

INTRODUCTION

Track and tunnel intrusions, whether by employees, the public or those with malicious intent, represent serious risks for a rail operator, ranging from safety and liability concerns to the catastrophic impact of an attack. Operators incur increased risk every time an employee ventures onto the tracks to perform his duties. And, with the world's busiest systems carrying 5 to 10 million people per day, the sheer number of passengers translates into a high liability risk. Attacks, while rare, carry disastrous consequences further driving the need for increased track and tunnel protection.

Protecting against tunnel intrusion in subway and rail systems is a daunting task, but one that is increasingly being addressed by operators and governments. In the US alone, the Department of Homeland Security allocates hundreds of millions of dollars annually to support the deployment of tunnel intrusion detection and other systems through the Transit Security Grant Program.

To be effective, solutions that provide track and tunnel intrusion detection must include two essential capabilities.

Immediate notification and assessment: Every second matters for track and tunnel intrusions. The system must notify security personnel immediately and simultaneously provide the ability to assess the cause of the violation.

Full-time protection: Solutions must detect intrusions at all times, regardless of variable lighting conditions and the movement of trains. During rush hour on many transit systems, trains pass every few minutes, making detection during periods of train motion a requirement.

While the necessities of these capabilities seem obvious, current technology solutions fall short in one or both of these areas.

EXISTING SOLUTIONS

Existing attempts for detecting track and tunnel intruders fall into three general categories: CCTV only; CCTV integrated with perimeter intrusion sensors; and conventional video analytics. Each is described below.

CCTV only: From the Security Operations Center (SOC), personnel attempt to monitor the site video and respond to potential threats. In actuality, the primary benefit is for after-the-fact analysis, since it is impractical for the security staff to actively observe hundreds (or even tens) of cameras. As such, this approach provides neither immediate notification nor full-time protection.

CCTV plus perimeter intrusion sensors: Combining video with perimeter intrusion detection systems, such as those based on laser, vibration, infrared or microwave, provide automatic intrusion detection, with video providing the ability to assess the violation. However, despite the improvement over a video-only solution, this approach fails because it does not provide full-time protection. With vibration sensors, the movement of an intruder is masked by the train motion and



laser, infrared and microwave beams are broken by the train regardless of the presence of humans.

In addition to the security gap, this approach has other disadvantages. It is expensive, since two complete and independent security systems (video and perimeter sensors) must be installed and maintained; the integration between the systems is complex and may require custom software development, which is time consuming and difficult to migrate with software upgrades; and the “time to assessment” of the violation can take valuable minutes since the right video feed must be found and rewound to the appropriate time for observation.

Conventional video analytics: Train motion, and its reflections, creates havoc for conventional video analytics systems. These systems were designed to detect motion against a stable, well-lit background, not a human in a dark tunnel with train motion, with their flashing lights and the appearance of people within it. As a consequence, with each passing train, these systems too frequently generate false alarms, easily amounting to hundreds per hour. To cope with this situation, these systems are typically either disabled as trains pass or generate too many false alarms, limiting security protection.

INTRODUCING VIDIENT TRACK AND TUNNEL INTRUSION DETECTION SYSTEM

Vidient’s Track and Tunnel Intrusion Detection (T2ID) System is a video analytics solution that has been developed specifically for the needs of subway and rail operators to detect track and tunnel intruders. The system instantly recognizes violators, regardless of the presence of a train, and provides the ability for immediate assessment. As a result, it helps prevent accidents, attacks and other malicious events.

What makes T2ID truly unique is its ability to recognize the presence of a train and self-adjust so that it ignores the visual effects of the trains’ motion and the presence of humans inside the cars. This virtually eliminates false alarms, maintaining the viability of the system in all conditions. Whereas conventional video analytics systems are overwhelmed by false alarms or disabled during periods of train motion, T2ID is not. By automatically sensing the presence of a train and tuning out its effects, the system provides full-time protection against track and tunnel intrusions.



T2ID offers the following unique advantages:

Immediate Assessment: Within moments of a violation, a video clip or image is delivered to security personnel whether they are in the SOC or on patrol. Instantly, an assessment can be made, and an action plan put in place if necessary. At moments like this, every second matters. Any delay in assessing the alert can result in more severe consequences and additional loss of life.

Full-time protection: Previous generation solutions don’t provide reliable intrusion protection when a train is in motion. T2ID solves this problem. With it, system security protection is available full-time – with or without the presence of a train.

Low Cost: With previously installed video surveillance equipment, the incremental cost to add effective, automatic track and tunnel intrusion protection is small.

Ease of installation: As a software solution, installation doesn't require mounting new cameras, burying cable or aligning sensors, all expensive propositions. With T2ID, you only need to load software and adjust parameters to deploy effective track and tunnel protection.

Flexible Deployment Options: T2ID supports edge-based and centralized system designs, thereby easily fitting in to existing network and computing architectures.

OPERATIONAL EXPERIENCE

St. Louis Metro

St. Louis MetroLink recently completed the implementation of Vidient technology to detect track and tunnel intrusions. Like many rail transit systems, the public has easy access to the track and tunnels from the platform area. Whether by employees or the public, authorized or unauthorized, Metro wanted immediate notification whenever someone accessed the track or tunnel areas. "Metro needed a system that provided notification, with the ability for rapid assessment," said Willie McCuller, Director of Security for the transit system. "For example, if the tunnel intrusion happens to be done by a member of Metro workforce, there is no need to generate an alarm or to stop the trains on this line. On the other hand, if the intrusion had been done by an unauthorized person then safety measures must be quickly applied. So, seeing who is entering the tunnel as the alarm is being received definitely played in favor of using video analytics system over other systems that provided less visual information."



Metro developed strict performance requirements for accuracy and false alarms. The first video analytics system tested, based on conventional video analytics technology, confirmed the impracticality of these other systems. It generated hundreds of false alarms per hour on passing trains. After switching to Vidient technology, the false alarms were virtually eliminated and no known intrusions have been missed.

St. Louis Metro has deployed a system that, for the first time, protects against tunnel intrusions without triggering false alarms on passing trains. "We feel we've made a significant improvement in public safety and security with this system," says McCuller. "It converts our video system from a recording-only system to be used for forensics too late after a bad event, to one that can prevent accidents and other malicious events. We are immediately notified of intrusions when they happen, and we can initiate the appropriate response. We are pleased with this breakthrough solution for track and tunnel intrusion from Vidient."

Southeastern Pennsylvania Transit Authority (SEPTA)

SEPTA recently deployed Vidient technology to detect tunnel intrusions and unauthorized entry into station and equipment areas. The system detects intrusions on the tracks and into tunnels and sends alerts to the security operations center for assessment and action, if necessary. To validate the performance of the analytics, they conducted a comprehensive program to test the accuracy of detection and the avoidance of false alarms. The detection tests included humans intruding into secure tunnel areas and portals. False alarm tests included humans standing at the edge of the detection region, debris entering the track area and the motion of trains. Hundreds of tests were performed, under a variety of lighting conditions, in tunnels and passageways. "The system met our stringent test requirements, even in extremely dark tunnels," said Chuck Lawson,

Lieutenant and Commander of the Special Operations Unit. “The Vidient system enhances our security protection against unauthorized accesses and helps improve safety for our employees.”

WIDESPREAD DEPLOYMENT

Deploying analytics across a transit system requires little change to the physical security and video infrastructure, since existing analog or IP cameras and CCTV recording systems can be utilized. As a software solution, and not one embedded within cameras or other video hardware, the Vidient system doesn't require new cameras or other changes in network infrastructure. The success of the use of analytics and the ease by which it can be installed leads to expanding the use of analytics for other security applications, such as:



Theft and Vandalism: Whether by vandalism or theft, rail suppliers and operators incur millions of dollars of damage and losses each year. Video analytics technology provides enhanced intrusion detection, many times at half the cost of fence sensors and other traditional technologies. Analytics systems can monitor for potential threats outside the perimeter, including stopped cars, speeding vehicles and abandoned packages.

Abandoned and unattended objects: Just as with tunnel intrusions, mass transit systems present unique challenges for detecting suspicious objects. Travelers temporarily block the view of the object, and most objects, while stationary, are not actually left unattended. Video analytics can detect suspicious objects that are not closely monitored despite typical platform traffic. Upon recognition of an object, video is delivered to officers to identify the origin of the object, assess the risk and develop an action plan.

Overcrowding: Growing crowd or traffic congestion may indicate an operational problem or even an emergency situation. Specialized analytics solutions can monitor both the degree of occupancy and the speed of movement by people and vehicles in user-defined areas, alerting personnel when any issues are detected.

Loitering: Loitering, either human or vehicle, is often a precursor to malicious or dangerous activities. Even with diligent monitoring of CCTV video by security personnel, detecting suspicious humans or vehicles near high value or secure areas is difficult. Operating 24 hours a day, video analytics identifies potential threats before trouble occurs.

CONCLUSION

Track and tunnel intrusions currently represent a high safety and security risk for rail and subway operators and one for which previous solutions have been inadequate. These solutions, developed for general perimeter intrusion without accounting for moving trains, do not provide sufficient protection under the unique requirements of rail environments. T2ID from Vidient is the only solution that has been proven, based on actual operational experience, to provide the capabilities essential for effective track and tunnel intrusion, whether indoor or outdoors.

Without significant changes to video or network infrastructure, Vidient's SmartCatch system offers benefits for a wide range of security challenges including identifying unattended objects, protecting against perimeter intrusion and detecting suspicious movements. Overall the use of Vidient technology decreases liability exposure and provides superior security protection, and by adding to an existing CCTV system, these benefits are realized with low incremental cost.