white paper security series

Automatic Threat Assessment

IFF: Identification, Friend or Foe

Automatic Threat Assessment

The continual threat from terrorist activities at critical facilities requires early detection before they can reach their target and complete their mission. This in turn has resulted in the need for advanced security systems that can effectively detect terrorist activity, while at the same time, reduce the need to address alarms caused by normal friendly activity. “Automatic Threat Assessment,” also referred to as Identify Friend or Foe (IFF), is the ability to automatically acknowledge alarms created by friendly assets and can be achieved with a security system that goes beyond the typical ‘intrusion sensor only’ configuration.

The addition of a tracking system associated with ‘friendly’ vehicles and personnel can provide the missing information necessary to tighten security, reduce the need to take action on alarms caused by friendly targets, all the while reducing the cost of threat assessment in terms of both material and personnel cost. Whether you are a security professional trying to secure the physical assets of your company, a consultant helping that owner or an integrator installing the system, it is import to understand how tracking systems and intrusion sensors can work together to automatically classify an ‘Actual Intruder’ with high confidence and without operator intervention.

THE NUISANCE ALARM

Typical intrusion sensors include intelligent fences, ground proximity sensors, RADAR, LIDAR and video analytics. The role of the intrusion sensor is to identify a breach and provide that notification to a security person so they may perform verification. As shown in Table 1, the formal alarm types received from intrusion sensors include: Intrusion Alarm, Nuisance Alarm, Environmental Alarm and False Alarm. The intrusion sensor strives to have a high detection rate and a low false alarm rate. For this reason, the nuisance alarm can be problematic as it reflects a real event for the intrusion sensor, but it’s often a non-event for the security operator. It is the verification of some of these alarm types that can be addressed with automatic threat assessment.

> ***The nuisance alarm, as defined, is problematic in the fact that it is a real event that must be verified.***

THE VERIFICATION PROBLEM

This security dilemma deals with detecting actual intruders or terrorists in a secure area, yet in an active environment with ‘normal’ vehicular and/or pedestrian traffic. Typically, a secure area employs many sensors to detect intruders. In actuality, these sensors only provide a ‘Suspected Intruder’ list. The follow on task is to decide whether or not to reclassify a ‘Suspected Intruder’ as an ‘Actual Intruder’. This process is typically a manual task and can be difficult, confusing and requires crucial time.

Take the example of routine landscaping, whereby the landscape crew needs to access a gate in order to address vegetation on both sides of the perimeter. This type of event proves problematic. Intrusion sensors, such as, radar, video analytics or

ALARM TYPES	DEFINITION	EXAMPLE
Intrusion Alarm	Detection of a specified target, attempting to intrude into the protected area.	This is a real intrusion event which requires action on the part of the security team.
Nuisance Alarm	Detection of an appropriate alarm stimulus, but which does not represent an attempt to intrude into the protected area.	These types of alarms may, or may not, require action by the security team. An example might include a visitor who inadvertently gets lost and wanders into a restricted area, or perhaps wildlife that breaches the perimeter.
Environmental Alarm	Detection of environmental conditions which exceeds the operational tolerance of the particular device.	As the name implies, these are alarms induced by items like wind, rain, shadows, vibration and snow.
False Alarm	Detection when there is no alarm stimulus.	This is an alarm caused by a mechanical or software malfunction of the system.

Table 1 - Understanding Alarm Types

Intrusion sensors, such as intelligent fence, radar and video analytics, strive to have a high detection rate and a low false alarm rate.

an intelligent fence will all alarm on this event with a high degree of accuracy. Even for very accurate systems that can uniquely track the object over a long period, it is highly likely that over the period of time the landscapers are in the area, the track will be lost causing the system to re-alarm on the same person or vehicle, as it represents a potential intrusion.

It may also be the case that the landscaping crew requires the opening of a gate in order to facilitate their work. If that gate is integrated into the facility's access control system via a dry contact or beam breaker device, it may continuously alarm while left open, or at a minimum, in the case of the beam, each time one of the workers or the vehicle passes through the entrance. In these situations, security will either need to validate each alarm by verifying it on a camera or having an officer follow the landscaping crew throughout their route.
Another typical action is to temporarily disable the intrusion sensor, which now leaves a portion of the facility susceptible.

Finally, the existence of a "friendly" alarm event that needs to continue to be validated can result in the security personnel becoming complacent and either not verifying it, or not verifying it in a timely manner. Each of these actions takes resources, inhibits security from reacting to a real event and can potentially increase the risk of intrusion by disabling and re-enabling sensors.

LOCATING "FRIENDLY" ASSETS

This is where a tracking system can combine with the intrusion sensors to provide additional value. Tracking systems consist of two main types of locating devices: GPS-Enabled devices and transponder devices. A transponder is a wireless communications device that emits an identifying signal in response to a specific interrogation signal.

Advances in Global Positioning System (GPS) technology have facilitated the growth of GPS enabled tracking devices, which contain two functional parts: GPS receiver and wireless communication. Modern, low cost GPS receivers can achieve an accuracy rating of less than 3 meters, provide an update once per second and do not require visibility to the open sky.

Wireless communication is used to transmit the GPS data to the C2 system (See Table 2). A typical data set includes time, date, latitude, longitude, altitude, heading, speed, quality of GPS signal, etc.

COMBINING DETECTION AND LOCATION

With an understanding of intrusion sensors' ability to locate and detect intrusions and tracking systems' ability to locate personnel and assets, it now becomes easy to see how the combination of these types of systems can result in automatic threat assessment. Routine situations that require

Wireless Type	Advantages	Disadvantages
UHF/VHF	Long Range (up to 30 miles) 1 Second Update Rate Signal Penetrates Building No Monthly Cost	Low Data Bandwidth Requires FCC License High Initial Cost
ISM (900MHz)	Medium Range (up to 10 miles) 1 Second Update Rate Moderate Signal Penetrates Building No Monthly Cost Does NOT Require FCC License High Data Bandwidth	Moderate Initial Cost
Cell Phone (GSM CDMA)	Large Regional Coverage Low Initial Cost	Moderate Monthly Cost 5-10 Second Update Rate
WiFi	1 Second Update Rate No Monthly Cost Moderate Signal Penetration through Buildings	Low Range (up to 500meters)
Satellite	Worldwide Coverage	Low Data Bandwidth High Initial Cost High Monthly Cost Limited Signal Penetration through Buildings

Table 2 - Understanding Wireless Communication for GPS Tracking

Tracking systems can be GPS-based, using satellite triangulation, or transponder based, which utilizes locally based sensors.

significant security involvement, such as the landscaping scenario, now become an event that can be automatically managed by the system. With the augmentation of a tracking system, the Command & Control system now has the ability to know friendly targets and their location. Further, this allows the system to perform a check before actually alarming. In the case of a perimeter alarm, it now has the intelligence to understand, within a level of confidence, that the object detected by the intrusion sensors is the same friendly item being tracking by the tracking system. If the system determines the targets to be the same object, the alarm can be suppressed, eliminating the need for security to verify the event.

A COMMON OPERATING PICTURE

The actual integration of these types of systems is not complex in terms of how to coordinate data. Interface documents exist for these types of integration and are done on a regular basis. Typical position and target information is communicated over XML in a standard format. However, to gain these benefits the tracking systems and intrusion sensors must all work within a common geospatial operating picture.

Geospatial, or geo-referenced systems, have the understanding of how the system and its data relate to real world coordinates: latitude, longitude, speed, heading, altitude and time. Systems with this trait have several distinct advantages including the ability to easily display and control data in a map based format. Moreover, the ability to understand where an object is currently located in time and space is what allows tracking systems and intrusion sensors to synergistically perform automatic verification.

Additionally, this combined knowledge of the target's track also allows the fusing of the GPS data and the intrusion sensor data into a single object and path. This further aids security by reducing target and track clutter on his Command and Control or PSIM (Perimeter Security Information System).

A typical example is a guard, enabled with a tracking device, performing a tour around a fence protected by video analytics enabled cameras. On a typical PSIM, a normal guard tour would result in two icons on the display, one friendly from the tracking system and one unknown from the video analytics. This scenario would also result in two similar object tracks. Security would need to review the situation and understand that this symbology represents a single target and a single track.

The combination of intrusion sensors and a tracking system allows for Automatic Threat Detection.

Integrating the tracking system with the video analytics system allows for a fusing of this data, and the resulting Command and Control symbology is a single target and a single track.

ADDITIONAL CONSIDERATIONS

There are additional considerations that need to be understood when combining a tracking system with intrusion sensors. These include update rate, time & location accuracies and overlapping coverage.

Ideally, all sensors would be synchronized when it comes to timing aspects, but this is typically not the case. Different timing between data updates and time inaccuracies can result in the inability for the systems to confidently conclude that two tracks were created by the same target. Transport delay, the transmission of the GPS data through the satellite, can also be an issue. For tracking devices, it's vital for the data to be received by the C2 system with a repeatable transport delay. Variability in the transport delay also decreases the ability to automatically verify the threat.

Geographic accuracy of both the GPS tracker and the intrusion sensor is another important factor in data fusion. Typical GPS trackers have an accuracy rating for 3 - 10 meters. Actual accuracy varies based upon the visible GPS satellites, tall buildings, body worn, RF interference, etc. Intrusion sensors also possess an inherent accuracy. Radar surveillance may have a resolution of 1m x 1m at close range, but it expands at far range to 1m x 20m. Intelligent fence sensors and video analytic systems can have resolutions that vary from 1m to 25m, based on the type of sensor and the terrain. These geographic inaccuracies can be handled to some degree by considering other factors, including heading, speed, previous track, but it's important to understand where these inaccuracies can occur.

Overlapping Coverage of surveillance sensors also affects data fusion. In the case of track fusion, this ability is only available is areas where both a geospatial intrusion sensor exists and a tracking system is operational. If there are gaps in the overlapping coverage, or if there are areas that do not include geospatial based intrusion sensors, then fusion is not possible in those regions.

There are also other scenarios, where multiple geospatial sensors exist and they may all detect the same intruder. The C2 system must take into account all these sensors and merge overlapping intruder targets prior to data fusion. This will result in the ability to continue automatic threat assessment.

CONCLUSION

Security personnel face a difficult environment. They are continually presented with new types of sensors to help them detect, assess and react to security threats. At the same time they are expected to perform this task within current or reduced manpower limitations. Solution providers must determine effective ways to aid the first responder in these tasks. One means of achieving this is through the fusing of intrusion sensor and tracking system data. This combination of sensors can help relieve the operator workload by automatically assessing alarms created by friendly targets. This sensor combination also provides the basis for enhanced situational awareness, allowing the display of geospatial, fused target and track information on the operator's C2 display.

Eric Olson is Vice President of Marketing at PureTech Systems. He has a diverse experience in design and marketing of high technology products. He can be contacted at eric.olson@puretechsystems.com or Follow on Twitter - @ericolsonaz

Steven Pisciotta is President of Remote Tracking Systens. He is a 10 year veteran of the security industry and he has developed and managed mission critical system for over 20 years. He brings a wealth of knowledge of software/hardware technologies and the security market. Contact Steve at stevep@remotetrackingsystems.com

NEXT STEPS

Tracking Systems: Want to learn about how tracking systems can help your operation manage a vast array of moving assets within a variety of different geographic zones, while maintaining security standards? Download this brochure on advanced real time GPS tracking.

8 Things to Consider When Designing a Camera Perimeter: There are many guidelines that have been released that provide information as to the type of security measures that should be considered when protecting these facilities. However, the details involved with making these measures a reality are often missing. This paper presents 8 things to consider when designing a camera-based security system, or when reviewing your existing one.

Tweet this Paper!

About Remote Tracking Systems

RTS is an engineering and manufacturing company specializing in Global Positioning Satellite based tracking and security solutions for the military, industrial, education, and airport sectors. RTS answers the need for economical, real time tracking solutions by defining, designing and producing GPS based systems and components which have remote tracking capability. With headquarters in Phoenix Arizona, Remote Tracking Systems serves national and international markets. To find out more about Remote Tracking Systems Inc. visit our website at www.remotetrackingsystems.com or contact Gary Pisciotta at 267-733-4177 or e-mail us at info@remotetrackingsystems.com.

About PureTech Systems

PureTech Systems Inc. is a manufacturer of wide-area perimeter surveillance software solutions including internally developed outdoor video analytics, PTZ Auto Follow, multi-sensor integration and a map-based (real object size) command and control. It is offered to fortune 1000 firms, petro-chemical, water and electric utilities, seaports, airports and federal, state and local governments. With headquarters in Phoenix Arizona, PureTech Systems serves national and international markets. To find out more about PureTech Systems Inc. visit our website at www.puretechsystems.com , follow us on Twitter or sign up for our email list.