A UNIQUE APPROACH TO ENSURING CONFIGURATION CONTROL OF DIGITAL COMPUTER SYSTEM SOFTWARE

R.J. Atkisson, Jr., K.G. Gavin and D.K. Harding
Proto-Power Corporation
Groton, CT

M.C. Annon
I & C Engineering Associates
Waterford, CT

ABSTRACT

The use of digital computer system software for control system applications and programmable logic controllers (PLC's) has become more prevalent, in the nuclear industry, over the last ten years. During this period, the need has increased to develop more options for effective and cost efficient means of maintaining configuration control and/or performing adequate verification and validation (V&V) of this type of software. Without exception, any of the organizations involved in the nuclear industry agree that proper configuration control of computer software is necessary to maintaining an adequate design basis. However, when this type of digital computer system/PLC software is applied to control system circuitry, as part of a retrofit or upgrade in an existing facility, appropriate configuration controls/V&V, are too often overlooked or misapplied.

In addition, there is a definite lack of clear guidance from the industry standards organizations, as to what constitutes appropriate configuration controls/V&V for this type of software, especially when the software is used in safety-related applications at nuclear facilities. This paper discusses a unique approach and technique that is significantly different from the more traditional software configuration control/V&V techniques. Several previous applications of the approach are discussed, including emphasis on its' use on the PLC used to control the Supercompactor and Repackaging Facility (SARF) at the Department Of Energy (DOE) Rocky Flats Plant (RFP). In addition to discussing the overall approach used, the unique features of the technique, as well as the benefits derived from the technique, are summarized.

INTRODUCTION

The need for configuration control of computer software has been recognized for many years. During this time, numerous nuclear industry documents have been developed to address the entire spectrum of configuration control related issues. References 1-9 represent some of the most commonly cited documents. These documents represent requirements, as well as guidelines for development of appropriate techniques to deal with configuration control of computer software. However, these guidelines and requirements have not been as effective as the industry would like them to be.

In addition, due to concerns over possible undetected system malfunctions, the Nuclear Regulatory Commission (NRC) has placed emphasis on the review of safety-related applications using microprocessor based systems. These concerns have resulted in the NRC taking the position that installation of digital based safety systems is an unreviewed safety question and may require NRC review prior to implementation (6).

There are numerous reasons contributing to the lack of effective configuration controls/V&V for these applications. One of the principle reasons is an apparent misconception by many personnel that instituting such controls creates complex administrative requirements. Another common reason is a mistaken belief that it is too complicated to check out all possible operational combinations and that typical field and/or factory testing techniques will identify any "bugs" that will adversely effect the designed application.

BACKGROUND

It was partially in response to these types of misconceptions and reasons, that two techniques were developed, almost ten years ago, to supplement the more traditional approaches for the review of control circuits. These techniques are based upon two proprietary PC-based computer programs, originally developed, for analyzing power plant control circuits. The first of these techniques is called "Truth-Analysis[sm];" the second, is called "Action-Reaction[sm]." Reference 10 summarizes one of the first uses of the technique on a fossil power plant retrofit application.

TECHNIQUE APPLICATIONS

Over the last nine years, the techniques have been enhanced and utilized on numerous fossil utility and nuclear industry projects. Some of these projects have included:

- For Light Water Reactors
  Main Steam Isolation Valve circuitry troubleshooting in a Solid State Protection System (SSPS); Auxiliary Feedwater (AFW) autoswitchover circuit investigation; investigation of inadvertent Fire Protection system actuation; system circuit design for AFW, Safety Injection (SI) and Diesel Generator Sequencer.
- For High Temperature Gas Reactors
  Control circuit design included as part of a major fluid system design modification; common mode failure review, of the control circuitry for the Emergency Diesel Generator, to support a response to questions from the NRC/ACRS.
- For Fossil Plants
  Bottom Ash Handling controls and PLC based Screen Backwash applications.

- For the SARF at Rocky Flats

  The objective of the DOE/RFP Supercompactor and Repackaging Facility (SARF) project was to effect the safe and reliable reduction of transuranic (TRU), TRU-Mixed, Low Level (LL) and LL-Mixed waste volumes at Rocky Flats Plant. The SARF has, in trial operations with soft waste, achieved nominal overall volume reductions of between 8:1 and 10:1.

The Supercompactor press is a 2200-ton vertical unit, using a single concentric mold capable of handling thirty-five gallon drums. A glovebox encloses the press, and this confinement exhausts to an existing building ventilation system. As shown in Fig. 1, waste enters the SARF through either the "Hard or Soft Waste" airlocks. Soft waste is hand sorted, precompacted into a 35-gallon drum (using a 30-ton low-force press), pierced and then loaded into the Supercompactor. Hard waste is conveyed directly to the piercers, and then loaded into the Supercompactor. After being supercompacted, the resulting 4" to 12" high puck is grappled into a 55-gallon loadout drum, for subsequent storage and ultimate shipment to disposal. Material movements through the system are controlled and operated through the use of a PLC.

To supplement the normal configuration management controls being used at RFP, the "Action-Reaction[sm]" technique was utilized on the review of the SARF PLC control schemes. The technique was used to develop logic diagrams from the PLC generated "ladder diagrams;" to verify the actual programming; and to assist in finalizing the system operation and design changes being considered to resolve problems discovered during system checkout.

KEY ISSUES

When faced with retrofits that involve complex control circuits at existing facilities, the designer and owner have to deal with several key issues related to configuration control and V&V.

One of these issues is the need to define what's appropriate and/or "adequate" for the situation. The concepts outlined in Refs. 1-9 are quite often not followed due to two common situations. The first situation occurs when design and/or licensing basis of the facility did not specifically commit to these criteria. The second situation occurs when the microprocessor based software is supplied as part of controls system "hardware;" and therefore, it is believed that the criteria (1-9) aren't applicable to such "hardware".

Another issue is often the lack of definitive criteria that applies to the specific control application being designed. While Refs. 1-9 outline good concepts, converting these concepts into acceptable work practices has proved to be a serious challenge for many companies.

However, accepting these types of approaches contradicts one of the basic concepts in these documents, i.e., finding "glitches" or "sneak circuits" during design reviews is usually less expensive and much safer than finding them during system checkout or actual operation. It is in the best interest of the designer and/or owner to utilize design/checkout techniques to eliminate these types of problems, as soon as possible, in the project.

Figure 2 depicts a PLC "ladder diagram" with examples of the errors that have been typically detected.

TYPICAL APPROACH

Even in organizations where configuration management systems are in place, it is not unusual for only minimal requirements to be invoked on control circuits that are based on microprocessor types of software.

Too often these requirements only invoke administrative controls on the copies of the software, and don't utilize a requirement for the appropriate independent verification of the software operation. Sometimes independent verification is invoked, but too frequently it is limited to a review of the software code or "ladder" without utilizing some sort of simulation and/or alternative "sneak circuit" type of analysis.

Sometimes, even these basic requirements aren't invoked since it is believed that component/system checkout and testing will confirm the adequacy of the design. Table I outlines examples of errors that have slipped through typical checkouts.

AN ALTERNATIVE APPROACH

The "Truth Analysis[sm]" and "Action-Reaction[sm]" techniques that were referenced above, represent two complementary approaches that can be used to assist in the implementation of effective configuration control or V&V for digital based controls.

The "Truth Analysis[sm]" technique is used primarily for analyzing new control systems being designed or major modifications to existing control systems. The technique performs a systematic analysis of all combinations of input signals and control device positions to identify potential errors in the control logic and/or inappropriate control output functions.

The "Action-Reaction[sm]" technique uses a control logic type of simulation program. It is most often used to diagnose system problems, provide operator training, and assess the effects of minor control system modifications. The technique provides an interactive representation of the control system by allowing the program operator to step through changes in the input signals and control device positions while the program identifies the corresponding changes in control output functions.

The application of the "Action-Reaction[sm]" technique, for the SARF, constitutes a fairly typical use of the technique. As part of the use of this technique on the SARF, the following activities were performed: (a) Developed a logic diagram from the existing PLC "ladder" and operating procedures; (b) Created "Action-Reaction[sm]" model from the logic diagram; (c) Identified any differences in component operation between the "Action-Reaction[sm]" model and the PLC "ladder;" (d) Reviewed the differences with the appropriate design and operations personnel to determine the preferred control functions; (e) Revised the PLC software to implement the desired changes; (f) Repeated steps a-e above, as necessary, and when additional operational changes were identified. During this application, numerous "sneak circuits" were identified that had not been able to be resolved during normal diagnostic testing. In addition, several potential modes of inappropriate component operation were detected. The "Action-Reaction[sm]" model also provided the SARF personnel with the capability to review the impact of alternative PLC software changes without having to go through all the trouble of actually making the PLC changes and operating the machine.

UNIQUE FEATURES

This section outlines some of the features that we consider to be unique to these types of techniques. For example, some of the features developed include:

- Systematic analysis of all combinations of input signal and control device positions verify correct logic system operations, as well as identify control logic anomalies.
- One to one verification of system operation to software logic, including assurance of 100% or 1:1 correlation of system software to hardware operation.
- Real-time, or proportional to real-time, simulation of system operation and/or control logic interactions.
- Designed to operate on an IBM personal computer, or compatible system, to enhance in-plant or field use.
- Allows evaluation of the impact on control system logic for proposed changes prior to actual system changes being implemented.
- Ease in identifying cause(s) of logic or component maloperation.
- Capability to evaluate proposed fixes to logic anomalies, that have been detected, to ensure that proposed fixes do not introduce additional maloperations.
- Operator training via nontechnical (user friendly) logic diagrams.
- Enhanced communications between operators and hardware technicians during troubleshooting.

CONCLUSIONS

As microprocessor based/PLC control systems use increases in the nuclear industries, the need to have effective and cost efficient means of maintaining configuration control and performing adequate verification and validation (V&V) of the software associated with these applications will increase. Either of the two techniques discussed in this paper, "Truth-Analysis[sm]" and "Action-Reaction[sm]" are a means of meeting this need. References 11 & 12 discuss two other approaches to achieving this goal.

Some of the specific benefits that have been realized through the use of the techniques discussed in this paper include:

- Pre-installation verification of correct systems operation.
- Assurance that all possible input combinations and resultant outputs have been reviewed.
- Elimination, or minimization, of software, hardware and/or wiring changes by the identification and correction of potential component maloperation.

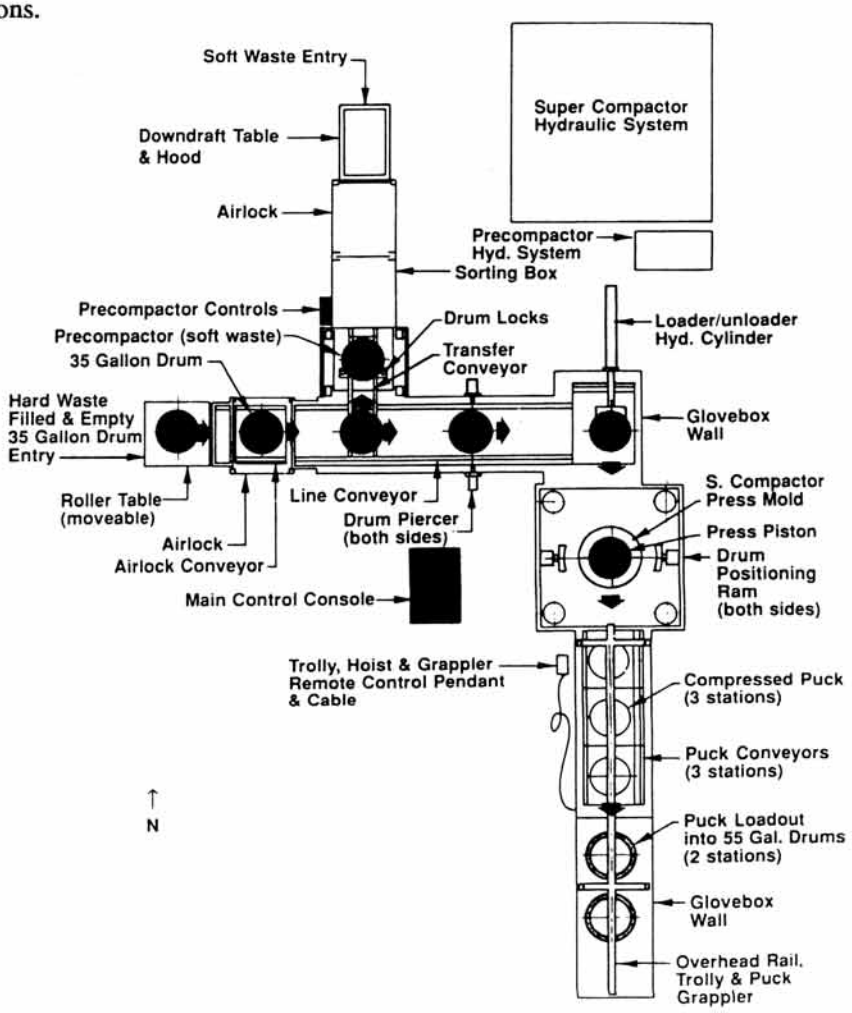

Fig. 1. Supercompaction and repackage facility plan view.

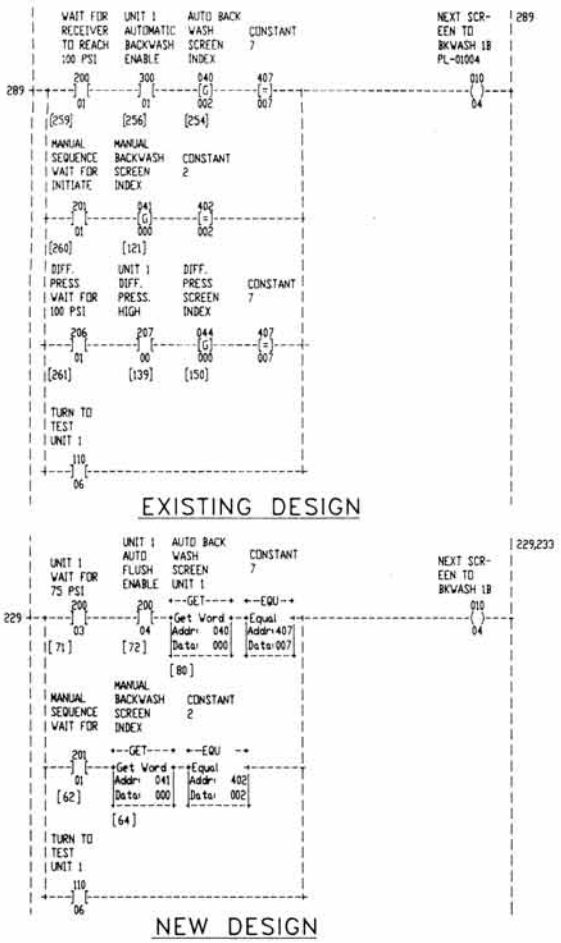

Fig. 2. Typical PLC application.

- Detection of design errors that could possibly lead to plant maloperation, equipment damage or personnel injury.
- Assurance of accuracy, through one-to-one correlation between a logic diagram and its respective schematic wiring/"ladder" diagram.

In addition, these features enhance operator confidence in understanding the new system's intended operation. Where some operators have difficulty understanding schematic wiring or "ladder" diagrams, logic diagrams or PC models are easier to understand. The logic diagrams also represent a user friendly format that can be used in the training of operations personnel. This type of format facilitates the communication of system maloperation between the operators and engineering or maintenance personnel.

Therefore, the determination of the acceptability or the impact of any proposed control system modifications, regardless of their reason or time of installation, can be analyzed by these techniques and the results accepted by the operators. This approach ensures that the proposed changes don't result in system maloperation before actual field changes are made, which can result in improving safety as well as potentially produce substantial cost savings.

REFERENCES

1. ANSI/ASME NQA-2, Part 2.7, "Quality Assurance Requirements of Computer Software for Nuclear Facility Applications."

TABLE I
Examples of Anomalies Found During Control System Evaluation

1. When screen backwash was initiated for a high differential pressure on one unit followed by a high differential pressure on the other units' screen, the logic allowed both units' screen valves to open simultaneously. This is unacceptable since purge volume is inadequate. (NOTE: This error and the correction are depicted on Fig. 2.)
2. The backwash "excessive time cycle" alarm was designed to monitor the number of automatic backwash operations in lieu of the time that elapsed from initiation of the automatic backwash signal. This is unacceptable because excessive time could elapse prior to "alarm" of a non-backwash situation which could potentially result in a plant trip.
3. It was determined that the logic sequencing for successive intake screen backwash cycling was incorrect because the control system would not advance to the next screen if the previous screen experienced a failure during its backwash cycle.
4. Identification of a component single failure which resulted in loss of the redundant safety related Emergency Diesel Generator System Operation.
5. Detection of a safety related control system common mode failure scenario which negated the auto-closure operation of the Main Steam Isolation Valves.
6. Verification of correct logic system design operation for the Auxiliary Feedwater (AFW) system autoswitchover from the Condensate Storage Tank (CST) to the Containment sump which occurred during an operating plant event. This evaluation also included the recommendation for control logic modifications which would enhance future AFW system suction autoswitchover operations during anticipated fluid system perturbations.
7. Detection of "sneak" circuits within AC and DC control logics which resulted in inadvertent operation of fire protection water deluge system for the Containment HEPA filters.

2. ANSI/ANS-10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry."
3. ANSI/IEEE-ANS-7-4.3.2-1982, "Application Criteria for Programmable Digital Computer Systems in Safety-Related Systems."
4. U.S. NUCLEAR REGULATORY COMMISSION, Regulatory Guide 1.152, "Criteria *for Programmable* Digital Computer Systems in Safety-Related Systems of Nuclear Power Plants," (November 1985).
5. U.S. NUCLEAR REGULATORY COMMISSION, NUREG/CR-2640, "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry."
6. U.S. FEDERAL REGISTER, Volume 57, No. 158, Pages 36680 & 36681, "Proposed Generic Letter: Analog-to-Digital Replacements Under the 10CFR50.59 Rule," (August 14, 1992).

7. INSTITUTE OF NUCLEAR POWER OPERATIONS, INPO 87-006, "Report on Configuration Management in the Nuclear Utility Industry," (July 1987).
8. U.S. DEPARTMENT OF ENERGY, DOE Order 1330.1C, "Computer Software Management."
9. U.S. DEPARTMENT OF ENERGY, DOE Order 1360.4A, "Scientific and Technical Computer Software."
10. L.J. PERCELLO, D.K. HARDING, & M.C. ANNON, "Truth-Analysis[sm] Technique Review of Plant Protection Logic Design for the Chalk Point Balanced Draft Conversion Project, " presented at the ISA International Conference and Exhibit, in Houston Texas (October, 1984).
11. Q.B. CHOU, J. KOZAK, & A. ACHTMAN, "Potential Application of ASIC Technology to Safety Systems of Nuclear Power Plants," presented at the 2nd Annual ISA/EPRI Joint Controls and Instrumentation Conference, in Kansas City, MO (June, 1992).
12. C.A. LEWIS, C.F. RADOCY, & A.C. DENYER, "Palo Verde's Safety Related PLC System," presented at the 2nd Annual ISA/EPRI Joint Controls and Instrumentation Conference, in Kansas City, MO (June, 1992).