HEAVY MOVABLE STRUCTURES, INC.
ELEVENTH BIENNIAL SYMPOSIUM
November 6-9, 2006

"The Future in Moveable Bridge Control: Fault Tolerant PLC and Remote Operation and Maintenance"

By

Omar Dumé
Electro Hydraulic Machinery Co.
1851 S.W. 31st Ave.
Pembroke Park, FL 33009
(954) 981-0023: Ph.
(954) 981-4022: Fax

Abstract

This presentation will describe in detail many of the features of a Fault Tolerant PLC systems as implemented on a Moveable Bridge. The highlights will include expected benefits like greater reliability, safe remote operation, and off-site troubleshooting. An explanation of the different Fault Tolerant configurations will be presented with various communication options for remote operation. In addition, the paper will show the possibilities for operator training through simulation and performance review testing being done through the existing PLC program.

Introduction

Picture this: as the bridge is raised near the afternoon rush hour, there is a failure on one of the limit switch signals, the bridge is stuck up in the air; more cars are lining up waiting for the bridge to go down, drivers get antsy and start honking their horns. The bridge tender has tried everything he knows and can't get the bridge to work. He desperately calls his maintenance technician, and after three tries he finally gets through, explains the problem, but the technician is more than an hour away, and with this traffic it would take him at least an extra hour to get to the bridge. It's about midnight when he finally gets the bridge to work, jumping out a permissive; he still has to come back the next day with the right parts to correct the original failure.

Now picture this: as the bridge is raised near the afternoon rush hour, there is a failure on one of the limit switch signals, but instead of the bridge getting stuck in the air it continues to operate normally, the bridge tender is notified of the failure by a message display and by a friendly computer voice. Also email and voice messages are sent to the maintenance technician. Fifteen minutes later the technician plugs in his laptop, connects to the bridge computer from a remote location, determines the exact origin of the failure, calls the bridge tender and lets him know that he will be there tomorrow with the right parts to correct the problem, but he can continue to operate the bridge as need.

We have seen the first picture happen many times, and it becomes a big headache for everyone involved, but on the other hand when we talk about a failure tolerant bridge system an uncomfortable feeling comes to most engineers and designers because there are still big doubts of the reliability and repeatability of these systems. This paper will explain how fault tolerant systems work, and present some of the benefits that can be effectively used in drawbridge applications, and try to ease our doubts by showing the reliability and repeatability of these systems.

Redundant Programmable Logic Controller (PLC) Systems:

A good definition of fault tolerant design can be found online in Wikipedia: "refers to a method for designing a system so it will continue to operate, possibly at a reduced level, rather than failing completely, when some part of the system fails".

Most fault tolerant systems are based on a redundant PLC. As its name describes it, redundant PLC systems consist of at least two controllers configured in such a way that, if failure is presented, the system can overcome a stoppage by discarding the faulty module and using its redundant partner.

They're many different configurations that can be used depending on the level of tolerance required. The most used configuration has two identical PLC systems, same processor, same type of input modules and output modules, all wired in parallel, so if one PLC fails the other will pickup immediately and continue the process.

Some PLC manufacturers sell PLC processors that easily can be configured for redundant applications. These processors when installed together operate in parallel, checking each other, and if either one fails the other one will continue to control the system on its own, until the faulty module is corrected. Both modules can be electrically isolated from each other, only a communication cable between the two is need (fiber optic or CAT5). This cable allows the CPUs to exchange information and know if the other has failed.

In high level fault tolerant systems a "voting" system can be used. So, instead of using two processors, a third CPU is added. This way each processor "votes" for each action to be done in the system. The votes should always be the same, but if one is different from the other two, and alarm will be given, but the system will continue to operate with the two CPUs that are the same. See Fig.1 and Fig.2.

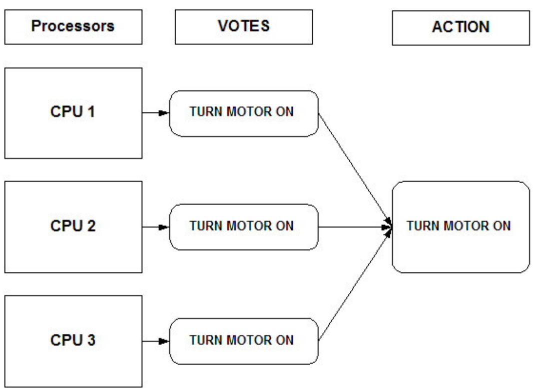


Figure 1

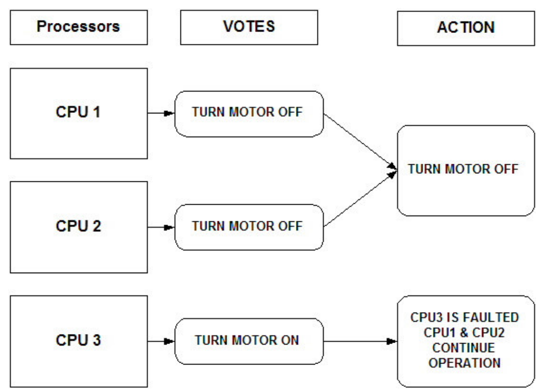


Figure 2

This voting system can also be used for the inputs. As an example, in a normal relay logic bascule bridge, the span fully open limit switch is normally used to stop the movement of the span, but if the relay or limit switch fails the span will continue to move, and hopefully it will be moving slow enough that the bumper blocks will make it stop without causing any major structure damage. In a redundant system with input voting we have many options to prevent such a failure to damage the structure. A second fully open limit switch can be added with a lot less wiring than a relay system will require, this will provide a second vote, and if one or more input modules are added the processor will have enough information to proceed safely through most faults.

A main concern when using PLC systems is that an output module can fail. On bridges we see many power surges caused by lighting. On older bridges surge suppression were never added or it was poorly designed causing damage to the electronic equipment when lighting struck, but with correct surge suppression design these faults can be greatly reduced. But even in the case of a damaged output module a fault tolerant system can overcome these faults and continue operation.

They're many output configurations but the most commonly used are the "T" and the "H".

Output "T" configuration

This is the most common and simple configuration, Fig. 3. It uses two outputs to power one load, so if one of the outputs fails the other output will continue to operate. The benefits of this configuration are the simplicity and that only two outputs are needed. On the other hand this configuration only protects if the output fails open (open circuit).

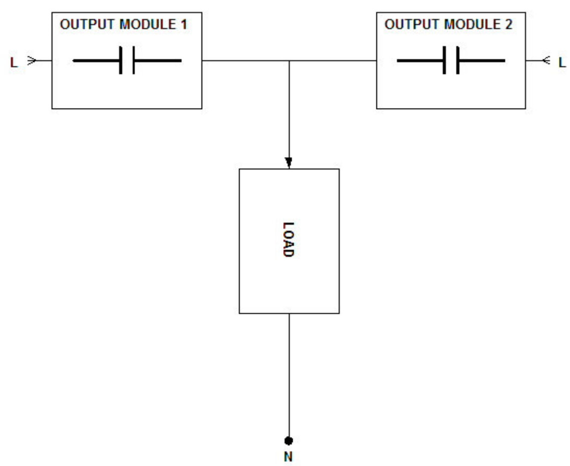


Figure 3

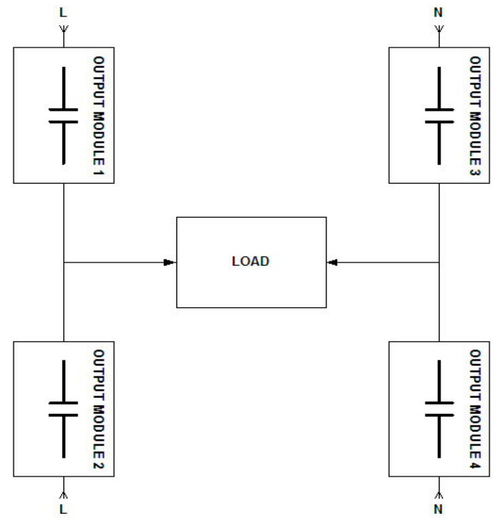


Figure 4

Output "H" configuration

The "H" configuration consist of two outputs providing the line or positive power to the load and two other outputs that provide the neutral or negative power, Fig. 4. This configuration allows for the most reliability because it protect against open or closed circuit failures.

This picture on the left shows a redundant PLC system installed on the Treasure Island Bridge in Florida. The Bridge is owned by the City of Treasure Island. This system was designed by EC Driver, the main contractor is Johnson Brothers and the electrical controls were done by Electro Hydraulic Machinery Company. Note the dual processors on the top and exact replica of the I/O racks on the bottom. Processors are electrically isolated and only communicate through a fiber optic cable.

Benefits
1.) Reliability:

A broken-down drawbridge is a big problem, either if it is stuck up in the air or if it can't open for boats; that is why reliability becomes such an important topic in these application and also why this fault tolerant technology becomes important to know and understand, because it is so much more dependable than a standard relay system.

A single PLC system reliability varies between manufacturers, but a typical system has a mean time between failures (MTBF) of about 5 years. Compare that to a Fault Tolerant system that has a MTBF of at least 50 years, and some manufacturers offer configurations with even higher MTBF. A Fault Tolerant PLC system is more reliable because of the combination of software and hardware architecture that constantly checks itself; processors are continuously monitored by a watchdog circuit and a synchronous detection circuit, input modules have an internal output circuit for each channel for the purpose of energizing each input for a short cycle to verify functionality, and output modules have internal current sensors to determine if each output is working properly or if there is a open or short circuit fault.

But even more impressive then having a better MTBF than a conventional system, is that it will overcome most common failures. So when a problem is presented the system can detect it and the redundant partner can kick in and continue operation. I like to use the analogy of a large cargo truck; it has many extra tires, if one of them is punctured it can continue without having to stop.

A standard relay circuit or PLC system can't overcome faults without intervention from the bridge tender or maintenance personal. So the bridge must be stopped until the problem is figured out and then apply the corrective measure. In a redundant system is the opposite, operation can continue and the corrective measure can be applied later when it's more convenient, not in the middle of operation or rush hour.

2.) Incorporation of features:

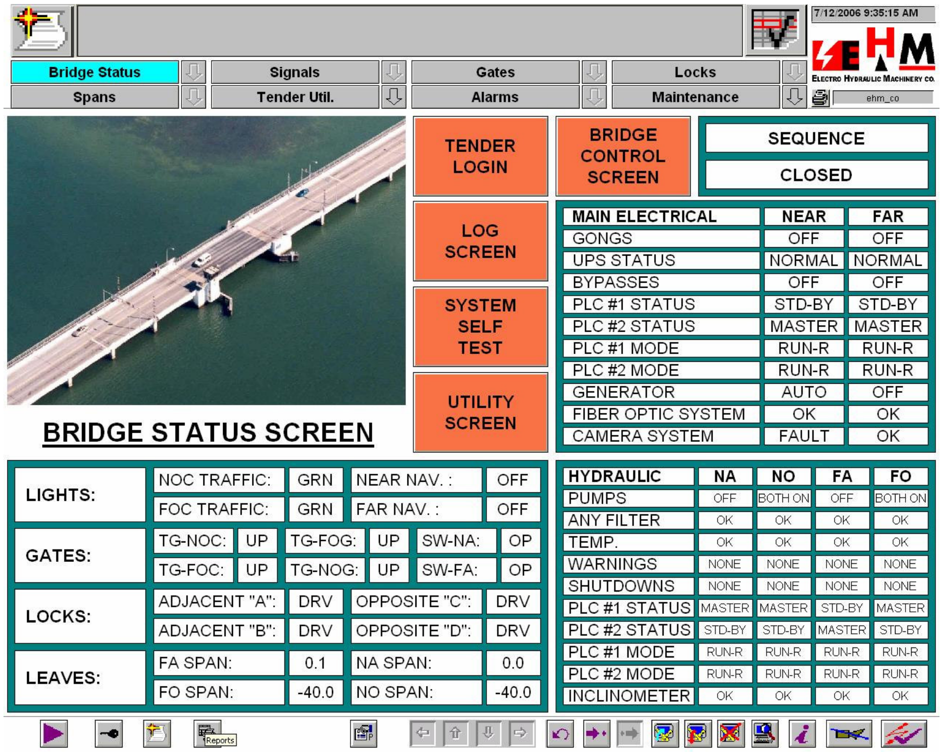
Of course the main reason to use a redundant PLC system is because of its reliability, but they're many other features that can be added that makes these systems very flexible and makes life so much easier for the bridge tenders and maintenance personnel, saving money and reducing or even eliminating downtime.

Some of these features are:

- ☐ **Troubleshooting:**

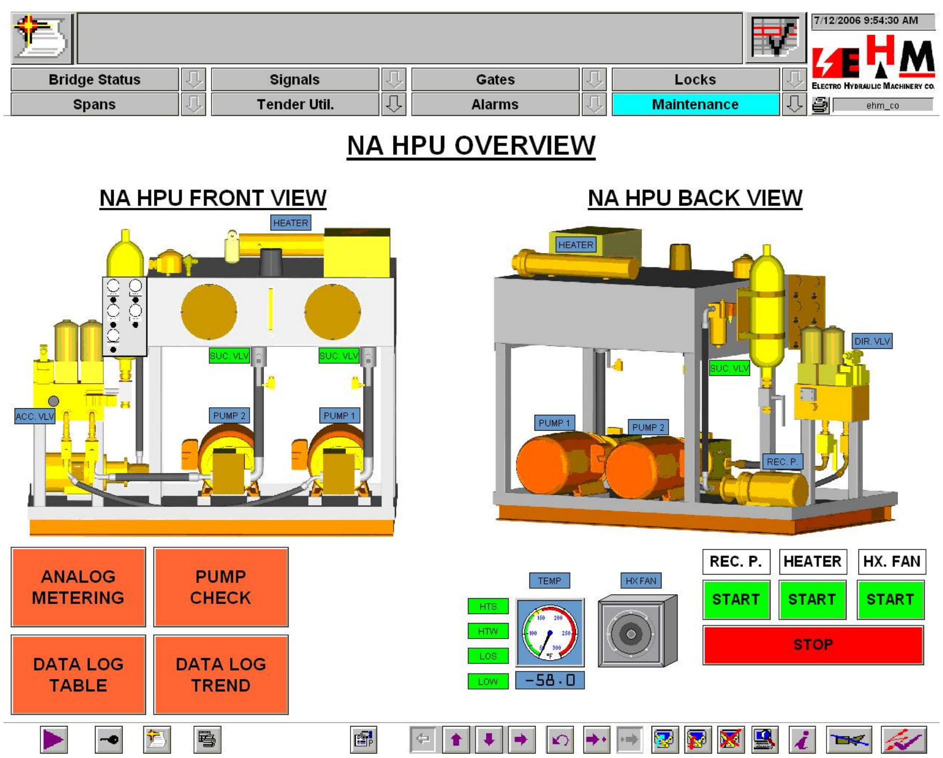
It's very difficult for new maintenance personnel to troubleshoot and find the cause of problems on older bridges because usually there are no schematics, they been gone for years, and even if he has some schematics they're probably old and don't reflect changes. So a small problem may become a nightmare trying to "fish out" wires.

A redundant PLC system has troubleshooting features that can pin point the source of the problem. The technician can plug a computer to the PLC and easily determine where the failure is coming from, and in some cases even specify the actual problem, for example it can determine a short-circuit, open-circuit, loss of power, etc.



These pictures are screenshots from the HMI used in the Treasure Island Bridge, programmed by Electro Hydraulic Machinery (EHM). The top screen shows the main menu with the general status of the bridge. Position of gates, locks and leafs are indicated. Also condition of processors, UPS, Camera System, Generator, Fiber Optic and HPU are shown.

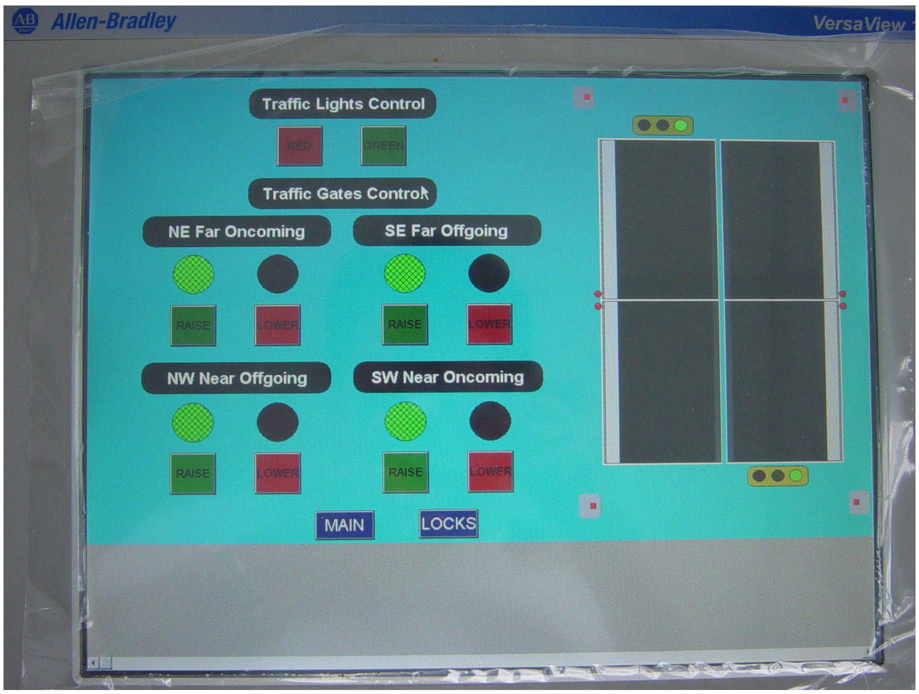
The bottom picture is maintenance screen that shows an overview of one of the Hydraulic Power Units. This screen will display details on the condition of the HPU, including pressure, flow, temperature, which valves are on, filter clogged, etc.



- **Advance operator interaction:**

Another great benefit is that these systems can interact with HMI (Human – Machine Interface) software creating endless possibilities. So now bridges can be operated from a computer instead of a console with lots of buttons. Operations can be even more simplified by using a touchscreen.

Flashing icons and message boxes can guide the bridge tender step by step on every opening, minimizing errors. Also a human like computer voice can be added to guide the operation or to warn in case of a problem or failure.



This picture shows a Touch Screen display used to operate the Palmetto Park Bridge. This Bridge is owned by Palm Beach County and the display and PLC system were installed by Electro Hydraulic Machinery (EHM). This system has a computer generated voice announcements for alarms and warnings. It also has a remote access modem that allows connecting to the PLC or computer to troubleshoot problems or download alarm and operation logs.

These systems can even be programmed so that new operators can be trained directly by the computer, and the bridge tenders can be giving periodic competence tests to check their skills and to refresh their memories on operation procedures that they don't normally use. New trainees can go through a full bridge opening operation step by step on the computer screen without ever turning the actual traffic lights to red or moving the bridge, all with the simulation software that can point out any mistakes done on the "practice" operation.

Also a great feature about using a HMI is that it can be programmed to have advanced troubleshooting features. So, instead of having to plug a computer, a maintenance technician can view all the needed information to troubleshoot on the computer screen including manuals and up to date schematics. Even a interactive troubleshooting flow chart can be added to guide the person through problems.

- ☐ **Data and alarm logging**:

Many failures on a bridge can be prevented or corrected before it ever happens if good records are kept of the bridge operation. For example, if a motor, when it first was installed, pulled 15 amps but 2 years later is pulling 22 amps this would indicate that there is a problem with the motor or there is some mechanical problem causing the extra load on the motor. In most cases there are no maintenance records, there is no information to compare to, so usually the motor ends up overloading causing a bridge breakdown.

But on these PLC systems a precise record can be stored and viewed as need, even 5 years after the bridge has been in operation. Some of the information that can be recorded are:

- Motor speeds and current
- Oil flow, pressure and temperature (for hydraulic bridges)
- Each bridge opening and duration
- Power failures
- Amount of time the generator has run
- If bypasses are used
- Warnings and Alarms

This information can be linked to create a warning or an alarm when a value is outside its normal range. So, going back to our previous example, if the motor is pulling 7 amps higher than before a warning will be displayed to the operator and he could call the bridge technician so he can find and repair the problem before it causes a failure.

- ☐ **Remote communication:**

Most PLC systems offer a wide range of communication options and protocols, including Ethernet. Adding a communication module with an Ethernet port to a redundant PLC would allow multiple computers to access information from the bridge.

As we mention before, there can be a computer at the tender house to operate the bridge, but there can also be a second computer on the far side of the bridge working as a backup. A modem can also be added to allow remote communication from an external computer, this way the maintenance personnel can call in the bridge with their laptop and download all the recent alarms and check if there are any problems that need immediate attention. Also administrative personnel can communicate to the bridge and download information they might be interested in like: amount of openings, average opening times, tender clock-in/clock-out, etc.

External communication is always a major concern because of the fear of the “hacker” trying to remotely take control of the bridge, but there are many security features to prevent this from happening. First, if the remote communication is done thru the internet, firewalls and multilevel encrypted passwords can be added to prevent intrusion from any unauthorized person. Second, if there still is a concern, instead of using the internet to communicate, a direct phone line can be used. With a direct phone line, now the person trying to communicate to the bridge needs a user id, a password, he also needs the phone number of the bridge, and also the phone line must be plugged in to the PLC’s modem.

- ☐ **Use of Close Circuit Television:**

Another benefit that hasn't been exploited much on bridge applications is the use of close circuit television cameras (CCTV). Many accidents even death have occurred because the bridge tender didn't see a pedestrian on the bridge and raised it with the person on the bridge. With a CCTV system a person or a vehicle can be detected and a warning can be given to the bridge operator so he can check the span before proceeding with the opening.

Similar technology is currently used on traffic lights to detect vehicles. Cameras are mounted on top of the traffic lights to determine if there are cars waiting, and if there are the lights will be changed to green.

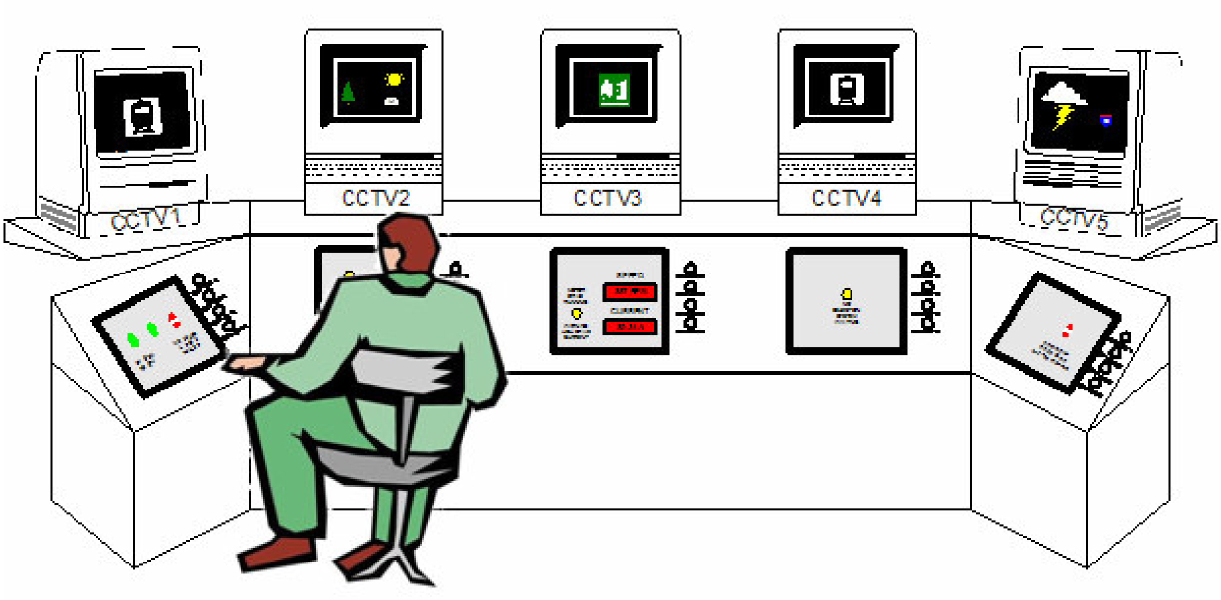
CCTV systems can easily be integrated in PLC applications. Many other features can be added and used also, for example, a camera with pan tilt and zoom (PTZ) can be used instead of a static camera, so the camera can be programmed to do a swipe of the whole span to make sure the bridge is clear before allowing the tender to open. Other cameras can also be installed under the bridge to make sure the channel is cleared before allowing to close.

Remote Operation

Most of the departments of transportation have central offices that monitor traffic data and also are dispatch centers for Road Rangers. These centers are usually state of the art facilities that can pull current status of any major highway or road on a click of a button, and even get a picture or video of congested areas. Some of these facilities even have tracking devices for their Road Rangers so they know exactly where each one of them is at any giving time so they can be more effective when dispatching to a problem spot.

Many have considered and inquired about remote bridge operation from a central facility, but time after time the idea is dropped and put to the side because no one trusts the current systems enough to use them in such an "ambitious endeavor". This is mind boggling, especially when you can see all the technology that is currently being used in these DOT facilities, and when all the benefits of a remote bridge are listed including the economical and logistical aspects.

With these Fault Tolerant Systems some of these fears will subside and probably in the near future bridges will be operated from remote centers. Using the before mentioned features a Remote Operation System can be designed to be reliable, because of the Fault Tolerant PLC; easy to use because of the advanced HMI features; and more importantly safe, because of the use of CCTV and because of how all these features can blend together.



The above picture shows a sketch of what a remote bridge operation center might look like, with one operator controlling five different bridges. He can monitor alarms and status of the bridge with touch screen displays and see actual traffic conditions through the CCTV. When an opening is requested, he can operate the bridge by following his screen prompts and he can verify the bridge is clear before opening by viewing the televisions.

Conclusion

A redundant PLC system in a moveable bridge application when designed and programmed properly creates a dependable structure that can repeat opening after opening, without failure of the electronic components, and even if there is a failure, the redundancy can "kick in" an continue operation until it can be resolved. That is what makes these systems safe and secure, the repeatability and being able to overcome most failures and continue operation without stopping.

What makes these control systems even more appealing is that they can be tailored to the end user's needs. Custom Human-Machine interfaces, advance troubleshooting, remote communication, etc; any features or option can easily be added and still maintain the reliability and safety of the system.

References:

1. Walczak , T., Maes , M., "Applying Safety Systems in Certified Environments Utilizing Remote I/O and Communications", ISA, 1998. Link: http://www.data-linc.com/articles/isa98tw.htm
2. Watkins, F., Dukich, S., "Back to School", AB Journal, 2001. Link: http://www.ab.com/safety/safety_now/april01/back_school/index.html
3. Allen-Bradley, "ControlLogix Redundancy Systems", User Manual, 2005.
4. GE Fanuc Automation, "Genius Modular Redundancy Flexible Triple Modular Redundant (TMR) System", User Manual, 1995.
5. Siemens, "Process Control System PCS 7 Fault-tolerant Process Control System", User Manual, 2004.