HEAVY MOVABLE STRUCTURES, INC.
TWENTIETH BIENNIAL SYMPOSIUM

October 7-10, 2024

Remote Operated Bridges
Best Practices and Future Technologies

Miguel Estrella, P.E.
Modjeski and Masters

SHERATON HOTEL
NEW ORLEANS, LA

Background

Movable bridges are nothing new, but their shift from medieval drawbridges to the modern infrastructure has been astronomical. With the addition of the technological powerhouse that is the programmable logic controller (PLC), movable bridges have become exposed to functionality once considered unthinkable. The most notable of these features is network communication, which has brought about the next breakthrough in movable bridges: remote operation.

Remote operation of movable bridges has seen growth in its adoption in both existing and new projects. However, issues that could be minor with a staffed bridge can disable a remotely operated bridge. Elements from the control system, the movable bridge itself, the site, and even external factors can create both immediate and long-term problems. But, despite the various concerns, remote operation remains a desired future, where maintenance and operation of movable bridges are easier and cost effective. It has also been proven with many successful ongoing and completed projects where solutions were developed to the troubles presented.

Like the movable bridge industry, innovation moves technology forward. New and developing technologies have shown potential use-cases for the industry. Technologies such as augmented and virtual reality can not only modernize trainings but also introduce new methods of remote operation. Internet-of-Things (IoT) and other alternatives can improve maintenance. Lastly, artificial intelligence (AI) shows the possibility for safer and potentially revolutionized operation of movable bridges.

Remote Operation Problems and Solutions

While remote operation can be considered the future of movable bridges, there are concerns that need to be addressed before any implementation can occur. Movable bridges consist of various different systems working together to make operation possible, but a few in particular play key roles in remote operation. Similarly, the condition of other external factors often need to be favorable for remote operation to have long term success. These particular elements and factors are discussed herein:

- PLC System
- Closed-Circuit Television (CCTV) System
- Public Announcement (PA) System
- Bridge Conditions
- Site Conditions
- Environment
- Power Source
- Networking
- Obsolescence
- Cost

Each of these concerns have issues that can arise in both locally and remotely operated movable bridges, but they can be a serious hindrance to the latter. While an on-site presence could be the solution to some of these issues for locally operated movable bridges, remotely operated bridges require adequate mitigation to prevent disabling bridge operation. However, despite these issues being valid concerns, there have already been numerous projects which have implemented common practice and experimental solutions to prove remote operation can be successful.

PLC System

The control system of a movable bridge is a marvel of technology, capable of integrating all electromechanical equipment with all the control equipment the Operator uses. At the heart of this is the PLC system, through which its components interfaces with the equipment and other subsystems. The PLC system can suffer from issues related to its industrial application, and despite being more simplified, it is often impacted with issues that affect common household computers.

The hardware required for a PLC system varies by project, but will commonly have the processor, input/output (I/O) and communication modules, human-machine interfaces (HMIs), and other miscellaneous equipment, such as power supplies and network switches. Most equipment is typically housed inside the control console and a main PLC cabinet, but it is common for remote cabinets to house remote I/O “drops” that communicate back to the PLC processor. The remote operation location may also have PLC equipment and an HMI to communicate with the local processor for operations.

Additionally, the PLC system will be programmed according to all the I/O used, the additional PLC control equipment, auxiliary systems, and most importantly, the sequence of operation. The programming can be considered as separate functions which join together for overall operation. The programming will often have functions that handle the PLC functions, such as reading and writing of I/O modules, operation of the HMIs, and communication with network switches. Similarly, there may be functions which handle interfacing with all the auxiliaries that make up the control system, such as flux vector drives, automatic transfer switches, CCTV systems, PA system, fire and security alarm system, and even decorative lighting system.

Hardware related issues are the most likely issues to occur with the PLC system, which can result in the bridge being unable to operate or operating unsafely. In particular, module failure is the most concerning, as failed modules can lead to loss of communication and/or incorrect equipment status. However, for bridges where remote operation is accomplished through an HMI, failure of the HMI will also disable operation. Most of the miscellaneous equipment required by the PLC system are often separate devices that can potentially fail through their own accord as well.

One possible example to consider is an instance where a remote PLC cabinet in a Machinery Room has an I/O module that monitors the machinery equipment, particularly the brake limit switches. The remote PLC cabinet also has a communication module that provides a networked connection to the PLC processor at the control console. In the event that the communication module fails, the connection to the processor drops and the PLC is unable to determine the status of the brakes, therefore it does not allow the bridge to operate.

A separate example to consider is an I/O module that monitors the full seated limit switch of the bridge. In the event that the I/O module has an issue, such as a damaged I/O point, or if limit switches does not operate correctly, the consequences can be more severe. A damaged I/O point can potentially misread the status of the fully seated limit switch as seated, or the fully seated limit switch contacts may have malfunctioned and indicate seated, despite the bridge not being fully seated. If this occurs during an operation, it would allow the PLC system to drive the span locks with the bridge being unseated which

can cause damage to the infrastructure and the span locks themselves (this is similar to fully seated bypass switches, but those are intentional).

Thankfully, PLC hardware issues such as those mentioned are rare, as reliability of PLC equipment have greatly improved over time. Even damaged I/O points are less of a concern as PLC system often have safety checks which determine if any I/O points have potential issues. But given the circumstance of potential hardware failure where a lack of on-site presence would prevent its quick replacement, the most common solution is redundancy. Providing a second component which provides a second signal to the system as backup can avoid shutdown of the system or unintentional operation from just one device failure. In some instances, even power supplies are provided a second redundant power supply. Some PLC manufacturers have even included automatic switching capabilities, so the system detects issues itself and switches power supplies when needed. Even a redundant network loop can resolve communication module failure, as it would connect to all the devices a second time and provide a backup communication route.

Software issues are less likely to occur, as programming is often thoroughly tested prior to the final installation, but should they occur, they would result in the bridge being inoperable. There is the potential of memory leaks that may only occur over extended periods of operation, resulting in a slow response or a freezing interface. Corruption of code is also a rare possibility, usually caused by power issues or electromagnetic interferences, and could result in malfunctions that compromise the PLC programming.

Software failure can typically be remedied by periodic power cycling and periodic backups. Any potential memory leaks would likely occur over extended operation periods, so it would require long-term observation. If any are found, it is best to update the code accordingly, but periodic power cycling can reset most memory issues. Backups of the PLC code and any other software should always be retained. It should also follow the 3-2-1 rule: 3 copies, 2 different media, 1 copy offsite. Having a copy of the PLC code on site can lead to speedy recoveries should there be issues. Periodic backup can also allow the system to revert back to stable releases should there be software update issues.

CCTV System

The CCTV system can be considered the second most important subsystem for remote operation. In locally operated bridges, it provides the Operator with the ability to view all areas of interest and any potential blind spots. Without this system, remote operations would not be possible, as not only do they allow the Operator to observe the real-time site conditions, but it is part of the United States Coast Guard (USCG) requirement for remote operation to have a clear unobstructed view of the waterway (USCG).

The CCTV system consists of cameras, CCTV monitors, network video recorders, workstations, and other miscellaneous equipment such as power supplies, network switches, and network repeaters. Cameras are positioned at strategic locations that provide the best view of the areas of interest. Most equipment is commonly housed in a CCTV cabinet kept on site. CCTV monitors are placed in the Operator’s Room for observation during operation. The CCTV system commonly has its own network switches and operates on a separate loop to the PLC system. The cameras, which are placed throughout the bridge, can receive their power from either Power-over-Ethernet (PoE) connections, or power supplies housed in local cabinets. Ethernet connections commonly provide the communication capability, but network repeaters or the use

of fiber optics are required when distance is too large. The remote operation location may have an additional CCTV monitor that displays select CCTV cameras at all times, with a remote workstation.

The CCTV system may have its own proprietary software for the cameras and workstations that handle video processing and recording. It will have a general software that provides a graphical interface for CCTV control at its workstations and personal computers. It may also have a software required for remote access of the CCTV system, or software that provides web access for remote viewing.

Similar to the PLC system, hardware failures in the CCTV system will prevent safe remote operation of the bridge as it could disable entire regions of the CCTV system from being observed. If the Operator is unable to observe the conditions of the site, it can be problematic especially if this is an area of critical interest, such as the waterway, roadway, or track level. Furthermore, they would no longer meet the USCG requirements for remote operation.

The loss of any region of the CCTV system, or even the lack of certain areas having coverage, can also result in the Operator being unable to security of the site. One particular example is the live railway track death in London Bridge Station in the United Kingdom in March 2020. While not a CCTV system (nor even movable bridge) failure in particular, this has resulted in scrutiny of the CCTV system, as there were not any cameras that had coverage of where the accident occurred (Chantler-Hicks, 2023). Blind spots on bridges can result in accidental injuries of pedestrians or damages to vehicles and boats when operating. Adequate and reliable CCTV surveillance can ensure that conditions are safe, and no one is in danger.

In these particular examples, redundant cameras that each face the same area of interest can resolve any single failed camera. Furthermore, point-tilt-zoom (PTZ) cameras can allow for a wider field of view from each camera, preventing the Operator from losing view of any areas of interest. An added benefit of these two solutions is that this would allow for a longer repair period, as there is no loss of coverage. An additional measure of safety is creating different view profiles, which can be triggered automatically should one camera fail, or from within the software. This would then ease the burden of the Operator needing to adjust cameras while an operation is pending.

While hardware failure in the CCTV system is a potential hindrance to a safe operation of remotely operated bridges, software failure is less of a concern when it comes to the CCTV cameras themselves. Most times, the issue is related to image processing, such as inability to display color images or turn off night vision mode. Image processing issues arise from environmental and site conditions, for example, incorrect placement that results in insufficient lighting for the camera to properly adjust. CCTV software is historically dependable and may only occasionally suffer from update related issues.

Any potential software complications can commonly be resolved by reviewing the operation and maintenance (O&M) manual, which provides information on the cameras and their settings. Should any issue with image processing be the result of camera software, the O&M manual would indicate what settings to adjust.

PA System

The last of the major control subsystems, the public announcement system is what allows the Operator to communicate with anyone present at the remotely operated bridge. The public announcement system typically consists of the intercom system and the marine radio. The goal of this system is to ensure safe passage of marine vehicles and protect the moving public.

The intercom system is primarily for pedestrian and vehicular bridges, as it commonly has external speakers aimed at oncoming traffic to keep them informed. Speakers are also provided under the bridge to announce information to any marine traffic that may be present. Other common equipment includes a desk mounted station capable of making announcements, wall stations positioned throughout for the traveling public to utilize, and a system controller. At least one method of remotely communicating with the intercom system is through a dedicated phone line linked between the system controller and a remote telephone unit. Dialing in this manner allows the Operator to remotely make announcements.

For all bridges however, the marine radio is the most important part of the public announcement system. This allows any nearby boat to contact the Operator directly, and vice versa. It is commonly stationed at the bridge itself near the local control console and may require a network device that converts the VHF signal to a network protocol signal transmitted to the remote operation location.

Hardware failure would be the most common issue for the public announcement system. However, while it may not necessarily disable remote operation, operating with a failed public announcement system increases operating risks. The failure of intercom speakers would hinder the ability to make emergency announcements when needed, and the failure of a marine radio would prevent boats from being able to contact the Operator. This is a striking example given the recent collapse of the Baltimore Key Bridge and the death of workers present on the bridge. While not a movable bridge, if intercom speakers were present, it might have been able to alert the workers and save their lives.

Intercom speakers are typically loud enough that redundant speakers may not be necessary. Providing additional speakers while strategically spreading them out would avoid loss of coverage from one speaker failure. In the event there is an emergency, and the intercom system has failed, having a system in place where the State Emergency Manager can send phone alerts can ensure the public is adequately warned.

For bridges where intercoms may not be necessary, such as railroad bridges with minimal pedestrian activity, an alternative public announcement system can be considered. In the Union Pacific Railroad (UPRR) Angleton and UPRR Freeport rehabilitation projects, speakers will be added to play pre-recorded audio messages that announce information, such as “bridge lowering” and “bridge raising.” Additionally, warning beacons are to be installed to provide visual indicators to boats of the operation, should they be unable to hear the messages.

Signs can also be installed with important phone numbers (preferably a general hotline) to provide a means for the public to contact the Operator in the event the intercom wall stations on a bridge are not operational. This provides a back-up method where anyone with a cellphone can contact the Operator regarding any bridge issues. Furthermore, providing signs on the piers and waterway (with phone numbers for operations only) can allow boats to reach the Operator if the marine radio is malfunctioning.

This was also solution included in both Angleton and Freeport; however, phone numbers were only included for Angleton.

Bridge Conditions

The control system is not the only point of concern when it comes to remote operation. The bridge itself can impact the design of remote operation systems and their risk management. The usage of the movable bridge can create problems, but the type of bridge also adds additional possible complications.

Most movable bridges are used for rail, vehicular, and pedestrian traffic, either exclusively or as a combination. Each will have their own unique requirements and follow separate standards. This is the case with rail bridges following the American Railway Engineering and Maintenance-of-Way Association (AREMA) standards over the American Association of State Highway and Transportation Officials (AASHTO) standards which is used for roadway and pedestrian bridges.

With rail bridges, a common concern is ensuring that USCG requirements on “unreasonable delays” are met with all operations. This could become a significant issue for remote operation should the bridge become stuck, whether through operation or loss of communication, and there is no on-site staff to remedy the issue. Revenue for railroads comes from trains operating, so any delays resulting from operation failures can result in loss of revenue.

With vehicular and/or pedestrian bridges, the concern of delays to the public from bridge operational issues is less of a concern. But there is potential for delays to emergency services, where the fire department, ambulances, or police would be unable to respond to emergencies because a bridge in their path is inoperable. But delays can also occur from other external factors, such as vehicles getting stuck on the bridge or pedestrians refusing to leave.

For a mixed use rail/pedestrian bridge, pedestrians refusing to leave could be an absolutely worst case scenario. Most rail properties have strict access requirements on their tracks and their own police force. But this does not prevent pedestrians from finding their way onto a rail bridge or resolve concerns where a pedestrian pathway is present on a rail bridge. In the event a pedestrian refuses to leave for an operation while no staff is present to assist in removing them and railroad police are not nearby, this could cause unreasonable delays to the marine traffic, resulting in fines from the USCG. But rail bridges are not the only possible targets of trespassers. There have been several instances, particularly in Chicago, where trespassers climb movable bridges for no apparent reason other than to create viral social media videos (Rosenberg-Douglas, 2020).

The best solution for avoiding bridge related issues is advanced preparation, whether that is during the design or prior to operations. One of the best practices is to establish a pre-check/pre-operation routine to avoid operational hiccups. This can help avoid delays, as if there is an issue prior to a planned operation, maintenance personnel can rush to the bridge and operate locally.

Additionally, establishing protocols for operation requests can ensure bridges are functioning when needed. The City of Milwaukee, which has several remotely operated bridges, has an operation checklist which requires that boats provide a minimum of two hour notice. This can allow Operators to observe the bridges well before an operation is required and resolve any potential issues. Similarly, it can provide

notice to pedestrians on the bridge and, should they not follow instructions, can provide enough time to contact local authorities to assist in clearing the bridge for operation. This preparation can then mitigate future incidents with pedestrians.

The different types of movable bridges can also have complications in remote operation. The most common movable bridges are the vertical lift, bascule, and swing type. Each bridge will usually have over-travel and/or fully seated limit switches interlocked with operation to avoid possible infrastructure damage. Over-travel, where the bridge exceeds its operating distance, is a significant concern as this could make the bridge get stuck, or worse, cause infrastructure damage. As mentioned previously, failure of the fully seated limit switches could allow the span locks to be driven when they are not aligned, which can cause infrastructure and span lock damage.

Vertical lift bridges will often also have the concern of skew control. With vertical lift bridges, more commonly for tower drive design, there is the potential for the bridge to go into skew, where the span goes out of level. This can result in the bridge getting stuck in its guides and cause damage. This is a particularly common issue at the Fore River Bridge (see Photo 01), where the span has recurring issues of the span getting stuck during operation. Back in 2020, it was confirmed that the bridge went into skew by a miniscule 2 feet, getting stuck and creating a significant traffic jam (Trufant, 2020).

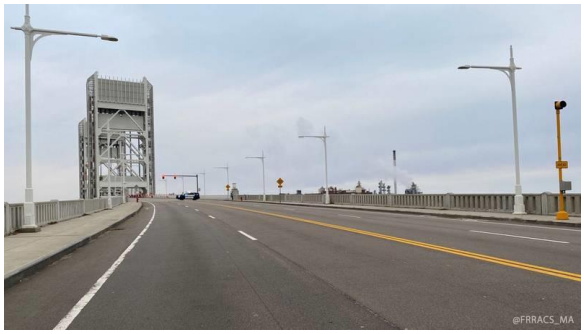

Photo 01: Fore River Bridge Closed After Getting Stuck (Boston 25 News Staff, 2022)

Concerns related to bridge type can often be remedied with additional hardware or software. Regarding tower driven vertical lifts, the PLC will continuously check span height on each side to avoid the bridge going out of level. But the program will depend on the accuracy of the equipment measuring height. Gareth Rees, P.E., provides a compelling recommendation of skew control in his technical paper, for utilizing direct skew indication (Rees, 2021). The use of components such as potentiometers, laser sensors, and inclinometers can give accurate indication of the height of the span, which allows skew calculations to be consistent, allows for independent components on each side and not require a combined source of skew control, such as synchro-tie motors. These recommendations are excellent design elements to consider for future remote bridges requiring skew control. In addition, redundancy through backup components or multiple different measurement devices can provide reassurance of skew calculations.

This course of action also extends to other bridge types as well. Regarding fully seated or overtravel issues, additional methods of monitoring (rotary cams, proximity switches, plunger switches, U-5 switches for rail bridges, etc.) can provide the controller with several confirmations to ensure bridge conditions are accurate. One example to consider is equipment for bascule bridges, where two limit switches can be provided for fully seated and overtravel on each side, for a total of eight switches on the bridge. This would be in addition to any rotary cam contacts monitoring the same conditions. An additional benefit of the PLC system would be the capability of monitoring limit switches, where it can compare the limit switch signals to the position it is supposed to be. In the event the bridge is confirmed to be in the fully seated state by other source, but one fully seated switch does not report its status, the PLC can create an alert indicating the malfunctioning switch.

Site Conditions

The surrounding area of the bridge, commonly referred to as the site, can have implications on remote operation as well. Some examples include the waterway, the bridge houses and any other accessible areas. Operators typically have the CCTV system accessible in the remote location to view the site at all times. When they receive a request for an opening, they will have to observe the site and ensure everything is in acceptable condition for an operation.

Photo 02: Boat Collision with Drawbridge (Yachts International, 2018)

The greatest concern related to waterways are boats, in particular, boat collisions. While some collisions may be spontaneous, boat operators will know well in advance if their boat has become unresponsive. The recent deadly collapse of the Baltimore Key Bridge once again serves as a warning of damage collisions can cause despite not being a movable bridge. However, collisions with the movable span is also a concern, though only occurs occasionally, as did in South Florida in 2014 (see Photo 02) (Yachts International, 2018). Boat detection systems can assist in avoiding similar collisions during operations.

Boat detection systems have become a common practice for movable bridges but is also a necessary solution for remotely operated bridges. There are several different technologies that can be used in boat detection, such as light detection and ranging (LiDAR), laser detection and ranging (LADAR), infrared, and microwave. However, the system detection implementation is typically either a curtain detection or signal reflection. Curtain detection is where a transmitter sends an electromagnetic signal (commonly infrared) to a receiver and any passing object will interrupt that signal which triggers an alarm. Signal reflection is where the transmitter and receiver are in one unit and constantly transmitting outward in a coverage area and should expect no reflection, similar to sonar. If an object enters that coverage area, the signal, which can be light, laser, or microwave, will reflect and return to the receiver, triggering an alarm.

Boat detection systems are able to immediately inform the Operator of any boats near the bridge and alert them to gain their attention. The Operator is then able to view them on the CCTV system and can contact boat operators if necessary. In addition to alerting the Operator of any nearby boats, they are also commonly used to monitor their position during operations. The UPRR Freeport project will include a boat detection system, primarily using microwave sensors with an additional LiDAR sensor as part of its remote operation upgrade. The boat detection system is a safety interlock mechanism in the control system, preventing the bridge from lowering while a boat is detected and halting lowering and raising if a boat is suddenly detected.

Fire safety is necessary to maintain the integrity of the site. There is commonly a fire detection system installed on bridges to detect smoke and heat. This is important as there is a plethora of sources on bridges that can cause a fire. Apart from physical damage to the structures present on the bridge, fires can destroy much of the equipment and personal belongings. One possible cause of fire is friction from the bridge

machinery, such as a brake not releasing properly and causing heat buildup on the shaft. Another cause can be short circuits in which the protective devices do not trip. The failure of any fire safety device, such as heat and smoke detectors, can have devastating consequences.

Overall security of the site is also of the utmost importance. Typically, a security alarm system is provided, which has door and window contacts to monitor the status of each entrance and exit of the accessible areas. In bridges where pedestrians can freely roam, there is the potential for trespassers to gain access to certain areas. This is less of an issue when the bridge is manned but is a serious security concern for remotely operated bridges. A few examples include an intruder being able to gain access to the room which houses the control system and operate the bridge, or worse a sophisticated hacker accessing the bridge control system in the same manner and being to remotely operate it. Another serious concern is accessibility to the machinery and ability to adjust equipment, such as the adjustment of hydraulic brakes, which can cause issues during operation. A small act of vandalism can impact remote operation, such as defacement of CCTV cameras or disabling of power equipment. Failure of any contacts allows intruders to go undetected and poses a potential window for unauthorized access.

Redundancy in the fire and security alarm systems can ensure that any sensor failure does not inhibit the systems detection capabilities. This can also assist in determining if any alerts are the result of sensors nuisance tripping, before setting off any alarms. Some panels may be capable of this but connecting sensors directly to the PLC and having self-checking logic (as simple as redundant sensors in series) can alert the Operator of nuisance tripping rather than setting off the alarms. Having additional CCTV cameras in locations monitored by the fire and security alarm system, such as the machinery room, control house, and other accessible areas, can allow the Operator to visually confirm any alarms. Periodic checking of these locations through the CCTV can ensure issues are not being missed by the systems and can also catch any vandalism that may have occurred.

Environment

A long-term problem for remotely operated bridges is environmental issues. A majority of movable bridges are located near bodies of water, which provides a level of moisture that most equipment is not designed around. The damaging result of this is corrosion (see Photo 03), which can result in equipment damage and eventually equipment failure. This can be a concern for equipment on remotely operated bridges where an on-site presence is not available to monitor equipment regularly. If there are any particular locations being subjected to more moisture and/or developing corrosion more than usual, it may be months before someone is able to inspect it and by then significant damage can be done.

Photo 03: Corrosion on Rotary Cam Housing (Personal Photo)

Photo 04: Interior of Housing Showing No Corrosion on Rotary Cam (Personal Photo)

Specifying equipment to be rated for these conditions can often mitigate these concerns. NEMA 4X and its IP equivalents should be the minimum rating for all exterior equipment, to not only protect against intrusion of the elements but also protect against corrosion (see Photo 04). Ideally all internal equipment would also be rated NEMA 4X if applicable to avoid equipment issues should the enclosures fail. In the case of Photos 03 and 04, the enclosure had an extensive lifetime since its installation and despite developing corrosion on the exterior, it protected the interior rotary cam well.

Seasonal conditions can also impact operational aspects of the remotely operated movable bridge. Weather such as heavy rain or snow during cooler months can affect the visibility of CCTV cameras. Without clear visibility of the site's conditions, the Operator may be unable to remotely operate the movable bridge. The frigid winter that some bridges are subject to can often have sub-zero temperatures. Most control equipment is typically not rated for temperatures that low, and just normal operation of the equipment can result in condensation build-up, which can result in water damage to equipment or in a worst case scenario, unexpected electrical shorts. Electrical shorts can often result to damaged I/O module points as discussed in the PLC section.

Conversely, the warmer months will often have rapidly fluctuating temperature changes until the summer, where some bridges can experience 100°F or higher. The quick temperature change can often cause thermal stress on sensitive electronics, but high temperatures can overheat equipment. Should any critical electrical equipment overheat, they would go offline until temperatures lower. However, in remotely operated bridges, this may not be possible for equipment housed in particular cabinets that would need to be opened for ventilation.

Additionally, the warmer months introduce factors that are not often considered when designing movable bridges, such as the biodiversity of the site. Insects are a common occurrence for movable bridges in general, but their presence can hinder remotely operated bridges. Capable of landing on CCTV camera lenses, insects can then block the camera's field of view. While a local Operator would be able to visually verify the site conditions, a remote Operator that relies solely on the CCTV system to verify site conditions may be unable to operate safely.

Most of these concerns can be resolved by specifying equipment to be rated for the temperature and environment of where they will be located. Projects in regions where temperatures vary widely should opt for devices that can operate in the standard industrial operating range -40°F to 122°F. Any enclosures and/or equipment with active electronics should include fans/air conditioners and heaters. This may require that those devices be housed in different rated enclosures, such as NEMA 3RX which maintains corrosion resistance while allowing ventilation. Fans and or air conditioners will prevent equipment from overheating in the hotter periods of the year, while heaters will prevent the build-up of condensation.

CCTV cameras themselves can be considered enclosures and should be treated as such. Many manufacturers include the option of having cameras be NEMA 4X rated and include internal heaters.

These will prevent corrosion from developing and will also prevent internal condensation build-up. CCTV cameras can also be provided with external wipers. For remotely operated bridges, this can allow the Operator to ensure the cameras lenses are always clear, either by wiping off any insects or repelling heavy rain and snow.

A separate weather condition that commonly occurs and can be year round is strong winds. It is commonly recommended that bridges do not operate during strong wind conditions, as they may not have been designed to operate against that level of loading. This can be a concern for remotely operated bridges where the Operator may not know the wind conditions of the bridge they are operating. A common solution to this is the inclusion of an anemometer for bridges to monitor the wind speed and direction. The anemometer can be integrated to the bridge control system, which will stop the Operator from accidentally operating during strong winds if they did not know of the site's wind conditions.

For most the above, periodic and frequent visual inspection not related to routine bridge inspections will also prevent issues from developing over time. If there are already issues, this will allow for maintenance to be scheduled as soon as possible.

Power Source

All bridges will have a power distribution system fed by an incoming utility service and commonly backed-up by a standby generator. Various equipment comprises the system, including transfer switches, panelboards, and transformers. The utility voltage is stepped down to 120VAC to be utilized by the control system and other line voltage equipment. A grounding and lightning protection system is also provided to protect the equipment and the bridge.

Power related issues are mostly the result of power source quality. Not often a concern in the United States, some electrical power grids can be "dirty." These power grids generate power that can have voltage spikes, frequency variations, or phase imbalance, which can also cause brownouts, where voltage drops below stable values. Issues elsewhere on the utility feed can result in outages, as well as the potential for surges from lightning strikes or the utility itself. A different power concern is also noise and harmonics, where interference can generate frequency issues and impact electronics.

These power concerns have significant risks for the PLC system which remotely operated bridges rely on. The PLC equipment will have electrical operating ranges of ±10% voltage and frequency. When brownouts occur in the power feed, PLC equipment can suddenly shutdown as the incoming power falls below the operating range. If there are electrical surges, it could expose sensitive electronics to large voltages which could destroy them. Lastly, the presence of noise and harmonics on the line, which can be formed from operation of motors, can have the PLC generating false signals or operate incorrectly.

"Dirty" power issues can simply be resolved with power conditioners. These devices will take incoming power and filter out spikes and noise to deliver stable power to electrical equipment. The addition of surge protective devices (SPD) can protect downstream equipment by driving large voltage spikes to ground. Line filters are also commonly used for systems using electronics, as they filter much of the noise that comes from electromagnetic interference (EMI) and radio frequency interference (RFI).

An overall solution is the inclusion of uninterruptable power supplies (UPS) for the critical electronic systems such as PLC, CCTV, fire alarm, and security systems. UPS's can typically include power conditioners, SPDs, and line filters as part of its internal power circuitry. They are also capable of providing battery back-up to equipment, which makes them an all-in-one protective device. This can assist in ensuring the control system is not affected by power issues.

Networking

The importance of networking cannot be understated for remote operation. The network-based equipment operates simultaneously to interconnect the bridge, the remote operator, the boat requesting a lift, and the traveling public if needed. The method by which they are connected, the cabling used, and even the method used by the PLC system for remote communication can vary and impact remote operation. Lastly, cybersecurity is a rising concern which can impact the security of remote operation functionality.

The PLC, the CCTV, and the PA system are all networked to allow remote operation functionality. Equipment will either utilize ethernet or fiber optic cable to interconnect them with network switches. Their connections can often be made in different topologies, such as ring or star, but the biggest concern is often dropped connections to the network switch or to any device in the networked system. Any module within the PLC system that loses communication can result in the PLC being unable to operate as it does not know the status of the bridge. If the CCTV cameras lose connection, it can prevent the Operator from viewing certain areas or if the CCTV cabinet loses connection, the Operator may be completely unable to access the system. The PA system losing connection would prevent the Operator from communicating with the traffic and being unable to warn of any emergencies.

As mentioned in the PLC system section, redundant network loops can mitigate dropped network connections. Once the loss of one connection is noticed, the redundant connection would allow the bridge control system to continue operating. Redundant network switches would also prevent operation failures if any network switches malfunction. If network connection drops frequently occur, periodic inspection can determine if it is a cable or connection point issue. Including sufficient spare network cables during installation makes it easy to replace failed cables and avoid the need for pulling new cables.

Concerns of the bridge's remote operation itself will depend on how the PLC is connected to the remote location. It is possible to connect the bridge PLC to the remote PLC through the internet, with the use of virtual private networks (VPN) or dedicated internet protocol (IP) addresses. It is also possible to connect it via a dedicated communication line, such as a direct fiber connection between locations, or hardwired signals, such as individual signals for each bridge control function. UPRR Angleton and UPRR Freeport are examples of hardwired signals, where the railroad signal system is integrated to the control system for remote operation of the bridges.

Each have their own cons in usability but also flaws for security. Internet connection allows remote operation from anywhere that has internet access. However, this method could expose the IP address of the PLC controller. Through advanced methods, it is possible for the controlled to be accessed by a hacker with the IP address and port scanning. Dedicated communication lines allow for a midrange distance but have the cost factor of needing fiber installations, while hardwired signals are for bridges controlled from offices near bridges that may not have bridge houses. The security flaw for these direct connections would be the potential to tap into the connection at a midpoint and access the device.

Regarding the remote connection methods, there are specific solutions to prevent unintended access. When it comes to internet-based remote operation, stronger firewalls can ensure only the intended users can access the control system. For systems where dedicated communication lines or hardwired signals are used, hardware and software based solutions may be necessary. To avoid any unintended access on dedicated communication lines, a logic-based "handshake" may be used where the local and remote PLC confirm their unique information prior to beginning any operations. All communication between the local and remote PLC should be encrypted as well, to ensure a secure data line and to prevent any snooping by potential hackers to duplicate the proposed "handshake."

Hardwired signals are a more complex issue, as just generating a signal on the line can often trigger the necessary circuits. Hardwired signals are more common on railroad bridges, as they often make use of the railroad signals system already in place. One possible solution is to have control equipment on both sides send a unique digital signal pulse on the wire, which is verified to ensure the signal is authentic and not noise or someone attempting to access it. Another solution to this situation is having the permissive signal in separate conduits from the remote operation signals. In this manner, if a hacker is able to access a junction box containing the remote operation signal wires, they will still be unable to operate the bridge. To avoid access to signal wires, all terminations should be located at facilities that are secured and monitored and all conduit runs should be direct buried in between.

However, the most dangerous issue is cybersecurity as any flaw can result in the operation of the movable bridge by unauthorized individuals. One particular cybersecurity issue that impacts almost all computers is security vulnerabilities. This could be the result of flaws found in internal components or software, but the potential of compromising the system remains. However, it is not just a possibility, as vulnerabilities have been found and exploited in Schneider PLCs in the past, with particular emphasis on how it could impact not only bridges, but other infrastructure such as solar parks, hydropower plants, and airports (WAQAS, 2023).

One possible scenario is an individual with malicious intent (a hacker, or a disgruntled employee) finding a way to access the local network (either through poor security or social engineering) of the bridge control system. While there may be security measures that prevent the individual from physically accessing the bridge controls, there may be cybersecurity exploits that allow them access through software. If these exploits remain unpatched, the individual may gain access to the remote operation capabilities of the bridge. In locally operated bridges, this is not a concern, as the bridge is only controlled by local methods. But when the system is remotely operated this, and other "cyber-attacks" are possible.

For vulnerabilities, it is important to follow the manufacturer recommendations on updates for all network connected devices. This may range from periodic software updates to the need for hardware replacement. The importance of site security cannot be understated, as the local network connection may be the easiest point for a hacker to access the system. This can include directly connecting to the internal network of the control system or even accessing it remotely through any vulnerabilities. But hackers are beginning to get access through other means, such as staff themselves.

Social engineering is a new method used by hackers, which can result in bridge staff themselves providing the hacker with the information needed. Hackers often spoof email addresses and contact employees to gather information or access their accounts through infected links. It is important to train

staff on the various methods of social engineering, so they do not unknowingly provide intruders with sensitive information.

Another potential attack includes distributed denial of service (DDoS). In this instance, the network of the bridge control system is overloaded by repeated access attempts from external sources. It is unlikely that malicious control of the bridge can occur from a DDoS attack, but it has the potential of disabling remote operation by preventing actual Operators from accessing the bridge control system. A stronger network detection system can this kind of web-based attack. The most applicable protection method for a movable bridge system is rate limiting, where the volume of network traffic is restricted from specific IP addresses. This mainly applies to bridges that have an internet connection and may need coordination with the ISP but can prevent any potential targeted DDoS attack.

Brute force attacks are also a possibility, in which hackers use continual guesses at passwords to gain access to a system. There are several different parts of a networked system a hacker could use to gain access. If there is a Wi-Fi network at the bridge, the hacker can use password cracking tools to determine the password and gain access to the Wi-Fi, which is often a weaker part of any networked system. Another option includes attempting to login to the network servers of the bridge control system using standard accounts such as “admin” or “root.” This biggest culprit in these kind of attacks is password security, as often the root control accounts are left with the default passwords, and this can make brute force attacks much easier. As bothersome as it may be, strict passwords policies with frequent change and minimum character requirements can mitigate this issue. This ensures that any leaked passwords available on the “dark” web are not usable, and no standard accounts have default passwords. Similarly, instituting a maximum number of attempts at logging in prior to a system lock can prevent most brute force attacks.

As mentioned in the AASHTO Guidelines for the Operation of Movable Bridges from a Remote Location, the goals of these attacks can vary. The intention could be to operate the bridge and cause infrastructure damage, or to obtain useful data for future use through data exfiltration (Moses, 2020). Some could be after money and will attempt to install ransomware to disable operation until they are paid. The potential for malicious use of the CCTV or intercom system is also a possibility. At a larger scale, it may be prudent for a nationwide campaign to test the networks of remotely operated movable bridges. A cybersecurity firm can be commissioned to not only investigate the vulnerabilities in these systems, but also stress test them and determine which attacks it is susceptible.

Obsolescence

Despite all other issues for components, the only issue that cannot be prevented is obsolescence. Like technology, companies continue to progress and advance their products. This will lead to new and improved equipment but will eventually results in discontinuation of existing products. While companies often retain a reserve of the product, once that reserve is exhausted there will be no manner to obtain it.

Additionally, obsolescence can result from companies going out of business or being acquired. With this, the knowledge of the products also disappear with the company. While acquisitions often provide a lifeline to companies, they may also be bought solely to remove competitors. This is a growing concern, given the recent trend of acquisitions resulting in consolidation in the electrical industry.

This is a possibility that can impact all equipment, but most can usually be replaced with a similar product without issue. However, many PLC components are proprietary, and their use is programmed into the system. Changing products may require an updated PLC code, but then even the programming software itself can become obsolete or discontinued. Worse, it may be required to update to newer programs or devices because security flaws are discovered that need patching. While using out-of-date software may work for the IRS (Jones, 2023), security flaws for movable bridges are too great of a risk.

There are limited solutions to obsolescence of bridge equipment. The most common practice is the stockpile of spare equipment. AASHTO and AREMA both offer a list of spare parts for the control system, but it is typically up to the contract specifications to determine a full list. It may be time for an updated spare parts section in AASHTO and AREMA, which not only accounts for spares of all subsystems, but also accounts for quantities with obsolescence in mind.

Product support is commonly 20 years with frequently used bridge electrical equipment. Manufacturers typically announce when their products are being discontinued, and a good course of action is to purchase replacements at this point. A possible plan of action could be record keeping of part failure and replacement. This historical record can then be used to purchase a quantity of spares based on the failure rate, as well as the anticipated remaining life of the bridge prior to the next rehabilitation.

As stated in the PLC System section, frequent backups of software can avoid obsolescence from company shutdowns, or their decision to completely erase products. A common occurrence in the digital market is the sudden decision to outright remove media or access to software, even if customers purchased it. This does not seem likely to impact software utilized by movable bridge control systems, but it remains a possibility, nonetheless.

Cost

Lastly, the issue most remote operation projects will have concerns about is cost. The solutions that are presented can add significant expense to any project, with some likely doubling the cost of an electrical system. A great analogy is the adage that building the safest car would be too expensive for most consumers, the best protected remote operation system would be too expensive as well.

However, in the case of remotely operated bridges, the long-term benefits can greatly outweigh the short-term cost, and is often the reason remote operation is considered in the first place. All manned locally operated bridges would need one Operator each, often in addition to a group of maintenance personnel that can go to any bridge as needed. Having bridges be remotely operated can reduce the staff necessary for the operation and upkeep of multiple bridges.

For certain organizations that are in charge of multiple bridges that are nearby to each other, fewer Operators can be designated to control multiple bridges from a central location. A project that exemplifies this is the Joliet Automation Project, where six nearby bascule bridges maintained by the Illinois Department of Transportation (DOT) are automated and controlled from an office in Joliet. In this instance, it is planned for three Operators to control two bridges each, which would half the number of Operators required.

Railroads also have the ability of using dispatchers to also operate the bridges. This can also simplify communication with the bridge, as the dispatcher can provide the bridge permissive when needed to operate the bridge, rather than communicating with an Operator. UPRR Angleton and UPRR Freeport are railroad bridges in which the dispatcher operates the bridge. Both also highlight the possible distances that can be achieved with remote operation, as Freeport will be operated remotely from the Freeport Yard Office Building located less than a mile away from the bridge, while Angleton will be operated from Spring, Texas, approximately 60 miles from the bridge.

Similar to railroads, less frequently used bridges or those located in remote areas often have a local maintenance personnel that operates the bridge as needed. Remotely operated bridges would allow this individual to operate the bridges from their main station, rather than having to physically get to the remotely located bridges. This can often save significantly on both travel time and maintenance time, as the individual can often determine if maintenance is required from what is reported by the PLC remotely.

As indicated in almost all previous sections, the main solutions are often redundancy or the use of additional products and methods. It is often not economically feasible to purchase four or even two of a product just to avoid hiccups. In cases where redundancy or backup methods are desired, the best solution is to do an analysis of the components used for the system. The following factors can be considered:

- What parts are critical?
- What parts are inexpensive?
- What parts are likely to fail?
- What parts are likely to be discontinued?
- What parts can be replaced with alternatives without compromise?

Ultimately, this can limit the redundancies or backups that would need to be included in the design. This can greatly reduce the short-term cost, while also providing a better and secured system. This practice may also be worthwhile in updating the spares parts list of the AASHTO and AREMA guidelines.

The Future of the Industry

Regardless of any potential problems, it is obvious that remote operation is a likely future for the industry. However, there are new and emerging technologies that can not only improve many aspects of remote operation, but movable bridges overall. Similarly, there are technologies which are in their infancy currently, but already show promise for future use. Discussion of these technologies now, can allow for adequate planning of implementation in the future.

Augmented and Virtual Reality

Augmented reality (AR) and virtual reality (VR) are a pair of technologies that have been available for decades but have only recently gained commercial acceptance. There are “smart” glasses available that offer basic AR features, such as showing a 3D directional arrows on the glasses to guide you when using a GPS-based application. There are also VR headsets that allow the user to enter virtual spaces, such as video games, and interact with the items in the game using physical actions. These devices can have significant impact on movable bridges in general, specifically operator training.

One of the complaints heard often regarding operator training is its stale delivery. Content is commonly delivered in a lecture prior to actual testing, in which many participants may grow weary of only

listening. Many people are also visual learners versus auditory learners, which can result in Operators not retaining information. AR provides the opportunity to augment what is observed by the Operator with information on a screen. Rather than discuss the many bypasses and sequence of operation on paper, this information can be presented on glasses while the Operator is looking at the console itself. This can be a long-term benefit, as the software could be retained and used for training new Operators long after the initial training done during commissioning. It can even provide Operators with refreshers or can remind them of which button should be pressed next if they make a mistake.

The display of information on screen can provide immeasurable benefits during maintenance as well. In a programmed "smart" glasses, the Operator can look at a particular component and the glasses would pull up the cutsheets or relevant plans, which can speed up maintenance (see Photo 05). This feature has found application not only in the manufacturing industry, but also in the medical and space fields. With this, the Operator can have the schematics of all the bridges maintained and display the plans on the glasses.

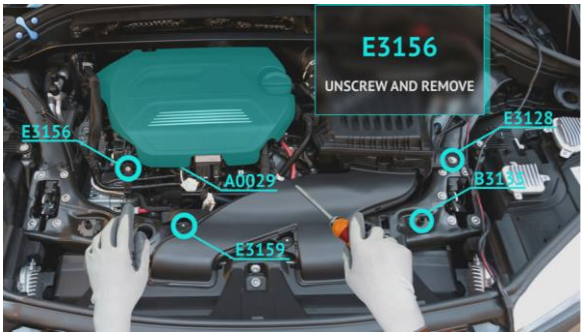

Photo 05: Example of AR Glasses Displaying Information of Components (Dhawan, 2021)

Virtual reality could also be suited for more generic training purposes. Similar to the 3D environment utilized in the National Highway Institute (NHI) Tunnel Safety Inspection, a 3D model of control consoles and bridges can be created for training. With a VR headset, Operators would be able to practice operation of bridges without concern of making mistakes. This can also be beneficial in showing the impacts that dangerous conditions can have, such as bridges going into skew or failure of deceleration. Like the NHI tunnel simulated inspection, bridges can have a simulated inspection environment where Operators can observe issues visually. These types of training can help individuals that are kinesthetic learners.


Photo 06: Example of VR Glasses Used for Remote Operation (Wingrove, 2022)

But one use case in particular has the potential to add a more realistic feel to remote operation. Through a combination of 360 degree cameras and sophisticated programming, a system could be developed which would allow the Operator to virtually be present at the bridge while remotely operating it (see Photo 06). Any possible consideration of this technology would be in its infancy, as issues such as latency could create dangerous conditions. Even the programming considered may be too complex to create and would be more expensive than a desk setup.

Internet-of-Things and Alternatives

Internet-of-Things (IoT) refers to the practice of most, if not all, equipment being capable of connecting directly to the internet. They would be embedded with their own internal sensors and computational functionality which would allow them to directly report data to a central location. There is potential for certain devices to become IoT based, but the application has already entered the movable bridge industry,

as SMART overloads can be considered a simple IoT device. Rather than motors having their own independent computer, the SMART overload that provides it power can monitor it and its external sensors, which then returns data to the PLC. It is also capable of doing calculations on its own, which allows it to plot trends and provide information for optimization. This data can then be sent to remote locations, which provides remote monitoring capabilities.

IoT may not find its way to equipment commonly used in movable bridges (it would not make logical sense to add internet functionality to mechanical limit switches, for instance), but SMART relays provide an excellent compromise in this application. These are often referred to as micro-PLCs, as they offer some level of computational capability and are relatively inexpensive. While not likely practical, a SMART relay could be added to many components to then self-monitor. Using the limit switch as an example, one possible application is the periodic testing while not in use through continuity. This would limit wires signals needed by the PLC but allow monitoring of the equipment. Should the limit switch fail testing, the SMART relay can alert the Operator for maintenance.

Artificial Intelligence

Artificial intelligence (AI) is becoming the newest buzz-word in many industries. Companies are rushing to introduce AI features to their products (even if most features were already neural network based), and this includes PLC manufacturers. Frost & Sullivan, in collaboration with Siemens, published a white paper in which the potential applications of AI in manufacturing are discussed (Sundaram & Natarajan, 2018).

AI can be considered technology that allows computers to simulate human intelligence. This commonly includes machine learning, where data is used to improve AI accuracy through deep learning. Deep learning then refers to the simulation of decision-making through neural networks. Lastly, neural networks refers to a computational model that mimics biological neurons for its decisions. As mentioned above, the concept is not new, as many technologies of the past have already utilized neural networks to improve their functionality (such as computer graphics processing).

Artificial intelligence has issues in itself that will need to be resolved in the coming years, including ethical, security, liability, accountability and access implications, however the possibilities in the movable bridge industry warrant discussion. Karthik Sundaram and Nandini Narajan mention several key features which can drastically impact the movable bridge industry and remote operation:

- Object tracking and anomaly detection.
- Usage analytics predicative maintenance
- Collision prevention and mitigation
- Interactive voice response system
- Autonomous operation

As PLCs begin implementing AI/machine learning features, there is the potential for improvements in many aspects of the movable bridge control system, as well as new optional features.

Photo 07: Example of Object Tracking Utilized for Pedestrian Detection (Boesch, n.d.)

Object tracking will allow the PLC to detect pedestrians and vehicles and process the data to determine traffic loads at various times of day (see Photo 07). This information is beneficial for creating operation request requirements, such as requiring more or less notice at certain hours of the day rather than large blocks. Object tracking would also be able to point out possible pedestrians or vehicles in blind spots the Operator may have. In the case of remote operation, where it is typically one monitor observing a small amount of the CCTV cameras, this could be beneficial. In addition to object tracking, anomaly detection can allow the system to determine if there are trespassers in certain areas or if traffic is heavier than expected and may be the result of something external.

Usage analytics predicative maintenance can provide useful information for scheduling maintenance, inspection, and procurement. If crucial equipment is performing worse than expected based on historical data, such as the main motor utilizing more current than expected, the system can create an alarm which can lead to a maintenance or special inspection. Similarly, the system can track each equipment and monitor their performance over time, and log if replacements are made. The system can use this data and indicate if a component is nearing end of useful life. This data can also be used to determine quantity of spares to purchase if the product is discontinued, as discussed in Obsolescence.

Collision prevention and mitigation is more applicable to autonomous vehicles, but its application can be used in movable bridges. In the Baltimore Key Bridge, the barge was unable to stop and collided with a fixed bridge. Had this occurred with a movable bridge, the bridge could be opened to avoid infrastructure damage and allow for further opportunity to stop the boat. Collision prevention would monitor any oncoming boats and can determine if it were in a path that would collide with the bridge. This can alert the Operator, who could take corrective action.

Collision prevention and mitigation would have been particularly beneficial in the incident where an inspected towing vessel collided with a remotely operated railroad bridge. Operator error had resulted in the bridge closing while the barge was still passing, as despite boat detection sensors indicating a boat was present, the Operator manually overrode the sensors and began lowering the bridge (USCG, 2023). In this instance, the AI of the system could have generated an alert to the Operator when they attempted to override the boat detection sensors, indicating that a boat is in fact present. The system could also determine mid-operation that a collision was imminent and stopped the bridge automatically, despite the override being provided.

Interactive voice response can automate marine radio interactions by communicating with boat operators directly. This is beneficial in the event there are no Operators available at the time, or if the time is outside of bridge operating hours. The system would be able to give a default speech to the boat operators, and potentially analyze the questions asked and provide more precise and relevant information.

The culmination of all of these technologies would then be autonomous operation. While artificial intelligence capable of actual human decision-making may be decades away, there are scenarios where it

may be acceptable for a bridge to operate autonomously with no input from an Operator. Through the use of object tracking and anomaly detection, the system could determine if the bridge can operate without human intervention. Predicative maintenance can determine if any equipment may fail during the operation, which can deter operation if no maintenance staff is available. Collision prevention would monitor the marine traffic and alert any boats that may collide through any means possible. Lastly, interactive voice response would communicate with boats that an operation can occur and go about opening the bridge.

While there are many valid concerns regarding autonomous movable bridge operations, there are use cases for it. In particular, for bridges with pedestrians and limited operations, such as railroad bridges in uninhabited areas, or during off hours, such as middle of the night with no traffic present, a bridge could potentially open by itself without issue. However, even in an ideal world, such a system would still require many operations to hone its data and ensure a minimal possibility of failure.

Conclusion

While remote operation may have concerns that can deter some from implementing it today, countless projects have proven that remote operation of movable bridges is possible. Their success showcase the possibility of the future, where multiple bridges can be controlled from a central location and lead to reduced operation and maintenance costs. With the inclusion of tested solutions, most problems that are considered become negligible and the movable bridge can be better designed and more secured. New technologies are also providing features that can greatly improve current designs and practices and reduce costs even further. Lastly, developing technologies are showcasing ideas that could one day alter the industry the same way remote operation is doing now.

Bibliography

Bhaskar, A. (2022, September 28). *How IoT Is Transforming The Manufacturing Industry.* Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2022/09/28/how-iot-is-transforming-the-manufacturing-industry/

Boesch, G. (n.d.). *Object Detection in 2024: The Definitive Guide*. Retrieved from Viso.ai: https://viso.ai/deep-learning/object-detection/

Boston 25 News Staff. (2022, May 27). *Fore River Bridge reopens after getting stuck in open position*. Retrieved from Boston 25 News: https://www.boston25news.com/news/local/fore-river-bridge-reopens-after-getting-stuck-open-position/ZJW4C73XA5ETNADPQNBC3FC35I/

Brophy, D. (2014, October 12). *The Celtic Tiger bridge that wouldn't open because of a lost remote control.* Retrieved from The Journal: https://www.thejournal.ie/sean-ocasey-bridge-remote-1713102-Oct2014/

Chantler-Hicks, L. (2023, December 13). *Calls for better CCTV at London Bridge station after man suffering mental health crisis electrocuted on train track.* Retrieved from The Standard: https://www.standard.co.uk/news/london/london-bridge-train-station-underground-tube-man-electrocuted-b1126370.html

Dhawan, H. (2021, November 12). *ENHANCING REPAIR AND MAINTENANCE WITH AUGMENTED REALITY APP DEVELOPMENT*. Retrieved from Neuronimbus: https://www.neuronimbus.com/blog/augmented-reality-in-repair-and-maintenance/

EECO. (n.d.). *Advanced Overload Relay.* Retrieved from EECO: https://eecoonline.com/inspire/get-smart-with-advanced-overload-relays

Electrical Wholesaling. (2022, June 27). *Siemens to Buy Brightly Software.* Retrieved from Electrical Wholesaling: https://www.ewweb.com/news/mergers-acquisitions/article/21245334/siemens-to-buy-brightly-software

Fade, L. (2021, December 10). *The Benefits Of Augmented Reality For Employee Training.* Retrieved from Forbes: https://www.forbes.com/sites/forbesbusinesscouncil/2021/02/12/the-benefits-of-augmented-reality-for-employee-training/

Farberov, S. (2020, August 18). *Chicago police hunt for six 'trespassers' who were seen perched on edge of bridge AFTER it was lifted up in 'reckless' video stunt.* Retrieved from Daily Mail: https://www.dailymail.co.uk/news/article-8640749/Chicago-investigating-trespassers-seen-viral-video-raised-bridge.html

IBM. (n.d.). *What is artificial intelligence (AI)?* Retrieved from IBM: https://www.ibm.com/topics/artificial-intelligence

Jones, J. H. (2023, February 15). *The IRS still runs on outdated applications and software from 1959, watchdog warns.* Retrieved from FEDSCOOP: https://fedscoop.com/watchdog-irs-outdated-software/

LTRC. (2022, February). *Skew Detection System Replacement on Vertical*. Retrieved from Louisiana Transportation Research Center: https://www.ltrc.lsu.edu/pdf/2022/capsule_22-2ST.pdf

Moses, R. S. (2020, August). *AASHTO GUIDELINES FOR THE OPERATION OF MOVABLE BRIDGES FROM REMOTE LOCATIONS.* Retrieved from https://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP20-07Task424.pdf

Rees, G. (2021, January). *Skew Detection System Replacement on Vertical Lift Bridges.* Retrieved from Louisiana Transportation Research Center: https://www.ltrc.lsu.edu/pdf/2021/FR_643.pdf

Rodewald, A. (2016, January 26). *Uncertainty for remote control bridges.* Retrieved from Green Bay Press Gazette: https://www.greenbaypressgazette.com/story/news/local/2016/01/26/uncertainty-remote-control-bridges/79295066/

Rosenberg-Douglas, K. (2020, August 19). *Viral video claims people were caught on Chicago River bridge as it was being raised. City says they actually climbed up.* Retrieved from Chicago Tribune: https://www.chicagotribune.com/2020/08/19/viral-video-claims-people-were-caught-on-chicago-river-bridge-as-it-was-being-raised-city-says-they-actually-climbed-up/

SAP. (n.d.). *What is augmented reality (AR)?* Retrieved from SAP: https://www.sap.com/products/scm/industry-4-0/what-is-augmented-reality.html#:~:text=Augmented%20reality%20definition,real%2Dlife%20environments%20and%20objects

Sundaram, K., & Natarajan, N. (2018). *Artificial Intelligence in the Shop Floor.* Santa Clara, CA: Frost & Sullivan.

The New York Times. (n.d.). *What We Know About the Francis Scott Key Bridge Collapse in Baltimore.* Retrieved from NY Times: https://www.nytimes.com/2024/03/26/us/key-bridge-collapse-baltimore-what-to-know.html

Trufant, J. (2020, February 27). *Stuck bridge snarls traffic during evening commute.* Retrieved from The Patriot Ledger: https://www.patriotledger.com/story/news/2020/02/27/stuck-bridge-snarls-traffic-during/1623777007/

USCG. (2023, April 19). *Findings of Concern - Sector Mobile.* Retrieved from United States Coast Guard Coast Guard Deputy Commandant for Operations: https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/foc/USCGFOC_012-23.pdf?ver=c7rfcXFgd0G7iDfitlJ9fg%3D%3D

USCG. (n.d.). *Coast Guard Bridge Remote/Automated Operation Request Guide.* Retrieved from United States Coast Guard Coast Guard Deputy Commandant for Operations: https://www.dco.uscg.mil/Portals/9/Remote_Operation_Request.pdf

WAQAS. (2023, February 17). *Controller-level flaws can let hackers physically damage moving bridges.* Retrieved from HACKREAD: https://hackread.com/hackers-physically-damage-moving-bridges/

Wingrove, M. (2022, May 10). *Virtual reality applied to tug training*. Retrieved from Riviera: https://www.rivieramm.com/news-content-hub/news-content-hub/virtual-reality-applied-to-tug-training-71045

Yachts International. (2018, July 28). *Drawbridge Crashes on 161-foot Trinity ROCKSTAR*. Retrieved from Yachts International: https://www.yachtsinternational.com/videos/drawbridge-crashes-on-superyacht

ZMS. (n.d.). *Corrosion in Copper and Aluminum Cables*. Retrieved from ZMS Cable: https://zmscable.es/en/corrosion-cables-cobre-aluminio/