Paper No. 43

Electrical/Electronic Components

Reliable Sensing For Heavy Moving Structures

R. Wayne McCracken, P.Eng
Byrne Engineering Inc.

HEAVY MOVABLE STRUCTURES, INC.

TENTH BIENNIAL SYMPOSIUM

OCTOBER 25 - 28, 2004
The Omni Orlando Resort at ChampionsGate

RELIABLE SENSING FOR HEAVY MOVING STRUCTURES

By:
R. Wayne McCracken
Byrne Engineering Inc.
Burlington, Ontario, Canada
905-632-8044

Introduction

Movable bridge operating reliability is extremely important. They are generally installed in locations where both marine and roadway traffic are essential for a variety of reasons, including the transportation of goods and materials and for the traveling public. Movable bridges are large and complex structures resulting in an increased probability of failures and also the magnitude of the consequences of these failures. It is therefore essential that a movable bridge be "designed for reliability".

The consequences of movable bridge failures may be categorized as follows:

- A failure may result in injuries to bridge operating personnel or to members of the public.
    - If a bridge locking mechanism were to unlock at a time when the bridge is intended to be locked, the leaf may become misaligned with the roadway causing a hazard to vehicles.
    - An unexpected motion may cause injury to bridge maintenance personnel.
- A failure could result in costly damage to the bridge structure or operating mechanisms that are essential to the bridge's motions.
    - The failure of wedges to be fully withdrawn or locked mechanisms to be in their unlocked position during the closing motions of a swing bridge is likely to cause substantial damage to these mechanisms.
    - If a bridge were to inadvertently close in the path of an oncoming ship, substantial and possibly irreparable damage could be done to ship and the bridge's structure.

- And a failure can result in significant financial loss to industry and to the traveling public as a result of delays caused by the failure.
    - Everyone is on a schedule whether it is the public traveling for business or pleasure, or the movement of goods and materials to and from industry. Significant delays will inevitably result in altered plans, missed production schedules and the like.

Operating safety and reliability requires a well-designed control system that is able to sense and prevent hazardous conditions. Safety and reliability of the operation of a movable bridge therefore requires reliable information regarding current bridge conditions and positions to base these control actions upon. This information is normally provided to the control system by sensors of various types located around the bridge.

A safe control system needs to monitor current bridge operating conditions and take appropriate control actions to ensure the following:

- Bridge opening actions must only be permitted to occur in a specific sequence and only at times when it is safe to do so. For a typical swing bridge, the following operating sequence must be carried out prior to the bridge leaf opening motion:
    - Traffic lights must sequence to red,
    - All entering and exiting traffic gates must be in their down position,
    - Traffic barriers must be in place and locked,
    - Leafs must be unlocked, and
    - Wedges (or similar devices) must be fully withdrawn.
- In addition to safe sequencing of bridge operations, the control system must also detect and prevent any unsafe actions. When unsafe conditions exist, motions that are in progress must be stopped and the bridge operator informed of the failure.
    - Many situations exist ranging from inappropriate manual override operation of any of the above devices. Appropriate responses to these conditions also vary depending on the design of the bridge.
    - Some conditions can result from mechanical failures that are not hazardous themselves but could cause mechanical damage if a motion were to continue. For example, wedges not fully withdrawn and locks not in their fully unlocked position while the bridge leaf is being closed.
- As well as control interlocks, the control system must ensure that speeds, accelerations & decelerations, and stopping motions occur at safe rates and are initiated at or before specific positions.
    - Speed, acceleration and deceleration must be kept within specified limits under normal operation, and may be required to be reduced to lower values during abnormal operating conditions.
    - Deceleration of motions must start at a position where the structure can be safely brought to rest within its permissible range of motion.

Sensors providing information to the control system can include many different types of devices. Mechanical contact limit switches and/or electronic proximity sensors are normally used to detect that the movable span or a bridge mechanism is in a specific position. Rotary encoders and other similar devices are frequently used to continuously provide information to the control system regarding the position of a physical structure or mechanism.

Control systems can generally be made quite reliable by using standard "good design practices". Well-designed PLC software can easily provide a variety of system safety checks during all bridge motions and the health of a PLC can be monitored by a "watchdog timer" or other standard methods. Hardwired relay logic, while simple and robust, is generally not capable of the variety of techniques that can be used to improve safety and that can be easily employed with a PLC based control system.

While PLC controllers and other control system hardware can usually be located where it is protected from the environment and physical "wear and tear", and can be protected from other hazards such as power line transients by standard and well-known techniques. Limit switches, proximity switches, rotary encoders and similar field sensors are difficult to protect and are usually exposed to the rigors of the environment.

In industrial applications, sensors are often located indoors in conditions that reduce their likelihood of failure. Sensors on movable bridges are however usually located out in the "real world" and are subject to a variety of hazards to their continued proper operation.

- Mechanical limit switches:
  - Can seize due to corrosion preventing the operating arm from spring returning to its unoperated position. This condition will cause the switch contacts to remain in their operated condition and provide erroneous information to the bridge control system.
  - In addition, a limit switch's operating shaft may jam, causing the operating arm to break or fail to operate, or the operating arm may become loose and simply fall off. As above, this will provide an incorrect indication of the bridge's condition to the control system.
  - Terminal connections may become loose over time or become corroded due to salt water exposure so that their connection to the control system becomes unreliable.
- Proximity sensors, as with other electronic equipment, can fail due to stray currents (welding, lightning, etc) or their electronics may simply fail spontaneously. In addition, targets provided for proximity sensors can become loose and move out of position or fall off.
- Rotary encoders can fail for many of the same reasons as proximity sensors and can come loose on their shaft and therefore report incorrect speeds and positions to the control system.
- The mounting hardware for any of the above devices can come loose so that the sensor falls off or fails to function correctly.
- Wiring to the position-sensing device can become grounded due to faulty installation, abrasion or due to the presence of conductive liquids such as salt water.
- Wiring can become disconnected due to loose connections or due to physical damage to conduit and cable.

As a result of the many failure mechanisms for bridge control system sensors, it is inevitable that sensors will periodically fail. Most movable bridge designs recognize the likelihood of sensor failures and provide "bypass switches" to allow continued operation despite the inevitable failures.

In many cases, bypass switches permit a bridge operator to recover from a sensor failure and allow the operator to continue to operate the bridge after he has assured himself that it is safe to proceed. Bypass switches themselves can be a "necessary evil" as it is sometimes difficult to ensure that it is actually safe to proceed. By operating a bypass switch, the operator of the bridge is telling the bridge control system that it is safe to proceed despite sensed field conditions that indicate that it is not safe.

There is often significant pressure for the operator to get the bridge moving quickly due to approaching marine traffic or simply the impatience of roadway traffic that is being held up. In addition, it can be difficult or impossible for the operator to view the location of the failure, as it may be inaccessible with the bridge not fully closed.

Operator training, ongoing maintenance, periodic inspection, good design practices and appropriate selection of position sensing devices can all significantly reduce the frequency of failures, however failures are an inevitable fact of life. In most cases, the best solution is to have pre-defined safe operating guidelines for the operator to follow in the event of a failure.

Reliable Sensing

Recognizing the importance of sensing reliability for movable bridges, we have developed a general methodology that is able to eliminate the adverse effects of most sensor failures. Our solution involves the installation of redundant sensing hardware and modular PLC logic (software) to monitor the redundant hardware. This combination is able to both detect most sensing hardware failures, and to provide continuity of operation in the event of a failure.

In our methodology, for each condition that needs to be sensed, a pair of sensors is used to provide redundancy (Refer to the wedge sensing example in Figure 1 below). The position and function of the pair of sensing devices is arranged to decrease the likelihood that one event will cause both sensors of a pair to fail simultaneously. To further enhance reliability, physically separated parallel systems of conduit and wiring can also be employed.

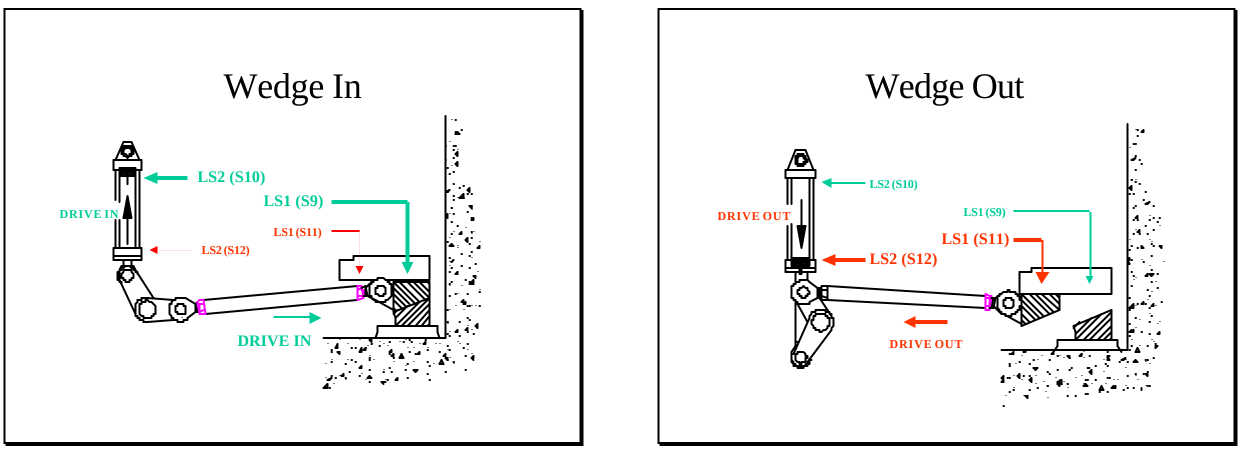

Figure 1

In the event that there is a failure of one sensor, the PLC control software is designed to detect the failure and use the other sensor of the pair to provide correct position sensing. The system can therefore still be operated safely in most cases. In fact, it may not be immediately apparent to the operator that a failure has occurred without some means of notifying him of the failure.

The arrangement of redundant sensors and PLC monitoring software provides the following functions:

- Detection of the loss of signal from a sensor.
  - For example: when a wire becomes disconnected or broken, or the sensor fails in the unactuated condition.
- Detection of an apparently permanently ‘on’ sensor.
  - For example: when sensor wires become shorted, or the sensor fails in the actuated condition.
- Proper detection of the actual bridge condition despite either of the above failures. In most cases this permits continuity of normal bridge operations.
- An alarm to alert the operator that a failure has occurred so that it can be repaired at the next available opportunity. (Note that normal operation can be continued except that repeated “nag”

failure messages will be provided to the operator during each bridge cycle as the failed item is repeatedly detected).
- Specific identification of the failed device and the nature of its failure to facilitate repair efforts.

The cost of implementing our solution is very low relative to the cost of failures in the operation of a heavy moving structure. It requires only duplication of relatively inexpensive sensors, possibly the installation of a redundant conduit and wiring system for sensors and a modular PLC software solution custom fit to the situation. The modularity of the software overcomes programming complexities and assists in providing a cost effective and maintainable final implementation.

Despite the modular PLC software and the simplicity of employing dual, redundant sensors, our solution is not completely "cookie cutter" and requires an accommodation for the peculiarities of the particular system for which it is being employed. Although the idea behind providing sensing reliability is simple, the actual implementation requires a thorough understanding of the system's operation and may involve some non-obvious compromises to achieve the greatest benefit.

As a side note, we feel that these techniques are applicable to many industrial control systems where the costs or other implications of failures warrant the moderate additional costs.

Outline of the Methodology

To start with, as with any bridge control system design, standard "good design" practices are used to reduce the likelihood of failures. High-quality and reliable devices are used to enhance system reliability. These devices are located to minimize failure due to physical damage, exposure to adverse environmental conditions, etc. Device locations are selected so that the sensed item is as close to the final moving element as possible, and where it is most likely that the desired condition will be sensed correctly. For example, when the position of a swing bridge wedge is to be sensed, the sensing device is usually arranged to detect the position of the actual wedge rather than to detect the position of an arm or shaft driving the wedge.

With our sensing methodology, for each condition needing to be sensed reliably, two independent sensors are used. Also where possible, both sensors of the pair are located to be physically separated from one another. This is done to reduce the likelihood that both devices will be damaged by a single physical event. The separation requirement frequently necessitates the sensing of different physical elements. In the wedge example above, the spacing requirement may necessitate that one of the sensors monitor the position of the wedge drive arm while the other senses the position of the actual wedge. If these decisions are made prudently (for example, the arm to wedge joint may be felt to be highly reliable and therefore unlikely to be the cause of a failure), and due to the reliability that results from these techniques, overall system reliability can be significantly enhanced.

For limit switches and proximity detectors, normally closed (NC) contact configuration devices are used. The normally closed contact configuration permits the continuity of the circuit to be monitored by PLC software at specific times when the sensor is expected to not be activated. For example, closed and nearly closed switches can be tested for continuity when the bridge is known to be in its open position. Detection of disconnected wiring to the switch, a bad or corroded connection to the switch or failed switch contacts can therefore be easily accomplished.

Next, an "operating time window" is determined for each pair of sensors. The window is selected to be wide enough so that both devices are assured to have operated within the allowed time if there has been no failure. Similarly the window is made narrow enough so that there is sufficient time to stop the motion if either one of the pair of switches were to fail to operate correctly.

The sensed condition is deemed to have occurred as soon as either:

- Both switches are seen to have operated at the expected time in the bridge operating cycle and within the permitted time window.
- OR, one switch is seen to operate at the expected time and the time window allowed for the second device to operate expires (presumably due to the failure of one of the switches to open its contact).

If warranted for the resulting increase in reliability, the designer can elect to use two physically separated wiring systems to connect to the #1 and #2 sensors in each of the sensor pairs (Refer to Figure 2 below for a simplified example). This arrangement would make damage to the control system conduit and/or cabling less likely to result in the failure of both sensors of a pair.

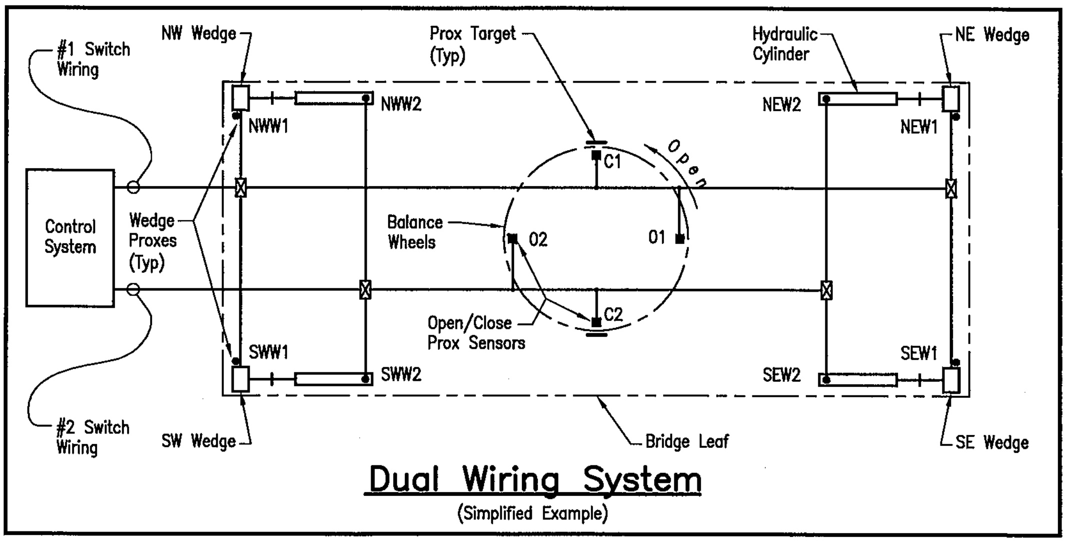

Figure 2

The result of these techniques include:

- That the failure of a single device is detected but normal operation can continue despite the failure, as long as the second device of the pair is functional.
- That the likelihood of failure of both sensing devices is minimized due to their physical separation. If repairs are reasonably prompt, it becomes highly unlikely that both switches of a pair will be non-functional at the same time.
- That the operator can be notified of the failure, the location of the failure and the specific type of failure (open circuit or closed circuit). This increases the likelihood that the failure can be repaired before a second failure occurs.
- The fact that the bridge can be operated normally but the operator will be notified again (nagged) at every operation, is also felt to increase the likelihood that it will be dealt with promptly.
- The costs of employing and maintaining this methodology are relatively inexpensive compared to the costs and other consequences of a failure.

Bypass Switches

As a final related item, we have employed an arrangement of bypass switches and an associated reporting methodology that is intended to increase the likelihood that critical failures to control system interlocks are dealt with in a timely and appropriate manner. Over the years while carrying out engineering assessments of the condition of movable bridges one of the most common control system related problems involves the abuse of bypass switches. Frequently bypass switches are used in the "heat of the moment" when the operator is under pressure to get the bridge moving and then are subsequently forgotten. Consequently, it has been a frequently observed problem that critical safety interlocks are permanently bypassed by Bypass Switches provided in the design of the control system.

We have arranged the bypass switches to be key accessible only to authorized bridge operating personnel to minimize tampering by others (Refer to Figure 3 below). We also have provided a wire tie and crimped seal to prevent casual operation of the bypass switches and as a visual indication of their operation. In order that the bypass switches can be easily used when required, we have provided wire cutters permanently chained inside the operator's control panel so that they can easily be used to cut the tie wire allowing a bypass switch to be used.

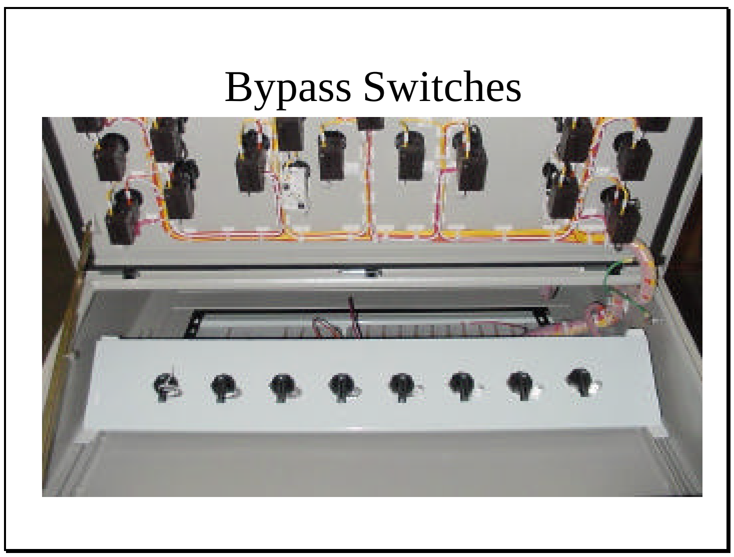

Figure 3

A 'Bypass Switch Log' form is provided, that the bridge operator is required to use whenever he finds it necessary to cut the tie wire and use a bypass switch. A signed and dated entry is made by the operator describing the event that made use of bypass switch necessary. Maintenance personnel then have the responsibility to determine and repair the cause of the failure. Once the repair has been carried out, the maintenance person then 'closes' the log item by describing the repair and initialing and dating the entry. He then uses a new tie wire and crimped seal to secure the bypass switch again. The crimping tool is intended to be kept in the possession of bridge maintenance personnel.

With the dual redundant sensing methodology previously described, it is hoped and expected that the use of bypass switches will be much less frequent than has been common in the past. However, they are still necessary in the unlikely event that an unrecoverable failure occurs.