Remote Controlled Marine Security of Locks

Inland Navigation Channels: Safety and Reliability

By: The St. Lawrence Seaway Management Corporation (SLSMC)

This presentation will be of interest and benefit as it provides insight into a working implementation of remote controlled, state-of-the-art security access control and intrusion detection of locks and bridges in an inland waterway system.

In 2008, when the ISPS code in Canada was implemented, the physical security of the Seaway's Canadian locks and bridges was improved. From 2013 to 2017, all of our locks were equipped with vacuum mooring technology, subsequently allowing for remote control of these same locks.

In 2015, while implementing remote control of the locks machinery, the increased level of marine security threat required even more security safeguards. The goals were to better protect against unauthorized access, have increased control of who was accessing our facilities and vessels, and also improve the continuous monitoring of those facilities. With our on-site staff being reassigned to remote operations control centers and therefore no longer available to personally monitor the locks, these goals could no longer be achieved.

For vehicles, access control points with dual motorized gates were installed, where cameras are used to perform vehicle inspections. Pedestrian identification reporting stations have also been established where persons requiring access (pilots, service to vessels providers, mariners, lock maintenance personnel, etc.) can get their identification and credentials validated using video and intercom technology prior to entering through a controlled access turnstile. Furthermore, non-automated access points are monitored through the use of an electronic key control system.

Continuous monitoring is performed using thermal imagery cameras with intrusion detection video analytic software. This has been a challenging application to design and configure as the intrusion detection system has to cope with several moving targets in an outdoor environment such as movement of ships, movement of lock equipment, public vehicles, nearby pedestrians, wildlife, etc. The thermal imagery intrusion detection is also complemented by break beams, motion detectors and conventional building intrusion detection hardware.

This project also involved a significant upgrade to our telecommunication and computing infrastructure. Local and inter-city network connections had to be improved for both bandwidth and latency to support all video, audio and control feeds. Additionally, we integrated the new security technologies within our cyber security; all central controls and networking cabinets are now physically protected and form part of the restricted area. Two form authentications for operator stations have also been implemented. Our security system software, along with our video control software are now running from a fault-tolerant physically distributed virtual computing environment.

In conclusion, access control and security incident response has now been fully integrated into the canal operators' roles. Remote controlled security protocols are being effectively applied without the need for a dedicated security department. Furthermore, this provides vessels with a more secure passage in our inland waterway system while also achieving our staffing optimization goals.