Session No. 530

Terrorist Attack or Safety Catastrophe? Save Lives and Lower Costs with Dual Purpose Safety and Security Systems

Michael J. Waugh, MS
THORAD Technologies Corp.
Neuric Technologies, LLC
Austin, Texas

Introduction

Safety hazards, employee mistakes, and security threats are primary concerns in the world of critical infrastructure and costly assets. Considerable time and money are spent avoiding loss of life, assets, and production. Early detection technologies that utilize an intelligent software system, coupled with commercially available thermal, optical and radar subsystems, provide both safety hazard and security threat detection systems. These systems result in increased production, while maintaining employee and process safety and remaining compliant with government standards.

Terrorism is increasingly considered a valid threat to our critical infrastructure. In a traditional terrorist incident**,** a target is selected and, typically, is either destroyed or heavily damaged. With respect to the attack on September 11, 2001, there are more deaths in the United States that are attributable to safety incidents.

Terrorist attacks and safety incidents have an overlapping zone of concern, which consists of sabotage. In some cases, the outsider is disguised as an employee or an employee may be co-opted to cause a safety incident. Included as well, in this sector, are acts of conspiracy and outright safety negligence. It is clear that a safety hazard, if left unattended, will likely result in a dangerous situation and, possibly, a catastrophic event.

Recent developments in innovative technological systems couple existing technology with cognitive software. The result of this coupling provides long-term compliance with the Department of Homeland Security (DHS) requirements, Environmental Protection Agency (EPA) regulations, and Occupational Safety and Health Administration (OSHA) standards. It is possible and certainly important to take advantage of integrating technology that enhances traditionally *separate, costly and complicated systems* with innovative and proprietary detection techniques. Video analytics provide limited detection reliability. It is highly advisable to utilize a proprietary software platform that detects potential safety hazards and security threats to ensure accurate threat detection from disparate inputs. Today it is a fact that the line between safety hazards and security threats is no longer clear. There is a gray zone within which safety, and security risks may be applied. A security threat, such as terrorism, disgruntled employees and criminal behavior, has proven to be a safety catastrophe, causing as much harm as an external attack. For example, a terrorist would likely be more innovative and as successful by paying or extorting an employee to leave an improvised explosive device (IED) inside an oil refinery.

It is imperative/ advantageous to integrate reliable thermal, optical, and radar technologies to detect, identify, track, and report security threats to elements of critical infrastructure as required by the DHS. The systems comply with the Maritime Transportation Security Act (MTSA) and Chemical Facility Anti-Terrorism Standards (CFATS) that mandate securing the nation's ports and chemical infrastructure against terrorism. The disastrous refinery explosion in Texas in 2005 triggered researchers at the University of Texas to develop two (2) systems that address the critical need for safety systems that reliably detect, identify, track, and report safety hazards, thereby providing primary and secondary fault detection systems required in large refineries and chemical plants. For the sake of this paper, we will call the safety hazard detection system Safety 1, and the security threat detection system Security 1. Combined, ***Safety 1*** and ***Security 1*** provide a single-source, integrated system that detects security threats ***and*** safety hazards in compliance with U.S. law at a fraction of the cost of existing systems.

The hardware elements used in ***Security 1*** and ***Safety 1*** are COTS (commercial off-the-shelf) items integrated into the systems. A recently developed cognitive brain (the ***Brain***) directs theses two systems.

The differentiators and benefits over current systems include:

- Immediately deployable, solar-powered systems to mitigate crisis situations
- Reduction in risk of disruption due to early, rapid risk identification and reporting
- Redundant and highly accurate safety risk detection and reporting, as primary or as a backup to existing safety systems that sometimes fail to alert facility operators (integration option)
- Substantial savings by mitigating risk
- Reduction in labor and insurance expenses
- Increase in risk assessment accuracy; proprietary automated options and ***Brain*** direction can identify and track risks without human interaction, while a human response determination is made as alarm-alerting requirements increase
- Rapid reporting of potentially costly events – interdict in a timely fashion

Federal authorities predict an increase in terrorism as our chemical and other heavy industrial base elements continue to age. The resulting vulnerable critical assets will provide problems that require these new and innovative solutions.

The Problem

A critical need exists for cost-effective, intelligent security threat and safety hazard detection systems in a very large market. This market consists of hundreds of airports, seaports, power plants, mining operations, petroleum refineries, chemical facilities, and thousands of unprotected offshore platforms and onshore critical infrastructure assets. Many of these assets are aging. The systems that once handled their security and safety requirements are no longer valid for the new and higher threat levels, as defined by DHS. Going further, research proves that current suppliers have not adequately addressed all of the requirements, as laid out by DHS and other regulating agencies to address terrorism and safety hazards.

DHS legislation (MTSA and CFATS for onshore/offshore petroleum operations and chemical facility security system requirements) requires that hundreds of installations be protected

against security threats. Security systems are being installed currently for maritime and seaport assets. This legislation requires petrochemical facilities to be evaluated in terms of threat and danger to surrounding areas, and then categorized as a Tier 4 to Tier 1 (highest) threat level facility. This determination is made, and DHS now requires higher risk facilities to be protected in accordance to their tier grade level.

The problem with the current systems is that they are labor-intensive both in process and operator interaction. The ***Brain*** enables both systems to tie together disparate pieces of information that result in timely valuable assessments. The effectiveness of this processor is very user friendly, faster, more effective, and it lends itself easily to retrofitting an industrial site.

Safety Hazards

Onshore and offshore petrochemical assets are at risk from minor to catastrophic safety hazard events. OSHA and EPA require that these assets provide a safe environment for workers and do not pollute the atmosphere. Nevertheless, component failure, errors in process control, and human error have resulted in billions of dollars in losses as well as loss of life. The conditions that led to the explosion at BP's Texas City refinery in March 2005 (resulting in 40 dead, 170 injured, and nearly $15B in losses), which would have been detected by ***Safety 1*** several hours prior to the explosion.

Interestingly, safety hazards can be caused by human intervention (sabotage), thus graying the line between a security and a safety threat. For example, a terrorist may coerce an employee through extortion to place an explosive device in a chemical plant that produces very toxic materials. This shows that it is important to provide protection in both categories with the integrated ***Security 1*** and ***Safety 1*** combination.

In addition, companies that fall under OSHA and EPA regulations may negotiate their fines assessed by the agencies. For example, a safety violation can easily warrant a $100,000 fine or greater, levied against an oil company. By the company demonstrating that they have taken measures to increase safety at the plant, and reduce the likelihood of further environmental violations, the company stands a better chance at negotiating reductions in fines.

Security Threats

Onshore and offshore petroleum assets are at risk from, but not limited to, extortion, theft, terrorism, and sabotage. The extensive U.S. energy infrastructure extends around the globe, where its assets are involved in exploration, transportation, refining, and distribution. Assets in the U.S., Europe, Middle East, Latin America, Africa, and Asia are at risk from terrorist attacks and extortionist demands. Americans are regularly kidnapped from offshore platforms and remote onshore areas. Thieves in boats target unmanned platforms where stealing one (1) or two (2) small items can render a platform "off line." **Current methodologies for mitigating these threats simply are not immediately effective.** The problem is so severe that DHS has mandated that all ports must be protected against terrorist attacks. (See USCG Regulations 105, 106, and 107) under the Maritime Transportation Security Act (MTSA).) Likewise, the MTSA requires offshore platforms to be protected against terrorist threats. In November 2007, the Bush Administration enacted the Chemical Facility Anti-Terrorism Standards (CFATS). Over 7,000 chemical facilities fall under CFATS, evaluated in July 2009, and ranked from low (4) to high (1) in terms of product toxicity and proximity to populated areas (among other variables). This list was made public in early August 2009. Some 219 facilities are Tier 1 facilities; 756 are Tier 2 facilities; 1,712 are Tier 3, and the remaining 4,319 have been designated Tier 4 facilities. ***Security 1*** addresses the various requirements of the CFATS "risk based performance standards." The most stringent security requirements (Tier 1 and 2 facilities) cover nearly 1,000 facilities. These

facility operators have conducted vulnerability assessments, and submitted site security plans to DHS. Violations of the CFATS regulations carry potential fines of up to $25,000 per day per violation. Installation of newer technology and the upgrading of older systems are expected to take place in the 2010-2011 timeframe and beyond.

Reasons for the breaches in security and safety mitigation, in both the safety and security disciplines, have their genesis in the lack of specialized software and hardware to address today's issues. These include:

- Failure to develop and use artificial intelligence, which brings together incoming streams of data from radar, thermal imagers and optical cameras to enable a system to evaluate and analyze situations that rules-based algorithms are not capable of handling. This applies primarily to security threat mitigation, such as border security, where the sheer amount of possible 'hits' and false positives is enormous.
- Lack of reliable, rules-based algorithms and artificial intelligence that provide a solid basis for evaluating thermal anomalies in petrochemical plants, oil refineries, and mines, where safety hazard detection and mitigation is essential to provide security and protect the environment.
- Need to increase reliability and refine special motorized devices that precisely aim imagers in a low-tolerance environment.
- Lack of innovative systems and their integration to make them flexible under hostile conditions that commonly occur in critical infrastructure asset conditions.
- Failure to apply leading-edge technology to harsh conditions where it would be easy to do so.

Human error is the primary reason that security threats and safety hazards events go undetected. The sheer number of tasks underway in complex facilities often overburdens operators. An unreported alarm condition, due to a system error or an alarm ignored by an operator, can be catastrophic.

The Solution

The solutions to the problems described above require hardware and software elements to ensure peak performance. The solution integrates thermal, optical, and radar technologies to detect, identify, track, and report security threats and safety hazards. The cognitive ***Brain*** is applied to operate the systems and, combined with algorithm-based software, it analyzes incoming radar, optical and thermal images to detect, identify, track, and monitor both threats and risks that immediately alert the operator to initiate a timely response.

Safety and Security Systems Working Together

As described above, critical infrastructure assets are vulnerable to both external and internal threats. Recent legislation mandates protecting these assets against terrorists and other threats. For this reason, two separate, but complementary systems were developed. ***Safety 1*** scans into a critical infrastructure (i.e., petrochemical, nuclear, etc.) facility to detect unintentional or man-made hazardous conditions according to site-specific safety parameters, and alerts the facility's control room and others, as necessary, to mitigate this risk. ***Security 1*** detects a

security threat approaching the asset, identifies it, and tracks its approach, while transmitting real-time images to the client's security command center. An attack on a refinery by terrorists would likely result in contamination and many deaths. ***Security 1*** mitigates this threat whereby these conditions result in an immediate warning to appropriate personnel via their Security/Safety infrastructure (and even via hand-held devices) that a dangerous condition exists. These solutions are essential for today's operating environment by providing early warning to control losses from terroristic acts against critical infrastructure and to mitigate the potential of a safety hazard-induced catastrophe. The examples below illustrate the use of these systems in the petrochemical industry, chosen due to the industry's significant size and vulnerability.

Safety 1 Risk Mitigation

Safety 1 provides real-time thermal readings, as well as other measurements, such as radiation, objects left behind, and other valuable video analytics. Typically, ***Safety 1*** mitigates risk in a facility where a fault in a complex and costly process could result in a catastrophic event. Such an event occurred in Texas City in 2005, resulting in $15 billion in losses. The anomalies leading up to this catastrophe would likely have been detected and reported ***10 hours prior to the explosion*** by a ***Safety 1*** system had it been installed in that area of the refinery.

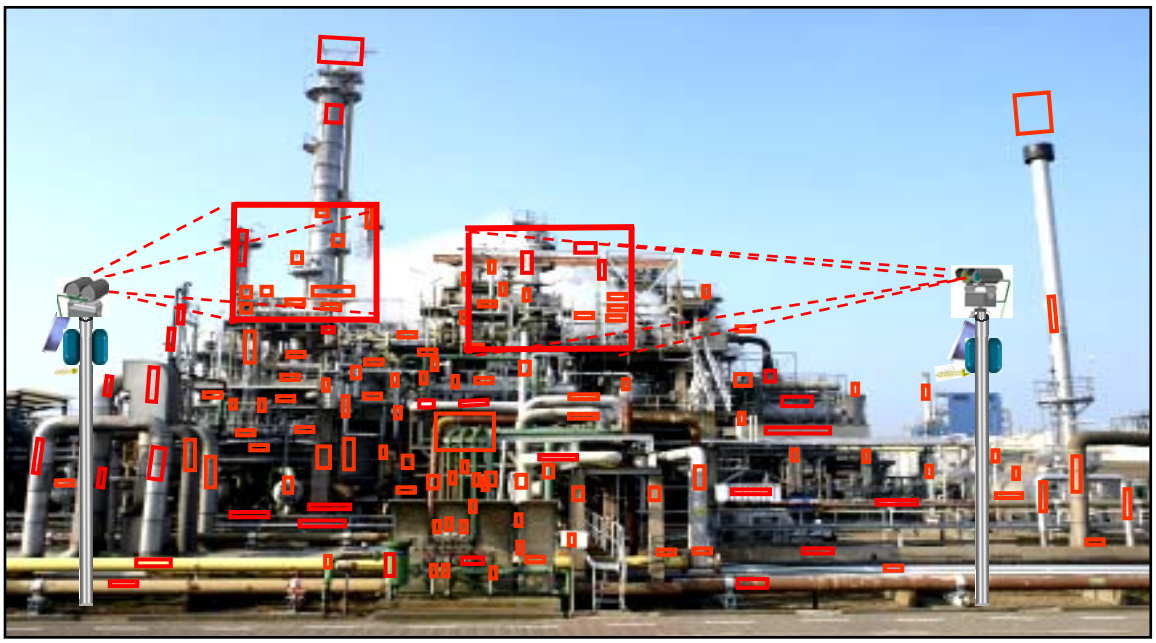

Figure 1. Safety 1 installed at a Petrochemical Plant

Such a catastrophe is avoidable. ***Safety 1*** detects, tracks, and reports a wide range of anomalies that could result in a catastrophic event. Integrating wireless thermal and optical imaging technologies enables it to scan for thousands of points in minutes for such anomalies and report them to the control room.

Live gas leak sensing option and accurate process evaluation capability detects thermal anomalies and senses flow irregularities to determine if safety limits are threatened and are likely to be compromised. Algorithms applied to video streams immediately trigger live video feeds for operators in the facility control room (and anywhere in the world) to mitigate these risks, save lives, and protect high-value assets.

Safety 1 also provides the basis for redundant monitoring of safety instrumented systems (SISs). SIS is a form of process control that is implemented in industrial processes, such as those of a factory or oil refinery. The SIS performs specified functions to achieve and maintain a safe state of the process and is focused on preventing catastrophic incidents. When it detects unacceptable or dangerous process conditions, it provides an alarm. Safety instrumented systems are separate and independent from regular control systems but are composed of similar elements, including sensors, logic solvers, actuators, and support systems. Safety instrumented function (SIF) is implemented as part of an overall risk reduction strategy, which is intended to reduce the likelihood of identified hazardous events involving a catastrophic release. The "safe state" is a state of the process operation where the hazardous event cannot occur, and should be achieved within one-half of the process safety time.

Safety integrated level (SIL) rated sensors and valve actuators are installed in the field to ensure that existing safety functions are performing to specification to protect complex and hazardous processes. Safety integrity level (SIL) is defined as a relative level of risk reduction provided by a safety function, or specification of a target level of risk reduction. In simple terms, SIL is a measurement of performance required for a safety instrumented function (SIF). Four SILs are defined, with SIL4 being the most dependable, and SIL1 being the least. A SIL is determined, based on a number of quantitative factors in combination with qualitative factors, such as development process and safety life cycle management. The requirements for a given SIL today are not consistent among all of the functional safety standards.

SIL-integrated safety transmitters and valve positioners for field safety and asset management are standard industry safety requirements. ***Safety 1*** will ensure they operate to specification; it is the ideal backup system for fault detection and process control safety management. Traditional systems utilize SIL-rated sensors and valves to transmit plant conditions to the control room. The ***Safety 1*** system provides a backup to these sensors and analyzes areas in the plant that are not monitored by traditional safety systems. This solution will allow comprehensive field device diagnostics to be combined with the overall control and safety solution to improve field asset management and elevate plant maintenance and operational performance. These valuable contributions include hazards and risks analysis, SIL validation and verification studies, documenting safety system specifications, online SIS proof testing, maintenance services, and parts management programs. The dual benefits of this safety management solution provide for integration with existing safety systems while maintaining the security of an independent environment from the mainline control system. The result is a unified safety system solution, elevating safety and process availability, production, and profitability. The cost efficient ***Safety 1***, coupled with a ***Security 1***, makes it the educated choice for small, medium, and large operators worldwide because of the dual-use capabilities in one platform. Therefore, whether the client has ***Security 1*** or ***Safety 1***, the transition to incorporate the other is relatively simple. Literally hundreds of onshore and offshore assets would increase their own operating safety by using ***Safety 1***. The deciding factor is whether they prefer to remain safety compliant and out of litigation by having this protection. U.S. oil companies have now begun installing onshore and offshore systems with many of the attributes included in the ***Security 1*** system.

Another factor worth mentioning is that adding radiation detectors to both ***Security 1*** and ***Safety 1*** expands the overall system's value to infrastructure facilities. Radiation detectors, combined with the thermal and optical imagers, provide the capability to detect materials used in a "dirty bomb."

Security 1 Risk Mitigation

Security 1 detects, tracks, identifies, and reports security threats to onshore and offshore assets. Integrating radar, thermal, optical and other sensors, along with other support equipment (i.e., explosion-proof enclosures), allows for installation in a wide range of facilities, such as airports, seaports, refineries and offshore platforms.

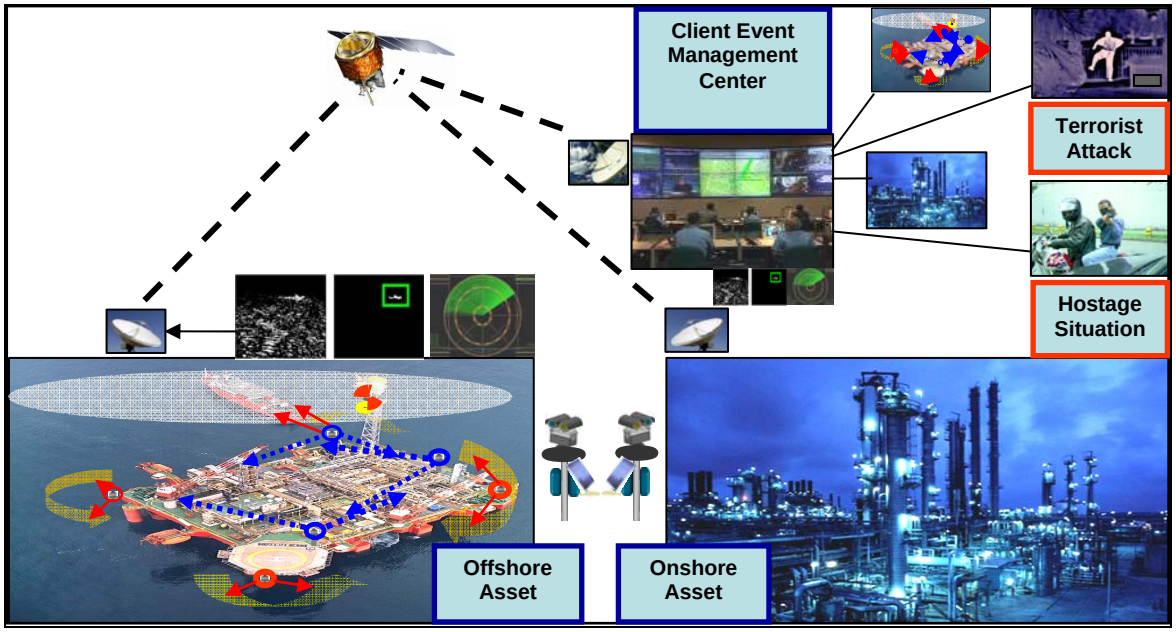

Figure 2. *Security 1* Onshore and Offshore Installations with Monitoring Station

Solar power and wireless transmission links make installing ***Security 1*** fast and straightforward. Advanced, upgradable software-detection algorithms and artificial intelligence ensure accurate analysis.

A Cognitive *Brain* Behind the Systems

The intelligence behind both systems is the cognitive ***Brain,*** which is configured and instructed in plain English, making it easy for operators to program. The ***Brain*** not only accepts input in plain English, it also accepts input from a wide variety of sensors and electronic devices. The ***Brain's*** ability allows it to accept a wide range of inputs and tie together disparate information, such as weather, terrorist information, and alarm conditions (***Security 1***) in one area, which may impact on another area; keep in mind that these areas are not necessarily covered by a traditional fault detection system. But with the ***Brain,*** the combined systems have a greater chance of predicting a failure in a more timely fashion, and alerting operators to developing situations. The performance characteristics provided by the ***Brain*** give both systems the performance necessary to provide top-level safety hazard and security threat detection, addressing both current and likely future requirements.

Coupling the ***Brain*** with conventional video analytics software provides automated surveillance scenarios by sending programmed text streams in English to the ***Brain*** when the particular algorithm identifies an anomaly.

Examples of this include:

- Tripwires
- Restricted areas
- Directional flow indicators (e.g., for traffic or human motion)
    - A person or vehicle going the wrong way on a walkway or roadway
    - A person or vehicle stopped on a walkway or roadway
    - A person detected in a buffer zone
    - A person detected climbing a fence
    - A person detected in a restricted area
    - A person carrying a weapon
    - An article left behind, such as a lunch box left next to a critical valve in a refinery, etc.

This technology actually provides the ***Brain*** with the ability to "see on its' own." Conventional video analytics systems do not provide the ***Brain*** with the ability to actually "see" a video image. Analytics software systems provide text information to the ***Brain*** about object classification and activity.

Researchers have developed a special vision system that accomplishes actual vision for both ***Safety 1*** and ***Security 1*** that we call ***Vision***. The ***Vision*** imagers produce 360° fields of view, binocular and telescopic vision, producing parallax and depth perception. This technology has been developed specifically for use with the ***Brain***. Without the ***Brain***, these imagers are without functionality.

Vision enables both ***Security 1*** and ***Safety 1*** to see and initiate its own surveillance; direct its attention to interesting activity; understand and decipher what it sees; and initiate appropriate response on their own. The transmission technology of ***Vision*** allows both systems to use less bandwidth and requires less electronic storage than existing video technologies. The ***Brain*** is "game changing" technology, and will have a powerful effect on the way video surveillance is deployed.

Conclusion

This paper outlines for all of us that safety hazards and security threats have common elements. These common elements need to be addressed by applying existing sensor technology, along with the ***Brain*** and ***Vision,*** to field ***Safety 1.*** The result is fewer safety hazards, and for ***Security 1,*** greater security threat detection, tracking, identification, and reporting. The architecture of each system lends itself to easily adding ***Safety 1*** to ***Security 1*** to field a system capable of detecting, tracking, identifying, and reporting *both* hazards and threats in real time to the local control room or a remote monitoring site. This advancement in mitigating risks is now a reality; we look forward to deploying it to reduce security threats and/or safety hazards, maintain within a cost-effective and efficient system, maintaining safety in our nation's critical infrastructure and other industrial sites. We can all sleep sounder with the ***Brain*** working for us.

<u>Estimated Benefit Potential</u>

The following represents the enormous potential for mitigating both safety hazards and security threats:

For Safety Hazard Detection Systems (***Safety 1***)*:*

a. Hundreds of U.S. petrochemical plants and refineries would benefit with ***Safety 1*** as a back up to existing fault detection systems under OSHA regulations. .

b. Petrochemical plants and refineries located in Latin America, Africa, the Mideast, and other problematic areas and operated by large U.S. oil companies would benefit from ***Safety 1*** providing backup to their fault detection system.

c. Facilities around the world would benefit from ***Safety 1*** as a detection and mitigation system for natural gas leak detection and vapor cloud detection. ***Safety 1,*** Class I, Division 2, thermal leak detector system, now under development, will provide low-cost leak detection for liquid natural gas (LNG) storage tanks and piping.

For ***Security 1*** Security Threat Detection Systems:

d. Approximately 7,000 U.S. petrochemical plants and refineries fall under DHS and CFATS security guidelines, and have been categorized into Tier 1 through Tier 4 facilities. An additional 200 facilities, located in Latin America, Africa, the Mideast, and other problematic areas, would benefit by utilizing ***Security 1*** and ***Safety 1*** systems.

e. Over 100 of the 6,000 offshore petroleum platforms that fall under the U.S. DHS are required to have security systems. Currently 62 (refining) platforms have these systems installed, while the remaining 6,000+ operate under a waiver by the U.S, Coast Guard. An increase in gulf coastal waters security threat (Orange to Red) could result in hundreds of additional platforms losing their waivers and being required to install systems.

f. An estimated 50 offshore platforms in foreign waters operated by U.S. petroleum interests have suffered attacks for kidnapping or other extortion or are at risk of such attack.

g. Over 30 large U.S. seaports fall under the DHS regulation. Some of these seaports are undergoing installation of initial security threat and radiation detection systems.

h. Over 300 U.S. airports fall under the DHS regulation. Some of these airports are undergoing installation of initial security threat detection systems. Hundreds of miles of the U.S. border with Mexico fall under DHS jurisdiction.

i. An estimated 200 precious metals and energy mines (such as coal) are located in hostile countries in Latin America and Africa, where attacks can shut down the mine, and kidnappings are common.

The evident need for reliable safety hazard and security threat detection systems requires examining new technologies that will benefit industry in terms of saving lives and maintaining production. Combining active detection technologies offers a solid view of what is to come in terms of protecting our critical and other high value assets with cost-effective systems.