Project 20-07, Task 424

AASHTO GUIDELINES FOR THE OPERATION OF MOVABLE BRIDGES FROM REMOTE LOCATIONS

Prepared for:

National Cooperative Highway Research Program
Transportation Research Board

of

The National Academies of Sciences, Engineering and Medicine

Prepared By:

Robert S. Moses, P.E.
HDR Engineering, Inc.
1037 Raymond Blvd. – 14th Floor
Newark, NJ 07102

August 2020

The information contained in this report was prepared as part of NCHRP Project 20-07, Task 424, National Cooperative Highway Research Program.

Table of Contents

ACKNOWLEDGEMENTS

This study was conducted for the National Cooperative Highway Research Program of the National Academies of Sciences, Engineering and Medicine, with funding provided through the National Cooperative Highway Research Program (NCHRP) Project 20-07, Task 424 AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations. The NCHRP is supported by annual voluntary contributions from the state Departments of Transportation. Project 20-07, Task 424 is intended to fund quick response studies on behalf of AASHTO. The report was prepared by Robert Moses, P.E. of HDR Engineering, Inc. The work was guided by a technical working group. The project was managed by Dr. Waseem Dekelbab, NCHRP Senior Program Officer.

EXECUTIVE SUMMARY

Federal Regulations require movable bridges over navigable waterways to open on demand or in accordance with an approved operating schedule. As such, movable bridge owners expend significant funds staffing bridge tenders at each bridge to safely operate the movable span and related traffic control systems to allow vessels to pass through the open draw. Over the last two decades, an increasing number of highway and railroad bridge owners have sought to reduce these expenditures by operating their movable bridges from a remote location, thus permitting a single bridge tender to operate more than one movable bridge.

The primary motivation of bridge owners to implement remote operations is to reduce their overall workforce of bridge tenders. Technology enhancements, and the reduction in costs to deploy same over the last decade have led to an increased appetite for implementing remote operations. The potential cost savings for State Department of Transportation (DOT) agencies and Local governments, railroad bridge owners and other bridge owners by replacing onsite movable bridge tenders with remote operating systems is significant; however, there are no published guidelines to inform bridge owners regarding the risks associated with remote operations and the requirements for implementing reliable remote bridge operating systems to ensure that both maritime and land traffic can transit these bridges safely with minimal delay.

The objective of this research project is to evaluate the risks associated with remote bridge operation and to develop AASHTO guidelines for implementation of reliable remote roadway movable bridge operating systems. The guidelines are intended to assist movable bridge owners and designers in the operational and technical considerations required to operate their bridges remotely. The research conducted yielded the conclusion that safe, reliable and efficient operation of movable bridges from remote locations is indeed feasible. Prudent design and application of technology in the bridge control, surveillance and communication systems will provide reliable means of remote operation. These technical enhancements paired with programmatic operation and maintenance protocols can provide remote bridge operations in accordance with applicable regulations while permitting bridge owners to potentially reduce their operating costs. The proposed AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations were developed to address all of these areas of consideration and are appended to this report.

1 CHAPTER 1 BACKGROUND

1.1 General

Movable bridges pose significant operating and maintenance costs to their owners. Per the Code of Federal Regulations, movable bridges are expected to be operable on demand or per an approved operating schedule thus requiring bridge tenders to be regularly assigned to each bridge. Even on frequently operated bridges, much of the tenders' time is idly spent awaiting the next bridge opening request. Given the improvements in bridge control, surveillance and communication technology, bridge owners have been exploring means to improve the operating efficiency of movable bridges and reduce labor costs where feasible.

Over the last two decades, an increasing number of highway and railroad bridge owners have explored the possibility of operating their movable bridges from a remote location, thus permitting a single bridge tender to operate more than one movable bridge. Technology enhancements, and the reduction in costs to deploy same over the last decade have led to an increased appetite for implementing remote operations. The primary motivation of bridge owners to implement remote operations is to reduce their overall workforce of bridge tenders. The potential cost savings for State Department of Transportation (DOT) agencies and Local governments, railroad bridge owners and other bridge owners by replacing onsite movable bridge tenders with remote operating systems is significant; however, there are no published guidelines to inform bridge owners regarding the risks associated with remote operations and the requirements for implementing reliable remote bridge operating systems to ensure that both maritime and land traffic can transit these bridges safely with minimal delay.

Of particular concern is the cyber-security risk associated with remote operating systems and considerations for reducing that risk. Cyber-attacks on these systems have the potential of causing major loss of life and severely damaging the nation's critical infrastructure, equaling or exceeding the effects of conventional attacks.

1.2 Objective

The objective of this research is to evaluate the risks associated with remote bridge operation and to develop AASHTO guidelines for implementation of reliable remote roadway movable bridge operating systems. The guidelines are intended to assist movable bridge owners and designers in the operational and technical considerations required to operate their bridges remotely. Remote operating systems are intended to be compatible with existing operating systems in place for ease and efficiency of deployment, training, and maintenance.

2 CHAPTER 2 Research Approach

The approach to develop the proposed guidelines included performing literature reviews, administering surveys, developing risk assessments, conducting technology assessments, and researching detailed examples of remote bridge operating systems.

2.1 Literature Reviews

The objectives of the literature review of relevant domestic and international research, guidelines, and current practices were to determine the current state of knowledge on (1) remote bridge operating systems and (2) issues related to remote bridge operating systems. This information is prescribed in the scope of work to be assembled from published and unpublished reports in use by state DOT, transportation agencies, railroad companies, and other bridge owners to learn about the available systems, the technology used to implement these systems, and the advantages or disadvantages inherent with these systems. Details of several distinct existing bridge remote operating systems were reviewed along with the general movable bridge operating regulations contained in Title 33 of the Code of Federal Regulations (CFR) Part 117 Subpart A to ensure that the United States Coast Guard (USCG) requirements and movable bridge regulations were considered throughout the research work and its results.

2.2 Survey Results

As the research commenced under this project, it became readily apparent that very little information is published with regard to remote operation of movable bridges, but based on the awareness of current practices, several movable bridge owners have been actively pursuing remote operation of movable bridges over the last 20 years. Given the lack of published information to this end, research was conducted in the form of written surveys and telephone interviews to movable bridge owners that have implemented remote operations to solicit best practices and lessons learned by owners whom have successfully implemented remote operation of their movable bridges.

Completed surveys were received from the following agencies:

- Wisconsin Department of Transportation
- CSX Transportation
- City of Milwaukee
- Ohio Department of Transportation
- Svenska Teknikingenjorer Sting AB (Control System Integrator, Sweden)

The surveys are located in Appendix A.

2.3 Risk Assessment

The research identified the risks associated with managing movable bridge operations, recognizing that the risks are the same whether operating locally or remotely; however, where the tender is stationed impacts how these risks are managed. Typical risks associated with movable bridge operations include:

- Life safety risk to navigation, vehicular (motorized and non-motorized, inclusive) and pedestrian users and bridge maintenance personnel during bridge operations
- Risk of delays to bridge users due to bridge inoperability or malfunction
- Risk of facility damage due to fire or unauthorized access

Implementation of remote bridge operations inherently introduces the need for additional means to mitigate these risks when compared to local bridge operation. A remote tender must have the same abilities of a local tender in order to safely manage risk, otherwise the potential for increased incidents may occur such as:

- Increased risk of safety-related incidents to navigation, vehicular and pedestrian users due to:
  - Reduction in tender visibility of the bridge and its users
  - Reduction in the tender's ability to communicate with bridge users (e.g. flag signaling with mariners)
  - Reduction in the ability to detect potential hazards or incidents at the bridge
- Increased risk of delays to bridge users due to bridge inoperability potentially caused by:
  - Introduction of additional control equipment required to operate remotely
  - Introduction of a communication link between the remote operating site and the bridge
  - Reduction in the ability to detect potential maintenance needs at the bridge
  - Unauthorized access/vandalism
  - Delayed detection of smoke or fire conditions
- Increased risk of unauthorized operations due to introduction of remote operating equipment and communication links, such as cyber-attack.

In order to implement additional mitigation techniques to manage the risks posed by remote bridge operations (compared to conventional local operation), technology enhancements, design improvements and operation and maintenance practices were researched and assessed for feasibility and practicality and included in the guidelines as appropriate.

2.4 Technology Assessment

Safe and reliable implementation of remote bridge operations depends on utilization of available technology to help manage the risks and requirements of remote operation. For the purposes of this research, technology was assessed for potential application in the following bridge operating sub-systems:

- Bridge Control System
- Surveillance System
- Communication System

Research was conducted to identify applicable system components and design practices that could be implemented to enhance safety and reliability of remotely operated bridges. Bridge control system components such as Programmable Logic Controllers (PLC), automated drive systems, and human machine interface devices were researched to determine the optimal requirements for application in remote operating systems. A host of surveillance technology was assessed as part of the research as identification of bridge users during remote bridge operations was deemed one of these most significant risk elements critical for safe operations. The communication assessment included researching two-way audible communication system between the remote operating site and the local bridge as well the communication link and cybersecurity measures to secure reliable data exchange between the remote and local sites.

2.5 Project Examples

In an effort to coordinate the research conducted with real-world applications of remotely operated bridges, several project examples were reviewed to identify common design practices and operational procedures to optimize reliability, safety and compliance with regulations. As part of this research, the Principal Investigator contacted several bridge owners currently operating bridges remotely or studying implementation of remote operations. Several public bridge owners were willing to share their project documents while the private rail owners were not agreeable to share examples.

Public highway bridge owners that currently operate remotely include the Wisconsin Department of Transportation (WisDOT) Northeast Region and the City of Milwaukee. The State of Illinois Department of Transportation (IDOT) is currently implementing remote operations for several bridges in Joliet, IL. This project is currently under construction. The City of Seattle Department of Transportation (SDOT) has studied implementation on five bridges under their jurisdiction.

Wisconsin DOT, Illinois DOT and the Seattle DOT have agreed to share their plans and studies with the Panel as part of this research project. Copies of the emails granting permission were received and were included in the task Interim Report. The file containing the compressed files of the plans and studies is stored in the Workfront project database with the filename:

NCHRP-20-07-Task-424-ID3A-02-2020-Ver0

Filesize: 1,011,749 KB (compressed)

The project examples were reviewed to identify common and innovative design features that provide for safe and reliable remote bridge operations in compliance with applicable regulations. The examples were also reviewed to assess the prescribed remote operating procedures. A summary of the features found in the project examples is as follows:

- Closed loop span motor drives under PLC-based control
- Redundant central processing units in the PLC control system
- Locally-based control system, independent of the remote control system
- Redundant span drives to minimize down time should the primary span drive system fail to operate
- Private, robust fiber optic communication links between the local bridges and remote operating station
- Redundant communication link to serve as a backup to the primary communication link
- Dedicated, remote operating station with numerous camera views, two-way communication system and comprehensive bridge control system interface
- Management of remote tender workload with two to three bridges under a single tender's purview
- Remote/local lock-out switch to prevent remote operation when local operations are required (in the case of performing routine maintenance, for example).
- Implementation of remote operations via a pilot program staffed with local tenders to oversee remote operations and intervene as required to optimize safety
- Implementation of contingency plans to operate the bridges locally should weather conditions or equipment malfunction prevent safe remote operations

- Utilization of multiple surveillance technologies to optimize safety to bridge users and mariners
- Ability to respond to a variety of bridge opening requests from mariners per Coast Guard Regulations such as marine radio, horn blasts, cellular telephone and visual signals

These design practices and operational procedures were considered for inclusion in the proposed AASHTO bridge remote operating guidelines. Many of these practices and procedures confirm the research findings that were developed in prior tasks in this project. The project examples reviewed provide validation of this prior research and offer real-world application of successful techniques for implementing remote bridge operations. These design features were then incorporated into the proposed guidelines.

3 CHAPTER 3 FINDINGS AND APPLICATIONS

3.1 Current Practices

Railroad owners were the first to implement remote operations over the last two decades for the primary reason that they control the bridge rail traffic users directly and therefore, could manage the risk of inadvertently operating the bridge with traffic crossing the movable span. Of course, the USCG has jurisdiction over movable bridge operations and the rail bridge owners discovered through their coordination efforts that most USCG Districts required remotely operated movable bridges to be stored in the normally open position for navigation and be lowered for rail traffic to pass as a condition of permitting remote operations. Once the rail traffic passes, the bridge would then be opened again for navigation thereby minimizing the potential risk of delays to mariners.

Early in the implementation of remotely operated movable bridges, management of marine traffic typically consisted of pre-recorded messages broadcast over marine radio and local public address system to warn of impending bridge lowering. Requests for bridge openings from mariners at on-demand bridges would typically be made via telephone for permitted bridges with advance notice requirements. These communication protocols which vary from standard operating procedures are specified for each applicable bridge in Title 33 of the Code of Federal Regulations Part 117 (33 CFR 117) Subpart B.

While these typical practices have been largely successful for rail bridge owners, highway bridge operators do not share the luxury of storing movable bridges in the fully open position. As highway bridge owners have explored or implemented remote operations, management of motorized vehicles, non-motorized vehicles and pedestrians present additional challenges. While the risks remain the same, whether operating locally or remotely – namely not opening a movable span while occupied by topside traffic or lowering the bridge onto or in the approaching path of a marine vessel traversing the navigable channel – additional risk mitigation techniques must be implemented to account for the tender being remotely located. Current practices employed by bridge owners operating bridges remotely include applying enhanced surveillance systems to monitor topside and navigable channel traffic as well as environmental conditions, deploying two-way communication systems between the bridge and the remote operating station and implementing additional supervisory controls to verify judgment and decision-making by the bridge tender during bridge operations.

3.2 Regulation Compliance

Movable bridge operations fall under the jurisdiction of the United States Coast Guard per Title 33 of the Code of Federal Regulations, Part 117 – Drawbridge Operation Regulations, hereinafter referred to as the 'regulations.' Subpart A of the regulations specify General Requirements for bridge operations while Subpart B lists the Specific Requirements for individual bridges that fall outside of the general requirements.

The general requirements cover all relevant obligations of mariners and bridge owners and the USCG's position is that a remotely operated bridge must comply with all pertinent requirements in the regulations. Owners that have successfully implemented remote operations have focused on said compliance. The research conducted under this project focused on developing design guidelines to fulfill all requirements contained in the regulations in a safe and efficient manner.

3.3 Guidelines Overview

The guidelines were developed and organized into the following categories:

- Programmatic Assessment
- Control Systems
- Surveillance Systems
- Communication Systems

The guidelines are attached in Appendix C. A brief summary of the findings relevant to the development of the guidelines are discussed herein.

3.3.1 Programmatic Assessment

In addition to a wide variety of technical requirements that must be addressed to implement remote bridge operations, the research revealed the need for bridge owners to perform assessments of their bridge operation and maintenance practices and develop procedures and protocols to effectively implement remote operations safely and effectively.

3.3.1.1 Remote Tendering Capacity Assessment

Implementation of remote operation of movable bridges will likely entail tasking the remote tender with responsibility for operating more than a single local bridge. In this case, the owner shall assess the current and future navigation traffic at each bridge to be remotely operated and determine the appropriate number of remote operating stations, tenders and tender shifts required to meet operating demands. In no case, should the workload of a remote tender delay requests for openings from mariners nor adversely impact safety and reliability of the remotely operated bridges. A navigation study shall be conducted to verify the number of remote operating stations is appropriate given the local bridges to be operated remotely.

3.3.1.2 Contingency Planning

Bridge owners undertaking remote operation of movable bridges should develop contingency plans to locally operate the candidate bridges should equipment failure or environmental conditions resulting in poor visibility prevent safe remote operations. While prudent design will preclude a single component failure from interrupting safe, reliable remote operations, contingency plans to operate the bridges locally will likely be required. The owner should consider proposed maintenance practices along with contingency operation plans when developing the maintenance program for remotely operated bridges.

3.3.1.3 Incident Response

Given that the local bridge tender is typically considered the first responder to emergencies and unexpected incidents on movable bridges, owners should develop incident response plans to effectively detect accidents, security breaches, fire alarms, etc. and respond expeditiously without undue delays to marine traffic. System designers shall consider the remote tender's ability to detect incidents and to be alerted of abnormal conditions through the prudent design of surveillance, communication and control systems.

3.3.1.4 System Compatibility

In order to minimize initial capital investment, bridge owners undertaking remote operation of existing bridges are likely to supplement existing bridge operating systems with new remote operating components. A technical assessment of the age, condition, availability and compatibility of the existing

system components should be made such that proper integration of the proposed remote operating system is assured. Depending on the results of this assessment, it is likely that capital for existing operating system upgrades will have to be programmed in addition to the remote operating system enhancements

3.3.1.5 Maintenance Considerations

Implementation of remote operations inherently introduces specialty equipment and devices that are not prevalent on locally operated bridges. Owners should consider the impacts and mitigation techniques posed by introduction of remote operating systems and develop maintenance plans and practices to effectively operate and maintain the additional components required to remotely operate movable bridges. In addition, protocols shall be developed and implemented to protect maintenance personnel present on remotely operated bridges.

3.3.1.6 Pilot Implementation

When planning implementation of remote operations for an owner new to remote operations or in a new geography, it is recommended that implementation occur with a preliminary pilot operation period such that the initial bridge to be remotely operated is served by a local tender in addition to the remote tender. The local tender would provide system oversight and supervise the remote tender actions and intervene if required in order to provide safe and reliable operations while the remote operating system is being tested and commissioned. The bridge owner should coordinate implementation requirements with the US Coast Guard and local authorities having jurisdiction.

3.3.1.7 Cybersecurity Assessment

When implementing remote operation of movable bridges, the owner shall undertake a cybersecurity risk assessment to assess the vulnerabilities, threat likelihood, and compromise consequences of each Operational Technology (OT) system to be deployed to implement remote operations and its operational environment. As per national and international standards, cybersecurity risk assessments typically require an onsite visualization and verification of control systems inventory, architecture, and network data flows. The documented end result of this assessment should be a unique risk matrix profile for the OT systems and environment with a prioritized set of recommended mitigations.

3.3.2 Control Systems

Research conducted on bridge control systems and the relevant AASHTO LRFD Movable Bridge Design Specifications identified the need for several requirements to be included in the proposed guidelines:

- The local control system at a remotely operated bridge must be capable of operating the movable bridge locally with all safety interlocks in place without reliance on the remote operating station and/or the associated communication link. An automated span drive system must be provided such that upon a single operating command initiated by the tender, the movable span will open or close to its end of travel limit under supervisory, closed loop control.
- The remote operating station shall have the ability to control and monitor each local movable bridge device, have a sufficient quantity of surveillance system monitors and controls to safely manage bridge users and be equipped with an effective two-way bridge user communication system. In no way shall the local bridge control system depend on the

remote system for proper operation during local bridge operations (when the remote system and/or communications link are out of service).

- The remote operating station, communication link and local bridge control system shall be designed such that a single point of failure does not render the bridge inoperable to the extent practical and typically employed on locally operated bridges. In no case shall a single component failure compromise safety to the bridge users nor cause damage to the bridge and its facilities.
- The remote operating station must be equipped with an Emergency Stop button such that remote tender can stop any local device while it is in motion without undue delay. This emergency stop function should utilize industry-recognized life safety protocols such that related control components are designed not to fail, but if they do, they fail only in a predictable safe way to stop operations (except in the case of span opening operations as noted above).
- A remote operating system lock-out/tag-out system must be provided at the locally operated bridge to prevent remote operation during maintenance functions as required.

3.3.3 Surveillance Systems

Research conducted on bridge surveillance systems identified the need for a comprehensive remote surveillance system provided at the local bridge to provide complete coverage of all vehicular, pedestrian and marine users. This system shall preferably consist of redundant equipment of varying technology to assure the safety of all bridge users during remote bridge operations.

In addition to relying on the tender's ability to interpret the presence of a bridge user using the surveillance system, the research yielded the need for integrating the control system with surveillance devices to back-check the tender's judgment with regard to identifying bridge users in vulnerable areas during bridge operations.

A supervisory control system algorithm integrated with the surveillance system must be implemented at a minimum for the bridge opening and bridge closing functions. Prior to opening the movable span, a surveillance device must be deployed to confirm no vehicles or pedestrians are in an unsafe location and validate tender visual interpretation that the bridge is safe to open. Similarly, prior to closing the movable span, a surveillance device must be deployed to confirm no vessels are in an unsafe location and validate tender visual interpretation that the bridge is safe to close. Supervisory controls beyond these minimum requirements are recommended for the safe passage of all vehicles, pedestrians and vessels. Consideration must also be given to protection of maintenance personnel while the bridge is being serviced. Supervisory devices to validate remote tender judgment can be configured as warnings or system interlocks at the discretion of the owner.

Given that the local tender serves as the primary first responder to on-site emergencies such as fire or unauthorized intrusion, conventional Intrusion Detection and Fire Detection Systems are recommended to be deployed on remotely operated movable bridges. These systems should be equipped with remote station monitoring such that the remote tender is alerted when these systems detect a problem. In addition, central station monitoring can be provided such that the proper authorities are alerted if a security breach and/or fire is detected at the local bridge site.

3.3.4 Communication Systems

The proposed guidelines define the need to provide a comprehensive two-way bridge user communication system for a remotely operated bridge such that the remote tender and bridge users can effectively communicate. At a minimum, this system must effectively receive and transmit communication signals to mariners per applicable USCG regulations.

In addition to the two-way communications system requirements, audible warning devices and microphones must be provided and located to communicate with mariners, motorists, pedestrians and cyclists as well as in restricted areas where maintenance personnel may be present. The location and audible sensitivity of microphones must be considered and be adjustable such that the remote tender is provided with useful audible feedback.

The remote and local bridge control system must be linked via a secured continuous communication link with minimal latency. Should the link fail, all motion at the bridge shall cease with the exception of continuing a movable span opening operation. In this case, the movable span shall continue to the fully open position under the supervisory control of the local bridge control system and automatically stop at the fully open position to allow the approaching vessel to pass.

3.3.4.1 Cybersecurity

The research also addressed the need for bridge owners and designers to assess cybersecurity. Research was conducted to:

- Identify means to mitigate and potentially eliminate the risk of cyber-attack
- Provide recommendations to establish cyber-security for remote bridge operating systems
- Incorporate cyber-security best practices including the voluntary guidelines created by the National Institute of Standards and Technology (NIST)

As a result of the research, it is recommended that bridge owners conduct a cybersecurity risk assessment when implementing a remote bridge operation program. The proposed guidelines address design considerations, operational protocols and maintenance practices relative to managing cybersecurity. A detailed memorandum of the research conducted on this topic is located in Appendix B.

4 CHAPTER 4 Conclusions and Suggested Research

The research conducted yielded the conclusion that safe, reliable and efficient operation of movable bridges from remote locations is indeed feasible. Prudent design and application of technology in the bridge control, surveillance and communication systems will provide reliable means of remote operation. These technical enhancements paired with programmatic operation and maintenance protocols can provide safe and reliable bridge operations in accordance with applicable regulations. These enhancements and programmatic actions are described in detail in the Proposed AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations in Appendix C.

One topic for additional research lies in the surveillance system domain, specifically with regard to identifying reliable systems to detect vehicles, pedestrians and vessels in vulnerable areas of the movable span without reliance on the bridge tender. Technologies such as pixel-recognition cameras, vehicle video sensing systems and motion sensors were identified as viable devices to deploy in this regard; however, as this technology continues to evolve, there may be improved devices offering enhanced reliability that may be worth investigating.

APPENDIX A Survey Interview Forms

AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations

HDR Engineering, Inc. has been commissioned by the NAS/NCHRP to research current practices for the operation of movable bridges from remote locations for the purposes of developing design guidelines for implementation of remote operating systems. Given your involvement with remote operation of movables bridges, your input is critical to identify the best practices in use today and lessons learned during implementation. Please take a moment to complete this survey and return to me by September 30, 2019. Thank You,

Robert Moses, P.E.
HDR Engineering, Inc.
Robert.Moses@hdrinc.com
Mobile: +1 917 324 4259

Movable Bridge Remote Operation Survey

Respondent Name:

Company: Wisconsin Department of Transportation – NE Region

Name of Movable Bridge Owner/Operating Entity: Wisconsin Department of Transportation/ City of Green Bay

Number of Movable Bridges Operated by Remote Control: 4/1

Names/Locations of Movable Bridges Operated by Remote Control:

1. Bayview Bridge/ Sturgeon Bay, WI
2. Michigan Street Bridge/ Sturgeon Bay, WI
3. Mason Street Bridge/ Green Bay, WI
4. Main Street Bridge/ Green Bay, WI (City of Green Bay - Owner. Lift from WiDOT Bridge)
5. Tayco Street Bridge/ Menasha, WI

Types of Systems/Technology Deployed to Remotely Operate Movable Bridges (Check all that apply):

☒ Programmable Logic Controller (PLC)
☒ Closed Circuit Television Systems
☒ Thermal Image Cameras
☐ Pixel-Sensing Cameras – Have the capability but don't utilize
☒ Public Address Systems
☒ Microphones
☐ Motion Sensors for Pedestrians – Tried these without success, so not used anymore
☐ Motion Sensors for Vehicular Traffic

☐ Motion Sensors for Navigation Traffic
☒ Radar Systems
☒ Pedestrian Gates/Barriers
☒ Private Fiber Optic Communications Link
☒ Leased Communications Link
☒ Wireless Communication Technology
☐ Other:
☐ Other:

Describe any issues encountered while operating movable bridges remotely:

- Motion Sensors for Pedestrians – Tried these without success, so not used anymore. Just view the sidewalks with cameras
- Camera placement was usually changed on a few cameras after they were in place to capture better views
- Camera shaking from placing the cameras in mid span, light poles and/ or high wind area.
- We call in local tenders for high boat traffic holidays. Never an issue but drawtenders felt more comfortable.

Describe if issues encountered were caused by, or furthered hampered by, remote operation:

- None
-
-
-

What advantages do you currently enjoy by operating remotely:

☒ Reduction in bridge operating staff
☒ Improved response to operational malfunctions
☒ Improved safety for vehicles – using cameras
☒ Improved safety for pedestrians – using cameras
☒ Improved safety for navigation traffic – using cameras
☒ Enhanced information / data gathered to improve maintenance
☐ Other: Planning to get camera views in the region office
☐ Other: Emergency services will be able soon to see the bridge views. Possibly divert responders to bridges that are not open.

What disadvantages do you currently experience by operating remotely:

☐ Decrease in overall safety to bridge users
☐ Increase in delays to navigation (compared to local operation)
☐ Increase in delays to vehicles, pedestrians (compared to local operation)
☐ Increase in maintenance costs due to surveillance equipment
☐ Increase in emergency response/troubleshooting due to system malfunctions
☐ Other:

☐ Other:

Are you able or willing to share public documents or non-proprietary information related to your remote bridge operating systems, such as Plans, Specifications, Reports, Photographs, etc. Please share documents or links with robert.moses@hdrinc.com or drop them into this OneDrive folder: 'Movable Bridge Remote Control Examples.' You received a link as a separate email from this survey.

- yes

Please share any other information you may consider relevant with regard to the design, installation, operation and maintenance of remote bridge operating systems:

- We are currently trying out new highspeed wireless tech.
- Finding a good camera system software critical
- Finding a good network company and plc company after the project is completed was critical for the tweaks needed after operation
- In our area, there weren't any companies that dealt with cameras on bridges so a lot of trial and error on placement.
- Break in period worked great to fine tune any details prior to full remote operations.
- Stay on top of the latest technology. Don't be afraid to try out improved products.
- If a new bridge house is being built, maximize the drawtenders house to have room for remote operations and plan open wire chase ways for expanding.
- Us the largest HD monitors you can fit/ afford
- Use good quality cameras with models that can be easily purchased and replaced.
- Budget for replacing electronic equipment (cameras, computers, servers, monitors, etc…)
- Make all camera, monitor's, servers and all electronic equipment placements are accessible. They will need to be replaced.
- We used hinged poles for cameras that worked out very well.
- Work with local emergency services to get access to the cameras views. They can't have control of the cameras.
- Be sure to interview the current drawtenders on views they would like to see when lifting the bridge.
- Get the Coast Guard involved early in the process.
- We added cameras to areas on the remote bridge that are problematic, so tenders can see those areas remotely on the monitors.
- We did create a Web Based vessel log site that all the bridges use for vessel movements, maintenance and accidents. It very helpful to see those things without being on the bridges.

Thank You for supporting this effort.

Sincerely,

HDR ENGINEERING, INC.

Robert Moses, P.E.

AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations

HDR Engineering, Inc. has been commissioned by the NAS/NCHRP to research current practices for the operation of movable bridges from remote locations for the purposes of developing design guidelines for implementation of remote operating systems. Given your involvement with remote operation of movables bridges, your input is critical to identify the best practices in use today and lessons learned during implementation. Please take a moment to complete this survey and return to me by September 30, 2019. Thank You,

Robert Moses, P.E.
HDR Engineering, Inc.
Robert.Moses@hdrinc.com
Mobile: +1 917 324 4259

Movable Bridge Remote Operation Survey

Respondent Name:

Company: CSX Transportation

Name of Movable Bridge Owner/Operating Entity: CSX Transportation **(All Railway Bridges)**

Number of Movable Bridges Operated by Remote Control: 5 Active / 4 Proposed / 3 in Construction

Names/Locations of Movable Bridges Operated by Remote Control:

1. Hilton Draw / Wilmington NC
2. Trout River / Jacksonville FL
3. St. Johns River / Satsuma FL
4. Hillsborough Canal / Tampa FL
5. Manatee River / Bradenton FL

Types of Systems/Technology Deployed to Remotely Operate Movable Bridges (Check all that apply):

- ☒ Programmable Logic Controller (PLC)
- ☒ Closed Circuit Television Systems
- ☐ Thermal Image Cameras
- ☐ Pixel-Sensing Cameras
- ☐ Public Address Systems
- ☐ Microphones
- ☐ Motion Sensors for Pedestrians
- ☐ Motion Sensors for Vehicular Traffic
- ☒ Motion Sensors for Navigation Traffic

☐ Radar Systems
☐ Pedestrian Gates/Barriers
☐ Private Fiber Optic Communications Link
☒ Leased Communications Link (local Telco. Circuit)
☒ Wireless Communication Technology (back up to local telco)
☐ Other:
☐ Other:

Describe any issues encountered while operating movable bridges remotely:

-
-
-
-

Describe if issues encountered were caused by, or furthered hampered by, remote operation:

-
-
-
-

What advantages do you currently enjoy by operating remotely:

☒ Reduction in bridge operating staff
☐ Improved response to operational malfunctions
☒ Improved safety for vehicles
☐ Improved safety for pedestrians
☒ Improved safety for navigation traffic
☒ Enhanced information / data gathered to improve maintenance
☐ Other:
☐ Other:

What disadvantages do you currently experience by operating remotely:

☐ Decrease in overall safety to bridge users
☐ Increase in delays to navigation (compared to local operation)
☐ Increase in delays to vehicles, pedestrians (compared to local operation)
☐ Increase in maintenance costs due to surveillance equipment
☒ Increase in emergency response/troubleshooting due to system malfunctions
☐ Other:
☐ Other:

Are you able or willing to share public documents or non-proprietary information related to your remote bridge operating systems, such as Plans, Specifications, Reports, Photographs, etc. Please share documents or links with robert.moses@hdrinc.com or drop them into this OneDrive folder: 'Movable Bridge Remote Control Examples.' You received a link as a separate email from this survey.

- NO

Please share any other information you may consider relevant with regard to the design, installation, operation and maintenance of remote bridge operating systems:

-
-
-
-

Thank You for supporting this effort.

Sincerely,

HDR ENGINEERING, INC.

Robert Moses, P.E.

AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations

HDR Engineering, Inc. has been commissioned by the NAS/NCHRP to research current practices for the operation of movable bridges from remote locations for the purposes of developing design guidelines for implementation of remote operating systems. Given your involvement with remote operation of movables bridges, your input is critical to identify the best practices in use today and lessons learned during implementation. Please take a moment to complete this survey and return to me by September 30, 2019. Thank You,

Robert Moses, P.E.
HDR Engineering, Inc.
Robert.Moses@hdrinc.com
Mobile: +1 917 324 4259

Movable Bridge Remote Operation Survey

Respondent Name:

Company: Svenska Teknikingenjorer Sting AB

Name of Movable Bridge Owner/Operating Entity:

- Swedish Transport Administration, approx 40 bridges, both road and railroad.
- Town of Gothenburg, one bridge.
- Town of Trollhattan, two bridges.
- Town of Vanersborg, two bridges.
- Town of Sodertalje, one bridge.
- Town of Uppsala, four bridges.
- ~~Town of Orebro. One bridge.~~
- Etc

Number of Movable Bridges Operated by Remote Control: See above.

Names/Locations of Movable Bridges Operated by Remote Control:

They are spread out all over Sweden. One example is Falsterbro bridge being remote controlled from Trollhattan. Distance 300 km. Also Hasslo bridge is being operated from Trollhattan. Distance just above 300 km. Usually several bridges in one channel-system operates from one location.

Types of Systems/Technology Deployed to Remotely Operate Movable Bridges (Check all that apply):

☒ Programmable Logic Controller (PLC)
☒ Closed Circuit Television Systems
☐ Thermal Image Cameras

☐ Pixel-Sensing Cameras
☒ Public Address Systems
☒ Microphones
☐ Motion Sensors for Pedestrians
☐ Motion Sensors for Vehicular Traffic
☐ Motion Sensors for Navigation Traffic
☐ Radar Systems
☒ Pedestrian Gates/Barriers
☒ Private Fiber Optic Communications Link
☒ Leased Communications Link
☐ Wireless Communication Technology
☐ Other:
☐ Other:

Describe any issues encountered while operating movable bridges remotely:

- Interruption in communication or other technical failure in remote system. Back- up needed.
- Low visibility. Back-up needed.
-
-

Describe if issues encountered were caused by, or furthered hampered by, remote operation:

- Total failure in communication between the locations, not common but it happens.
-
-
-

What advantages do you currently enjoy by operating remotely:

☒ Reduction in bridge operating staff
☐ Improved response to operational malfunctions
☒ Improved safety for vehicles
☒ Improved safety for pedestrians
☒ Improved safety for navigation traffic
☐ Enhanced information / data gathered to improve maintenance
☐ Other:
☐ Other:

What disadvantages do you currently experience by operating remotely:

☐ Decrease in overall safety to bridge users
☐ Increase in delays to navigation (compared to local operation)
☐ Increase in delays to vehicles, pedestrians (compared to local operation)
☒ Increase in maintenance costs due to surveillance equipment
☒ Increase in emergency response/troubleshooting due to system malfunctions

☐ Other:
☐ Other:

Are you able or willing to share public documents or non-proprietary information related to your remote bridge operating systems, such as Plans, Specifications, Reports, Photographs, etc. Please share documents or links with robert.moses@hdrinc.com or drop them into this OneDrive folder: 'Movable Bridge Remote Control Examples.' You received a link as a separate email from this survey.

- We have to check this with the bridge-owners, see below
-

Please share any other information you may consider relevant with regard to the design, installation, operation and maintenance of remote bridge operating systems:

We are mainly designing the systems. Operators varies due to contracts.

Thank You for supporting this effort.

Sincerely,

HDR ENGINEERING, INC.

Robert Moses, P.E.

City of Milwaukee

Overview:

The City of Milwaukee operates 21 movable bridges. Over the last eight years, the city has endeavored to remotely operate 12 of these movable bridges from other locally staffed movable bridges. A summary of the bridges is as follows:

Feature Under	City Number	Structure Number	Bridge Location	Local Bridge Tender also Remotely Operates the Following Bridges, as applicable			Operation/Staffing (Remote indicates bridge is not locally staffed)
MKE	100	B-40-952	Broadway, 101 North	Plankinton	Emmber		Manned 24 hours
MKE	101	B-40-548	Water Street, 400 North	S. 6th	N. 6th	Kilbourn	Manned 24 hours
MKE	103	P-40-523	St. Paul Avenue, 100 West	Michigan			Remote
MKE	104	P-40-868	Clybourn Street, 100 East				Remote
MKE	105	P-40-886	Michigan Street, 100 West	St. Paul			Manned 24 hours
MKE	106	B-40-488	Wisconsin Avenue, 101 West	Clybourn			Manned 7 am to 11 pm
MKE	107	B-40-544	Wells Street, 101 West				Unmanned
MKE	108	P-40-881	Kilbourn Avenue, 100 West				Remote
MKE	109	B-40-980	State Street, 101 West				Remote
MKE	110	B-40-757	Juneau Avenue, 100 East	Highland	McKinley/Knapp		Remote
MKE	111	P-40-864	Cherry Street, 100 East				Unmanned
MKE	112	B-40-406	Pleasant Street, 400 East				Unmanned
MKE	118	B-40-62	McKinley Av, 221 W., Knapp St.	State			Unmanned
KK	200	B-40-591	Kinnickinnic Avenue, 1964 South	1st Street			Manned 24 hours
KK	201	P-40-830	1st Street, 2000 South				Remote
MEN	300	P-40-539	Plankinton Avenue, 100 West				Remote
MEN	301	B-40-413B	6th Street Bascule, 177 South				Remote
MEN	301	B-40-414B	6th Street Bascule, 216 North				Remote
MEN	303	B-40-605	Emmber Lane, 144 North				Remote
MEN	304	B-40-550	16th Street Bascule, 200 North				Inoperable
MKE	1018	B-40-907	Highland Avenue, 100 West				Remote

Lessons Learned:

The City's operations and maintenance staff has identified the following best practices/lessons learned from implementing remote operation of its movable bridges:

1. Speakers, microphones and intercoms are necessary for the remote tender to hear what is happening at the remotely operated bridges from the remote operating site and to communicate with maintenance staff and bridge users at the remotely operated bridges. For example, if a pedestrian or bicyclist passes the gates when the bridge is in operation, the remote tender must be able to verbally instruct the user to return to a safe location.

2. Simplicity seems to work better than over-engineered systems. For example:

    a. Having actual buttons and levers seem to be more operator friendly than touch screens.
    b. Control panels should not seem too complicated. When there are too many different commands and steps it confuses the operators.

3. Regular maintenance on the computer programming is required with these systems. If the PLCs are not communicating correctly, you can't count on the operator to pay attention to the on screen commands. If you tell someone to ignore the fault for one reason, people do not always recognize a true problem.
4. Problems that have occurred on our bridges are not a factor if it is a manned bridge or a remotely operated bridge. In others words, we have not had a problem with a camera or bridge operation control over the fiber cable during a bridge opening. An additional advantage the City of Milwaukee has with our movable bridges are the majority are within a mile radius from each other so we can respond quickly if there is a malfunction.

Wisconsin Department of Transportation – Northeast Region

Overview:

The Wisconsin Department of Transportation operates approximately 20 movable bridges statewide with the vast majority of them located in the Northeast Region (NER) of the state. The NER has been readying at least five bridges for remote control by retrofitting the control systems with modern PLC-based systems. The Bridge Program Manager in the USCG Cleveland District has been hesitant to permit remote bridge operations given the lack of a central policy from USCG Headquarters in Washington, DC. The NER has been proceeding to prepare for this ultimate USCG approval.

Lessons Learned:

The NER maintenance team has been spearheading the effort to implement remote control of its movable bridges. They have provided a variety of technical and non-technical lessons learned as follows:

1. Standardize on a modern PLC platform that will be supported by the manufacturer for the foreseeable future. These systems tend to become obsolete but can be migrated to the next available product. Standardization promotes efficiency in stocking of spare parts and programming.

2. The local police departments “love” to get camera feeds from the CCTV systems deployed. Consider all relevant stakeholders and see how they can be engaged to help support remote operation implementation.

3. For communication systems, look to use dedicated communication lines not shared by other entities where feasible. Get a network specialist involved early in the process to take into account Internet Protocol (IP) addressing of IP cameras and control equipment. IP addressing should be standardized across all bridges and this should be planned from the beginning of the project.

4. Add more cameras than you think you need. They are relatively cheap and can provide the remote tender reassurance during malfunctions. For example, the NER located a camera focused on the tail locks of one bridge rather than relying solely on the indicating lights. This camera view provides assurance to the remote tender that the locks are driven when the indicating lights malfunction, thereby allowing traffic to use the bridge while the system is diagnosed.

5. For system cameras, specify equipment that is upgradeable such that cameras can be easily changed out as technology improves. Consider using thermographic cameras to detect pedestrians. On one of their through-truss bridges, this proves to be helpful finding people that try to hide within the trusses during operations. This is a good example of how safety upgrades can be implemented as part of a remote operation initiative.

6. For camera views, test locations before permanently locating them. Specify vibration proof mounting details, use crank-down poles to access cameras and locate cameras down on the piers to get good views of navigation.

7. Install a high quality, two-way public address system. Locate microphones to detect navigation traffic and locate speakers to talk to pedestrians, bicyclists and small boat mariners.

8. The NER has been conducting Public Information Meetings to solicit input from the travelling public and mariners on the remote control initiative. They have also been routinely engaging the USCG.

Ohio Department of Transportation

Overview:

Ohio DOT commissioned a study of the feasibility to remotely operate four movable bridges for ODOT which was performed in 2013 by HDR. Based upon the results of the study and funding realities, ODOT is implementing remote operation of the Port Clinton Bridge from the Craig Bridge. The project is currently in construction. The remote operation implementation has been combined with replacement of the bascule leaves and installation of a new control system. The contractor for this project is Ruhlin Co. and Perram Electric Inc.

Project Status:

Given the project is in construction, no specific lessons learned were reported; however, during the discussion, the following issues were reviewed:

ODOT is concerned with cost implications of the dedicated T1 line for the communication and video data. The leased line cost is noted to be extremely high and on the same order of magnitude as an operator's labor cost.

CSX Transportation

Overview:

CSX has forty-seven (47) movable bridges on the network they operate over. Forty-four (44) are owned and maintained by CSX. In 2015 CSX embarked on an initiative to automate, and remote control these bridges by January 1, 2021. There were 3 different types of remote control methods developed:

1. Automate with local control – the bridges were completely automated to raise after trains pass over the bridge and lowered locally by the train crews from the cab of the locomotive using Dual Tone Multi Frequency signals.

2. Automate/bridge tender control - multiple bridges (3 to 4) were upgraded, automated to operate from a single operator command and controlled remotely from a central location by one bridge tender.

3. Automate/train dispatcher control – the bridges were automated and controlled by the train dispatchers from the centralized train dispatcher office.

Anticipated Issues:

1. Labor – CSX is a closed shop. Union work rules had to be addressed.
    a. Operators – bridge tenders, depending on the location and the predecessor railroad, were either United Transportation Union (UTU) or Brotherhood of Maintenance of Way Employees (BMWE) workers. Depending on the means by which the bridge was now being controlled, meant crossing union lines (UTU to BMWE, or vice versa), or crossing seniority districts within the Organization's authority.
    b. Maintenance – The craft of employees to maintain the new control system had to be established. Historically the maintenance of the electrical systems on the bridge belonged to the International Brotherhood of Electrical Workers (IBEW). These were electricians traditionally working with high voltage service to the bridges. The new control system with computers and HMIs is low voltage control circuitry, not within the skill set of the IBEW employees. Whereas the Brotherhood of Railroad Signalmen (BRS) do have the skill set, but by past practices have not dealt with bridge maintenance, again crossing union lines.

    To address these issues meant involving CSXT Labor Relations Department and negotiating new agreements, with the organizations.

2. Upgrading bridges to a state of Good Repair – The condition of structural, mechanical, and electrical systems varied from bridge to bridge. A majority of the bridges needed extensive repairs to be made reliable prior to automating. A substantial investment would be required before any return on that investment would be realized.

3. Long lead times on materials – The aggressive schedule set (44 bridges in less than 5 years) meant the design time and long lead times for the material would be challenging. The large

mechanical components such as rack gears, pinion gears, shafts, and bearing are custom fabricated and 6 to 8 month lead times are typical.

4. Expanded Scopes – As with any new project the unknowns will be manifested in scope creep. We could have had a better handle on what the scope was going to be by spending more time evaluating them up front.

5. Startup debugging – Any new control system will have glitches. CSX was able to minimize these glitches with sound proven system designs, thorough reviews of contractor controls systems submittals, and shop testing.

6. Systems integration – Integrating the new control systems into the existing CSX signal and communication network was necessary for effective maintenance and operation of the bridges. Maintaining the security of the communication network and safe operation of trains was paramount. Integrating the different platforms and achieving the expectations proved to be difficult primarily due to a lack of coordination during the planning phase between the communications group which maintains the CSX private communication network and the bridge group responsible for deploying the remote operating systems. Issues such as communication infrastructure availability and connection points to enable remote operations were not identified early in the design process resulting in delays during construction when final communication connections between the bridge to be remotely operated and the remote operating station had to be made.

7. Financial – The Return on Investment (ROI) for this initiative would be measured in green dollar cost savings realized by the number of bridge tender positions eliminated projected over a specific time frame. Many of the bridges were not manned 24/7. For those bridges it was a challenge to meet the Corporation's expected ROI. One benefit that could not be measured is an intangible benefit is the increased reliability of bridge operation. Reduced train delays and maintenance cost were realized.

Unanticipated Issues:

1. Communications
    a. Infrastructure – Remote controlling bridges requires an extensive and robust communication system. The means to communicate between the bridge and control centers was achieved using various media: fiber optics, wireless and satellite links. In all cases, to some degree, new infrastructure had to be constructed. Although the new construction of this infrastructure was anticipated, the degree of effort required was not. These networks are all closed, CSX-owned networks.
    b. Internal and external – Remote controlling bridges impacted a wide spectrum of entities within and outside the company. Labor Relations and General Counsel were brought in to negotiate new contract terms. Operating Rules Department wrote new rules for the train crews to follow. The signals department had to design railroad interface modules. The communications department had to design and construct the communication links. The facilities department had to provide new primary and backup electrical services.

Consulting Engineers and Outside Contractors were brought in to make repairs to the bridges and to design and construct the new system. The US Coast Guard, and Federal Railroad Administration governs the operations of RR movable bridges and had to be satisfied that safe operation of both marine and rail traffic can be maintained. Keeping all stakeholders informed in a timely manner presented a challenge.

2. Costs
    a. Engineering – Unlike fixed bridges, movable bridges involve not only structural engineering discipline but also involves mechanical and electrical engineering disciplines. The coordination effort expands exponentially and the degree of effort is is reflected in the project cost.
    b. Construction – As with the engineering cost the construction cost increased beyond initial internal estimates due to the operating systems (control, and communication) required.
3. Expanded scopes – While expanded scopes were anticipated the magnitude of the increase was not determined until well into the process.

Conclusions:

Reflecting on the project thus far, lessons learned would be:

1. Communicate often and clearly with all involved, more so than you ever had on any other project.
2. Know the conditions of your bridges and budget for reliability repairs accordingly.
3. Know the condition and capacity of your communication network. Anticipate increased demands in the future.
4. Know that movable bridges are expensive and remote controlling them is even more expensive.
5. Have the patience and political drive to see the project through. Benefits will not be realized until the project is nearing completion.

APPENDIX B Cybersecurity Memorandum

NCHRP Project 20-07 / Task 424

AASHTO GUIDELINES FOR THE OPERATION OF MOVABLE BRIDGES FROM REMOTE LOCATIONS

FINAL DELIVERABLE: Task 5 Cybersecurity

Prepared for
National Cooperative Highway Research Program
Transportation Research Board

of

The National Academies of Sciences, Engineering and Medicine

Lead Investigator: Robert S. Moses, P.E.
Lead Task Manager: Raphael Costa, P.E.
HDR Engineering, Inc.
Newark, NJ
August 2020

AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations

Table of Contents

Task 5: Cybersecurity

Goals as stated in research project scope of work:

- ***Search for means to mitigate and potentially eliminate the risk of cyber-attack.***
- ***Provide recommendations to establish cyber-security for remote bridge operating systems.***
- ***Incorporate cyber-security best practices including the voluntary guidelines created by the National Institute of Standards and Technology (NIST).***

Context

IT/OT Clarification

Information Technology (IT) is primarily focused on the systems that provide for the communication, collection, control, and manipulation of data. Operational Technology (OT) on the other hand covers the systems used in the monitoring and operational control of virtual or physical devices. The OT domain scope therefore covers a wide gamut from industrial operations to facilities to drones. Moveable bridges leverage OT control systems for the control and monitoring of bridges and their environments.

For better understanding, it should be noted that there are many terms and acronyms used to describe the various sub-scopes in OT: "Industrial Control Systems" (ICS), "Control System" (CS), "Process Control Systems" (PCS), "Supervisory Control and Data Acquisition" (SCADA), "Programmable Logic Controller" (PLC), "Distributed Control System" (DCS), and "Discrete Processing Control" (DPC). In this section, we will refer generically to the movable bridge system as a control system (CS).

Remote Access VS Remote Control Clarification

Cybersecurity standards and best practices often place Remote Access functionality in the high risk category. NIST defines Remote Access as "the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities."

The movable bridge control system will be accessed via an extension to a remote site which is effectively just an extension of the internal network(s). **Remote Control of movable bridges therefore is not "Remote Access"** and therefore does not inherit all of the assumed vulnerabilities of this category.

That is not to say there are no vulnerabilities, but when applying the NIST security controls in this section, the documented category for remote access will not be relevant.

Cyber Attack Scope

"Cyber Attack", an often sensationalized phrase, typically refers to an attempt by hackers to damage or destroy a computer network or system. In an OT environment, the focus is on hacking control systems to compromise the critical infrastructure it controls/monitors. Regardless, the practice of mitigating vulnerabilities in OT cybersecurity must cover a wider "attack" scope to include:

- Infrastructure Damage
    - Ex/ Controlling the movable bridge in such a way that the safety of property, vessels, vehicles, and personnel is compromised
- Denial of Service (DOS): the reduction or loss of service
    - Ex/ a movable bridge cannot be operated by the control system, can only be operated intermittently, or can only be operated at slower/faster speeds than normal

- Malicious Use: the use of a system/network for purposes other than intended or expected
  - Ex/ Access to the control system or network allows pivoting to a different target system/network
  - Ex/ the bridge moves/opens/closes at random changing speeds causing vibration and unsafe operational states
  - Ex/ Video systems are hacked to provide access for surveillance of other targets
- Data Manipulation: The manipulation of process data
  - Ex/ HMI screens (and perhaps even the video) show operational states that are not accurate so that the bridge operator unknowingly executes commands that cause damage or safety events
  - Ex/ Set points for closed loop control are compromised such that the bridge opens/closes too little or too much
- Data Exfiltration: Theft of data
  - Ex/ Control System process data showing the internals of how the bridge is operated is exported for offline analysis and reconnaissance for planning a future attack

Cybersecurity Risk, Assessment, and Mitigation

Cybersecurity risk is best evaluated by a comprehensive cybersecurity risk assessment that drills down into the vulnerabilities, threat likelihood, and compromise consequences of each Operational Technology (OT) system and its operational environment. As per national and international standards, cybersecurity risk assessments typically require an onsite visualization and verification of control systems inventory, architecture, and network data flows. The documented end result is a unique risk matrix profile for the OT system(s) and environment with a prioritized set of recommended mitigations.

Note that **cybersecurity risk can be mitigated but not eliminated completely generally due to environment, resource, schedule, and cost restraints**. The ranking of risk mitigations therefore is used to guide the selection of risk reductions within the known constraints.

Cybersecurity risk assessment for each movable bridge has not been included or planned as part of this evaluation so certain generalizations are necessary. Given the three factors of risk (*vulnerability*, *likelihood*, and *consequence*), it is expected that the *consequences* of digital manipulation (insiders hacking, outsider hacking, coding mistakes, etc.) are mostly known and can be objectively itemized. However, vulnerabilities, threat likelihood, and mitigation ranking will need to be estimated based on various technical, business, and environmental assumptions.

NIST Cybersecurity Framework

Well known in the cybersecurity community, NIST provided the NIST Cybersecurity Framework (NCF) as a structure to classify and group all other NIST cybersecurity documentation. This document section will also use this structure to review the recommended best practices and risk mitigations correlated with the NIST 800 series.

The NCF provides five color coded categories (Identify, Protect, Detect, Respond, and Recover) to broadly classify best practices in OT. Each of these best practices is then detailed out into requirements cross-referenced to other NIST documents.

Some of these requirements are technical in nature, some are more related to establishing and maintaining business guidelines, processes, and procedures.

IDENTIFY

You cannot protect what you do not know you have.

PROTECT

The scope of this category addresses both startup best practices as well as ongoing maintenance.

Startup protections are typically technical design and build tasks focused on securing the network, attached network devices, and software.

DETECT

Outside an obvious physically visible affect, if a movable bridge control system was compromised (intentionally or not) would it be detectable/detected?

RESPOND

For the relevant movable bridge and location, if the control system is compromised are there local resources able to respond? Are responders familiar with the relevant control system and capable of cyber forensics?

RECOVER

For the relevant movable bridge and location, could the control system be restored, protected from future compromise, and placed back into normal operation within an acceptable timeframe?

For movable bridges, this would include mechanical states. For example, a bridge half open/closed.

Focusing on Moveable Bridges

Current Bridge Control System Assumptions

In the absence of control system and cybersecurity risk assessment data, we must make certain assumptions and generalizations about the variations in deployed IT system and network architecture, OT control systems, secondary systems, and items being controlled and/or monitored. These assumptions are grouped here by current state and future state.

Current State

- Control System
    - System Architecture: Bridge control systems are primarily PLC driven (the PLCs contain most/all of the programmed logic and device interaction) and HMI computer workstations are used primary for PLC interaction (monitoring/control).
        - Larger control systems typically include one or more servers and workstations that are virtualized for easy backup/restoration/redundancy.
    - Network Architecture: the bridge control systems share the same network.
    - PLCs (Ethernet/serial): the PLCs are network connected (Ethernet) but the PLC controlled/monitored devices (motors, sensors, etc.) are serially connected.
    - I/O Servers/Gateways: the bridge control systems are not expected to have I/O servers or gateways
        - I/O Servers and Gateways are typical found in larger more complex systems where they serve a number of functions to include protocol language translation. Bridge control systems are unlikely to have the complexity and size to need them.
- Secondary Systems
    - Video: At least some video systems are Ethernet based and share the same network as the control system
    - Radio: Not networked Voice over Internet Protocol (VOIP).
    - Sensors: Some networked, some serially connected to PLC
    - Microphones: Not networked VOIP
    - Fire Alarm System: networked but a standalone system serially connected to sensors. May be serially connected to PLC for alarm notifications.
    - Notification Systems (Public Address, Message Boards): not networked VOIP.

Future State

- Control System: The control system and network architecture will be extended to a remote facility and integrated with one or more local secondary systems.
- Secondary Systems:
    - Secondary systems will be added and/or upgraded with network connectively such that they can be controlled/monitored locally as well as remotely.
    - Secondary systems will share the same network connecting the remote facility with primary control and monitoring

Bridge Control System Cyber Vulnerabilities

Most control system vulnerabilities exist independent of the threat vector (path taken for compromise) and source of threat (local or remote). Vulnerabilities can affect all OT systems to include secondary

systems like video and remote sensors. Most vulnerabilities are technical in nature, but some can be business or organizational. The following paragraphs drill down on a few examples.

Technical

- Denial of Service (DOS): A DOS attack prevents use of the system and can occur at any time.
- Man-In-The-Middle (MITM): An MITM attack intends to present to the control system user(s) an invalid picture of current status (bridge position, location of personnel/vehicles/trains/etc., alarm status, etc.) with the intent of tricking the user into directing the control system to take an incorrect action. MITM could be represented as incorrect data on an HMI monitor display or video screen.
- Code Injection: PLC and/or SCADA code could be modified to provide unintended operation or operational control. This level of compromise could enable any level of random functionality as well as disable all digital interlocks and safety code.
- Process Data Manipulation (Set Points) – PLC set points control (for example) the starting and ending point for an open or close operation. Manipulation of any set points could effectively damage the bridge or limit the amount that it opens or closes. A clever set point manipulation would make invalid bridge operation to appear to be a mechanical failure.
- Process Data Manipulation (Real-time item value edits) – Certain process items (also called tags) could be manipulated in real time such as speed, On/Off, etc. so as to cause unsafe operation and/or damage to the bridge or motor functionality
- Process Data Manipulation (Logs) – Log data could be manipulated or cleared. This would affect forensics investigation efforts in responding to a cyber-event.

Organizational

- Restoration Delay – Inability to respond to a cyber-event within an acceptable timeframe is a vulnerability in itself. This can be caused by poor documentation, no incident response plan/team, lack of cyber forensics expertise on the incident response team, poor backups, etc.
- Lack of Cyber Awareness & Training

Bridge Control System Cyber Threats

Cyber threats to a control system refer to “entities (persons and/or automated software) which attempt unauthorized access to a control system device and/or network using a data communications pathway”.

This access can be directed from within an organization by trusted users or from remote locations by unknown persons using the Internet. Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. Malware delivery methods can be manual or automated.

Cyber threats cannot contribute to cyber risk unless they are able to leverage one or more cyber-vulnerabilities in such a way as to incur consequence or cost. Cyber threats require a pathway and delivery method.

- Threat Pathways
    - Physical Access
    - Remote Access
    - Media
    - Communication Providers (Internet, Private/Leased Lines, etc.)

- Threat Types:
    - Malware, Virus, Worms, Spyware, etc.
    - Firmware Replacement, SQL and/or Software Code Injection, PLC code
- Delivery Methods:
    - Corrupted Software, Updates/Patches, and Firmware
    - Real-time connected manual surveillance and active hacking
    - Attachments in Messaging/Email/etc.
    - Insider Access
    - Corrupted Media

Bridge Control System Compromise Consequences

In the absence of any manual protections and/or lockouts, compromise of a movable bridge control system can incur significant consequences to include human safety and financial impacts (property/bridge/entity damage and/or interruption in commerce).

The following consequences are presented as a top 5 list of worst case scenarios from digital compromise:

- Bridge opens (partial or full) with traffic pending or on the span
- Bridge closes (partial or full) with traffic under the span
- Bridge operates in such a way as to cause damage to the bridge mechanisms
- Bridge operation freezes in full or partial open/close
- Bridge operator operates bridge in unsafe manner due to inaccurate digital information (video, HMI displays, sensors, etc.)

Compounding Factors

- The timing of cyber hacking of a movable bridges for boat and train traffic can exponentially increase the consequences of any cyber event.
    - Boat/Barge traffic: if the bridge was opened and a large boat was proceeding, if a cyber-event then closes the bridge (partially or fully), the inertia could prevent them from stopping. A visual and/or radio warning could be too late to be effective.
    - Train traffic: if the bridge was closed and the train was proceeding, if a cyber-event then opens the bridge (partially or fully), the inertia could prevent them from stopping. A visual and/or radio warning could be too late to be effective.
    - Consequence would also increase if any vehicle or pedestrian traffic was on or near a span during a cyber-event.

Bridge Control System Risk Mitigation Best Practices

The NIST 800-53 (IT Security Controls) "Security and Privacy Controls for Federal Information Systems and Organizations" and the NIST 800-82 (OT Security Controls) "Guide to Industrial Control Systems (ICS) Security" provides an exhaustive list of mitigations that can be applied to reduce cybersecurity risk. Even accounting for overlap between the two, there are over 1300+ potentially applicable security controls depending on an organization's structure and the size and complexity of its control system(s).

The ISA/IEC 62443 cybersecurity series is the only worldwide standard for OT cybersecurity. ISA 62443 and the NIST 800 series are complementary in nature and therefore both are referenced in this document.

Given the number of potential security controls as well as the available documentation scope (NIST and ISA documents comprise many thousands of pages) there are a great many organizational and technical best practices that could be beneficial to movable bridges. To keep this scope manageable we have limited the best practices to a Top 10 list with significant importance to movable bridges.

Because of the variations in organizational and control systems structures, any Top X list of best practices in any OT environment could vary in content. The priority of each as well could change based on an organizations resources, budget, age of control system infrastructure, schedule, regulatory environment, etc. Each environment therefore is unique and has a unique cybersecurity risk profile that can only be documented through a thorough OT cybersecurity risk assessment.

With that said, there are best practices in control systems commonly at the top of the list in most organizations as they are complimentary to or a precedence to others. Given the nature and criticality of movable bridges as well as the assumption of remote access (via internal extended networks only) we can tune this list further. It should be noted that not all components of each best practice are listed here but rather those components critically related to movable bridges. Note as well that the best practices listed here are not in any implied order.

1. IDENTIFY: Asset Inventory Management

You cannot monitor, analyze, protect, or recover what you do not know you have.

Without this documentation, vulnerabilities cannot be fully known, and mitigations cannot be fully realized. For example, a PLC or software version may be at risk and has an update available. Without documentation, neither the vulnerability nor the mitigation could be known.

Asset Inventory requires comprehensive documentation to include the following:

- All OT Hardware, Software, and Firmware (physical or virtual):
  - Hardware: workstations, servers, firewalls, routers, switches, PLCs, devices (both physical and virtual) to include vendor, make, model, firmware revision, and serial number.
  - Software: Licensing, version, OS requirements, patches
- All OT networks and connections should be diagrammed based on the ISA Purdue Model
  - When multiple sites are involved, each site must be detailed, but a rollup view of all sites must be provided. Microsoft Visio tabs and overlays is one option available that can provide this document presentation view.
- All baseline OT data protocols and data flows should be mapped (as an overlay) on a Purdue

Model network diagram
    - OT devices and systems have unique languages, commands, and behaviors on a network. These can be mapped as a baseline of "normal" such that abnormal can be quickly determined.
    - This mapping is also necessary in forensics and recovery operations
- OT Tag Database: Control systems have numerous control points (often called items or tags) for read and write. Every control system tag, its source, its type (raw IO, calculated, software defined, etc.), and address should be documented (often as a list in an Excel format).
- Configurations:
    - PLCs, Switches and Firewalls
    - Each network interface should be documented with IP Address, MAC, and IP Ports used
    - Software
- Licensing: All Software Licenses
- Test Plans: Functional Acceptance Test (FAT) Plans should be available for recovery purposes

Guideline Reference Standards

- ISA 62443-2-1:2009 4.2.3.4
- ISA 62443-3-3:2013 SR 7.8
- NIST SP 800-53 Rev. 4 CM-8, AC-4, CA-3, CA-9, PL-8

2. IDENTIFY: Cybersecurity Risk Assessment and Management

Every OT system, environment, and governing organizational structure has a unique risk profile of vulnerabilities, threats, likelihood, and consequences.

Removal of all risk is typically cost prohibitive so mitigations must be prioritized and targeted based on a number of factors to include the organization's priorities, constraints, risk tolerances, and assumptions. An assessment of the operational environment can also provide useful safety, regulatory, financial, technical, and human resource data. All of these inputs combine to support operational risk mitigation selection.

A Cybersecurity Risk Assessment is key in determining and documenting the risk profile of your OT system, organization, and environment. Because of the evolving technology and threat environment, Risk Management also recognizes the need to reevaluate and revalidate assessed data on a periodic basis.

Guideline Reference Standards

- ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12, 4.3.4.2
- NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5, PM-4, PM-9, PM-11, PM-12, PM-16

3. IDENTIFY: Governance – Policies, Procedures, and Processes

Cybersecurity requires organizational policies and procedures to insure established cybersecurity mitigations are maintained and improved over time.

One example of the necessity of policy, procedure, and would be in the governed use of the PLC key

switch (reference this section's best practice *Access Control: Physical Security*):

- Example Policy: When any movable bridge is in the operational state, the PLCs must be in the RUN mode position to avoid the modification of firmware or PLC code from any network source.
- Example Procedure: When PLC firmware updates or code modifications are necessary, Form XXX-123 must first be documented and approved prior to authorization by Transport Administrator. Form XXX-123 must include a copy of the approved processes and the schedule for their application.
- Example Processes: The list of steps to include change of state of the bridge of offline, backup of existing PLC code and firmware, unlock of the PLC to remote, deployment of code/firmware, testing of code/firmware, approval of test, relock of PLC to RUN only, and placing the bridge back into the operation state.

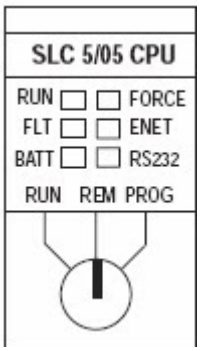
Guideline Reference Standards

- ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3, 4.3.2.6.5
- NIST SP 800-53 Rev. 4 PM-8, PM-9, PM-11, SA-14

4. PROTECT: Access Control: Physical Security

Physical access to OT assets should be managed and protected not only from external tampering but also from internal sources (insiders) as well. Access should be governed by policies, procedures, and processes.

- Network Wiring: Access to any Ethernet interface via cabinets, enclosures, ports, and wiring runs could provide an unnoticed avenue of compromise for the entire system. This is especially true for long runs over publicly accessible environments.
- PLC controllers: Wherever possible PLCs should have physical key switch capabilities that enable the system to lockout remote changes or programming. Local key access is required to set the PLC in another state. Typically, approval of this action (and others) is preceded by organizational procedure based on established cybersecurity policy.
- Enclosures: OT network, PLC equipment, connection points, switches, and all Communications/LAN/WAN equipment should be locked in enclosures and panel doors should initiate control system alarms when opened. Remote media access ports are not available to the operator.
- HMI workstations should be located in locked enclosures as well and media access ports should not be accessible to operators.



Guideline Reference Standards

- ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8
- ISA 62443-3-3:2013 SR 2.3, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
- NIST SP 800-53 Rev. 4 AC-2, AC-4, AC-17, AC-18, AU-12, CA-7, CM-3, CM-8, CP-8, PE-2, PE-3, PE-4, PE-5, PE-6, PE-9, PE-20, SC-5, SC-7, SI-4, SR, MP-2, MP-4, MP-5, MP-7

5. PROTECT: Access Control: Identity Management

Given a movable bridge in operational state, any user with workstation (also called HMI) display access could potentially operate the bridge in an unsafe manner. In a similar vein, any user with access to the software, firmware, and/or a network port could do the same.

- Credential Management: Access to physical and logical assets and associated facilities must be limited to authorized users, processes, and devices.
- Least Privilege: access rights for users and programmers should be limited to the bare minimum permissions they need to perform their work
- Separation of Duties: wherever possible, critical operations should require more than one person to initiate

Guideline Reference Standards

- ISA 62443-2-1:2009 4.3.3.5.1, 4.3.3.7.3, 4.3.4.3.2, 4.3.4.3.3
- ISA 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7, SR 7.6
- NIST SP 800-53 Rev. 4 AC-2, AC-3, AC-5, AC-6, AC-16, all AI items, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10

6. PROTECT: Encryption: Data-in-Transit

Control of a movable bridge from a remote location over a private dedicated link should require encryption for all communication streams (control system, video, security, sensors, etc.).

- Remote Fiber Runs: Hacking methods are available to tap fiber without detection so encryption should be used to protect against surveillance and mapping of the control system data flows. It is assumed that physical security methods are also applied to cable runs.
- Wireless: Wireless should be avoided due to its susceptibility to jamming and hacking. However, sufficient encryption methods do exist to protect the data streams in the case where there are no other feasible direct wiring capabilities.
- Encryption Level: recommend NIST Federal Information Processing Standard (FIPS) 140-2

Guideline Reference Standards

- ISA 62443-3-3:2013 SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.2, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
- NIST SP 800-53 Rev. 4 AC-4, AC-17, AC-18, CP-8, SC-7, SC-8

7. PROTECT: Network Segmentation

Many of the NIST PROTECT best practices are focused on preventing an adversary from compromising an OT network/system from the outside. The best practice of network segmentation assumes an adversary has already compromised the network. It designs the network in such a way as to limit or slow the impact/damage of any compromise.

This best practice segments the network based on the ISA Purdue Model using a combination of technologies to include:

- OT aware firewalls
- Virtual LANs (VLAN)

Guideline Reference Standards

- ISA 62443-2-1:2009 4.3.3.4, 4.3.4.5.6
- ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 5.1, SR 5.2, SR 5.4
- NIST SP 800-53 Rev. 4 AC-4, AC-7, IR-4

8. DETECT: OT Continuous Monitoring

If the control system was compromised, in the absence of any visible behavior, how would it be known?

Intrusion Detection and Intrusion Prevention

OT Network Intrusion Detection Systems (IDS) have been fine-tuned over the last five years. These systems are designed to establish a baseline of "normal" operations, such that "abnormal" operations can be flagged. Some OT aware Firewalls and some IDS systems also have the capability to stop any activity from occurring outside of a baseline. These systems are called Intrusion Prevention Systems (IPS).

The maintenance challenge for IDS software is in controlling and obtaining updates over the internet. Options exist to aggregate software updates on an offline server and deploy/test them when disconnected and not in production.

- Investigate and install a OT aware network IDS and establish an operational baseline
- Integrate IDS alarms with the existing control system alarm display
- Consider an IDS/IPS integrated OT Firewall solution
- Refer to the Governance best practice in this section: establish Policy, Procedure, and Processes for maintaining the IDS.

Endpoint Protection

Control System workstations and servers need to have software that monitors and prevents compromise to the operating system. The maintenance challenge for endpoint software is in controlling and obtaining updates from the internet. Options exist to aggregate software updates on an offline server and deploy/test them when disconnected and not in production.

- Periodic Vulnerability scanning
- Continuous Ethernet port traffic scanning
- Refer to the Governance best practice in this section: establish Policy, Procedure, and Processes for maintaining endpoint protection.

Monitoring Logs and Alarms

Any IDS/IPS or Alarm Log system becomes irrelevant unless the logs and alarms are responded to. This could have an impact on staffing, skill requirements, or inspire a 3rd party reliance for monitoring. Refer to #9 Best Practice: OT Event Response

Guideline Reference Standards

- ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7, 4.3.4.3.8, 4.3.4.5.9, 4.4.3.3

- ISA 62443-3-3:2013 SR 3.2, SR 6.1
- NIST SP 800-53 Rev. 4 AC-4, CA-2, CA-3, CA-7, SI-4, AU-6, AU-12, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, SI-3, SI-4, RA-5

9. RESPOND: OT Event Response

If the control system was compromised, what would be the response?

Installing and configuring IDS/IPS or Endpoint protection is not a significantly relevant mitigation without an event response plan.

- Refer to the Governance best practice in this section: establish Policy, Procedure, and Processes for monitoring and responding to IDS/IPS alarms. This includes notification to the relevant internal operational authorities as well as (if warranted) law enforcement.

Guideline Reference Standards

- ISA 62443-2-1:2009 4.3.2.5.3, 4.3.4.5.1, 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4, 4.3.4.5.5
- NIST SP 800-53 Rev. 4 AU-6, CA-2, CA-7, CP-2, CP-3, CP-10, IR-3, IR-4, IR-6, IR-8, PE-6, RA-5, SI-4

10. PROTECT & RECOVERY: OT Event Recovery

Assuming the bridge control system was compromised and it was noticed and reported, what timeframe is acceptable for restoring bridge operations?

Comprehensive backups allowing full restoration should be securely stored and maintained as part of the best practice “Asset Inventory Management”:

- Workstation operating systems, software applications, code versions, and licensing
- PLC Firmware and Code versions
- Configuration export backup files for PLCs, Firewalls, Switches
- Virtual Machine Images
- OT Inventory Documentation

Restoration techniques vary in the time required to restore to full operation. A worst case restoration would require workstation reinstallation of OS, software, applications/code, and licensing. It could also include replacement of equipment or the restoration of PLC firmware and code. Testing and validation of all systems would require stepping through a documented test plan. Prior to restoration, the system may need to remain offline in a compromised state so that cyber forensics can analyze and evaluate the cyber event.

A valid timeframe for both forensics and restoration might be hours to weeks depending on the response plan, response time, and technology used for backup and redundancy.

In order to speed workstation restoration there are a number of design techniques available to include:

- Warm or Cold redundant workstations and/or PLCs
- Virtual Machines and snapshots
- Terminal Server systems that image and restore the OS/Apps with each restart

Guideline Reference Standards

- ISA 62443-2-1:2009 4.3.4.3.9
- ISA 62443-3-3:2013 SR 7.3, SR 7.4
- NIST SP 800-53 Rev. 4 , CP-4, CP-6, CP-9, CP-10, IR-4, IR-8

Bridge Control System Recommendations

In the best practices section, we selected a Top 10 list to effectively reduce thousands of pages of national/international organizational and technical standards and provided a manageable top 10 list of best practices for movable bridges. As previously documented, there are a great many other best practices applicable to this space but these Top 10 are a preferable place to start.

We can now take the Top 10 list and summarize it into six business focused actionable information.

Recommendation #1: Consider AASHTO practice and procedures alignment with both NIST and ISA

NIST documentation is heavily weighted to the IT domain as the vast majority of its documentation originated by and for IT. While NIST 800-82 is focused on OT, it represents a small subset of the full featured OT standards in ISA/IEC 62443.

Recommendation #2: Conduct OT Cybersecurity Risk Assessments for each Movable Bridge

A comprehensive onsite OT Cybersecurity Risk Assessment is essential to secure design. It effectively determines the OT system "As-Is" state and provides the "To-Be" design that will securely service current and future requirements.

The risk assessment can cover a wide range of scope but it is recommended to include the following:

- As-Is State Onsite Design Evaluation and Documentation
    - OT Asset Inventory
    - Purdue Model Network Diagrams and Protocol Data Flows
    - Vulnerability Analysis
- To-Be Planned Design
    - OT Asset Inventory (recommended adds, upgrades, and replacement)
    - Purdue Model Network Diagrams and Protocol Data Flows
    - Risk Mitigation
    - Guidelines, Policies, Procedures, and Processes
        - OT Mitigation and System Maintenance
        - PLC and/or HMI Development, Code Changes, and Testing
        - Credential Management
        - Documentation
        - Backup Maintenance
        - Event Response and Event Recovery
        - Operator Training and Awareness

Recommendation #3: Mandate OT Intrusion Detection and Prevention (IDS/IPS)

Control systems for movable bridges are fairly static and simple. PLC and HMI code does not change frequently as in many industrial control systems. The baseline established for IDS therefore could be safely used to prevent any malicious network activity outside of the baseline.

An IDS/IPS integration would reports all "attempts" to infiltrate the network but they would not be successful.

Recommendation #4: Mandate PLC Run Mode Locks

Only certain PLCs have physical switches to prevent code and/or firmware changes locally or remotes. Due the critical nature of bridge control, these types of PLCs should be standard in bridge control system

network architectures. Policies and Procedures are required to control key access for new firmware and code updates.

Recommendation #5: Mandate Encryption

This includes all data and video communications via Ethernet that are both local and remote.

Recommendation #6: Mandate Cyber Awareness Training

While not specifically listed in the Top 10 best practices, it is assumed that the creation of guidelines, policies, procedures, and processes will result in the need to provide training.

APPENDIX C Proposed AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations

To be published by AASHTO COBS