2022 Heavy Movable Structures Biennial Symposium

October 17-20, 2022

Implementation Considerations for Remote Operation of Movable Bridges

An overview of the research and findings that led to the development of the AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations.

About the Authors:

Rob Moses has delivered the inspection, rehabilitation and/or design of over 250 movable bridge projects, including vertical lift bridges, bascule bridges, rolling lift bridges, swing bridges and other variations. He is a licensed Professional Engineer in 17 states. Mr. Moses has served as Project Manager, Project Engineer and/or Lead Engineer on numerous national and international movable bridge projects, including inspections, rehabilitation designs and designs for new construction. His areas of expertise include movable bridge evaluation, alternatives analysis, and mechanical and electrical systems including power distribution systems, control systems, motor-drive systems, hydraulic systems, remote control and preventative maintenance. Rob attained his Bachelor of Science degree in Electrical Engineering from Bucknell University in 1991.

Raphael Costa is in responsible charge of HDR's Movable Bridge Program and is accountable for the delivery of inspection, design and construction support projects involving movable bridges. Raphael has been involved in over 150 movable bridge projects and has been providing engineering support to Movable Bridge Owners and Asset Management Contractors for 22 years. His areas of expertise include all types of movable bridge electrical and controls systems including remote control and monitoring systems. Raphael holds a Bachelor's and Masters of Science in Electrical Engineering from the University of South Florida, and an MBA from New York University.

2022 Heavy Movable Structures Biennial Symposium

October 17-20, 2022

Implementation Considerations for Remote Operation of Movable Bridges

An overview of the research and findings that led to the development of the AASHTO Guidelines for the Operation of Movable Bridges from Remote Locations.

By:

Rob Moses, PE – HDR Engineering, Inc.

and

Raphael Costa, PE – HDR Engineering, Inc.

Table of Contents

ACKNOWLEDGEMENTS

This paper is an overview of a study that 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. This project designated by Project 20-07, Task 424 was intended to fund quick response studies on behalf of AASHTO. The work was guided by a technical working group. The project was managed by Waseem Dekelbab, NCHRP Senior Program Officer.

DISCLAIMER

The opinions and conclusions expressed or implied are those of the authors and the research agency that performed the research and are not necessarily those of the Transportation Research Board or its sponsoring agencies. This report has not been reviewed or accepted by the Transportation Research Board Executive Committee or the Governing Board of the National Research Council.

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.

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: Jason Lahm

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: R. Matthew Crawford

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: Per Saresand Sikstrom

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.

Identify
Protect
Detect
Respond
Recover

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.

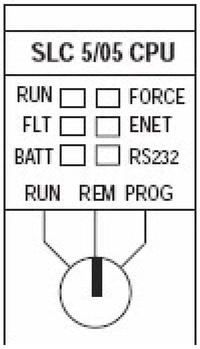
Guideline Reference Standards

- 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

Table of Contents

1 GENERAL PROVISIONS

1.1 Applicable Codes, Standards and Regulations

These guidelines provide recommendations for implementation of remote operation of movable highway bridges. They are intended to assist movable bridge owners in the evaluation and mitigation of the risks associated with transitioning movable bridges from local to remote operations. These guidelines are intended to supplement to the AASHTO LRFD Movable Highway Bridge Design Specifications.

Design specifications common to both locally operated and remotely operated bridges are not covered by these guidelines; the designer is directed to the aforementioned AASHTO LRFD Movable Highway Bridge Design Specifications for guidance in this regard. The concepts of bridge operation safety and reliability through application of design principles such as redundancy and reduction on dependency of tender skill are emphasized in those specifications.

These guidelines are not intended to supplant proper training or the exercise of judgment by the Designer and state only the recommended requirements necessary to address public safety relative to remote operations. The Owner or the Designer may require the sophistication of design or the quality of materials and construction to be higher than these minimum requirements at their discretion. The parts of these guidelines referring to design, workmanship and erection are intended to be recommendations for the designer to be included as required in the specifications written for the specific project.

The authority to regulate movable bridges across the navigable waters of the United States is vested in the Secretary of Homeland Security whom has delegated this authority to the Commandant of the U.S. Coast Guard. In accordance with the Code of Federal Regulations Title 33, Volume 1, Part 117, Subpart A, Paragraph 117.42, "upon written request by the owner of a drawbridge, the Coast Guard District Commander may authorize a drawbridge to operate under an automated system or from a remote location." Therefore, it is recommended to contact the Coast Guard District Commander at early stage of planning a remote bridge operation system to obtain Coast Guard recommendations and advice. These guidelines establish best practices that support the bridge owners' requests in seeking the Coast Guard regulatory approval of operating movable bridges remotely.

1.2 Design Philosophy

When considering the minimum requirements for remote bridge operations, the owner must first consider their ability to implement the proper operation and maintenance program required to safely and efficiently operate the candidate movable bridges in accordance with USCG regulations, specifically the Code of Federal Regulations Title 33, Volume 1, Part 117, Subparts A and B. Compliance with these regulations is paramount and must not be impacted by implementation of remote operations.

In order to comply with these regulations, the owner may be required to complete programmatic studies and actions to ensure that remote operations are undertaken safely, reliably and with due planning required to manage the remote operating systems effectively. Recommended studies and risk assessments that should be performed by the bridge owner or designer are included in Section 3 and consist of programmatic assessments of remote tender operational capacity, contingency planning for local operations, incident response, maintenance considerations and cybersecurity assessment.

Section 4 of these guidelines provide recommendations for the development of control systems to ensure the safety of maritime and roadway users while the bridge is operated from a remote location. This section covers key components and factors required to implement a satisfactory remote bridge remote operating system.

For remote bridge operation, surveillance technologies are required to replace visual and audio capabilities of the local bridge tender. Sections 5 and 6 provide recommendations for implementation of surveillance and communication systems to effectively monitor and communicate with vehicular, pedestrian and marine bridge users.

Upon satisfactory completion of the programmatic assessment required to implement remote operation of movable bridges, a technical assessment needs to be developed such that safe and reliable remote operations are implemented. These assessments should be submitted to the Coast Guard as part of the bridge owner's request to implement remote operations.

Design and implementation of remote operating systems are recommended to follow the design philosophy as outlined herein:

a. 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. Under remote operation, the movable span shall be operated by an automated span drive system 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.
b. The remote operating station shall have the ability to monitor and control each local movable bridge and related devices, have a sufficient quantity of surveillance system monitors and controls to safely manage bridge users and be equipped with an effective two-way communication system providing the remote tender with the ability to listen and speak to bridge users. 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).
c. The remote operating station, communication link and local bridge control system shall be designed such that the failure of a single component does not render the bridge non-operational 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.
d. 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.
e. 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. Failure of the communication link should stop all operations in a similar manner as the emergency stop function except as noted in section 1.2.d.

f. A surveillance system must be 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.

g. 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; however, implementation as system interlocks is recommended.

h. A comprehensive two-way bridge user communication system must be provided such that the remote tender and bridge users can effectively communicate. At a minimum, this system must effectively receive visual, audible and/or radiotelephone bridge opening requests and transmit communication signals to mariners per applicable USCG regulations.

i. A remote operating system lock-out/tag-out system must be provided at the locally operated bridge to prevent remote operation as required. In addition to the two-way communications system requirements, audible warning devices and microphones must be provided and located in restricted areas where maintenance personnel may be present.

2 ABBREVIATIONS, DEFINITIONS AND COMPONENT CLASSIFICATIONS

The following abbreviations are used herein:

AASHTO – American Association of State Highway and Transportation Officials

CCTV – Closed Circuit Television

HMI – Human Machine Interface

IEC – International Electrotechnical Commission

ISA – International Security Alliance

LRFD – Load and Resistance Factor Design

NEC – National Electrical Code

NEMA – National Electrical Manufacturers Association

NESC – National Electrical Safety Code

NFPA – National Fire Protection Association

NIST – National Institute of Standards and Technology

PLC – Programmable Logic Controller

USCG – United States Coast Guard

VFD – Variable Frequency Drive

VMS – Variable Message Sign

VOIP – Voice over Internet Protocol

Definitions and component classifications for the following terms as used herein:

Automated Span Drive System – A closed loop movable span motor-drive system equipped with field devices and control logic designed to ensure the correct sequence of operation, interlocking for protection of machinery and personnel, control of dynamics such as acceleration, deceleration, speed and skew in the case of a vertical lift span without intervention from the tender nor dependence on tender skill to safely operate.

Communication Link – The network media dedicated to transmitting and receiving data between a remotely operated movable bridge and the remote operating station.

Cybersecurity - The state of being protected against the criminal access or unauthorized use of electronic data, and the measures taken to achieve this state.

Designer – The system design engineer tasked with implementing safe operation of movable bridges from remote locations.

Information Technology (IT) – The study or use of systems such as computers and telecommunications for storing, retrieving, and sending information.

Offgoing Gate – Refers to the warning or barrier gate that a vehicle will encounter after crossing a movable bridge in the proper travel lanes. These gates are intended to warn or stop vehicles approaching a movable bridge from the wrong direction.

Oncoming Gate – Refers to the first warning or barrier gate a vehicle will encounter when approaching a movable bridge from the proper travel lanes.

Operational Technology (OT) – The systems used in the monitoring and operational control of virtual or physical devices such as control systems applied for the control and monitoring of movable bridge operation.

Owner – The owner, or entity authorized on behalf of the owner, of a movable bridge and/or remote operating facility.

Programmable Controller – A micro-processor based industrial controller such as a Programmable Logic Controller, Programmable Automation Controller or industrial computer used for machine control.

Programmatic Assessment – A study or examination of operational and maintenance procedures relative to the strengths, vulnerabilities, risks, needs and requirements to safely implement remote operation of one or more movable bridges.

Regulations – Code of Federal Regulations Title 33, Volume 1, Part 117.

Remote Operating Station – A bridge control console located outside of a movable bridge control house such that the tender does not have a clear viewing area of the roadway and navigable channel without the use of supplemental equipment.

Remote Operation – Operation of a movable bridge from a location other than on the site of a local bridge from the local bridge control console.

Tender – The individual responsible for safe operation of a movable bridge, whether remotely located or locally stationed on a movable bridge.

3 PROGRAMMATIC ASSESSMENT

3.1 General

When considering implementation of remote bridge operations, the owner must consider the programmatic modifications to their movable bridge operation and maintenance program required to safely and efficiently operate the candidate movable bridges in accordance with USCG regulations, specifically the Code of Federal Regulations Title 33, Volume 1, Part 117, Subparts A and B. Compliance with these regulations in a safe manner is paramount and must not be impacted by implementation of remote operations. Several areas of recommended assessments and program modifications are described in this section.

3.2 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 operating 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 Contingency Planning

Bridge owners undertaking remote operation of movable bridges should develop contingency plans to locally operate the candidate bridges should equipment failure or untenable environmental conditions 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.

3.4 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.

3.5 Bridge Condition and 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 bridge age, overall condition including structural, mechanical and electrical elements, and 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. All structural, mechanical and/or electrical deficiencies must be restored to full operational condition prior to transitioning the bridge to remote operations.

3.6 Maintenance Considerations

Implementation of remote operations inherently introduces specialty equipment and devices that are not prevalent on locally operated bridges. Equipment deployed for remote operations inherently requires more frequent inspection and maintenance compared to systems deployed on locally operated bridges. Owners should consider the impacts and mitigation techniques posed by introduction of remote operating systems and develop inspection and maintenance plans and practices to effectively assess, 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.

3.7 Pilot Implementation

When planning implementing 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.

3.8 Cybersecurity Risk 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.

At a minimum, three factors of risk should be evaluated: vulnerability, likelihood, and consequence. It is expected that the consequences of digital manipulation (insider 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. In the proposed OT environment for remotely operated bridges, the proposed methods to mitigate vulnerabilities should address the following cybersecurity risk assessment scope:

- Infrastructure Damage, e.g. 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, e.g. 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. For example:

    - Access to the control system or network allows pivoting to a different target system/network
    - The bridge moves/opens/closes at random changing speeds causing vibration and unsafe operational states
    - Video systems are hacked to provide access for surveillance of other targets
- Data Manipulation: the manipulation of process data. For example:
    - HMI screens (and perhaps even surveillance video) show operational states that are not accurate so that the bridge tender unknowingly executes commands that cause damage or safety events
    - Set points for closed loop control are compromised such that the bridge opens/closes too little or too much
- Data Exfiltration: Theft of data, e.g. 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

3.9 Remote Operation of Multiple Bridges

When remote operation of multiple bridges from a single remote station is provided, restrictions must limit the tender from controlling multiple bridges during the same time frame. The operation of a single bridge, either opening sequence or closing sequence, must be started and completed before the tender initiates the operation of a second bridge.

The only exception to this restriction is for a case where two adjacent bridges are normally operated in unison by a single tender at the local site. If this case is provided for, there must be sufficient monitors, operating simultaneously, to enable the tender to observe all conditions at both bridges.

4 CONTROL SYSTEMS

4.1 Control System Design

The intent of this section is to provide guidance for the design of reliable bridge control systems that address safety factors for marine and roadway users with the implementation of remote bridge operating systems. The electrical system design shall adhere to current standard practices for industry standards including the AASHTO LRFD Movable Highway Bridge Design Specifications as well as other relevant codes such as NEC, NEMA, NESC and NFPA. This section will cover the key components and factors to supplement a conventional movable bridge control system required to implement a satisfactory remote bridge operating system. This section applies to all various movable bridge types such as bascule, vertical lift, and swing bridges.

For remote bridge operations, safety enhancements such as supervisory controls and interlocking, additional surveillance systems and two-way communication systems shall be provided to protect pedestrian, vehicular and marine traffic from unsafe operations. The remote control system design shall employ system redundancies to prevent single component failure modes and to provide reliable and robust control systems where communication is critical to diminish system interruption and avoid delays to safe bridge operations.

As part of the remote control system design, the system shall incorporate a secured network topology to elude cybersecurity threats to local and remote communication networks which can be breached from malicious parties. Secure network control practices and protocols shall be in place, and the use of cyber-secure design principles shall be implemented to avoid any unforeseen cyber threats.

4.2 Control System Architecture

4.2.1 General

The local means for controlling a movable bridge shall be provided via a control workstation, Human Machine Interface (HMI) or control desk located in the bridge control house. For remote operations, a duplicate workstation, HMI or control desk shall be installed at the remote operating location. A Programmable Controller shall be installed at both the local bridge and remote operating location for implementing remote bridge operations. These controllers shall be networked to the local bridge control system via a communication link. Communication links may encompass the use of fiber optic cables, copper telecommunication cables, radio communication controls, and wireless systems.

The control system shall be designed to allow for local or remote bridge operations ensuring the correct sequence of operation with system interlocking in order to protect bridge users and operating machinery. Control system components such as Programmable Controllers, Human Machine Interface (HMI) devices, and closed-loop span motor drives such as a Variable Frequency Drive (VFD) shall be employed to preclude the need for tender skill to safely control the movable bridge and related components. A supervisory control system shall be installed both locally and at the remote operating site to mimic functionality and interlocking to allow for safe remote operation. The intent is to replicate bridge operation and provide surveillance and communication enhancements as if the tender were physically operating from the control house locally on the bridge.

Remote bridge operating systems shall be provided with system monitoring and data logging capabilities to facilitate maintenance and minimize system downtime to prevent delays to bridge users.

Consideration should be given to providing remote access to system information in real-time to permit diagnosis, troubleshooting, and trend identification in the event of control system malfunction. System monitoring shall continue in the event of loss of the communication link by incorporating data logging into the local bridge control system to store data.

4.2.2 Modes of Operation

Control systems for remotely operated bridges shall be designed to be operable locally without reliance on the remote operating system. Selection of local or remote operation of a movable bridge shall be selected via a keyed mode of operation control switch installed on the local control desk or in a secured location at the local bridge. With the keyed control switch in the local position, remote operations shall not be possible. Conversely, with the keyed control switch in the remote position, local operations shall not be possible.

4.2.3 Remote Operating Sequence

The operating sequence and interlocking requirements described in AASHTO LRFD Movable Highway Bridge Design Specifications shall be adapted and modified as described in this section to permit remote operation. The operating sequence and interlocking requirements shall be modified as necessary for specific bridge types.

Enabling Remote Bridge Operations

Step 1: To enable remote bridge operations, the local/remote mode of operation control switch at the local bridge must be in the remote position. In addition, the local bridge emergency stop pushbutton must not be depressed and bypass switches shall be in the 'Off' position.

Step 2: A secure remote tender interface, such as a keyed control switch or username and password, must be enabled at the remote operating station.

Step 3: The remote tender shall be capable of receiving bridge opening requests from marine vessels in the vicinity of any of the local bridges equipped for remote operations. Bridge opening requests by marine vessels may be made via marine radiotelephone, audible sound signals and/or visual signals.

Step 4: The remote tender shall select the appropriate bridge to be operated via input on the remote operating station. The remote control system shall enable the respective bridge's control system, surveillance system and communication system at the remote operating station.

Step 5: The remote tender shall respond to marine vessel opening requests at the appropriate bridge via marine radio telephone, sound signals and visual signals as required by the US Coast Guard.

Step 6: The remote tender shall be provided with sufficient CCTV monitors to view marine traffic, vehicular traffic, non-motorized traffic and pedestrians at the local bridge to be operated. The remote tender shall have the ability to select or adjust CCTV camera views in order to effectively observe all bridge users and focus on critical locations such as traffic gates, pedestrian gates and movable span.

Step 7: The remote tender shall have the ability to address bridge users via a public address system at the local bridge. This public address system shall also be equipped with sufficient microphones at each bridge such that two-way audible communications may take place between the tender and bridge users.

Step 8: An emergency stop button or device shall be provided as part of the remote operating station such that the remote tender can stop all devices or span movement at the local bridge on command. Resumption of remote bridge operations may only occur after the tender resets the emergency stop function and initiates the appropriate command.

Step 9: The remote tender shall have the ability to select the appropriate control and span drive system to be utilized at the local bridge to be operated. The remote operating station shall annunciate any warnings or alarms that may impede remote bridge operations prior to initiation of opening the span. When devices such as gates, locks or the movable span are operating, visual indication of such movement shall be provided on the remote operating console or user interface until operation ceases.

Open Span

Step 1: Initiate the traffic control devices and audible warning devices to signal roadway and pedestrian traffic to stop. To supplement the audible warning devices, the remote tender may announce the impending bridge operation via the public address system at the local bridge.

Step 2: Upon visual verification that roadway and pedestrian traffic has stopped in the proper locations, lower one oncoming warning gate while visually verifying it is safe to operate until fully lowered. After the first oncoming gate is fully lowered, proceed with lowering the other oncoming warning gate.

Step 3: Upon visual verification that roadway and pedestrian traffic has cleared the movable span and gate areas, lower one offgoing warning gate while visually verifying it is safe to operate until fully lowered. After the first offgoing gate is fully lowered, proceed with lowering the other offgoing warning gate.

Step 4: If the bridge is equipped with barrier gates, proceed to lower each individual barrier gate in a manner similar to the warning gates as described in the previous step.

Step 5: Unlock all span locking devices.

Step 6: Upon verification it is safe to open the movable span, initiate opening the span. The control system shall provide supervised control, monitoring and indication of span movement. At the fully open position, the span shall stop, the brakes shall set and the navigation lights shall be changed from red to green.

Close Span

Step 1: Upon verification that all marine vessels have cleared the open movable span and that it is safe to close the movable span, initiate closing the span. The navigation lights shall be changed from green to red and the control system shall provide supervised control, monitoring and indication of span movement. At the fully closed position, the span shall stop and the brakes shall set.

Step 2: Lock all span locking devices.

Step 3: The remote tender should announce the impending raising of the warning and barrier gates via the public address system. With permissive interlock from locking devices, the tender raises the barrier gates, followed by offgoing warning gates then oncoming warning gates. Alternatively, the barrier gates and warning gates may be raised automatically in the proper sequence via a single command initiated by the tender.

Step 4: The remote tender manually returns traffic signals from red to green. Alternatively, if the tender initiates an automatic command as described in the previous step, the traffic signals shall change from red to green once all permissive interlocks are satisfied.

4.2.4 Control Logic

4.2.4.1 General

Control logic for remotely operated bridges should be implemented via programmable logic controller, programmable automation controller and/or industrial control computer systems. While existing relay control logic may be adapted for remote operations, the designer should consider feasibility and economy of adding remote operating capabilities to existing relay control logic systems. System design shall include redundant processors and the ability for remote diagnosis and resetting of processor errors from the remote operating station. System design shall provide trouble alarms and maintenance messaging on the remote operating station for all major span operating devices. Such alarms and messaging should be stored in a memory module or industrial computer for remote downloading on demand.

Control logic shall be designed such that local operation of a remotely operated bridge is feasible without reliance on any component in the remote operating system. The designer may consider utilizing relay control logic as a local backup control system to the programmable control system.

In order to prevent unauthorized access to program modifications, processing units shall be provided with keyed 'Run Mode' locks normally deployed in the locked mode with the key stored in a secure location. Similarly, for industrial control computer systems, access to the system program shall be secured through a firewall and password-protected programming interface. Password protection must not reside solely with a single individual. A second individual must have access if the primary person is not available.

4.2.4.2 Interlocking Requirements

Similar to locally operated bridges, control logic for remotely operated bridges shall be designed to ensure the correct sequence of operation through the use of interlocking logic for the protection of bridge users, maintenance personnel and machinery, and control of dynamics such as movable span acceleration, deceleration, speed and skew. Interlocking requirements for remotely operated bridges should consist of enhanced features to verify remote tender interpretation of visual surveillance and aural communications during critical functions of bridge operations to minimize tender error and optimize safety as follows:

- During warning and barrier gate lowering operations, implementation of an interlock or a remote tender warning signal to prevent lowering of the gate should a vehicle or pedestrian occupy the path of the gate about to be set in motion or in the fully lowered position.
- Upon initiation of a span lock pull command or wedge pull command, provide an interlock or a remote tender warning signal to prevent operation should the presence of a vehicle, non-

motorized vehicle or pedestrian be detected on the movable span or in hazardous proximity to it during span lock and movable span operations.

- Upon initiation of a span open command, provide an interlock or a remote tender warning signal to prevent operation of the span should the presence of a vehicle, non-motorized vehicle or pedestrian be detected on the movable span or in hazardous proximity to it.
- Upon initiation of a span close command, provide an interlock or a remote tender warning signal to prevent operation of the span should a vessel be detected in or approaching the open movable span.

Proper application of field devices, sensors and surveillance components dedicated to providing these enhanced interlocks and/or remote tender warning signals given the bridge location, operating frequency and volume of bridge users shall be considered by the system designer. Suggested technologies for these interlocks are described elsewhere herein.

4.2.4.3 Bypass Switches

The use of bypass switches to provide a means of operating the bridge or a device when a field device or sensor malfunctions shall be prohibited during remote operations. Protocols for bypass switch use for remotely operated bridges shall be to operate under local operation whenever bypass switch use is required. Provisions shall be included for installing keyed locks or seals on each local bypass switch cover. Means shall be provided to monitor the status of bypass switches from the remote operating station and remote operations shall be disabled if a bypass switch is in use.

4.2.4.4 Emergency Stop

Remotely operated bridges shall be provided with emergency stop functions, at both the local operating console and the remote operating console. Additional emergency stop functions may be provided in the machinery rooms or other locations at the discretion of the designer to promote a safe local environment for maintenance or emergency response personnel on remotely operated bridges. The local emergency stop functions shall be effective and enabled regardless of whether the bridge is being operated locally or remotely. The remote emergency stop shall be enabled during remote bridge operations and may be enabled during local operations at the discretion of the designer.

The emergency stop pushbutton shall be prominent on the remote and local operating consoles and where deployed elsewhere. The designer shall consider use of a large, red, mushroom head pushbutton which illuminates once depressed and maintains a depressed state until manually lifted to reset. The remote emergency stop device shall utilize fail-safe design logic and programmable controller hardware interfacing with emergency stop devices shall be safety-rated Input/Output modules or contacts.

Once an emergency stop device is activated, all motion on the bridge and related components shall stop. Annunciation of the emergency stop shall be communicated to the remote tender and displayed on the remote operating console. Reactivation of motion of the bridge cannot commence until the emergency stop device is physically reset and the tender reinitiates a motion command on the operating console. Bypassing of emergency stop devices shall not be permitted.

4.2.4.5 Control of Standby Power

Remotely operated bridges should preferably be fed from backup sources of electric power such as dual utility feeders from different power grids or a standby engine generator set interfaced to the bridge power bus via an automatic transfer switch. The remote tender shall have the ability to monitor the viability of available power sources and enable a backup power source remotely, if desired. Standby engine generator sets shall be provided with signage alerting maintenance personnel to the potential of remote activation of the generator as well as a cutout switch to prevent automatic starting of the generator during maintenance functions.

4.2.5 Field Devices and Sensors

4.2.5.1 General

Remotely operated bridges shall utilize field devices and sensors to monitor bridge users and operating systems to supplement the visual and aural surveillance and communication systems as specified elsewhere herein. Field devices and sensors shall be included to provide annunciation of potentially unsafe conditions to the remote tender and to provide interlocking circuits where required to augment bridge user safety.

4.2.5.2 Pedestrian and Non-Motorized Vehicle Detection

Beyond use of video surveillance, the designer shall apply additional field devices and sensors to detect the presence of pedestrians, cyclists and other non-motorized vehicles in vulnerable areas during bridge operations. It is critical that the control system provides the remote tender with annunciation or interlocking circuits to prevent lowering of the warning and/or barrier gates if a pedestrian or cyclist is detected in its path of motion and to prevent operation of span locking devices, center wedges, end wedges and movable span if pedestrians or cyclists are detected inside the lowered gates. Various devices may be considered for pedestrian detection including motion detectors, infrared sensors, thermal image cameras, intelligent beacon sensing technology or other relevant devices.

4.2.5.3 Roadway Traffic Detection

Beyond use of video surveillance, the designer shall consider applying additional field devices and sensors to detect the presence of vehicles in vulnerable areas during bridge operations. It is critical that the control system provides the remote tender with annunciation or interlocking circuits to prevent lowering of the warning and/or barrier gates if a vehicle is detected in its path of motion and to prevent operation of span locking devices, center wedges, end wedges and movable span if vehicles are detected inside the lowered gates. Various devices may be considered for vehicle detection including video vehicle sensing, inductive loop sensors, motion detectors, infrared sensors, thermal image cameras, intelligent beacon sensing technology or other relevant devices.

4.2.5.4 Marine Traffic Detection

Detection of marine traffic on remotely operated bridges shall be provided to supplement the visual and aural surveillance and communication systems as specified elsewhere herein. Consideration shall be given to providing sensors to detect approaching marine vessels that may require bridge openings and to detect the presence of vessels in the open movable span during bridge operations. It is critical that the control system provides the remote tender with annunciation or interlocking circuits to prevent closing of the open movable span onto vessels traversing or approaching the open movable span.

Devices to detect marine vessels approaching the movable span may include radar sensors, video vehicle sensing or other devices. For movable bridges with significant commercial marine traffic, consideration should be given for the remote tender to monitor commercial vessels through the use of Automatic Identification System (AIS) marine monitoring applications at the remote operating station. At locations used by large vessels the tender must be provided with the information concerning the time and distance needed by those vessels to come to a stop. Monitoring devices should be considered that would cover the entire relevant distance.

Channel sensors should be provided to detect vessels immediately approaching or under the open movable span. The channel sensors shall be interlocked with the bridge control system to detect a vessel passing under the open movable span and stop the movable span from closing if in motion. The remote tender shall not be able to initiate closing of the span until the vessel clears the limits of the open movable span.

4.2.6 Lightning Protection

Given the prevalence of solid-state components on remotely operated bridges, lightning protection is required per the AASHTO LRFD Movable Highway Bridge Design Specifications. Lightning protection for the facility housing the remote operating station is also recommended. Lightning protection systems, where specified, shall be designed in accordance with NFPA 780 and all relevant codes per the authority having jurisdiction of the bridge and remote operating facilities.

4.3 Local Operation

4.3.1 General

Remotely operated bridges shall be provided with a local tender interface such that the bridge can be operated locally, independent from the remote operating system. Control logic shall be designed to ensure the correct sequence of operation, interlocking for protection of machinery and personnel, control of dynamics such as acceleration, deceleration, speed and skew of the span. Consideration should be given to providing a redundant local operating system, such as a relay control logic backup system to operate the system should the primary operating system be non-operational.

4.3.2 Lock-out/Tag-out Provisions

Safety to maintenance personnel on remotely operated bridges must be considered by the system designer. Provisions for locking out remote operations during maintenance functions should be considered beyond the keyed mode of operation control switch to be installed on the local control desk or in a secured location at the local bridge as previously described. Code compliance, particularly with regard to lockable motor in-sight disconnect switches, lock-out tag-out facilities and procedures and effective communications with the remote tender from the local bridge shall be provided on each remotely operated bridge.

The status of the keyed mode of operation control switch and motor in-sight disconnect switches shall be monitored by the remote operating control system and control of the movable span and its auxiliary systems shall be disabled should these switches be in the ‘Local’ or off position, respectively. Switch status preventing operation of the bridge shall be annunciated on the remote operated console such that the remote tender is made aware of maintenance operations prior to initiating a bridge opening sequence.

4.4 Remote Operation

4.4.1 General

Remotely operated bridges shall be provided with a remote tender interface such that the bridge can be operated remotely with sufficient visual and aural feedback from the local site to provide a safe operation. The remote operating system may depend on the functionality of the local control system for proper operation. Control logic shall be designed to ensure the correct sequence of operation, interlocking for protection of machinery and personnel, control of dynamics such as acceleration, deceleration, speed and skew of the span. Consideration should be given to providing redundant control system elements such that a single source of component failure does not render the system non-operational nor compromise any safety features.

4.4.2 Remote Operating Station

The remote operating station shall consist of a bridge control console or workstation computer, monitors, and input devices; a CCTV control station equipped with system controllers; large format CCTV monitors; a public address system microphone, speaker and/or headset; and a marine radio with a handset. .

The remote operating console shall offer control and indicating devices that would be typically found on a local control console. These features may be implemented using manual operating devices or virtually through the use of Human Machine Interface (HMI) devices. The remote operating console shall be provided with a physical Emergency Stop device as specified above.

4.4.3 System Monitoring

4.4.3.1 General

When implementing remote operation of movable bridges, the system designer shall consider augmentation of control system monitoring capabilities. While a particular level of supervisory control is specified to be incorporated into the control systems of remotely operated bridges, a complimentary level of system monitoring and data acquisition is recommended to facilitate system maintenance and troubleshooting.

4.4.3.2 Annunciation and Troubleshooting

The system designer should consider the appropriate level of system monitoring to be implemented on remotely operated bridges. The ability of maintenance personnel to respond quickly to unexpected system incidents shall be taken into account and used to provide the level of remote system warnings, annunciation and troubleshooting capabilities. At a minimum, the remote tender shall have the ability to receive system feedback and diagnose control system problems similar to what a local tender would be capable of from the local operating station.

5 SURVEILLANCE SYSTEMS

5.1 Video Surveillance Systems

5.1.1 General

Closed circuit television (CCTV) systems are required to provide visual surveillance of the local bridge roadway, sidewalks, navigable channel and secured areas, such as the control house and machinery rooms, to the remote tender during remote bridge operations. CCTV systems are also required to detect visual bridge opening requests from mariners such as flag and light signals per USCG regulations. In addition to the CCTV system, additional video surveillance technologies and field devices shall be considered and applied where appropriate to provide a safe operating environment for all bridge users.

5.1.2 Closed Circuit Television Systems

Comprehensive CCTV systems are required to provide unobstructed video images to the remote tender, respond to camera control signals from the tender, and ensure video images can be transmitted to remote locations for observation. A sufficient number of individual CCTV cameras and viewing monitors should be provided to display continuous, dedicated views of critical areas of the bridge including the upstream and downstream views of the navigable channel, the movable span roadway, sidewalks and bridge approaches.

The CCTV system interface should be designed and programmed such that the most effective camera views are displayed on the monitors during critical sequences of bridge operations. System interface shall be user-friendly and not require regular intervention or control by the remote tender during bridge operations. Consideration should also be given to providing the ability to record continuously or an event from any video source to support incident response operations.

Cameras may be provided with pan-tilt-zoom (PTZ) capabilities to provide the remote tender the ability to focus on a particular area; however, PTZ cameras shall not be applied as a means to minimize the number of dedicated cameras at each local bridge. Camera housings, PTZ mechanisms and related exterior components shall be weather-tight, corrosion-resistant and vandal-resistant. Considerations should be given to providing camera housings vented with a thermostat-controlled heater and blower and/or provided with a wiper to prevent the build-up of condensation and water droplet accumulation on the housing window.

5.1.3 Infrared Cameras

Infrared cameras may be applied to improve visibility for the remote tender during low ambient light conditions. The designer shall consider the relatively limited viewing range when applying night-vision, infrared cameras. Additional cameras may be required for safe operations in low light conditions.

5.1.4 Thermal Image Cameras

Depending on the structural configuration of the local bridge to be remotely operated, particularly where a bridge has blind spots such as through-truss spans, thermal image cameras may be applied to supplement CCTV camera views. Thermal image cameras may be applied to detect vehicles or pedestrians potentially shielded from view by obstructions or for vessels in the navigable channel. Thermal image cameras should be specified to produce a temperature sensitive image capable of differentiating the temperature of the structure from the temperature of vehicles, pedestrians and vessels in the respective camera view. Thermal image cameras may be applied as a secondary means of surveillance during low visibility conditions but should not serve as the primary means for verifying the presence of bridge users in vulnerable areas.

5.1.5 Video Vehicle Sensing

Video vehicle sensing technology, commonly employed in intelligent transportation systems (ITS), may be employed to provide system interlocking or annunciation during critical bridge operating functions, such as initiation of unlocking span locking devices. Pixel-recognition cameras programmed for video vehicle sensing may be applied on the roadway areas between the lowered gates and be programmed to detect any out of place objects in this camera view and prevent operation of the span locking devices in anticipation of a bridge opening. The bridge control system, interfaced with the video vehicle sensing system, could issue a visual and audible warning that an object is detected on the movable span to alert the remote tender. At the discretion of the system designer, this function could also be programmed into the bridge control system as an interlock to automatically prevent unlocking of the span locking devices and opening of the movable span should a vehicle be detected between the lowered gates.

5.2 Intrusion Detection

Intrusion detection shall be provided both at the local bridge and the remote operating site in order to secure the bridge and its ability to be operated by unauthorized personnel. The bridge control house, machinery rooms, fender system access points and other vulnerable areas shall be secured and locked with provisions for remote monitoring by the tender. The remote tender, and other authorities at the discretion of the bridge owner, shall be automatically notified if a secured location is breached. The intrusion detection system may also be interfaced with the two-way communication system in order to issue a verbal message to unauthorized trespassers.

5.3 Fire Detection

Remotely operated bridges shall be provided with fire detection systems to detect fire or smoke conditions in the local control house, machinery rooms, generator room and other critical areas. For the protection of local maintenance personnel, alarms and detectors shall be interconnected and capable of monitoring all detectors and signaling all alarms in the event of a fire hazard.

Detectors shall be powered by a 120-volt nominal power supply with battery back-up. Heat detectors units shall be fixed temperature at 135 degrees F (56 degrees C) and rate-of-raise rating of 15 degrees F/min. (10 degrees C/min) and installed in the generator room. All smoke detectors, heat detectors and alarming devices shall be installed per local codes and manufacturers' instructions.

5.4 Surveillance Field Devices

5.4.1 General

Safe operation of remotely operated bridges is largely dependent upon effective visual surveillance of the bridge users and operable devices at the locally operated bridge. The system designer shall consider implementation of additional surveillance field devices to supplement the visual surveillance system in order to verify interpretation of system views by the remote tender. These devices shall be integrated into the remote operating supervisory control system in the form of annunciation of warning alarms to the remote tender and incorporation of system interlocks to prevent unsafe operation of the movable span, span locking devices and traffic control equipment. A variety of devices should be considered by the system designer taking into account unique features at each remotely operated bridge.

5.4.2 Inductive Loop Sensors

Inductive loop detectors may be applied to enhance surveillance of vehicles in areas that are to remain clear during bridge operations, such as under the traffic warning and barrier gate arms. Loop detectors installed in the roadway under the path of each gate arm may be interlocked in the bridge control system to prevent lowering the gate onto a vehicle should one be detected. The designer should consider the feasibility of effective installation and performance of loop detectors given the roadway surface and environment.

5.4.3 Intelligent Beacon Sensing Technology

Intelligent Beacon Sensing Technology, typically utilized in ITS applications, may be applied on remotely operated movable bridges as part of a larger traffic management network or to sense traffic flow trends over the movable span. This technology may be applied as part of an incident management strategy to sense changes in traffic flow but it should not be relied upon as a means to detect the presence of roadway users nor for life safety applications.

5.4.4 Motion Detectors

Motion detectors may be applied to alert the tender of the presence of pedestrians, cyclists, motorists, mariners or trespassers in the sensing area of the detector. These detectors can be incorporated into the bridge supervisory control system to provide a warning signal to the remote tender or as an interlock during critical portions of bridge operations. Motion sensors may also be applied to detect maintenance personnel and/or intruders in unauthorized areas such as machinery rooms. Intelligent programming practices to screen out nuisance signals may be applied as determined by the system designer, but generally motion sensors should be secondary sensing devices and not relied upon as a primary life safety element during bridge operations.

5.4.5 Variable Message Signs

Variable message signs (VMS) may be applied on remotely operated bridges to provide messages to motorists and pedestrians during bridge operations and to manage unforeseen incidents. VMS applications may include annunciation of impending bridge operations and messaging to motorists to manage incidents. VMS may also be used on bridges to communicate with mariners that may not have a marine radio to provide messaging of impending bridge openings or unforeseen bridge operational outages.

5.4.6 Channel Sensors

Navigable channel sensors, or an equivalent means of surveillance, shall be applied to monitor marine traffic in the navigable channel traversing the open movable span and to prevent closing of the movable span if a vessel fouls the area covered by the channel sensors. Preference should be given to back checking the tender's judgment by providing channel sensors as an interlock to the supervisory control system during bridge closing sequences such that span closing is prevented if a vessel is traversing the open movable span.

5.4.7 Radar Detection Systems

The system designer may consider adding radar detection systems at the locally operated bridge to identify approaching marine traffic. Provisions should be made to alert the remote bridge tender of approaching traffic at the prescribed distance or envelope determined by the system designer. Application of radar detection systems should be considered with regard to early warning of approaching vessels to supplement the two-way communication system between the remote tender and mariners and/or as an interlock function to prevent closing of the movable span should an approaching vessel be detected. Radar detection systems can be programmed to survey wide or narrow bands of coverage and as such, they can also be applied to scan the navigable channel before closing an open movable span.

5.4.8 Automatic Identification System

On remotely operated bridges that have significant commercial marine traffic, the remote tender may be equipped with a workstation to monitor vessel Automatic Identification System (AIS) information. AIS systems to monitor commercial vessel transponders may be useful to track approaching vessels such that the remote tender can plan for bridge openings. AIS could also be applied to transmit information from the remote tender to commercial vessels with regard to bridge inoperability or emergencies.

6 COMMUNICATION SYSTEMS

6.1 General

Remote operating systems require effective communication systems such that the remote tender can communicate with the local bridge users and receive communications from the locally operated bridge site. The critical elements of an effective communication system for remote operations include a Two-Way Public Address System, Marine Radio, Telephone and a Communication Link to carry communications between the remote operating station and the local bridge.

6.2 Two-Way Public Address System

Remotely operated bridges shall be equipped with two-way communication systems such that the remote tender can effectively communicate with the bridge users. The system designer shall specify a two-way public address system consisting of a remote microphone at the remote operating station and local loudspeakers for the tender to broadcast verbal messages to vehicular and pedestrian users and local microphones and remote speaker for the remote tender to listen to aural communications at the local bridge site. The remote microphone and local loudspeakers shall be utilized to effectively direct motorists and pedestrians that do not follow the traffic control signals and to deter unauthorized entry.

The communication system shall be designed such that the remote tender is able to hear aural signals at the local bridge, such as an air horn from marine users requesting a bridge opening which is generally an acceptable method for requesting a bridge opening. Local microphones shall be provided at the bridge with a remote speaker provided at the remote operating station such that the remote tender can acknowledge request for openings and to aid in incident detection similar to what a local tender may be capable of hearing on site. If a remote tender is tasked with operating more than one bridge, the remote speaker must be supplemented with annunciator that indicates which bridge microphone is receiving aural signals. The remote bridge tender must be able to respond with the prescribed air horn blasts to an aural request for an opening or with the appropriate visual signal, such as a flashing light, in the case of a visual opening request such as flagging or signal light from mariners.

6.3 Marine Radio

In addition to the public address system, the remote tender must be able to receive and transmit verbal messages broadcasted over the local bridge marine radio from the remote operating station. The remote tender must be able to acknowledge bridge opening requests and communicate with local marine traffic. A remote marine radio, or an interface that allows the remote tender to receive and broadcast marine radio transmissions to each respective locally operated bridge, is required to be installed at the remote operating station. The communication between the local and remote marine radio stations may be linked via a voice over Internet protocol (VOIP) system on a dedicated remote communication link.

6.4 Telephone

A landline telephone is required for the remote bridge tender to communicate with emergency response personnel, maintenance crews and to receive bridge opening requests via telephone, if applicable. Multi-line phones can be used if multiple phone numbers are available for mariners to call or these phone numbers can be consolidated into a single bridge opening request line where feasible. Provision of a conventional telephone at remotely operated bridges for the use of local tenders and maintenance personnel, when present, is also recommended.

6.5 Communication Link

6.5.1 General

A secure communication link consisting of a hardwired or fiber optic connection shall be provided from each local bridge to the remote operating station. Clearly defined Quality of Service protocols shall be in place, or dedicated communication links shall be provided for control systems, video surveillance and two-way communication systems. In addition, the system designer shall specify a reliable, secure backup communication link capable of providing the same level of service as the primary link.

6.5.2 Fiber Optic Connections

Fiber optic cabling for means of communication between the local bridge and the remote operating station may be single or multimode. The system designer shall ensure the proper mode of operation is utilized for proper communication link between local and remote sites. All fiber optic drop cable between cabinets and backbone cable may be either single or multimode type and shall be sized per the designer. All underground fiber optic cabling either buried or trenched shall not be installed with power conductors in pull boxes, vaults, or conduit.

Fiber optic cables shall contain a dielectric central strength member and dielectric outside strength member to prevent buckling of cable and provide tensile strength. The fiber optic cable shall be capable of withstanding a pulling tension of 600 pounds during installation without decreasing the fiber characteristics after the tensile load is removed, and without damage to any components of the fiber optic cable.

Fiber optic cables shall contain a dry water blocking material to prevent the ingress of water within the outer cable jacket. The water blocking tapes and yarns shall be non-nutritive, dielectric, resistant to mold/fungus, homogeneous, and free from dirt and foreign matter. A dry water blocking material for fiber optic cables shall be used for either aerial or underground installations. A dry water blocking compound shall be longitudinally applied around the outside of the central buffer tubes.

The fiber optic cable shall be jacketed with medium density polyethylene (MDPE) that is free of blisters, cracks, holes, and other deformities. The nominal jacket thickness shall be a minimum of 0.03 inch. The jacketing material shall be directly applied over the tensile strength members and water-blocking material. The MDPE shall contain carbon black to provide ultraviolet (UV) protection and shall not promote the growth of fungus. The jacket shall be continuously marked, at no less than 5 foot intervals, with the cable manufactures name, fiber type, count, date of manufacturer, and the sequential marked cable length indicated by the marking. The markings shall be legible and of contrasting color to that of the cable jacket.

Fiber optic cables shall include loose buffer tubes that isolate internal optical fibers from outside forces and provide protection from physical damage as well as water ingress and migration. The buffer tubes shall provide freedom of movement for internal optical fibers. The buffer tubes shall allow for expansion and contraction of the cable without damage to internal optical fiber. The fibers shall not adhere to the inside of the tube.

6.5.3 Wireless Connections

Wireless communication systems may be utilized, preferably as a backup to a fiber optic link. The system designer shall detail a fully integrated, redundant wireless system to include cellular/PCS wireless modems, wireless Ethernet radio transceivers, or wireless broadband radio transceivers including all necessary hardware and software to operate a secure network.

Wireless equipment shall conform to the National Electrical Code (NEC), the National Electrical Safety Code (NESC), Underwriter's Laboratories (UL), and all local safety codes. If equipment is installed on utility poles, comply with all regulations and codes imposed by the end user of the affected utility poles.

6.5.4 Cybersecurity

6.5.4.1 General

The system designer shall consider applicable cybersecurity practices when implementing remotely operated bridges including both NIST and ISA recommended standards. NIST documentation is heavily weighted to the Information Technology (IT) domain as the vast majority of its documentation originated by and for IT. While NIST 800-82 is focused on Operational Technology (OT), it represents a small subset of the full featured OT standards in ISA/IEC 62443.

6.5.4.2 Risk Assessment

For each remotely operated bridge as well as the remote operating station, a comprehensive onsite OT Cybersecurity Risk Assessment shall be conducted to determine secure design requirements. The risk assessment shall effectively determine the OT system "As-Is" state and develop the "To-Be" design that will securely service current and future requirements. At a minimum, the risk assessment scope shall 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
        - Programmable Controllers and/or HMI Development, Code Changes, and Testing
        - Credential Management
        - Documentation
        - Backup Maintenance
        - Event Response and Event Recovery
        - Tender Training and Awareness

6.5.4.3 Security

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

- 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.
- Programmable controllers: Wherever possible Programmable Controllers should have physical key switch capabilities that enable the system to lockout remote changes or programming. Local key access is required to set the Programmable Controller in another state. Typically, approval of this action (and others) is preceded by organizational procedure based on established cybersecurity policy.
- Enclosures: OT network, Programmable Controller 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 tender.
- HMI workstations should be located in locked enclosures as well and media access ports should not be accessible to tenders
- Facilities containing OT Assets such as local bridge control houses and remote operating centers should be physically secured against intrusion, monitored for unauthorized intrusion and monitored for fire/smoke conditions.
- Provisions for backup electric power supplies should be made at local and remote operating facilities

6.5.4.4 OT Intrusion Detection and Prevention (IDS/IPS)

Control systems incorporating Programmable Controller and HMI components shall be protected with intrusion detection and/or prevention integration. The baseline established for IDS shall be safely used to prevent any malicious network activity outside of the baseline. IDS/IPS integration would report all "attempts" to infiltrate the network as a means to monitor attempted cybersecurity breaches.

6.5.4.5 Encryption

The system designer shall specify encryption of all data, video and audio communications carried via Ethernet, both to and from the remote operating site and the local bridges.

2022 Heavy Movable Structures Biennial Symposium

October 17-20, 2022

Implementation Considerations for Remote Operation of Movable Bridges

Knowledge Quiz

1. Currently, there are no movable bridge owners in the United States remotely operating movable bridges.
   a. True
   b. False

2. Typical risks associated with movable bridge operations include:
   a. Life safety risk to navigation, vehicular (motorized and non-motorized, inclusive) and pedestrian users and bridge maintenance personnel during bridge operations
   b. Risk of delays to bridge users due to bridge inoperability or malfunction
   c. Risk of facility damage due to fire or unauthorized access
   d. All of the above

3. 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:
   a. Increased risk of safety-related incidents to navigation, vehicular and pedestrian users
   b. Increased risk of delays to bridge users due to high traffic volume
   c. Both a. and b.
   d. None of the above

4. Which of the following system design features have been incorporated into movable bridges currently being operated remotely:
   a. Closed loop span motor drives under PLC-based control
   b. Non-redundant span drives
   c. Both a. and b.
   d. None of the above

5. Movable bridge operations fall under the jurisdiction of the United States Coast Guard per Title 33 of the Code of Federal Regulations, Part 118 – Drawbridge Operation Regulations.
   a. True
   b. False

6. What scope of attack should be implemented to mitigate vulnerabilities in Operational Security:
   a. Infrastructure damage
   b. Denial of service
   c. Malicious use

    d. All of the above

7. Which of the below is a viable cybersecurity threat pathway to remote bridge operating systems:
    a. Access to the motor disconnect switch
    b. The bridge operations log
    c. The bridge Programmable Logic Controller programming terminal or laptop
    d. The bridge VHF marineradio

8. Remote bridge control system design should employ non-redundant systems to prevent single component failure modes:
    a. True
    b. False

9. What devices are recommended to be incorporated into the surveillance systems of remotely operated movable bridges:
    a. Fire detection systems
    b. Closed circuit television cameras
    c. Both a. and b.
    d. None of the above.

10. One-Way public address systems are recommended for use on remotely operated movable bridges:
    a. True
    b. False

HMS
HEAVY MOVABLE
STRUCTURES

2022 Heavy Movable Structures Biennial Symposium

October 17-20, 2022

Implementation Considerations for Remote Operation of Movable Bridges

Knowledge Quiz Answer Key

1. a.
2. d.
3. a.
4. b.
5. a.
6. d.
7. c.
8. b.
9. c.
10. b.