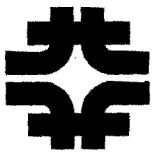

Fermi National Accelerator Laboratory

Dzero General Support

The Use of Programmable Logic Controllers (PLCS) at Dzero

D0 Engineering Note 3823-000-EN-527

5/5/2000

R. Hance

Fermilab

15 December, 1999
Submitted 14 January, 2000

To: John Cooper
From: Richard D. Hance
Subject: The Use of Programmable Logic Controllers (PLCs) at Dzero

This memo is in response to your request to Hugh Montgomery for a "Summary of the use of APACs and other PLCs at Dzero".

There are no "APACs" PLCs in use at Dzero. However, there are other brands of PLCs being used in various functions. These functions are as follows:

1. Pyrotronics Fire Protection System.
2. Operator control and monitoring of heating, ventilation, and air conditioning (HVAC).
3. Operator control and monitoring of cryogenic delivery systems,
4. Operator control and monitoring of the superconducting solenoid energization system.
5. Monitoring of oxygen sensors for Oxygen Deficiency Hazard (ODH) conditions.
6. Monitoring of the electrical power system.
7. Control of the Hi-bay lighting.
8. Monitoring of "freeze alarm" sensors on pipes under the portakamps.
9. Various "consumer applications" i.e. bottled water dispenser, etc.

Regarding "fail safe operation":

None of these systems except for the Pyrotronics Fire Protection System (and one related exception) rely on PLCs for safety to personnel or protection of property. Traditional "fail safe" methods are used as the primary defense against "incidents". The Pyrotronics system is of course rated for such service, and is maintained by the Fire Protection Group of the Facility Engineering Service (FESS). Dzero personnel do not have access to its programming. However, there is a common link involving personnel safety between the Pyrotronics system and the uncertified HVAC system (see items 1 and 2). Brief discussions of the various systems are provided below. The discussions are indexed to the functions involving PLCs noted above.

1. The Pyrotronics fire protection system monitors smoke detectors in the fixed and moving counting houses; and in the air ducts in the building HVAC system. It also monitors flow switches in the building sprinkler system (in order to sense activated sprinklers). Its outputs include alarm horns, halon discharge systems, door releases; and Fire and Utility System (FIRUS) contacts to summon the Fire Department if necessary. This system also provides a signal to the HVAC system in case of smoke in the ventilation ducts so that the HVAC system can selectively turn off its fans to avoid spreading the smoke through the ventilation ducts. However, the HVAC system is NOT designed,

validated and maintained to life safety standards and thus perhaps should not be relied on to implement this function if indeed this function is desireable. This may require further anlysis to determine the impact on personnel safety. See also item 2.

2. Factory implemented discreet upper and lower temperature limit interlocks protect heaters and chillers in the HVAC system from extreme temperatures caused by component failure, etc. While this provides for equipment safety, there still remains a personnel safety issue regarding the possible spreading of smoke throughout the ventilation ducts. As was described above, this could happen in the event that the HVAC system would fail to shut off fans in response to a command from the Pyrotronics fire protection system due to smoke in a ventilation duct. See also item 1.
3. Appropriately rated discreet pressure relief valves are installed on all pressurized systems (cryo or otherwise) to protect against overpressurization caused by component failure, control failure, or inappropriate control operation. This proprietary system has been reviewed and approved by the Division Safety Committee. Barring an unknown design flaw, the cryo system is fail-safe.
4. A hardware interlock and quench detection system protects the solenoid from overvoltage, overcurrent, overtemperature at connections, and quenches caused by component failure, etc. This proprietary system has been reviewed and approved by the Division Safety Committee. Barring an unknown design flaw, the solenoid system is fail-safe.
5. ODH sensors are monitored by a PLC; but are not used to control fans for ODH protection. The sensors are for operator information only. An appropriately rated sump (argon system), and evacuation by continuously running exhaust fans (argon and helium systems) provide protection against oxygen deficiency hazards caused by component failure, etc. Barring an unknown design flaw, the ODH system is fail-safe.
6. The Dzero electrical power system is monitored; but not controlled by PLC. The system is protected by appropriately rated circuit breakers against overloads caused by component failure, etc.
7. Independent "emergency" battery powered light fixtures provide personnel safety in the event of a lighting system failure in the hi-bay. The hi-bay lighting is controlled by PLC in order to provide a timed sequence to the shutdown of lighting in the evening; and to share "night light" duty among the banks of light fixtures.
8. The portakamp "freeze alarm system" hardly warrants mentioning since the only user programmable parameters are the number of channels and the alarm setpoints. It is comprised of a commercial device with a dedicated, pre-programmed PLC. One is located in each portakamp. The device monitors sensors mounted on the water pipes under the portakamps. The water pipes are protected from freezing by automatic heat tapes. However, if one of these tapes should fail and the temperature of the pipe approaches freezing, then the PLC will provide a signal to FIRUS and building maintenance personnel will be notified. The PLC provides no control and acts only in an advisory capacity.
9. The consumer applications of PLCs at Dzero are mentioned here only as a reminder that they do in fact exist. They appear in all sorts or applications that can effect personnel or property safety. A bottled water dispenser is cited above (the PLC controls water temperature). Another application is a PLC controlled ovens (presently in lab B and lab 3) that might be used to cure epoxy. An operator input or a PLC failure could overheat the sample and ruin it. Etc. etc.

Regarding "intrusion by unauthorized users":

Three of the systems, which are actually comprised of several PLCs, are in fact ultimately interconnected by ethernet and are accessible via Fermilab's wide area network (WAN) and hence the internet. They are therefore susceptible to intrusion by unauthorized users. The systems are as follows:

1. Operator control and monitoring of heating, ventilation, and air conditioning (HVAC).
2. Operator control and monitoring of cryogenic delivery systems,
3. Operator control and monitoring of the superconducting solenoid energization system.

The "front door" to all of these systems is software that runs on Windows NT workstations. The framework of the software is called "FIX" (Fully Integrated Control System) by Intellution. The specific user interface is called DMACS (Distributed Manufacturing and Control Software). This software has essentially four levels of protection as follows:

1. A user must possess a working version of the software.
2. A user must supply a hardware key (dongle) on his workstation to activate the software.
3. A user must gain access by supplying a valid password with control privileges for each function (cryo, HVAC or solenoid).
4. The software uses encryption techniques in its network data exchanges. Encryption precludes anyone from "sniffing" out passwords; or using simple "terminal emulator" programs to issue commands.

Nevertheless, an extremely knowledgeable person could conceivably "hack" into one or more of these three "front end" systems; or possibly directly into the ladder logic of a PLC. Our vulnerability however, appears to be primarily to operations and not to safety. For example:

If a hacker were to gain access to the cryo controls, he could not override hardware safety devices such as pressure relief valves. Thus, although he could seriously disrupt operations, he could not force the system into an unsafe mode of operation. For example, he could decrease the cryogen flow to the solenoid leads which could ultimately result in the solenoid quench detection circuitry turning off the solenoid and discharging it into its dump resistor.

If a hacker were to gain access to the solenoid controls, he could turn off the power supply and discharge the solenoid. He could not however, turn ON the power supply and CHARGE the solenoid unless all of the hardware interlocks were made up and the system was safe and ready to run. At the very minimum, the configuration locks on the power panels and the power supply must be manually removed by an authorized person. Furthermore, none of the solenoid interlocks can be overridden by high level DMACS commands, or by low level tampering with the PLC ladder logic. The PLC monitors the interlocks; but it can not control them. All interlocks are hardwired directly into the power supply and dump switch. It should also be noted that the solenoid system is hardware interlocked against operation beyond its designed current of 5000 Amps.

If a hacker were to gain access to the HVAC system, he could modify temperature setpoints and disable ventilation fans. However, he could not force any equipment to operate outside of safe parameters.

Conclusion

With the exception of control of HVAC ventilation fans, and their shutdown in the case of smoke in the ducts, all implementations of PLCs in Dzero have been made within the fundamental premise that no uncertified PLC apparatus shall be entrusted with the safety of equipment or personnel. Thus although PLCs are used to control and monitor all manner of intricate equipment, simple hardware interlocks and relief devices provide basic protection against component failure, control failure, or inappropriate control operation. Nevertheless, this report includes two observations as follows:

1. It may be prudent to reconfigure the link between the Pyrotronics system and the HVAC system such that the Pyrotronics system provides interlocks to the ventilation fans instead of control inputs to the uncertified HVAC PLCs. Although the Pyrotronics system is certified and maintained to life safety standards, the HVAC system is not. A hardware or software failure of the HVAC system probably should not be allowed to result in the situation where the ventilation fans in a smoke filled duct continue to operate. Dan Markley is investigating this matter.
2. It may also be prudent to examine the network security of those systems connected to the Fermilab WAN (HVAC, Cryo, and Solenoid Controls). Even though the impact of a successful hack might only be to operations, it might nevertheless be disruptive and could be expensive. The risks should perhaps be analyzed. One of the most attractive features of these systems, from a user's viewpoint, is their unlimited networking. The unlimited networking that makes the systems so convenient to legitimate access also makes them vulnerable to illegitimate access.

********** End of Report **********

Reviewers & Contributing Editors:

Gene Fisk
Mark Fitzpatrick
Marvin Johnson
Kurt Krempetz
Dan Markley
Hugh Montgomery
Russ Rucinski
Harry Weerts