

Securing the Supply Chain

Container Security and Sea Trial Demonstration Results

January 2005





Table of Contents

1. Executive Summary
2. The Unsecured Supply Chain
3. Current Methods In Use To Secure the Supply Chain
4. RAEWatch Solution Description
5. Sea Trial Demonstration, Results and Implications
6. The Role of Government and Industry



1. Executive Summary

In October and November 2004, RAE Systems performed two sea trials to prove the feasibility of using sensors to continuously monitor the integrity of intermodal shipping containers from point of origin to point of destination. This white paper reviews the compelling need for container monitoring, lays out the details of the sea trials, presents the results from the RAEWatch wireless sensor modules that were used to monitor radiation, intrusion, temperature and shock and summarizes possible next steps to deployment.

This white paper shows how the field tested, RAEWatch sensor modules can successfully be used by shippers, shipping companies and government monitoring agencies to provide enhanced security and be integrated with existing logistics systems and technologies without impeding commerce.

2. The Unsecured Supply Chain

Hutchison Port Holdings is one of the largest terminal operators in the world and handled 42 million containers in 35 ports in 2003. According to Gary Gilbert, Chief Security Officer at Hutchison, "Each of the 42 million containers that went through our facilities around the globe was a Trojan horse. We don't have the ability to truly know if the containers have been tampered with."¹

And the situation faced by Hutchinson is only the start. There are 12 million cargo containers in the worldwide inventory, moving among major seaports more than 200 million times each year. Every day, more than 21,000 containers arrive at U.S. seaports from foreign countries filled with consumer goods, from televisions to clothing to toys. In fact, about 90% to 95% of U.S.-bound cargo moves by container.²

Modern society is heavily dependent on the efficient, reliable and cost-efficient movement of goods through this supply chain, and it's clear that the stakes involved in securing it are enormous. The proliferation of the intermodal container has functioned as a catalyst to economic growth, and the prosperity and power of the U.S. is dependent on having stable, available access to global markets these containers provide.

These 40' x 8' x 8' containers are ubiquitous, moving from truck to ship to rail to truck and back again, and the sheer volumes in play have enabled massive economies of scale: major retailers and manufacturers in the U.S. can ship 30 tons of goods from points in Asia to the West Coast of the U.S. for about \$1,600.

However, this system was developed with a goal toward speed and cost, not security. Safeguards were not a part of the original business, and this leaves us with a vulnerable system that represents a frightening threat to not only the commercial power of the U.S. but also the safety of its citizens.

In March 2003, Stephen E. Flynn, Ph.D., Commander, U.S. Coast Guard (ret.) provided written testimony to The U.S. Senate Governmental Affairs Committee about the state of container security. In that report, he noted that the supply chain supplies both opportunity and motive for an attack:

Opportunity derives from the almost complete absence of any security oversight in the loading and transporting of a box from its point of origin to its final destination, and the fact that growing volume and velocity at which containers move around the planet create a daunting “needle-in-the-haystack” problem for inspectors.

Motive is derived from the role that the container now plays in underpinning global supply chains and the likely response by the U.S. government to an attack involving a container. Based on statements by the key officials at U.S. Customs, the Transportation Security Administration, the U.S. Coast Guard, and the Department of Transportation, should a container be used as a “poor man’s missile,” the shipment of all containerized cargo into our ports and across our borders would be halted.

As a consequence, a modest investment by a terrorist could yield billions of dollars in losses to the U.S. economy by shutting down—even temporarily—the system that moves “just-in-time” shipments of parts and goods.³ A 2002 report from The Brookings Institution reported that a weapon of mass destruction shipped by container or mail could cause damage and disruption costing the economy as much as \$1 trillion.⁴ The utility of this approach has already been proven: in a statement reported in the New York Times on December 19, 2004, Osama Bin Laden commented that the original \$500,000 investment on the part of Al Qaeda on September 11, 2001 had cost the U.S. economy over \$500 billion.⁵

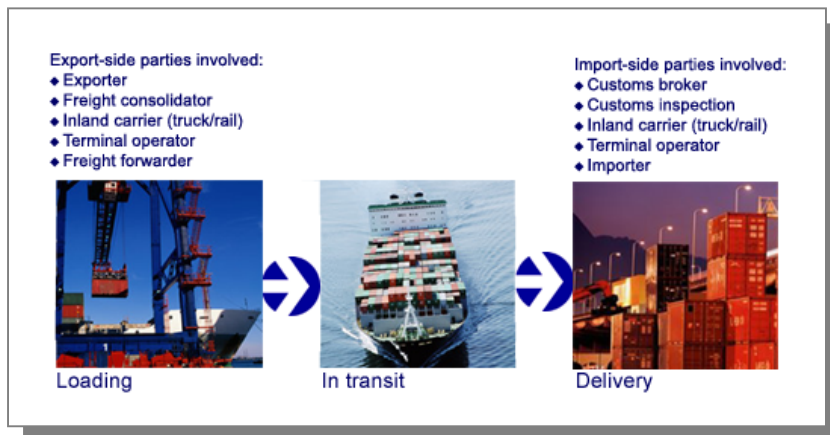


Figure 1. The global supply chain is vulnerable due to changes in modes, changes in the custody and control of cargo, and changes in the legal/security jurisdiction of cargo. (Adapted from U.S. Government Accounting Office chart.)

While the threat of terrorist attack clearly carries the potential for economic damages, the supply chain is also vulnerable to economic losses from theft. This will be the topic of the next volume in the RAE Systems white paper series, which will discuss risk management and the role of sensing networks in mitigating the nearly \$50 billion a year that is lost in high-value cargo theft.⁶

3. Current Methods In Use To Protect The Supply Chain

The global supply chain will never be made completely secure by relying solely on the use of technology. However, the Department of Homeland Security stressed in a recent document that a multi-layered approach of integrated, coordinated approaches should be used to effectively secure the supply chain. In addition to enhancing the physical security of the supply chain, using intelligence to target, identify and inspect 100% of high-risk cargo, the government and industry should work together to “ensure that Federal resources are leveraged to meet prioritized threats



and vulnerabilities along the supply chain including the acquisition and deployment of technologies, including spurring research and development in key areas.”⁷

One key area in particular is addressing the question of integrating sensor networks with supply chain databases and existing import/export processes to enable global importers and exporters to more effectively manage and monitor their maritime cargo while fulfilling the complex requirements of U.S. and international trade laws.

The solution demonstrated by RAE Systems in autumn 2004 integrates automated global trade management solutions with a variety of RAE Systems’ wirelessly networked security sensors.

The joint offering combines RAE Systems’ robust RAEWatch wireless sensor networks (described below) and a suite of web-based applications from a major provider of global trade management solutions that streamline and automate the information exchanges associated with the international movement of goods. The sensor data provided by RAEWatch is not software-specific and can integrate with any database or logistics systems such as those used by major package shipping companies. RAEWatch security sensors are deployed in cargo shipping containers to monitor radiation, intrusion, shock and temperature.

RAEWatch sensors seamlessly transmit data to logistics and trade compliance applications, merging the container’s identification and security status with standard shipment and manifest data. Should a container be breached, RAEWatch sends an alert to the database, enabling the customer to contact appropriate security and customs authorities to prevent breached containers from clearing customs without inspection.

As a result, logistics and supply chain personnel now can more easily manage their trade compliance requirements while gaining unparalleled visibility and active early warning into whether their cargo containers have been breached, well before they arrive in port.

4. RAEWatch Solution Description

RAEWatch is on the leading edge of an emerging concept called pervasive sensing. Pervasive sensing consists of hundreds or even thousands of wireless sensors, communicating across secure, self-healing, ad-hoc networks. Pervasive sensing provides the eyes, ears and noses that can never be adequately scaled with human measures, and therefore plays a central role in a technological solution component of securing the supply chain.

The RAEWatch wireless sensor bundle can be permanently installed in containers for end-to-end supply chain logistics. With IEEE 802.15.4 compliant architecture, RAEWatch networks are immune to interference from radio sources such as Wi-Fi and cell phones, and have a one- to two-year lifespan when used in temporary, battery-powered deployments. RAEWatch networks provide monitoring of radiation, temperature, shock and intrusion, and are expandable to include a variety of other sensors.

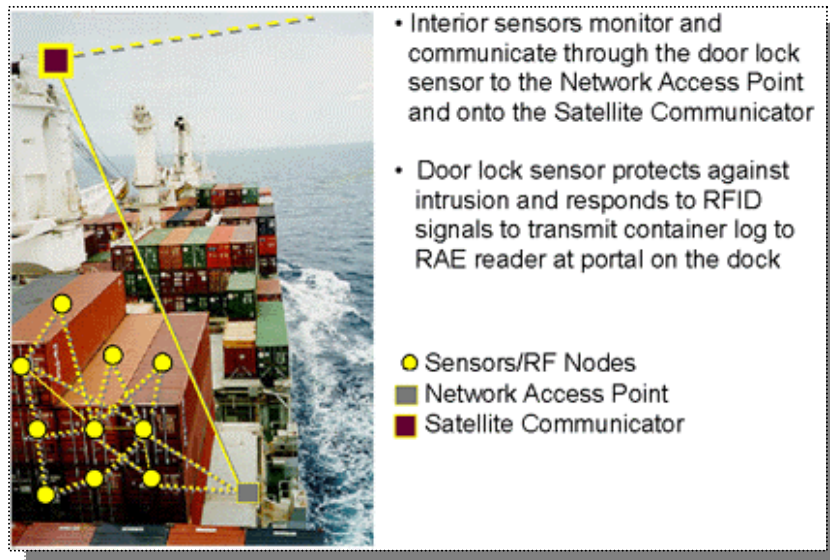


Figure 2. RAEWatch integrates temperature, shock, humidity and radiation data to ensure container integrity.

RAEWatch sensors self-configure as mesh networks, also known as point-to-point-to-point or ad hoc, multi-hop networks. Routing data through intermediate nodes is not only rapid, but also self-healing because data packets automatically reroute through an alternate path if one link fails.

In a real-world mesh network, the network provides each node with multiple data transmission paths, forming a mesh. Each node communicates its existence as well as other information with its neighbors, allowing various algorithms to determine the best way to transmit end-device data to the network coordinator. Some networks communicate this information on demand, when a message needs to be sent, while others maintain it actively.

5. Sea Trial Demonstration, Results and Implications

RAE Systems recently completed two sea trials using a container owned by Matson Navigation Company. Matson is one of the leading U.S. domestic carriers and is the principal carrier of containerized freight and automobiles between the West Coast and Hawaii, Guam and Mid-Pacific.



Figure 3. Loading the container containing RAEWatch sensors at the Port of Oakland.



The first trial involved a container shipped from Oakland, California, to Honolulu, Hawaii, on October 7, 2004. The second trial involved a container shipped back from Honolulu to Oakland and took place from November 9 to November 23.

The equipment was loaded in Honolulu on November 9, the container was loaded into the vessel on November 11, and the ship departed November 12. The vessel arrived five days later in the port of Oakland and the container was delivered to RAE Systems headquarters in Sunnyvale, California on November 23.

The trial focused on determining the performance of RAE Systems' wireless sensing network behaviors:

- **Environmental Characteristics Profile.** How will RAEWatch perform in a wide range of temperatures that occur in a transoceanic shipment? How will humidity affect readings? How will sudden accelerations and decelerations of containers during loading, unloading and during transit affect the equipment?
- **Event simulation and detection.** In real-world conditions, will the sensors detect and communicate events when they occur?
- **Datalogging.** Will the networks report data properly? Two scenarios were tested: (1) the event log, which created a time-stamped capture of the number of events occurring within a specific time window, and (2) the periodic log, which captured high and low readings during a periodic time window.

In summary, given the current sensing, communications and power conservation technologies, the RAEWatch module proved itself capable of providing a reliable security solution in the cargo container environment.

Specifically, the trial tested how the sensors performed on the following tasks:

- Detecting and logging readings from radiation, intrusion, shock and temperature.
- Responding to queries from the reader device for information on readings, alarms, date/time, and the container identification number.
- The ability to set and change the container identification number via the reader device.
- The performance of the power-saving sleep mode of RAE Systems' mesh networks.
- Whether and how well the mesh networks respond to a "wakeup" call from an RFID (radio-frequency identification) trigger.

The instrumentation involved in the trial included:

Sensors:

- CsI (TI) Gamma Sensor (Meets ANSI 42.32)
- Motion Sensor
- Dual-Axis Accelerometer
- Temperature Sensor
- MultiRAE Plus (CO, H₂S, O₂, LEL, VOC)
- MiniRAE 2000

Communications

- RM2420 - IEEE 802.15.4 compliant, 2.4GHz, 250kbps OQSPK Direct Sequence Spread Spectrum
- Low Frequency RFID

Radiation Simulator

- Cs-137 5.0 μ Ci sample periodically exposed to gamma sensor

Power

- Lithium Battery

The RAE Systems networks were successful in the following tested areas:

- **Sensing and communicating.** RAEWatch provided extensive characterization of the cargo container environment during the entire journey, from origin to destination. The equipment was able to simulate and the monitors were able to sense events in the target environment, and were able to transfer that sensor information to a reader device using mesh network wireless technology.

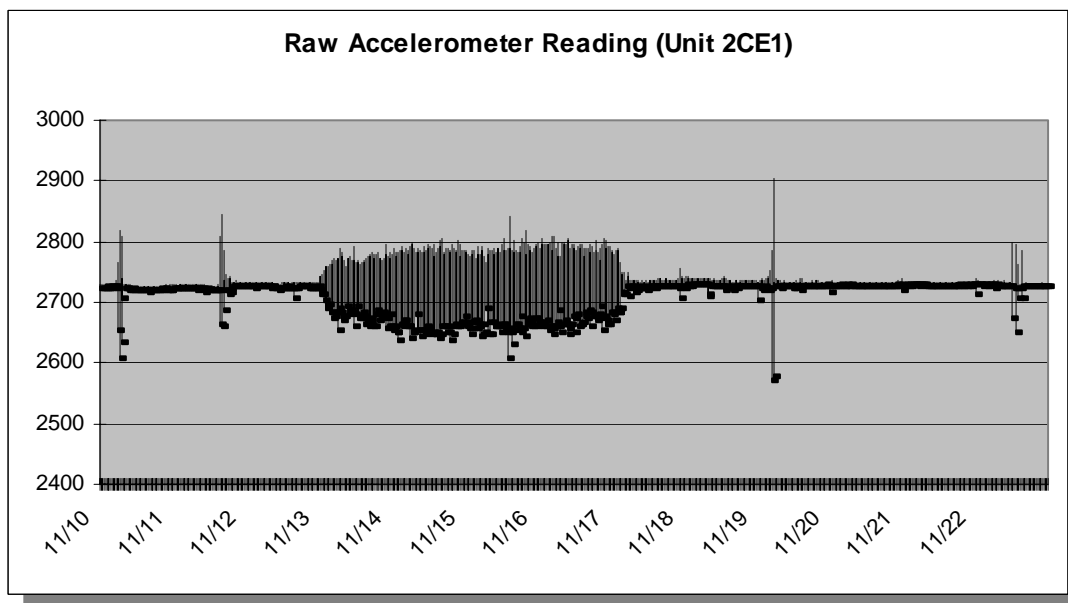


Figure 4. The container environment is stressful, characterized by wide temperature variations and movements. Containers are subject to violent movement during loading and unloading as well as sustained vibration during the voyage. The graph above shows the raw accelerometer reading provided by RAEWatch during one trial.

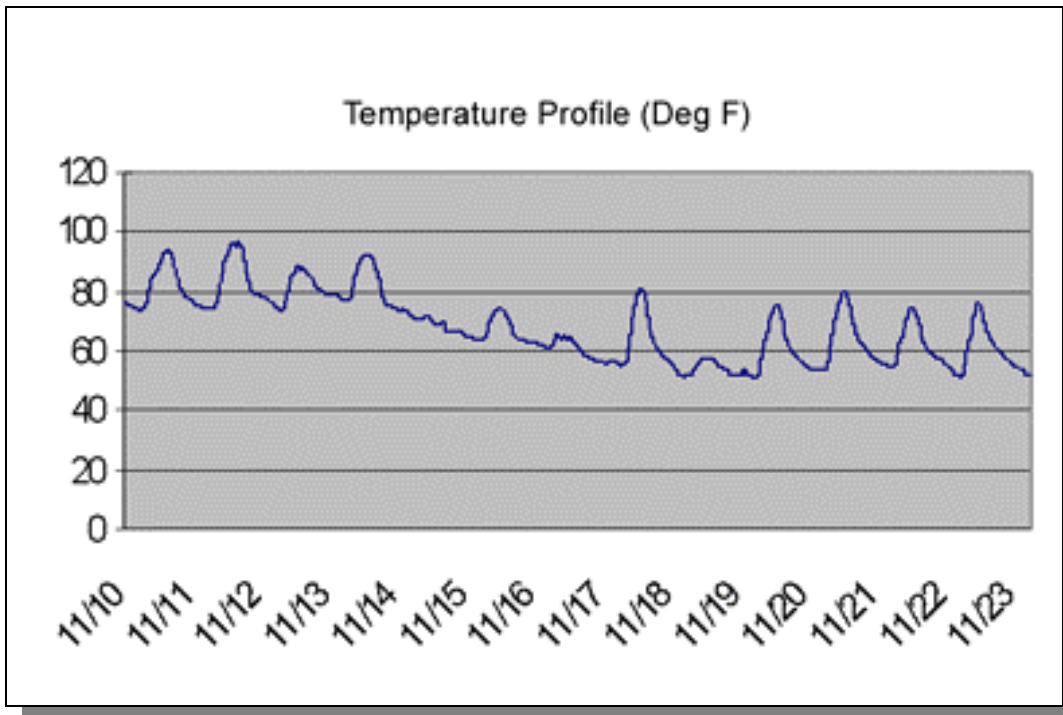


Figure 5. RAEWatch provided a comprehensive, detailed record of temperature fluctuations in containers throughout the voyage. Real-time temperature readings enable shippers to identify unusual spikes that might damage perishable goods in transit and assist insurance companies in assessing liability.

- **Datalogging.** The sensors were able to log both periodic and event data. The sea trial verified the ability of RAEWatch to detect radiation and intrusion events with no false alarms.

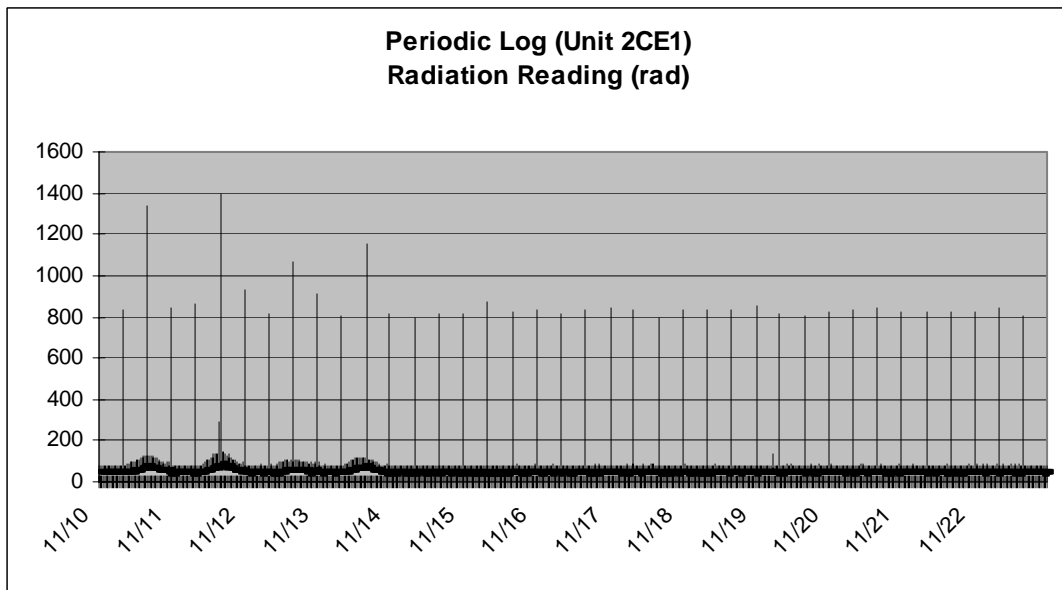


Figure 6. RAEWatch successfully detected radiation events as released by a radiation simulator containing five μCi of Cesium-137.

- **Power conservation scheme.** The networks were able to conserve power by putting the RM420 into sleep mode, and were able to be activated at an appropriate time using RFID technology.

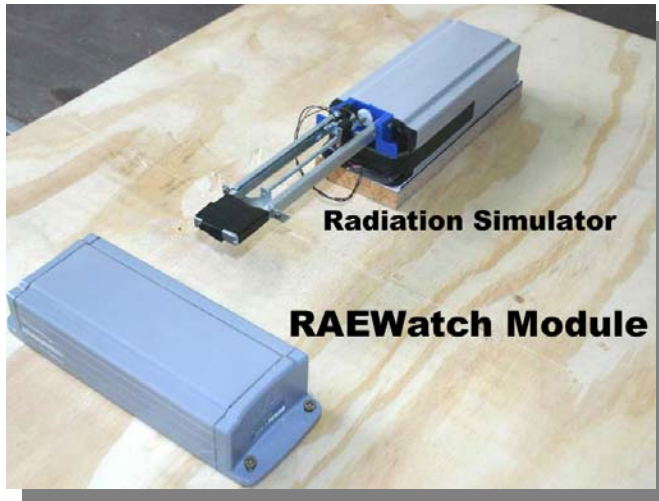


Figure 7. Small RAEWatch module sensor units with automated radiation ready to install in the container.

6. The Role of Government and Industry

The Department of Homeland Security envisions a system for supply chain security that “mitigates the evolving terrorist threat and facilitates the free flow of global commerce in order to ensure the physical and economic well-being of the United States and its trading partners.”⁸ This shipping security system calls for the use of sensors in containers, has been mandated by congress, and was signed into law by President George Bush as part of H.R. 2443, the Coast Guard and Maritime Transportation Act of 2004.

Achieving this vision seems daunting to anyone familiar with the complexities of moving an enormous volume of goods across various modes, through changes in control and with differing legal and security parameters. Yet the potential threat demands a forceful, swift, preventative response that includes technology, processes, and partnerships among public agencies and private organizations.

No one organization can ensure the integrity of the supply chain on its own. Initiatives do exist, such as Operation Safe Commerce, started by the U.S. Department of Transportation and the U.S. Customs Service. The Container Security Initiative was launched by U.S. Customs and Border Security, as was the Customs Trade Partnership Against Terrorism (C-TPAT).

As the Department of Homeland Security vision comes to fruition, RAE Systems is accelerating the development and testing of monitoring and deterrence solutions. The technology has been proven to function effectively in the real-world conditions of a transoceanic voyage.

Shipping companies must have a solution that provides enhanced security for a large volume of containers while not impeding commerce. The RAE Systems sea trials successfully demonstrated RAEWatch, a field-tested solution that can be integrated into other technologies and processes that shippers and government agencies require.

Endnotes

- (1) As quoted in Frontline Solutions Magazine, July 1, 2004.
- (2) Remarks made by Senator Susan Collins (R-ME), Chairman, Committee on Governmental Affairs, March 20, 2003.
- (3) Written Testimony before a hearing of the U.S. Senate Governmental Affairs Committee on March 20, 2003 by Stephen E. Flynn, Ph.D. Commander, U.S. Coast Guard (ret.) Jeanne J. Kirkpatrick Senior Fellow in National Security Studies and Director, Council on Foreign Relations Independent Task Force on Homeland Security Imperatives.
- (4) Testimony by JayEtta Z. Hecker, Director, Physical Infrastructure Issues, Government Accounting Office, Before the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, November 18, 2002.
- (5) Technology Asset Protection Association in Frontline Solutions Magazine, September 1, 2004.
- (6) The New York Times, December 19, 2004.
- (7) Department of Homeland Security, National Cargo Security White Paper, version 1.8, page 1.
- (8) Ibid.