SAND2014-20304C

THE ANNULAR CORE RESEARCH REACTOR ROD CONTROL MODIFICATION PROJECT

Joshua Emmer, Patrick Snouffer, and Michael Black
Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185
jemmer@sandia.gov; psnouff@sandia.gov; mkblack@sanida.gov

ABSTRACT (Abstract Head)

The Annular Core Research Reactor (ACRR) at Sandia National Laboratories is a 2.4 MW steady state, 35,000 MW pulsing Research Reactor. In early 2013 there was an occurrence of outward rod motion of three control rods when an inward command was issued by the operator. The outward motion of the three rods resulted in a reactivity insertion of approximately $0.04. Other regulating rods were inserting considerable negative reactivity and the reactor remained well shutdown. This incident resulted in a five month shutdown period to allow two projects to progress in parallel: a Forensics Project to determine the cause of the un-commanded motion and a Rod Control Modification Project to design and implement an engineered solution to prevent further occurrences of uncontrolled outward regulating rod motion. Applying the results of the Forensics Project and a requirement to ensure more direct operator control over regulating rod motion, the Rod Control Modification Project developed a three part solution path. These solutions were divided into sub-projects; 1.0) Addition of an electronic relay between the motion controller and the rod drive motor; 2.0) Modification of the LabVIEW software to monitor rod motion; 3.0) Modification and improvement of the motion controller code. Subsequent to these projects, a Rod Control System Upgrade Project (RCSU) was initiated to provide a long term solution and an extensive upgrade to the ACRR Reactivity Control and Instrumentation and Control Systems. The RCSU project is currently progressing.

1 INTRODUCTION

The Annular Core Research Reactor (ACRR) is located at Sandia National Laboratories and is a modified TRIGA design. It is a pool type reactor with UO_2-BeO fuel arranged in a hexagonal grid. There is a 9” central cavity that provides a flat spectrum for large irradiation experiments. ACRR can perform prompt-critical operations (pulses and transient rod withdrawals) and steady state (SS) operations. There are 4 integrated safety systems; the Instrumentation & Control System (I&C), Reactivity Control System (RCS), Plant Protection System (PPS), and Wide Range System (WR). The RCS consists of 2 safety rods (SR), 6 control rods (CR), and 3 transient rods (TR) that are used to control the critical condition of the reactor. The RCS uses a Programmable Multi Axis Controller (PMAC) from Delta Tau to control rod motion.

There have been several rod motion events at the ACRR in the last 9 years for which the reactivity control system did not respond as expected by the Reactor Operator (RO). These events have cause ACRR to be shutdown for various time periods (days to weeks). This meant that stakeholder confidence in the system was slowly degrading. When another anomaly occurred in January 2013, the stakeholders requested ACRR shutdown until the cause of the anomaly was determined and a solution was implemented. The anomaly that caused this reaction occurred when the RO was performing an Auto-rundown (ARDN) command, expecting all the rods to move downward or stay at the bottom, when 3 CR moved from the bottom to 98 rod units (RUs) (~1cm) and inserted approximately $0.04 of reactivity. With

the other rods inserting considerable negative reactivity the reactor remained well shutdown. This was considered “uncommanded” rod motion and was unacceptable from the stakeholders.

Based on these events, an engineering change to the RCS was designed and implemented to give ACRR ROs more direct control over regulating rod motion as another means to prevent un-intended rod motion. This engineered solution is a combination of hardware and software modifictions.

2 PROJECT APPROACH

There were two projects that were initiated because of the control anomaly: a forensics project and a modification project. These projects were conducted in parallel and were both completed within 5 months of the anomaly.

2.1 Forensics and Cause

The forensics investigation consisted of a team of subject matter experts that reviewed the documentation and design of the system. The team included members of the operations, engineering, and safety basis departments as well as ACRR system experts and contractors external to Sandia National Laboratories. The goals of the team were to:

- Find the cause of the occurrence to the most precise location as possible.
- Communicate findings with engineering, operations, and other projects concerning this occurrence.

Initially it was not known what could have caused CRs 3, 4, and 5 to move out to exactly 98 RUs and stop. The hardware was studied to determine if it could have caused this precise movement. The SS PMAC controller is responsible for issuing drive commands, which includes independent step and direction signals, through the 8S cards (PMAC output cards) and Allen-Bradley enable relays to the NextStep micro-stepping amplifiers. The step and direction signals are amplified by the NextStep components and sent to the stepper motor. The stepper motor expects a precise, complex pulse train from the step signal, used to rotate the motor at a certain speed, and a positive or negative potential from the direction signal to determine whether to rotate clockwise or counter-clockwise. It is highly unlikely that a faulty ground or another type of wiring failure could have caused three rods to move to the exact same position and stop at the same time.

Review of RCS and I&C drawings did not uncover any hardware concerns which would only affect three of the six CRs. The 8S cards connect to two regulating rods per card, and the Allen-Bradley enable relays, NextStep micro-stepping amplifiers, and stepper motors only connect to one axis. There would have to be multiple hardware failures in these components in order to get three of the six control rods to move to the same location. Visual inspection of the Reactivity Control (RC) Bay cabinet did not find any issues with the wiring or hardware of the components.

RO error was also considered as a potential cause to the anomaly. However, there are no combinations of buttons that could be pressed by the RO to make three of the six CRs move at 98 RUs at the same time. To move only three CRs, the RO would have to individually shim each rod to the desired position.

Testing the ARDN sequence after the anomaly in various initiating states failed to reproduce the motion seen on January 7th. It was concluded with high confidence that the January 7th anomaly was not caused by hardware malfunction or operator error.

The team then began a thorough review of the motion controller code. Each bank of regulating rods has its own digital Programmable Logic Controller (PLC) where motion commands are issued based on logic, variables, and latches. Similar logic, including the ARDN routine, is used by each of PLCs to

control the motion of all rods. The first command issued for the ARDN sequence is a “go to 3600” command. This commands a rod to go to 3600 encoder units, 98 RUs, regardless of whether the rod is above or below that position. Immediately following the “go to” command is a check to see if the rod is below 101 RUs. If the rod is below 101 RUs, the PLC issues a “stop”, “slow down”, and “go down” command sequence. If a rod starts below 101 RUs when ARDN is initiated, it will be issued the commands “go to 3600”, “stop”, “slow down”, and “go down” in a single scan of the PLC. The PLC code appears to assume all of the regulating rods are above 100 RUs when ARDN is initiated since it commands rods to “go to 3600” before checking to see if the rods are below 101 RUs. This is strengthened by the fact that the comment next to this command says “start moving down”. The purpose of this specific section of code is to slow the rods to a stop as they pass 101 RUs before stopping at the bottom of the core.

To determine if the code would in fact allow three rods to move up to 98 RUs and stop under certain conditions, a test was conducted where latches for the ARDN routine were set manually to not allow the “stop, slow down, down” section of the code to execute. This test was able to recreate the anomaly and CRs 3, 4, 5 drove to 98 RUs and stopped when ARDN was initiated. This test proved that the January 7th occurrence could have happened if some of the commands in the ARDN sequence were lost or not issued. Specifically, if three variables were flipped in memory the anomaly would result.

The PMAC manuals were reviewed to determine if it was possible to lose commands issued from the PLCs. This review uncovered statements that suggest commands could appear to be reordered or not executed at all. The ARDN sequence is the most taxing on the controller – moving all rods at once. The literature revealed that it is possible to overflow the execution buffer if commands are sent too quickly. If this overflow occurs, the controller will drop commands. Once the command queue is open, new commands will be executed per the PLC code; however the dropped commands will be lost. Additional offline testing was able to show that issuing commands too quickly causes buffer overload and will result in lost commands. As coded, control rod commands are issued with CR3, CR4, and CR5 at the end of the sequence. Additional code review found unlatched stop commands, issued every cycle and filling the buffer.

The testing and manual reviews show that a buffer overflow in the SS PMAC is a plausible cause for the January 7th anomaly. The Forensics Team provided suggestions for code improvement to the integrated project team.

2.2 Overview of Modification Project

The modification project team was assembled at the initiation of the project with membership consisting of ACRR reactor operators, engineering, safety basis, subject matter experts, and integrated work management. The goal of the team was to design and implement an engineered solution using established engineering and safety basis processes to provide a more direct method of controlling regulating rod motion, consider software changes that will improve the reliability of the reactivity control system, and ensuring that system changes are properly reflected by configuration management. Project deliverables included a fully tested modification to the RCS, changes and updates to configuration documents, and updated operational procedures. The management expectation for this project was to seek a predominately “analog” solution to help insure that a PMAC upset within the RCS cannot cause an unintended increase in reactivity that is unsafe. Management’s specific direction was for direct reactor operator control over PMAC motion with an independent check of rod drive speed and direction.

The modification project team assembled several times to brainstorm possible solutions in alignment with the management expectations. Several options presented by the team were considered to be feasible. Hardware modifications that involved unique or custom built components (like custom printed circuit boards) were considered less desirable because of the time involved to develop and test these components. Software modifications within PMAC and LabVIEW codes were identified to correct deficiencies that

had been recently identified and to align with safety software best practices. The project team developed a solution matrix that considered the technical options and project goals, and proposed an engineered solution that is a combination of hardware and software modifications, which can be sub-divided into three distinct categories as follows: an RO Enable Relay circuit (an effectively “analog” electrical hardware modification), Drive Motion Watchdog (LabVIEW software modifications), and PMAC Software Modifications. A detailed description of these three changes is provided in the following section.

3 MODIFICATIONS

3.1 RO Enable Relay

The intention of this modification was to add a direct operator controlled relay between the PMAC and the motor. There was a new relay added in series between the existing PMAC controlled Allen-Bradley enable relay and the Next Step drive. There is a relay for each drive axis and the new relays are controlled by the reactor operator through the shim switch and the bank select switch. This only allows a motor’s relay to be energized (i.e. drive signals able to be sent to the motor) when the operator selects the bank the motor is in and moves the shim switch to the UP or DOWN position, except during ARDN, TRW MODE, and the new DRIVE MAINTENANCE keyswitch. The shim switch will default to the STOP or neutral position when the operator is not actively holding it in the UP or DOWN position, which will de-energize the new relays. The system of new relays only allows one bank of regulating rods to be enabled at a time except during ARDN and the DRIVE MAINTENANCE function. ARDN requires that all of the new relays be energized at once and the DRIVE MAINTENANCE function allows all the RO enable relays to be energized from the high bay so maintenance procedures can be conducted directly from the PMAC computer. The existing ARDN function will be rewired and re-programmed so that the reactor operator has to actively hold the button during the ARDN sequence. TRW MODE will remain operational by allowing the TRW CONNECT push button to energize the new relays for the TR. The RO Enable relay circuit is shown in detail in figure 1 below. A consequence of this modification will be the loss of automated SS functions (i.e. AUTO MODE and AUTO LEVEL). These features were removed from the Lab View and/or PMAC code.

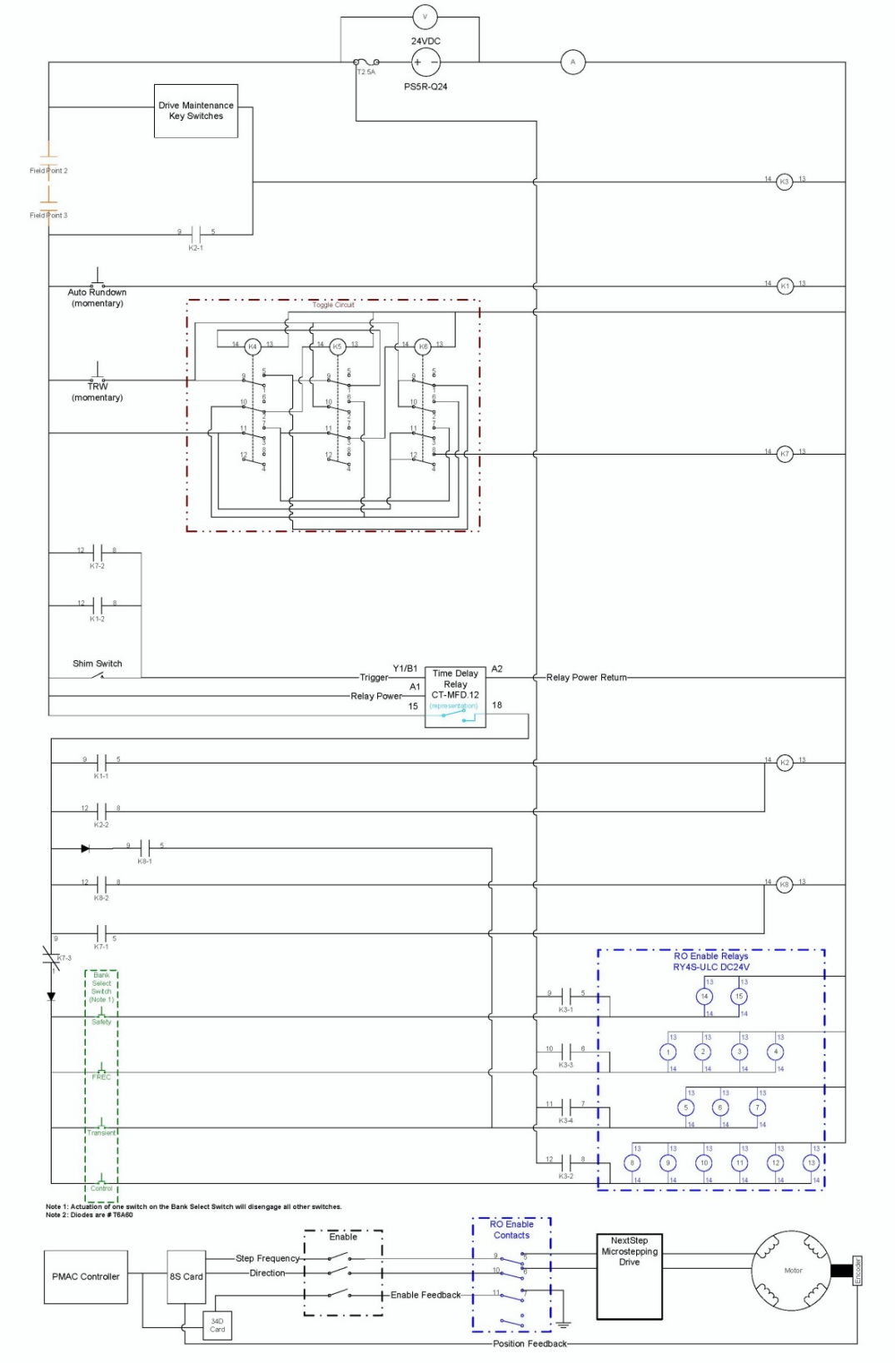

Figure 1: RO Enable Relay Circuit

RO Enable Relay Assumptions:

- All new hardware components are available COTS items, or easily fabricated on site to meet schedule constraints.
- Modified portions of the system are compatible with the existing ACRR systems.
- Modification interfaces with existing systems are manageable and do not impact the safety functions of these systems.
- Changes to the Human/Machine interface are minimal and the effects of modifications are transparent to RO during normal operations.
- Training requirements for the modifications are captured by updates to existing ACRRF procedures, and no new procedures will be required.

3.2 Drive Motion Watchdog

This modification adds features to the LabVIEW code to monitor rod motion. This is done by monitoring the rods' speed and direction using existing rod position information in DAC1. These checks provide audible and visual alarms to the RO and a drive motion cutout whenever there is: a mismatch between the actual direction and commanded direction, a mismatch between actual speed and commanded speed, or drive motion with no commands. The Drive Motion Watchdog (DMW) initiates a drive motion cutout by integrating with the RO Enable Relay circuit through two existing FieldPoint Relays that will be normally closed during operations. DAC1 will open them when limits are exceeded. The FieldPoint relays are in series with the SHIM and ARDN signals in RO Enable Relay circuit causing the analog enable relays to de-energize and stop rod motion. To integrate with the new relay circuit, AUTO submode and AUTO LEVEL will be removed so that it is no longer a functional mode. As an enhancement, the X-Y error code display window on DAC1 will be modified to provide a log of past errors and show some recent previous errors.

LabVIEW Software Modifications Assumptions:

- AUTO submode and AUTO LEVEL will no longer be available.
- The DMW will operate two "enable permissive relays" in series in the analog enable relay train. The relays are hosted by FP-420 Relay modules already in the system.
- The LabVIEW changes will integrate with the new relay circuit and PMAC changes where the LabVIEW code boundary affects them, or where they affect the LabVIEW code boundary.

3.3 PMAC Improvements

The changes for this part of the modification address improvements identified by the Forensics Project Team to improve the logic of the current PMAC code and align it better with PMAC-PLC coding best practices. Changes include changing the ARDN speed to the same speed as FAST, changing the "JOG TO" command in ARDN to a "JOG DOWN" command, moving the ARDN routine to its own PLC, and improving the latching logic, as needed, to alleviate buffer overload issues. Additionally, ARDN will no longer be a momentary pushbutton with a latch; the code will be changed to require the operator to push and hold the ARDN button. Legacy auto-leveling functions and automatic submode functions will be removed from the code and the system will no longer have such capabilities. Conditioning statements will be added to the code to ensure unnecessary commands are not filling buffer space.

PMAC Software Modifications Assumptions:

- The current “not up / not down” logic will continue to serve as the indication for PMAC to stop normal rod motion.
- The PMAC will continue to receive the same inputs, up and down, from the shim switch in the same fashion through the 34d card.
- The current PMAC over speed trip will remain the same.
- The ARDN function will be changed from a momentary pushbutton with latch to a hold-down-till-done function.
- ARDN will become more conservative (i.e. only command downward motion at a slower speed).
- AUTO submode will no longer be available.
- The time delay relay in modification 1.0 will not cause following errors on loss of SHIM commands.
- The DMW will operate two “enable permissive relays” in series in the analog enable relay train. This loss of this analog permissive to rod motion without PMAC awareness will generate a following error.
- PMAC changes will improve its reliability and help address a potential cause to the 2013 rod motion anomaly.

4 FUTURE WORK

4.1 RCSU Project

The modifications described in the above sections were intended as a temporary solution to the aging Reactivity Control System. Several components are at end of life and are currently no longer supported or manufactured, with critical spare parts at a minimum. The Reactivity Control System Upgrade (RCSU) Project was initiated to upgrade the ACRR reactivity control system and key interfaces to better align with stakeholder expectations, current and proven state of the art technology, and to continue to meet the mission of advancing nuclear technology through applied radiation sciences and unique nuclear environments – into the future.

The RCSU project is currently progressing and is expected to be completed in early 2016. TA-V reached out to industry partners to design, test, and install the new system. The new systems will replace the PMAC and FieldPoint components with National Instrument’s Compaq RIO components. This project will also replace the current network design with more a more redundant, virtualized one. This project will not replace any of the existing NextSteps, motors, or regulating rods.

4.2 Unintended Consequences

There were two unintended consequences from these modifications: spurious trips due to a low fidelity velocity calculation based off rod position values and loss of holding current to the motors when a DMW trip happens. The spurious trips become an operator inconvenience and are going to be minimized with a planned upgrade of the algorithm. The loss of holding current is not an issue the majority of the time and was not discovered until a ~18 months after the modifications were made. As the motors age and experience wear, there can be slight losses in the friction of the lead screw. When holding current is removed (from a spurious DMW trip) with the rods moving in a downward direction there is a small probability that the rod with have enough momentum to overcome the friction and continue traveling downward due to gravity until holding current is reapplied. This was seen on one control rod during an Auto-rundown command during a steady-state operation and was able to be reproduced during trouble shooting.

5 CONCLUSIONS

The control rod anomaly that was the reason for these modifications was very minor and was understood to pose no safety concerns once the root cause was determined. In the era of digital systems, causes of failures are not necessarily intuitive and can be difficult to determine. Fully understanding how the software behaves and its possible failure modes can save time during an anomaly. Many “insignificant” anomalies in a single software system can cause stakeholders to lose confidence in the system which could lead to extended downtime. Understanding these failures and correct them before this happens in important. “Normalizing the deviation” of these failures can be a risk to operational time.

Some basic principles for digital motion were identified and implemented in the modification project that should be implemented in systems during design instead of after the fact. The most important idea is that the reactor operator should always have a way to control rod motion between the final software determination for motion and the motor. This prevents rods from moving because of software failures. It is also a good practice if using digital systems for motion control to have two separate programs agree that motion is commanded before a motion command is issued to the motors.

6 ACKNOWLEDGMENTS

The authors would like to acknowledge all of the team members that helped to make the projects a success.