REMOTE CONTROLLED MARINE SECURITY OF LOCKS

By: Luc Boisclair, P. Eng

INLAND NAVIGATION CHANNELS: SAFETY AND RELIABILITY

This article provides insight into a working implementation of a remote controlled, state-of-the-art security access control and intrusion detection system at locks and bridges in an inland waterway.

The Story

The St. Lawrence Seaway Management Corporation *(SLSMC)* operate and maintains all Canadian Locks, Bridges and Channels that allow domestic and foreign vessels to navigate from the Atlantic into the Great Lakes. We manage 13 locks, 18 movable bridges, 13 km of approach walls, a power generation plant, fixed bridges and channels spread over 325 nautical miles (600 km). Our mission is to serve our customers by passing ships through a safe, secure and reliable waterway system in a cost effective, efficient, environmentally and socially responsible manner to deliver value to the North American economy.

In 2008, when the IMO (International Maritime Organization) ISPS (International Ship and Port Facility Security) code was implemented in Canada, the physical security of the Seaway's Canadian locks and bridges was improved mainly by installation of perimeter fencing, manual access control gates and basic PTZ (pan-tilt-zoom) surveillance cameras. Security responsibilities, including monitoring, were assigned to our locks personnel. Our Operations Control Center staff also had approximately 100 cameras available to validate security issues, although these were primarily used to support marine traffic operation.

In 2013, the Modernization Project was started, with the goal of increasing safety of operation, along with cost efficiency by 1) automating vessel mooring in order to remove the dangerous handling of steel mooring lines & 2) controlling our locks remotely from our Operations Control Centers. From 2013 to 2017, all locks were equipped with vacuum mooring technology along with controls and telecommunication for remote operation.

In 2015, improvements were required to our security posture during the re-assignment of our lock personnel to the Operations Control Center. Consequently, our Marine Security Project was created and integrated along with our modernization efforts. The objectives were to increase protection against unauthorized access, increase access control of our facilities and vessels, and improve the continuous monitoring of those facilities.

Within the next three years, the Marine Security Project would see to the implementation of the new security system at 13 locks, 7 free standing bridges and multiple other administrative, maintenance or support function buildings. Although we preferred at the time to use a design-build contractual approach, there was a need to quickly fix a few vulnerabilities. That civil work immediately created a fast track situation causing us to proceed with some in-house design followed by a main design contract and finally, a main supply and install contract with a national security company.

The Technology

Those requiring access include our own lock maintenance and operations personnel, pilots, mariners, vessel service providers, etc. Identification & access control smart cards are now issued by the Seaway for most regular users, while others can have their credentials validated remotely.

The St. Lawrence Seaway Management Corporation, lboisclair@seaway.ca
Canada

For vehicle access control, dual motorized gates were installed and cameras were added in strategic locations to perform vehicle inspections. Drivers are now asked to step out of the vehicle and open doors to allow the remote operator to view contents of the vehicle.

For pedestrians, single person turnstiles with reporting stations have been installed. Pedestrian can now gain access by using their access card followed by a pin code entry or they have their identification validated by the remote operator who uses a camera mounted on the reporting station and an intercom to interact with the person requesting the access.

Additionally, non-automated access points are monitored through the use of an electronic key control system. Access to these manual gates, which are less frequently used, is done by first 'borrowing' the appropriate key from a key dispensing box. The key control system is integrated into our security software and allows the operator to track the older of the key.

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 such as movement of ships and of lock equipment, public vehicles, nearby pedestrians, wildlife, etc., in an outdoor environment. The thermal imagery intrusion detection is also complemented by break beams, motion detectors and conventional building door and window closure detection hardware.

Several PTZ (pan, tilt & zoom) IP (Internet Protocol) cameras were also installed at each of our locks to improve investigation capabilities and promptly respond to security incidents. PA (public address) systems were already present at some locations in a different capacity and were upgraded to have improved coverage at all locations.

In the Operations Control Center, the software for security and video systems form an integral part of the lock operators' workstations. The security system software's intrusion detection alarms automatically triggers camera placement and video playback loops within the video system software. Digital video recording is generated for all camera feeds, including thermal video.

This project also involved a substantial 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 applied cyber security measures to our new security technologies. All central controls and networking cabinets are now physically protected and form part of the restricted area. Two factor authentications for operator stations have also been implemented. Both software for the security system and video control are now running from a fault-tolerant physically distributed virtual computing environment.

How it Works

Access control and security incident response activities are fully integrated into the lock operator's role. The security protocols are effectively applied without the need for a dedicated security department. For incidents that cannot be managed remotely, a roving team member is sent to investigate and/or if there is an imminent threat, local police is called. We also have maintenance personnel that can respond around the clock, interrupting their maintenance activities being conducted at a nearby structure or maintenance center.

The benefit is that the operator has constant situational awareness of anything which could impact the security of the transiting vessel. The operator knows who is at the lock and is in constant communication with the vessel master (pilot or captain) to ensure integrated security. Furthermore, this provides vessels with a more secure passage in our inland waterway system while also achieving our staffing optimization goals.

Since security tasks must be executed flawlessly, one main challenge is to ensure that we have sufficient staff to do both security and operations tasks in a variable staffing environment. When vessel traffic is light, the Operations Control Center is not fully staffed and when peak of work arise, staffing

needs to be quickly ramped up. It is therefore critical to minimise false alarms and keep the security system operating at peak performance in order to avoid the generation of any additional and unnecessary burden to operators.

In the beginning, access control or intrusion detection response duty was considered a distraction to the operator from their core task of processing vessels. With change management, time and proper training, security tasks are now an integral part of normal operation, much like safety and transit efficiency.

This is not only a technology implementation project. The improved security posture is maintained through several layers of multifaceted security measures that includes improved physical security, social engineering, cyber security, all of which are interconnected. In order for the system to remain effective, the technology needs constant care and support.

The new security system was designed to cover the application of MARSEC Level 1 though it will also facilitate operation at MARSEC Level 2 without substantial additional staffing costs. At MARSEC Level 3, our operation would be temporarily shut down and as such there are not any specific provisions for MARSEC Level 3 in this project.

Lessons Learned

One success story was the test of the integration between the security system, the video analytic software and the video display software early in the design. Although all suppliers claimed interoperability, a certain amount of customization was required. Those requirements were defined ahead of time, which allowed us to shorten implementation time and costs.

On the constructive side, the following items were either unexpected or did not go as well as anticipated;

- Overall security system performance accountability: Holding the general contractor of the security project accountable for the overall performance of the system was not possible. Malfunctions and limitations could develop within any of the telecom, networking, computing or software layers, which we would internally be responsible to resolve. In addition, because of the environment, the security contractor did not want to commit to meeting a certain level of false alarm rate standards. As this issue extends into the future, it will be difficult to establish an in-service support and maintenance contract with a sole provider, along with a defined service level agreement.

- It was quickly realized that intrusion detection using video analytic processing of thermal imaging could not be designed and scoped with precision ‘on paper’. ‘Dead spots’ were identified only once the installation of the first set of cameras on a lock was completed, and thus, additional hardware was required to correct deficiencies through trial and error. Although equipment manufacturers and designers had software tools to evaluate the theoretical coverage, some modifications were in fact required. Several weeks of auto-learning mode and manual tweaking of the physical mounting, zone definition in the software, etc., was required to get the false alarm rate to a reasonable level. Some of these efforts are still required when seasons and/or weather conditions change. Every season brings various challenges, such as the angle of the sun, different types of precipitation and varying wildlife. Finally, as minor changes to technology occur, or changes to the environment are required, constant support from technicians is essential on a steady state mode, in order to ensure the false alarm rate stays within manageable levels.

- This project involved several layers of complexity;
    - Two languages (French and English)
    - Two geographical regions with previous regional standards
    - Mixed technology starting points
    - Some local specific requirements
    - The need to keep existing systems in place while the new system was being rolled out through different go-live dates for each individual location.
    - With a fast paced technology development, some of the selected components were declared obsolete before being installed.
    - Evolving requirements: during the deployment of the new system, other ideas were being tested and designs were continuously being improved.

Conclusion

Although the project timeline had to be extended by one year, we were able to provide the basic functionalities on schedule to support the remote control of the locks. Our Marine Facility Certificate of Operation has recently been renewed for 5 years; a testimony of our capacity to meet regulation requirements in the new operating model.

Furthermore, this project provides vessels with a more secure passage into our inland waterway system, while also achieving our staffing optimization goals.