

# A HIGH RELIABILITY CONTROL SYSTEM

J. Callahan, J. Collins, A. Qualls, IUCF, 2401 Milo B. Sampson Lane, Bloomington, IN 47408

W. Hunt, Indiana University Computer Science Dept., Bloomington, IN 47405

## Abstract

This paper describes part of an innovative control system developed for the Cooler Injector Synchrotron (CIS). This system achieved specifications oriented to accelerator applications which could not be met with commercial hardware and hence may be of interest to other laboratories. The system displays high levels of performance, reliability, maintainability, and repeatability. It is VME based and employs fiber optic data transmission for high noise rejection; actively redundant modules with automatic switch over for high reliability; and built in test and self diagnosis with centralized failure and system health monitoring for rapid maintenance. Several modules, designed and manufactured at IUCF, are described. This paper focuses on the Non-ramping Controls Subsystem.

## 1 OVERALL SYSTEM

There were four major goals which drove the CIS control system design: precision, repeatability, reliability, and maintainability. The overall system architecture was driven by the requirement for a precise control system. Electromagnetic Interference (EMI), which is intense in our environment, limits the precision of DACs and ADCs connected to power supplies over long copper cables. To combat this we designed the system as a fiber optic star network with the DACs and ADCs located near or in the power supplies themselves. (Figure 1). Locally, each DAC/ADC module has opto-isolation to avoid interaction among power supplies. The central computer, a DEC Alpha, drives two VME 6U communications crates located adjacent to the computer. The communications crates are populated with VMIC 5231M fiber optic (FO) communications modules which are linked to remote 3U and 6U crates by fiber optic cables. Each remote crate has a VMIC 5231S FO module which plugs into the local VME backplane. The remote crates can hold up to ten HI-REL DAC/ADC modules. Another consideration in providing precise control is to avoid interactions between power supplies. When DACs/ADCs controlling multiple power supplies have large common mode signals on the control lines, unwanted interactions between the supplies can result. To prevent this interaction, the DAC/ADC modules were designed with optically isolated data and a low capacitance power supply module which were also designed and manufactured at IUCF. This approach provides near total noise immunity (160dB @ 60 Hz) and permits highly accurate control of power supplies and other devices.

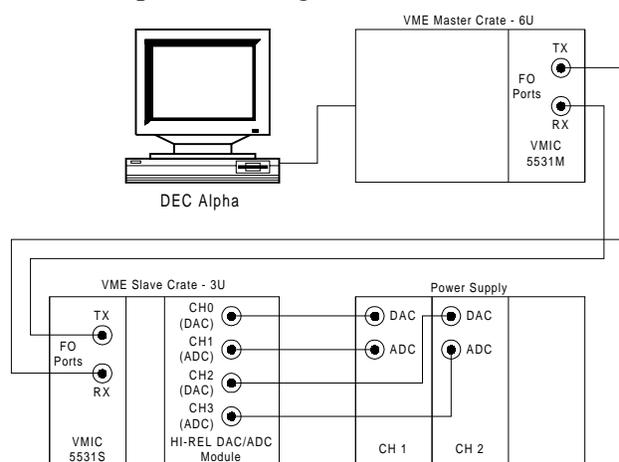


Figure 1 Beamline DAC/ADC - Overall System Design

## 2 REPEATABILITY

Repeatability refers to being able to reproduce runs, perhaps years later. We frequently run different energy levels and different particles and, historically, it has taken many hours to re-tune the cyclotrons and cooler after each energy/particle change. There are several reasons for this including magnet hysteresis, but a significant cause is drift in the DAC/ADCs and the power supplies, as well as calibration differences when DACs and power supplies are replaced after failures. There are two kinds of drift which are important here. One is temperature drift induced by changing temperatures, the other is long term drift induced by changes in component characteristics over time. Our DAC/ADC modules display 3 ppm/°C of temperature drift. To attain this level, at reasonable cost, we were forced to design our own DAC/ADCs. These modules operate by generating a ramp whose end points are tied to voltage references of great temperature stability (3 ppm/°C). The input and output voltages are then compared (Figure 2) to the ramp in order to set the output voltage (DAC) or measure the input voltage (ADC). A byproduct of this design is that the same channel can serve as either a DAC or an ADC depending on an external switch selection. The modules which we have produced have four channels which can be set to any combination of DAC or ADC (Figure 2).

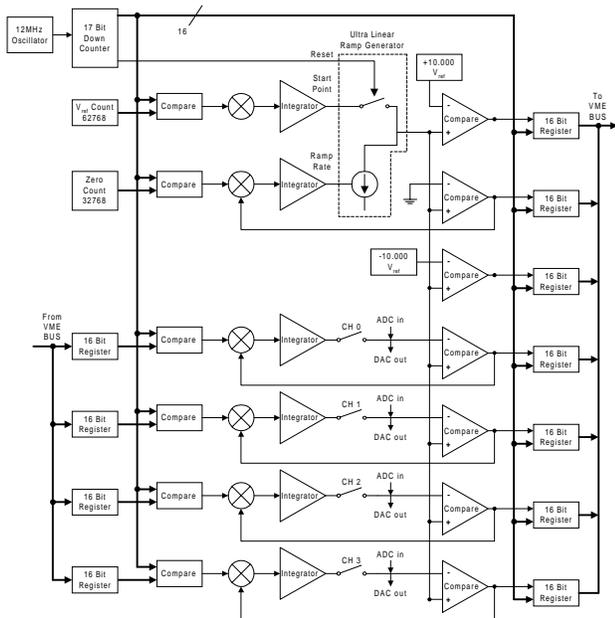


Figure 2 16 Bit, 4 Channel DAC/ADC Block Diagram

### 3 REDUNDANCY

To combat long term drift, we take advantage of a feature which was originally designed for reliability reasons, as will be described presently. Each DAC can be read back by the central computer and its output compared to its input, providing a direct measure of drift. If the DAC is in calibration, the computer examines the output of the power supply as measured by the ADC. If drift is detected here, we know that either the ADC or the power supply is in error, but not which. However, each power supply is controlled by two DAC/ADC modules in an actively redundant configuration. The central computer therefore has the ability to compare the output of two separate ADCs. If both agree, to within calibration accuracy, we know that the power supply has probably drifted or malfunctioned. If the ADC's differ, we know the problem is with the ADCs. If the problem is with the ADC, the central computer has the ability to switch the module to it's backup and the primary module can then be removed and repaired or recalibrated. This feature also permits us to automatically scan the system and determine that all DACs/ADCs and power supplies are functioning and are within specifications. A key requirement of this approach is to calibrate power supplies and DACs/ADCs which are nearing their calibration limits.

### 4 COMMUNICATIONS LINK

The communication modules which link the DAC/ADC modules to the main computer do not have automatic switch over. To protect against communications failure, the primary and backup DAC/ADC modules are located in different crates. A failure in the communications

module, backplane, or backplane power supply is detected by the module as a loss of communication. If the FPGA detects a loss of communications it switches to the backup module. The master communications modules at the main computer are also located in two separate 6U VME crates so that a failure of the primary crate results in a switch over of all primary modules to their backups. The only common point in the system is the Alpha computer itself which is not duplexed.

### 5 RELIABILITY

Another major design goal is reliability. Beam time is expensive. We wanted CIS to be highly reliable and we were also laying ground work for the proposed Light Ion Synchrotron and for possible medical applications of proton therapy which require high reliability. The first step in "reliability by design" is to insure that individual modules have as high a reliability as possible. Good design, careful component selection, and heavy parts derating yield a high reliability design. The next step is carefully controlled manufacture to insure that the design reliability is actually achieved. At IUUF, we developed an ISO9000 compliant production facility (as yet unaudited) with full Electrostatic Discharge (ESD) protection to produce these modules. We have had approximately 50 units in service for 9 months with no failures to date.

#### 5.1 MEAN TIME BETWEEN FAILURE (MTBF)

However, when large numbers of modules are used in a system, the overall system MTBF is additive and hence, can be quite low, even when the individual MTBFs are high. One of the best ways to improve system MTBF is to provide active redundancy. Active redundancy provides a back up module which takes over automatically when the primary module fails. What makes active redundancy so attractive is that the probability of failure of two devices, in a given interval, is the product of the individual failure rates. When those rates are low, the product is extremely low. If failures are detected immediately and the failed unit replaced quickly, the system MTBF can approach years. In CIS, critical devices are controlled by two DAC/ADC modules. The primary module is normally in control. The DAC/ADC module has a field programmable gate array (FPGA) designated the "health" FPGA which continuously monitors fourteen (14) parameters within the module. If these parameters go out of established ranges, a failure is detected. The primary DAC/ADC module then relinquishes control to the backup. The switch over occurs in less than a millisecond and will not usually be noticed by the controlled device at all. The failure information is sent to the main computer. The primary unit is also monitored by it's backup module via a "heartbeat" line. If the primary unit fails catastrophically or loses power, the back up unit takes over automatically. As mentioned previously, the main

computer can also direct a changeover to the backup module if the primary module drifts out of calibration.

### *5.2 MEAN TIME TO REPAIR (MTTR)*

Maintainability determines mean time to repair and consists of two components: diagnosis and repair time. Typically time spent diagnosing failures contributes 90% of MTTR. In order to minimize MTTR, we designed in a number of built in test features to facilitate diagnoses of problems. For active redundancy to be effective, it is necessary to detect failures and replace the offending module. The DAC/ADC modules report their health and primary/backup status to the main computer and display it on front panel LEDs. The failed unit can then be replaced. The modules have a “hot swap” capability which allows us to replace a failed module without turning off power to the crate. We expect an order of magnitude reduction of MTTR from approximately 3.1 hours to typically 15 minutes.

## **6 CONCLUSION**

The non-ramping control system displays high reliability and very low drift. Other portions of the CIS control system are described in other papers.