each ZONER™ emits a burst of ID signals at four different power levels each with respective identifiers. If the door of the container is open, all four signals of the ZONER™ are "heard" by the outside network of RFID readers (RELAYER™). When the door is closed, only some (if any) of the signals will be "heard" by the RELAYER™ network in the quiescent state.

Tampering is immediately reported to the destination port and custom authorities and other need-to-know parties. If video-monitoring infrastructure is incorporated, tampering events can be configured to trigger direct feeding of relevant cameras to the proper port and custom authorities. The communications to monitoring agencies are typically via satellite systems during transit or a fixed network for port, terminal, and storage facilities.

Rev B: May 3, 2005