HEAVY MOVABLE STRUCTURES, INC.
ELEVENTH BIENNIAL SYMPOSIUM

November 6-9, 2006

Failure of the Control System on the East Half of the Hood Canal Bridge

Tim Benson, P.E.
Washington State Department of Transportation
and
Mark Van De Ree, P.E.
Parsons, Brinckerhoff, Quade and Douglas

DOUBLETREE UNIVERSAL STUDIOS
ORLANDO, FLORIDA

Executive Summary

The Hood Canal Bridge is a 1.4 mile long floating draw bridge located in western Washington. On August 18, 2005, a potentially catastrophic fault occurred on the bridge. The fault was with the PLC control system (programmable logic controller) of the east structure floating draw span. The fault caused PLC outputs to energize without operator commands and without operators present. Electrical equipment, including motors, was energized and operating. The drive motors were in a locked rotor condition for an extended period (approximately two hours), destroying them.

The fault caused no injuries or fatalities, but put the east structure out of service for an extended period. Having avoided a potentially fatal catastrophe, attentions were focused on repairing the damaged equipment and returning the bridge to service. Attention was also focused on investigating and mitigating the cause of the fault. Such a fault has never occurred with this control system since its commissioning in 1985. In-depth investigations into the cause of the PLC fault were inconclusive. One suspected cause of the fault was an outdated I/O (input/output) controller card. Outdated PLC cards were replaced with newer versions. The bridge was restored to service approximately ten weeks after the fault occurred. Special operating procedures were put in place until the control system could be re-configured to be fail-safe. A year later, to date, the fault has not reoccurred.

With the type of control system configuration used for the east structure, all safety interlocks became bypassed as a result of the fault. The east structure end locks were released, the drive motors activated, and the traffic gate was operating – all with the bridge open to traffic. Since the west structure has a semi-independent control system, neither the west endlocks nor longitudinal centerlocks released. In fact, the west endlocks and centerlocks held the draw spans together for two hours while four 40 horsepower drive motors on the east structure were energized and trying to open the spans. Refer to Figure 1.

In 1985, the PLC control system was retrofitted to the east structure to partially replace the original 1961 control system. As a result of this investigation, it was determined that the PLC retrofit configuration was deficient by present standards. The retrofit configuration did not have safety shutdowns external to the PLC, and hardwired overcurrent protection was operated through the PLC.

Present day standards and recommended good engineering practices for controls system are now available. These standards and practices have been evolving for PLCs in the control systems engineering discipline since the 1970s. They include the use of watch dog timer circuits, master control relay safety shutdowns, and external hardwired relay safety circuits, among others. Some of the standards specifically define what is considered a "good engineering practice" in the context of SIS (safety instrumented systems). The standards are applicable to public life safety systems on movable bridges and include the ISA-84 (2004, revised from 1996) (Instrumentation Systems and Automation Society), IEC-61511 (International Electrotechnical Commission) and TUV Rheinland North America SIL (Safety Integrity Levels). Control system engineers and designers should begin to incorporate SIS standards and practices into all new, replacement, and rehabilitated movable bridge control systems.

Introduction

The Hood Canal Bridge

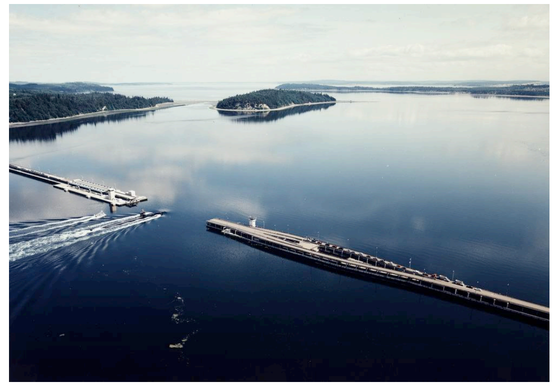


Photo 1: The Hood Canal Bridge: Photo taken prior to widening of the west half of the bridge.

The Hood Canal Bridge is a floating concrete pontoon bridge which spans the 330 foot deep Hood Canal connecting the Olympic Peninsula to the Kitsap Peninsula in western Washington. The floating portion of the bridge is 7,450 feet long and has two retractable draw spans in the center which can be opened to form a 600 foot channel for marine traffic. It carries one lane of traffic in each direction. Originally built in 1961, the west half of the bridge was destroyed in a storm on February 13, 1979. A new, stronger west half was built and opened to traffic in 1982. At that time, the bridge control system consisted of an ungrounded 240 volt a.c. relay based control system which communicated across the draw spans by way of a leased submarine telephone cable. After notification by the telephone company that they would continue to lease the telephone cable to WSDOT, but would not replace the cable if it was destroyed, plans were made to upgrade the control system to ensure its reliability. In 1985 the system was modified to incorporate Square-D, SyMax Model 500 programmable logic controllers (PLCs) and a wireless communications system. This resulted in a hybrid system. The ungrounded 240 volt a.c. control relay system on the west half of the bridge was retained, while the east half utilized the new PLC for control logic using a grounded 120/240 volt a.c. control system. The submarine telephone cable is still in service and used to provide redundancy to the wireless system.

At this time, the Washington State Department of Transportation is presently in the process of building a replacement bridge for the structurally deficient east half, widening the west half of the bridge and the approach spans to provide shoulders for disabled vehicles to meet FHWA requirements, and replacing the hybrid control system.

The Control System Fault

The Malfunction

On the evening Thursday, August 18, 2005 at approximately 11:30 p.m. the bridge was undergoing construction work to facilitate the widening of the west half of the bridge and the east and west approach structures. The WSDOT construction inspector noticed that the traffic had increased and saw that the east structure’s stop signals and traffic gate warning lights were flashing. He reported this to the Olympic Radio operator who called out the on-call bridge tender who arrived at 1:15 a.m. Friday morning. The bridge tender went to the control tower on the west half of the bridge and found that all of the indicating lights on the control desk for the east half of the bridge were lit. When he was unable to gain control from the control desk in the west control tower, he went to the east control tower and found that all of the indicating lights on the east half of the control desk were lit as well. Since he was still unable to control the bridge, he went to the PLC cabinet on the floor below and turned the primary and back up PLCs to “HALT” using the keyed switches which turned everything off at approximately 1:30 a.m. He observed that the west end locks had rotated into the OPEN position, that the machinery rooms smelled like overheated motors and that the drive motors were hot to the touch.

Initial Investigation

Charles Collins and Tim Benson, the electrical engineers from the WSDOT Bridge Preservation Office arrived on Friday morning to investigate the malfunction. After interviewing the bridge tender, they performed an initial survey of the status of each piece of equipment. They then opened the local disconnect switches or circuit breakers to all machinery and locked them out to ensure that no bridge movement could occur. Charles Collins then turned the main processor from “HALT” to “RUN.” He observed that the output module lights all came on. At the same time, the indicating lights on the two control desks for the east half of the bridge all came on. This included the indicating lights for both the ON and OFF condition of each control. He then connected the programming lap top computer to the PLC programmer and discovered that all of the coils in the ladder logic were forced ON, even though the “FORCE” indicating light on the processor module was not on or blinking. He then selected the command to clear all forces and the lights on the output modules returned to their normal state. The force light was then tested by forcing a single coil and then clearing it and it operated properly.

Visual inspection and megger testing of the four 40 horsepower d.c. drive motors found that the motors had been subjected to severe overheating. It was apparent that they had been operated at locked rotor current for at least two hours. Arrangements were made with a motor repair facility in Seattle and WSDOT maintenance forces began disconnecting the four drive motors and preparing them for delivery. After initial steam cleaning and testing, the motor repair shop recommended a complete refurbishment and rewinding of the four drive motors.

As one of WSDOT’s on-call consultants, Parsons Brinckerhoff Quade and Douglas was contacted and an expedited agreement was processed to perform an investigation of this fault on an emergency basis.

The Fault Investigation

The control system fault presented a formidable challenge to investigate and solve. The bridge serves the U.S. Navy nuclear submarine base in Bangor, WA and its proper operation is extremely critical. The electrical equipment was old and was no longer supported by the manufacturers. During the past 20 years of operation, there were no similar failures or faults with the PLC control system reported. An investigation into the control system fault was performed the week of September 5, 2005. The purpose of this investigation was to identify what caused the PLC outputs to be energized, assess all resulting damage, and recommend remedial action. Washington State Department of Transportation maintenance and engineering personnel with the assistance of Parsons Brinckerhoff Quade and Douglas, Inc. conducted interviews, field testing, and field inspections for this investigation.

A team of technical experts was assembled to provide in-depth analysis of all control systems components and sub-systems. The technical experts included manufacturer representatives familiar with the specific components of the control system and drive system. Preliminary findings were used to expedite a recovery from the fault.

The investigation focused on PLC components and the wireless communication system components. Inspections and testing were performed to determine if the control system and motor drive systems were suitable for continued service. It was important to keep in mind the electrical and controls equipment was 20 to 45 years old. Investigation objectives were as follows:

1. Identify cause(s) of control system fault(s).
2. Identify similar historical occurrences with Square D, SyMax model 500 PLC.
3. Recommend preventative measures.
4. Determine condition of Louis Allis Motor/Generator Drive Systems.
5. Document all equipment:
    a. PLC system hardware, firmware, and software.
    b. Modem and wireless communications components.
    c. Drive motor/generator and drive electronics.
6. Perform visual inspections
7. Record measurements
    a. Motor and generator insulation resistance
    b. Feeder conductor insulation resistance
    c. Feeder conductor continuity
8. Assess operational readiness
9. Operational testing

Control System Description

The control systems for the east and west structures are semi-independent. The system for the west structure is a hybrid, single phase, 60Hz, 240 volt a.c. ungrounded system. The west structure control system uses a PLC to facilitate wireless communications with the east system. The east and west structures each have control towers with control desks. The systems are configured to allowed complete bridge operations and control from either control desk. The west structures control desk is the one predominately used.

The control system for the east structure is a hybrid single phase, 60Hz, 120/240 volt a.c. grounded system. A portion of the control system uses two pole, 240 volt a.c. circuits for PLC outputs. The PLC system installed in 1985 replaced most of the hardwired relay controls and interlocks with software based control logic. The PLC power originates at a UPS (Uninterruptible Power Supply), is filtered by an Islatrol brand power filter, feeds through Square-D brand power supplies and connects to the PLC CPU (control processing units) racks and PLC I/O (input/output) racks. Refer to Figure 2 for the PLC system architecture, and Photographs 2 and 3.

Photo 2: East Structure Control Cabinet

Photograph 3: Square D SyMax Model 500 (Type SCP-523) PLC w/CRM-210 LI Module (Local Interface)

The PLC system is a Square-D brand SyMax model 500. The CPUs are configured for a bumpless, hot failover from the primary to the backup PLC. Local and remote I/O racks are used with LI (Local Interface) modules, having two communication channels.

The LI communications cable is a four wire twisted shielded cable. The communications cable is switched through reed relay output modules from the primary to the backup PLC processor.

The primary and backup PLC processor and LI racks are interconnected through SyNet Network Interface modules using a SyNet coax cable.

Preliminary Findings and Recommendations

The preliminary findings and recommendations were as follows:

1. The fault caused PLC outputs to energize without operator commands and without operators present.

2. Electrical equipment including motors was energized and operating. The drive motors were in a locked rotor condition for an extended period destroying them.

3. One suspected cause of the failure was a Square-D communications card CRM-210 that communicates PLC commands to the I/O. The CRM-210 is a local interface card with a revision level H. The most current revision made was level N before Square-D stopped making them years ago (late 1980s). It is possible the revision level H cards were recalled by Square-D in the 1980s, although this was not verified.

4. Three CRM-210 revision level N cards have been located for sale through the local distributor. It was recommended that two of these cards be purchased, one to install and one for a spare.

5. In addition to purchasing the CRM-210 cards, the following was recommended before operating the east half:

    a. Maintain the practice of keeping all east half motor circuit breakers open until a bridge operation is needed. Since the east half was not presently operational, this would apply to the traffic gate and endlocks. Once the drive motors are replaced their circuits should also be kept opened. When the east half is made operational, the practice of opening all motor circuits should be maintained until the east half control system is reconfigured to be fail-safe.

    b. Verify all Square-D cards have revision levels suitable for continued service.

    c. Refurbish both motor drive generators in a motor shop. Megger testing showed insulation resistances to the generator frames to be less than 200 ohms. This resistance should be above 10 mega ohms. Testing of the 100 hp induction motors for each motor generator set showed they are acceptable for continued service.

    d. The d.c. drive motor overcurrent protection did not function during the fault. The overcurrent relays are believed to be operational, but the relay contacts are connected through the PLC and are not hardwired to the motor contactors. This configuration essentially bypasses the overcurrent protection regardless of the overload relay condition. The fault caused the PLC outputs to the motor contactors to be energized, therefore commanding the contactors to remain closed.

The d.c. drive motor overcurrent relays are very old (early 1960s) and should be sent to an electrical shop to be tested. Refer to Photograph 4. Testing should include insulation resistance (megger), and load testing. Preliminary megger testing in the field showed no signs of insulation failure. The existing overcurrent relays can be put back into operation if they pass the load test, but should be removed from the PLC.

e. The generator exciters, Saber 3200 d.c. drives, appeared to be suitable for continued service. The electronic drives were installed around 1977 replacing the original Metadyne exciters from the 1960s. It was recommended these drives be refurbished in an electronics shop to replace the original electrolytic capacitors. Before this is done, spares should be located since there are only two installed exciters on the bridge with no spares or spare cards. It is preferred the generators and motors be installed and operated for a while before changing out the exciters. This approach will help control and isolate any start-up problems while making the east half operational.

f. Clean or replace all motor contactor and starter contacts including the east traffic gate.

The east traffic gate should be inspected in detail for mechanical or electrical damage. The gate was reported to be continually operating for an extended period driving the arm to the “UP” position, resetting itself mechanically, and then driving again.

Interviews

The bridge was undergoing major rehabilitation and replacement construction when the fault occurred. The night shift construction inspector for WSDOT noticed the east structure stop signals flashing and the traffic gate lights flashing. Although the Inspector’s Daily Report (IDR) shows the time at 11:30pm, an interview with the inspector confirmed the time was actually a few minutes (five or less) before 11:30pm during a critical concrete pour. The inspector called Olympic Radio (a WSDOT dispatch center located in Tacoma, WA) who in turn contacted the on-call operations and maintenance personnel for the bridge.

The bridge tender arrived on site at 1:15am Friday (August 19) to clear the fault. The construction flagger was waiving traffic along when the tender arrived. The tender could not obtain control from the west tower control desk. He went to the east tower control desk and still could not obtain control. He finally went to the PLC cabinet in the east tower and placed the primary and backup PLC processors in halt mode using the key switches. This shut everything down, at approximately 1:30am Friday (August 19). The tender smelled a hot motor smell and noticed all four drive motors were hot to the touch.

The bridge electrical technician was on the bridge working late Thursday night. He did not notice anything unusual when he left the bridge shortly before 11:30pm Thursday (August 18). He was working on the east structure auxiliary generator disconnect. He heard a vehicle on the east structure lower deck while he was working, but he didn’t see anybody. The electrical technician called Olympic Radio during his work to inform them he was performing generator tests that would produce bridge status alarms through the alarm dispatch PC (personal computer). He remembers leaving the bridge between 11:15pm to 11:20pm.

Interviews determined the drive motors were in a locked rotor condition for approximately 2 hours.

WSDOT Bridge Preservation electrical engineers arrived on site Friday August 19. They switched the key switch on the east structure primary PLC processor from halt to run mode and noticed most, if not all, output module lights on. The primary PLC was the operating PLC at that time. They connected the laptop programming terminal to view the control program online. They noticed that all software based output coils were forced on. They also noticed the force indicating light on the processor module was not on or blinking. The engineers selected a command to clear all forces, and the output module lights went to a normal state. Most were now off instead of on. The force indicating light normally blinks when a force is entered by the programming terminal. This force light was later tested to verify it was working. It was tested by forcing a single output on, and was working correctly.

The manufacturer was asked to furnish details for the operation of the force indicating light. The original equipment documentation, Square-D Instruction Bulletin 30598-105-03, states clearly that control register address 8186 bit 5 controls the force indicating light. It also states this bit cannot be altered by any means. A copy of Instruction Bulletin 30598-105-03, page 35, is shown in Figure 3. It has not been determined how or why the forced light was not on or blinking while all of the output coils in the PLC program were forced to the on state. Had the forces been deliberately placed using the programming terminal, the force indicating light would have been on or blinking.

Bridge Conditions

The east and west structure control systems communicate using PLC modems and serial communications. The modems communicate between the east and west control towers using wireless transceivers. A dedicated telephone line is used as a backup.

The PLC communications were using the wireless transceivers when the fault occurred. East and west PLC control systems were energized and the PLC communications system was energized. This is the normal state even when there are no bridge operations. The PLC output module power for the east control system has no provisions to be easily de-energized and is therefore normally kept energized.

PLC Equipment

A complete inventory of the PLC modules was made and the fault conditions summarized by the PLC manufacturer's representative for Schneider Electric, Telemecanique Automation Services. The system components are obsolete and no longer supported by the manufacturer. Some modules are available from third parties and some may be repaired or serviced in special cases.

The Local Interface modules (LI) CRM-210 were found to be old revisions. The LI modules communicate PLC commands to the I/O. The most current revision for this module is level O, but the level O module is not compatible with the balance of the installed PLC system according to the manufacturer's representative to Modicon/Schneider Electric, Telemecanique Automation Services. The most current compatible revision for the LI module is level N. The revision for one of the installed LI modules was revision level H and the other level N1. The LI module with revision level H was installed in the rack with the primary PLC processor which was in control at the time of the fault.

Discussions with PLC representatives and their company associates raised the possibility that the LI level H modules may have been defective. Subsequent revision to the module may have corrected the defects when they were last produced over ten years ago. The SyMax Equipment Survey report by the representative recommended the CRM-210 revision level H module be removed from service immediately. Refer to Table 1 for the SyMax Equipment Survey report.

There have been no conclusive reports, service notes, recall notifications, or written history about LI module defects or failures from the manufacturer. Further discussion with the PLC representative and his company associates led to discovery of a somewhat similar CRM-210 LI fault at a different facility. The fault was caused by a power surge and resulted in the PLC outputs cycling on and off. It is not known if the PLC system had any UPS or power filters. The PLC processor was damaged by the power surge and was replaced. The CRM-210 LI module appeared to be functional at first. When the system was energized with a new processor, the outputs cycled on and off continuously. Replacing the LI module corrected the fault at the facility.

The CRM-210 LI modules have image tables for I/O commands that are independent of the PLC processor. The image tables represent the state RAM (random access memory) associated with the register bits that control the I/O status. Thus, on/off commands for the PLC outputs are ultimately controlled by the CRM-210 modules. Commands include freezing the outputs in the last state and resetting the output states. It is conceivable that a fault in a CRM-210 module could result in energizing all of the PLC system outputs. Refer to Figure 4: Square-D Instruction Bulletin 30598-247-03, page 9.

As part of the on site investigation the week of September 5, the WSDOT electrical engineer erased the PLC processor memory in the primary PLC. He loaded the current file copy of the program into the primary processor and energized the PLC control system. The program memory in the backup processor was not disturbed. The system started up and appeared to be functional. All I/O modules including the reed relay and triac output modules appeared to be functional. The primary to backup transfer was tested and operated successfully. The size and rung count of the program loaded into the primary processor was noted to be the same as that residing in the backup processor. Before it was erased and reloaded, the size and rung count of the program residing in the primary processor was noted to be the same as the program residing in the backup processor and the same as the file copy program.

Wireless Communications

The serial communications between the east and west structure PLC systems uses wireless transceivers and a hardwired telephone line for a backup. The communication system architecture cannot be discussed in more detail due to security concerns.

The system was operating on the wireless transceivers when the fault occurred. The PLC and communication systems are normally kept energized even while the bridge is not operating. This is a typical practice for control systems. Two wireless communication technical experts from independent companies inspected the wireless communication system. All components were found to be functional. Several tests were conducted to induce a communications failure and duplicate the fault. Power was cycled and cables were connected and disconnected, but the communications was restored successfully each time with no faults.

The experts found no reasons to suspect the control system fault could have originated with the wireless modem communication system.

Motor/Generators

The main drive motors for the east structure are 125V d.c., 40 hp motors. There are four drive motors. The motors are connected to provide two operating pairs, or loops, having their armature windings in series. A d.c. generator providing 75kW, 250V d.c. and 300 amps energizes each drive loop. Generator output voltage is varied using an electronic static exciter for the generator field. The variable voltage provides for variable drive motor speeds. There is a west loop (1E) and an east loop (2E). Each of the two d.c. generators is run by a 480V a.c., 3-phase induction motor rated at 100 hp.

The control system fault energized all PLC outputs commanding the drive motors to run, the end locks to release, the brakes to release, the traffic gate to operate, and the advanced flashing warning lights and flashing traffic lights to operate. The bridge center locks (longitudinal locks) that hold the east and west structures together did not release because they are controlled by the independent west control system.

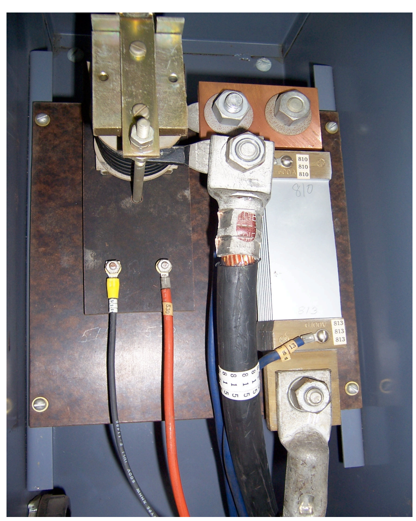
The main drive motors were therefore running in a locked rotor condition for approximately two hours. Destructive overheating resulted. The main drive motors for the bridge were removed at the time of this investigation. It was reported that the north west drive motor was not as extensively damaged as the other three. However, all motors, including the spare motor, were sent to a local motor shop to be refurbished.

When the PLC system was added to the east structure in 1985, the hardwired interlocks for the motors were moved to the PLC control program. This included the control of the drive motor contactors and the overcurrent protection relay controls. It is not certain the overcurrent relay activated during the fault; but even if it did, the motor contactors would not have opened to protect the motors because the PLC outputs controlling the contactors were forced on.

The motor overcurrent protection relays are circa 1960's style relays. The relays are a Square-D model SJ-8542 and are now obsolete. The relay coil is directly in line (series) with the motor armature circuit. As the current increases to a trip point, the magnetic coil pulls against the calibration spring and opens a set of normally closed contacts. The relay is automatically reset when the current drops below the trip point. Refer to Photograph 4.

When the damaged drive motors were repaired, they were reinstalled. This occurred after the initial on site investigation. WSDOT engineering and maintenance personnel observed these overcurrent relays operate while commissioning the rewound and refurbished drive motors. Operating trip currents for the relays were reported to be approximately 600 amps, but exact measurements were not obtained.

Originally, each overcurrent relay contact was hardwired to the motor contactor to complete a control circuit and energized the motor contactor to start the motor. Opening the overcurrent relay contacts de-energized the motor contactors and stopped the motors. With the PLC controlling the motor contactor when the fault occurred, the PLC output stayed energized and defeated the overcurrent relay. Direct replacements for the overcurrent relay with an automatic reset are available.



Photograph 4: 1E (West Loop) D.C. Overcurrent Relay (E-C75-E)
Square D Model SJ 8542 w/ Calibrated Shunt

The motor generator sets were tested to determine if they were suitable for continued service. The a.c. motors were acceptable for continued service. The 1E (west loop) generator showed a very low insulation resistance between the fields and the generator housing. The value was 0.2 mega ohms where values over 10 mega ohms were expected. The generator showed low insulation resistances between the armature and housing, and between the interpoles and housing.

The 2E (east loop) generator showed an extremely low insulation resistance between the armature and the generator housing. The value was 0.02 mega ohms where values over 10 meg ohms were expected. The generator showed low insulation resistances between the fields and housing, and between the interpoles and housing. Generator commutators also showed signs of minor overheating due to overloading. The d.c. generators were not acceptable for continued service. The main drive motor contactor contacts were deeply pitted due to overloading and opening under overload conditions.

Operational Testing

Since the main drive motors were destroyed, the east structure draw span could not be operated. The d.c. generators were not operated or load tested on the bridge because of their low insulation resistances.

The PLC system was cycled on and off several times from the UPS and locally in the PLC cabinet. The PLC halt key switch was cycled several times from the run to the halt position. Following each test, the PLC system started up and appeared to be functional. There were no error or fault diagnostic lights lit on any modules, and the I/O module channels were functional. The failover from the primary to the backup PLC was functional.

The east traffic gate and traffic signals were successfully operated from the west control console using the PLC system and the wireless modem.

Conclusions

A control system fault caused PLC outputs to energize without operator commands and without operators present. Electrical equipment, including motors, was energized and operating as a result. The drive motors were in a locked rotor condition for an extended period, destroying them. There were no PLC module failures identified. The PLC control system was reset by clearing all forced points. Later, the program was reloaded and system power was cycled off and then on. The PLC operations were tested and appeared to be functional.

The cause of the fault could not be repeated, isolated, or conclusively identified. It was more likely caused by equipment failure (hardware or firmware) than by a software failure. Direct human intervention was not the cause. It is possible that events leading up to the fault, such as testing the auxiliary generator or power surges and outages, may have caused, or contributed to, the fault. It may be possible for a power surge to have this effect even with good power filtration and a UPS for surge protection. A power surge could enter the system components through the input power feed, or back feed through the non-isolated output modules. There is one documented case from the manufacturer of a somewhat similar fault being caused by a power surge. Although, there were not enough details of the case to be conclusive. Poor quality control system grounding may also be a contribution factor.

One suspected cause of the failure is a Square-D communications module CRM-210. CRM-210 LI modules have image tables for I/O commands that are independent of the PLC processor. It is conceivable that a fault in a CRM-210 module could result in energizing all of the PLC system outputs.

A CRM-210 module with a revision level H was located in the primary PLC processor rack. When the fault occurred, the primary processor and this CRM-210 module were in control. The most current revision made was level O before Square-D stopped making them many years ago (late 1980s). Revision level N is the most current revision made that is compatible with the installed PLC system. It is possible the revision level H modules were recalled by Square-D in the 1980s, although this cannot be verified since the manufacturer no longer has these records. All of the PLC modules for the east structure bridge control system were checked for revisions levels. Many of the modules in use are old revision levels and most of the equipment is obsolete.

The PLC control system architecture design is deficient. There are no external hardwired watchdog timer circuits monitoring the PLC system health. The PLC output power bus is not interrupted with an emergency stop switch or a master control relay. The d.c. drive motor overcurrent relay contacts are connected through the PLC and are not hardwired to the motor contactors. This configuration essentially bypasses the overcurrent protection.

The d.c. drive motor overcurrent relays are very old (early 1960s). After equipment repairs were completed, WSDOT engineering and maintenance personnel observed the overcurrent relays operate while commissioning the replacement drive motors. The PLC system, when installed in 1985, replaced most of the hardwired relay controls and interlocks with software based control logic. This includes control of the overcurrent relay that should have remained hardwired to the motor contactors.

The east traffic gate and traffic signals were functionally tested and appeared to be operational. The appearance of a successful operation does not preclude the possibility of latent mechanical or electrical damage.

The east structure was returned to service November 2005, approximately 10 weeks after the fault occurred. There have been no further reports of control system failures or faults during the nine months since equipment upgrades and repairs were completed. Inspections of other movable bridge control systems is warranted where similar equipment is in service and where there may be the absence of an adequate fail-safe control configuration.

Recommendations Considered

1. Maintain the practice of keeping all east half motor circuit breakers open until a bridge operation is needed. Since the east half was not operational at the time, this would apply to the traffic gate and end locks. Once the drive motors were replaced their circuits should also be kept opened. When the east half was made operational, the practice of opening all motor circuits should be maintained until the east structure control system was reconfigured to be fail-safe. A replacement of the PLC control system or the wireless communication system was not recommended at this time since the entire east structure is scheduled for replacement.

2. Redesign and reconfigure the east structure control system to be fail-safe, and fault tolerant to the greatest extent practical.

    a. The PLC controls need external hardwired watchdog circuits monitoring the PLC system health.
        1. Option 1- provide external watchdog timers to protect against most PLC fault modes including unintended forced inputs and outputs.
        2. Option 2- provide external watchdog relays and to protect against unintended forced outputs only.

b. The PLC output module power bus must be independently controlled and interrupted with an emergency stop switch and a master control relay. These are provided for with each watchdog circuit considered in Options 1 and 2.

c. The overcurrent protective relay and motor contactor controls must be removed from the PLC and replaced with hardwired circuits.

d. The overcurrent relays can be automatically resetting; but, there must be a circuit added to prevent a motor from restarting until given a command by the bridge operator following an overcurrent trip.

e. Reconfigure the east traffic gate circuit to insure the gate will be driven "UP" and not "DOWN" should this fault occur again. With the Option 1 watchdog timer and master control relay circuit, there is a short period when a fault could result in lowering the gate unintentionally. This period would be the few seconds while the PLC first boots up when initially energized, and the two seconds needed to activate the master control relay from the watchdog timer. This is not a concern with the Option 2 watchdog circuit because it has no time delay.

   A very simple circuit can insure the gate will always be driven "UP" should this fault occur again. Connect a relay directly to the PLC "UP" demand contact. Use a normally closed contact from this relay and connect it in series with the "DOWN" starter coil. Whenever the PLC demands an "UP" operation, the "DOWN" starter will be disconnected from the circuit.

3. Field Testing:

   a. Test PLC triac output modules to verify all channels are functional.

   b. A root cause analysis performed by the manufacturer was considered for the primary PLC processor, backup PLC processor, and CRM-210 modules. The manufacturer was not able to perform a root cause analysis for this obsolete equipment.

4. Three CRM-210 revision level N modules were located for sale through the local distributor. It was recommended that WSDOT purchase two of these modules, one to install and one for a spare.

5. Refurbish both motor drive generators in a motor shop.

6. Refurbish and rewind the four drive motors in a motor shop.

7. The d.c. drive motor overcurrent relays should be sent to an electrical shop to be tested. Testing should include insulation resistance (megger), and load testing. The existing overcurrent relays could be put back into operation if they pass the load test, but should be removed from the PLC. If they do not pass the load test, fuses should be considered to protect the motors from high current until replacements or alternatives are found.

   As an alternative, the overcurrent relays may be calibrated in the field by a trained d.c. motor technician. Near overcurrent conditions can be momentarily attained when first starting a bridge operation. The relay can be set just above the normal starting current needed to move the draw pontoon.

The generator exciters, Saber 3200 d.c. drives should be refurbished in an electronics shop to replace the original electrolytic capacitors. Before this was done, spares should be located since there are only two installed exciters on the bridge with no spares or spare cards.

8. Clean or replace all motor contactor and starter contacts including the east traffic gate.
9. The east traffic gate should be inspected in detail for mechanical or electrical damage. The gate was reported to be continually operating for an extended period driving the arm to the "UP" position, resetting itself mechanically, and then driving again. The fully up limit switch should be hardwired in the motor starter circuit to prevent the "UP" operation after the gate is already up.

Corrective Actions

Redesign of the Control System

Given the cost involved in redesigning the east half control system, the fact that the new east half of the bridge is under construction and will be installed within the next 3 years, the fact that replacement of the CRM-210 has most probably resolved the immediate cause of the control system fault, and the fact that the practice of keeping all east half motor circuit breakers open until a bridge opening is called for, WSDOT has elected not to proceed with an interim redesign of the control system to be more fail-safe and fault tolerant.

PLC Equipment

The CRM-210 Local Interface module which was found to be revision level H was replaced with a revision level N module and the PLC is operational at this time.

WSDOT engineering and maintenance personnel determined all PLC triac output module channels are functional.

D.C. Drive Motors

The four 40 horsepower d.c. drive motors which where subjected to the lock rotor overcurrent were completely refurbished and rewound. This consisted of three motors that were original equipment on the bridge and a fourth "spare" motor which had been installed in place of the fourth original motor which was malfunctioning prior to the control system fault. The fourth original motor was steam cleaned, reinsulated and refurbished. The three rewound original motors and the refurbished original motor were reinstalled and are in operation at this time. The "spare" motor was returned to storage.

MG Sets

The two 75 kW d.c. generators were steam cleaned, reinsulated, refurbished and reinstalled and are in operation at this time.

WSDOT engineering and maintenance personnel observed the overcurrent relays to operate while commissioning the replacement drive motors. Operating trip currents for the relays were reported to be approximately 600 amps, but exact measurements were not obtained.

Generator Exciter Drives

The two Saber 3200 drives were sent to a shop for refurbishment. They were reinstalled and are in operation at this time.

Motor Contactors

The contacts on the motor starters and contactors have been cleaned and are operating properly.

East Half Traffic Gate

WSDOT engineering and maintenance personnel verified there was no electrical damage to the east traffic gate.

Telemecanique Automation Services a brand of Schneider Electric

The following list contains the results of our on site information gathering efforts as well as current service status and pricing for each module.

Qty.	Class	Type	Series	Current Series	Purchase Price	Exchange Price	Repair Price	Note:
1	8020	SCP-522	K	M	N/A	N/A	N/A	1
1	8020	SCP-523	M	M	N/A	N/A	N/A	1
3	8030	CIM-101	A	N/A	N/A	N/A	N/A	2
3	8030	COM-221	B	N/A	N/A	N/A	N/A	1
8	8030	COM-271	B	N/A	N/A	N/A	N/A	2
2	8030	CRM-210	1 ea. H, 1 ea. N 1	O	$ 1,643.00	$ 859.71	$ 658.79	
8	8030	CRM-220	3 ea. A, 1 ea. C, 2 ea. D, 1 ea. E, 1 ea. F	F	N/A	N/A	N/A	2
1	8030	CRM-222	C	F	$ 788.00	$ 412.01	$ 346.85	
2	8030	CRM-510	E	I (rev. 5.00)	$ 2,626.00	$ 1,373.57	$ 1,055.19	
2	8030	DOM-225	B	N/A	N/A	N/A	$ 323.20	3
32	8030	GOM-231	A	N/A	N/A	N/A	$ 323.20	3
8	8030	GRK-210	B	N/A	N/A	N/A	N/A	1
16	8030	HIM-101	B	D	$ 286.00	(see note)	N/A	4
1	8030	HRK-200	B	E 1	$ 1,289.00	$ 674.41	N/A	
3	8030	PS-30	C	N/A	N/A	N/A	N/A	1
4	8030	RIM-121	B	F	$ 1,690.00	$ 883.87	$ 679.06	
1	8030	RIM-131	A	C	$ 1,398.00	$ 731.38	$ 615.99	
3	8030	ROM-121	B	E	$ 2,047.00	$ 1,070.89	$ 822.08	
2	8030	RRK-100	B	E 1	$ 685.00	$ 358.50	$ 323.20	

Notes:

1. Available for service and purchase only on a case by case basis. Contact local Service / Sales office for assistance.
2. Obsolete item, no service or sales available.
3. Repair only, available for purchase only on a case by case basis. Contact local Service / Sales office for assistance.
4. Repair not offered. Exchanged only if the unit is in warranty. If it is out of warranty a new unit must be purchased.

As is seen in the table above a large percentage of the modules listed are either obsolete or in a service only status. This system has nearly reached the extent of our ability to provide continued service.

D-4

Table 1: Symax Equipment Survey Report

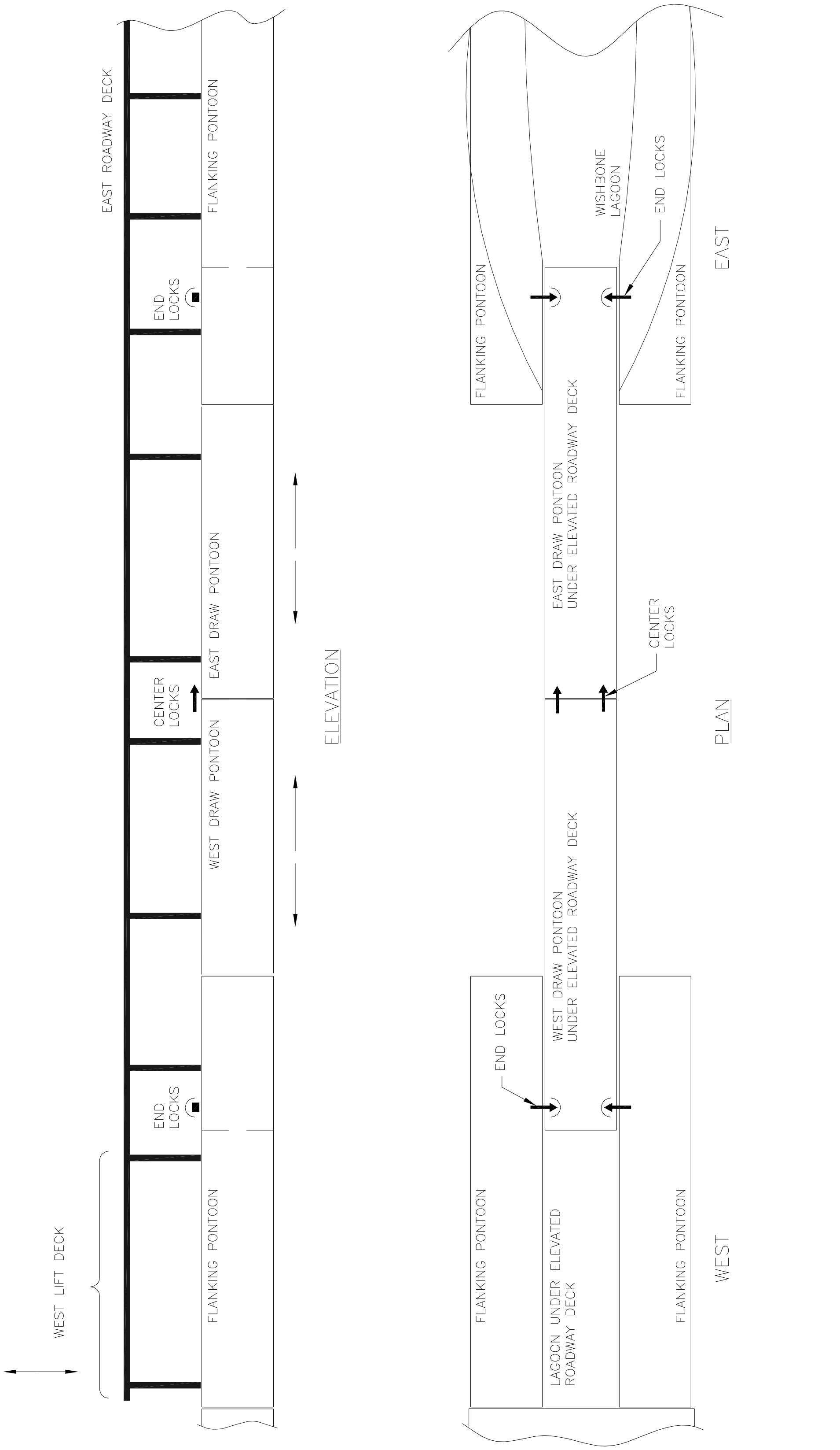
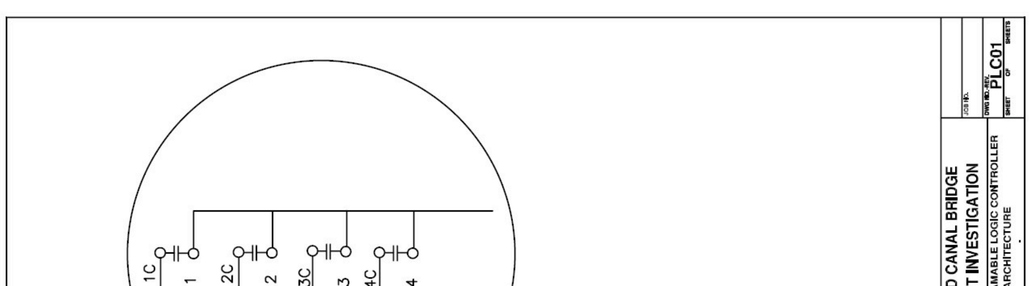


FIGURE 1: HOOD CANAL BRIDGE



CONTROL REGISTER ADDRESS	DESCRIPTION
8186	The individual bits of this register are used for "flagging" certain processor conditions. These bits can be examined but cannot be altered by any means. **8186-1** The HALT/RUN status of the processor is represented by this BIT. 1=HALT (Processor Halt light flashing), 0=RUN or DISABLE OUTPUTS. **8186-2** This BIT is energized when the processor is scanning the user program but the outputs are disabled. 1=DISABLE OUTPUT (Processor Run light flashing), 0=HALT or RUN. **8186-3** When this BIT is energized, this indicates that the processor is in the RUN mode. 1=RUN (Processor Run light on steady), 0=HALT or DISABLE OUTPUTS. **8186-4** When this BIT is energized, this indicates that an error has been detected in user memory (Memory light on), 0=Memory light OFF, 1=Memory light ON. **8186-5** This BIT is energized when some device is forcing inputs or outputs on or off through either the PROGRAMMER port or COMM port (Force light on or flashing), 0=No Forcing, 1=Forcing. **8186-6** After the processor sends update status to an output or internal register, it reads that status to insure a proper transmission. This BIT is energized when the data read from an output or register does not match the data written into it (i.e. read after write error). 1=Read after write error (I/O error light on), 0= Transmission valid. **8186-7** This BIT represents the physical status of the processor keyswitch and will be energized when the keyswitch is in the HALT position. 1=Keyswitch in HALT, 0=Keyswitch not in HALT. **8186-8** This BIT represents the physical status of the processor keyswitch and will be energized when the keyswitch is in the DISABLE OUTPUTS position. 1=Keyswitch in DISABLE OUTPUTS, 0=Keyswitch not in DISABLE OUTPUTS. [Note: The remaining BITS in register 8186 are reserved for internal use by the processor.]
8187	This register contains the number of rungs entered into memory by the user.
8188	The number contained in this register represents the processor type and firmware revision. The three most significant digits represent the Type number (refer to paragraph 6.0) and the least significant digit represents the firmware revision. Example: A Model 500 version 2K RAM processor with firmware revision number 7 would have the number 5217 in this register.
8189-8190	These registers contain the memory size (in bytes). Bits 9 through 16 of 8189 contain the number of bytes per word defined for the processor.
8191-8192	Memory used (in bytes).

14.0 — ADVANCED INSTRUCTION SET

14.1 Introduction

This appendix provides a brief summary of the advanced instruction set that is supported by the Model 500 processor. An introduction as well as a general description of each instruction exclusive to the Model 500 processor is provided. These advanced instruction capabilities include: matrix operations, scan control, and the immediate communication update function. Also included is a description of the operation of the Model 500's asynchronous (FIFO) shift register instruction which differs slightly from that of the Model 300 processor.

14.2 Matrix LET Instructions

A matrix is defined as a group of consecutive registers. The general format of a matrix LET instruction is shown in Figure 14.1. A matrix LET instruction can contain a matrix on one or both sides of the equal sign.

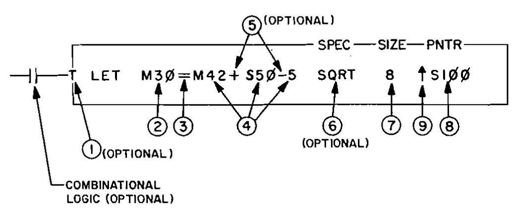


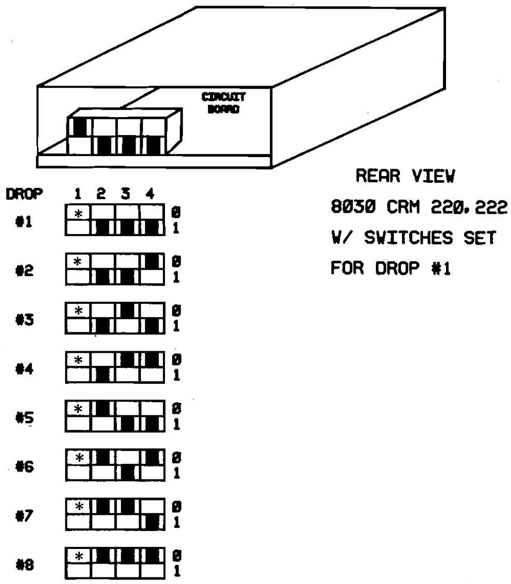
Figure 14.1 — Matrix LET Instruction

The matrix LET instruction is programmed as a horizontal box with the word LET as the first entry in the box. The other entries appearing in the LET box are explained as follows:

1. If desired, a matrix LET operation can be programmed to be transitional (operate only once on each open to closed transition of the preceding combinational logic). If the LET operation is **not** transitional, the operation will be performed on each scan of processor memory (assuming the preceding combinational logic is closed).

Figure 3: Symax Instruction Bulletin

Set the switches for the appropriate drop as shown in Figure 3.5 - RI switch settings.



*For each channel, the drop (RI module) farthest from the LI must have switch 1 set ON, to a (1). Only one drop per channel requires this switch to be set. Failure to do so may result in a noise susceptible communications link.

Figure 3.5 - RI Switch Settings

Label terminology may vary. The following equivalent terms are used:

0	O	UP	OPEN	OFF
1	X	DOWN	CLOSED	ON

Either one of these labels will be located on the side of the RI module.

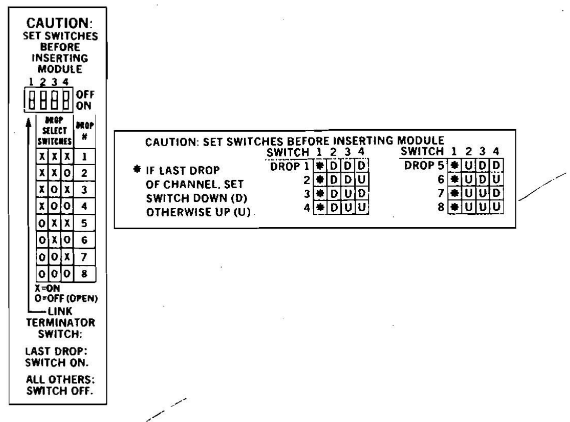


Figure 3.6 - RI Module Labels

4.0 OPERATION

4.1 General Description

Local and remote interface modules allow a programmable controller to communicate with remote I/O (digital and register input and output type devices).

The LI/RI interface system consists of:
1. A local interface module (LI) which plugs into a register slot of the rack containing the CPU.
2. A remote interface module (RI) placed in the CPU slot of a digital I/O rack or the first slot of a register rack.
3. An interconnecting cable between the LI and RI(s) consisting of dual twisted shielded pair.

Both the LI and RI modules have diagnostic LED's indicating the status of the communication link, individual drop operation and module operation.

The local/remote I/O interface system is a high speed serial, multi-channel, multi-drop system. The local interface (LI) receives instructions from the CPU. The LI then serializes this information and transmits it to the appropriate remote interface (RI). An LI module does this over either of its two independent communication channels. Each channel operates full duplex at a rate of 31.25K baud.

E-5

The RI interprets this data, verifies and acknowledges it and then acts accordingly. The information being exchanged is stored in an image table located in each LI and RI.

The continuous exchange of information between the LI and RI image tables is independent of the CPU scan. Transmitted information includes ON/OFF commands for I/O as well as storage register information and housekeeping functions (i.e. loss of communications, error control, freeze or reset of I/O).

The LI module stores control register information while the RI maintains its own specific drop information. This information (user programmable bits) defines the action to be taken in the event of a fault at any drop. It can allow the operational drops to keep running or to shutdown. The shutdown state of the outputs will then be either a reset (OFF) or freeze (last state) condition.

Actual programming steps are described in the programming equipment instruction bulletins. For details on user programmable bits, refer to Appendix D, LI Control/Status Registers.

4.2 Local Interface Registers

Two versions of the LI module are available. The first, Class 8030 Type CRM-210, has 512* registers; and the second,

Figure 4: Square-D Instruction Bulletin