Guarding the Tracks in Montreal

The Montreal Metro is Canada's second busiest subway system, and North America's fourth busiest in total daily passenger usage, delivering an average of 1,241,000 daily unlinked passenger trips per weekday (as of Q1 2013). The Metro is operated by the Société de transport de Montréal (STM), Montreal's metro transit authority. STM operates one of North America's largest urban bus and rail rapid transit schemes, serving the third-largest number of passengers overall behind New York and Mexico City, and attracting the second-highest ridership per capita behind New York. (See http://en.wikipedia.org/wiki/Montreal_Metro and http://en.wikipedia.org/wiki/Soci%C3%A9t%C3%A9_de_transport_de_Montr%C3%A9al.)

Figure 1 – The Place-des-Arts Metro station in Montreal on a busy day

In 2008, STM sought to improve public safety by some automated means of detecting people intruding on the tracks and into the tunnels of the Montreal Metro. They already had a substantial video surveillance system based on Loronix software running on Windows servers. Almost 300 of the several thousand cameras were viewing the Metro tracks and tunnels. Intrusion detection by video analytics software running on Windows servers would fit well into STM's existing infrastructure and information technology skills.

No one had ever successfully deployed a video-based intrusion detection system on such a large scale in the difficult metro rail environment, in which camera views are often filled with the large motion and illumination variations of a train. This makes motion-based video analytics temporarily useless. But Vident Systems of California had successfully deployed its SmartCatch video analytics software running on Windows servers for rail intrusion detection on a small scale. SmartCatch already had advanced capability to reliably recognize a walking or running human being – even with only 60-70 pixels on the target. (See Figure 2.) Vident committed to solving the problem of dominant train motion and STM contracted them.

Figure 2 -- Small human figure detected by SmartCatch on the tracks in the Montreal Metro

STM was well aware that the performance of video analytics for intrusion detection is a trade-off between the probability of correctly detecting an intrusion and the rate of false alarms. STM knew that too many false alarms would cause operators to lose confidence in SmartCatch. If control center operators saw too many false alarms, they would stop trusting the system and tend to regard alarms like the cries of the boy who cried “Wolf!” falsely and thus got no attention when he actually detected a wolf. Operators might even turn the system off.

Many video-based intrusion detection installations can tolerate up to one false alarm per camera per day. But with almost 300 cameras running video analytics in the Montreal Metro, a much lower false alarm rate would be essential. If these cameras were generating one false alarm per camera per day,

there would be a flood of false alarms -- one every 4-5 minutes on the average, worst at busy train times because train motion is the primary trigger of false alarms. This would be intolerable. The false alarm rate had to be much lower, while maintaining 90%+ correct detection rate.

Normal operations in Montreal generate about 200 authorized intrusions by work crews every day, giving a very useful ongoing check of sensitivity. The Montreal Metro authority required that there be no more than 0.5 false alarms per camera per day – about 150 for the whole system. Thus correct detections would at least be noticeably greater than false alarms.

For almost a year, Vidient and STM cooperated in the development of improved SmartCatch software that could successfully detect a human intruder on a catwalk right next to a moving train filling most of the camera's view – while generating a minimal number of false alarms. (See Figure 3.) As demonstrated in a week-long acceptance test in August, 2009, and again in the summer of 2011, the result is a false alarm rate of 0.15 to 0.20 false alarms per camera per day. The ratio of correct detections to false alarms is at least 5 to 1, giving the operators confidence in the system. The probability of correct detection is approximately 95%.

Figure 3 -- Intruder detected by SmartCatch on a catwalk next to a moving train in the Montreal Metro

The SmartCatch deployment has made a notable improvement in public safety. According to Claude Ouellet, Professional Engineer and Manager of Telecom Operations Engineering at STM, "The principal reason to use SmartCatch is to be notified right away when a person gets onto the tracks from the platform, or is getting into the tunnels. When this happens, our control center can immediately turn off the power on the rails, advise the person to evacuate with speakers in the station, and get our agents on site immediately. This may prevent people from getting electrocuted or hit by an oncoming train. This also reduces the time for our police officers to get into the tunnel to arrest the person. Every time a person gets into the tunnels also causes a service interruption of many precious minutes. SmartCatch is helping us to reduce this time, and better protect our public."

SmartCatch has also been quite useful for detecting vandals who enter train yards with intent to paint graffiti on the trains. They have been promptly caught in the act and arrested.

SmartCatch works by combining advanced computer vision with the detailed knowledge of human operators. While SmartCatch can filter out trains, handle fast-changing illumination, and distinguish a person from other motion, skilled staff must precisely define various regions of interest in each field of view. "When setting up a new SmartCatch system, it is very important to define precisely the borders of the zones that need to be monitored for intrusions in order to prevent false alarms when people merely get close to the controlled areas -- for example, the top versus the bottom of stairs that lead from the platforms down to the catwalk in the tunnel," says Monsieur Ouellet.

Successful use of SmartCatch also requires thoughtful integration with the operations of multiple departments. Crews who maintain the CCTV cameras must always inform SmartCatch administrators of any activity that might change any camera's resolution or field of view, because the borders of the zones mentioned above must be carefully matched to the changes. Another example is given by Monsieur Ouellet: "Since SmartCatch detects any human intrusion into the tunnels or onto the rails, good processes and employee collaboration are required in order to notify the control center every time that normal operations require an authorized track or tunnel intrusion. If employees forget to advise the control center in advance, it generates an unwanted distraction and loss of precious time for control center operators." Furthermore, while authorized intrusions are useful as an ongoing check of SmartCatch sensitivity, good employee communication must clearly distinguish these from unauthorized intrusions requiring emergency response. Otherwise, control center operators may become desensitized by too many unexpected alarms and miss unauthorized intrusions.

STM expressed its continuing confidence in SmartCatch in 2012-2013, when it upgraded its thousands of video surveillance cameras from Loronix to Verint Nextiva video management software. Since 2012, SmartCatch has been developed, delivered, and supported by AgilityVideo LLC (http://www.agilityvideo.com) under an exclusive license to all of the SmartCatch technology. STM contracted AgilityVideo to integrate SmartCatch with the new Verint Nextiva video management system and to provide ongoing technical support. This conversion was completed in spring of 2013, ensuring benefit from SmartCatch for years into the future.

STM and AgilityVideo continue to cooperate to maintain and improve the performance of SmartCatch in Montreal. Several future feature improvements are being considered:

1. Delivery of SmartCatch intrusion alarms to STM's overall command-and-control system built by Alstom
2. Automatic audio warnings from loudspeakers triggered by SmartCatch intrusion alarms
3. Using electronic access control information to filter out SmartCatch detection of authorized intrusions

About the Author

J. Michael Rozmus (http://www.linkedin.com/in/rozmus) is the founder and CEO of AgilityVideo LLC (http://www.agilityvideo.com), provider of SmartCatch automated video surveillance and other services related to large-scale video surveillance – especially for the protection of critical infrastructure. He can be reached at mrozmus@agilityvideo.com.