NBSR REFUELING CANON CONTROL SYSTEM UPGRADE

Elia Shteimberg
Nuclear Research Center
Negev, PB 9001, Beer Sheba 84190, Israel
eli.sht@gmail.com

Dağıstan Şahin
Center for Neutron Research
National Institute of Standards and Technology
100 Bureau Dr., Gaithersburg, MD 20899 USA
dagistan.sahin@nist.gov

ABSTRACT

National Bureau of Standards Reactor (NBSR) uses a refueling cannon system in-between 38-day reactor operation cycles. The refueling canon system is an electro-mechanical system to transfer fuel elements between the reactor vessel and the storage pool. The system was in service since the initial construction of the reactor, during which time few upgrades had been made. Since the last upgrade, the system operating interface was an electrical panel that consisted of pushbuttons and lights that demanded frequent care and maintenance. The instrumentation was controlled by an analog relay logic circuitry, superseded by Programmable Logic Controller (PLC), which was only capable of basic instructions, preventing implementation of any complex control logic. The manufacturer support for this PLC modules and hardware had been diminished for many years. PLC configuration and programming software required an outdated DOS PC platform and communication hardware, that made it infeasible to configure the PLC using modern computer system interfaces and utilize the configuration software to make changes as required. These issues, along with new operational and safety requirements and the need for a modern, high performance user interface led to a decision to upgrade the Refueling Canon control system with a modern PLC and PC based Human Machine Interface (HMI). The new control system was designed using Industry standard, modern PLC hardware for easy maintenance. PLC software application was implemented as a well commented, readable and modular program code that uses function blocks for repeating code to simplify the maintenance and future changes. Control logic and operating conditions from the existing controller were reverse engineered and implemented precisely in the new program logic. The upgrade produced four main benefits. First, a computer HMI interface was designed and developed in accordance to current industry standards. Second, the HMI was designed to include all the operator procedures, with automatic guidance and error preventing features. Third, engineering safety features were introduced, that define safe equipment operation in case of power failure or PLC power cycling and for the shutdown state of the system. Finally, the old control cabinet experienced numerous changes over the years, resulting in tangled, hard-to-trace, unlabeled wiring, leading to difficult maintenance and troubleshooting. Thus, the upgrade included a total redesign and rewiring of the control cabinet electrical circuitry. In this paper, we discuss our experience in reverse engineering an aging system and the design, verification and validation, testing and installation of the replacement system.

Key Words: Control System, PLC, HMI – Human Machine Interface, Safety Analysis, V&V - Validation and Verification.

1 INTRODUCTION

National Institute of Standards and Technology (NIST) hosts a 20 MW tank type research reactor, namely National Bureau of Standards Reactor (NBSR). The primary purpose of the NBSR is to serve as a neutron source for scientific research. Built in 1960s, the NBSR has grown into a major neutron source facility hosting over 2000 guest researchers annually. The reactor is operated for 30-day intervals, followed by refueling and maintenance shutdowns. During refueling, a fuel transfer system (FTS) is used to move fuel elements to and from a storage pool. The original fuel transfer control system (FTCS) was based on an analog relay circuitry. Over thirty years ago, the FTCS was upgraded using GE Fanuc Series One PLC (Programmable Logic Controller)[1] system, which reached its lifecycle on October 1, 2017 [2]. Furthermore, there were undocumented changes, specifically in wiring, which made it problematic to perform maintenance or repairs. As with other aging reactor control and support systems, a digital upgrade was inevitable for continued safe operation of the reactor. Undoubtfully, there were numerous challenges for such an upgrade due to uncertainties it involves and the changes it requires, especially for reactor operators. This paper describes the background of an aging control system, challenges we encountered and resolutions. We discuss the details about the reverse engineering, verification and validation, testing, documentation, training and version control activities that were employed in upgrading the FTCS.

1.1 Background

FTS is an electro-mechanical system used to transfer irradiated fuel elements between the reactor vessel and the storage pool. The system has been operational since the start-up of the reactor. Over the years, upgrades have been made, with the latest major upgrade of the system replacing relay based analog circuitry with a GE Fanuc Series One PLC (Programmable Logic Controller)[1].

The fuel transfer control system (FTCS) was designed to operate system equipment, including valves and hydraulics, by means of the manual control interface and provide status lights to the operating panel. Growing maintenance demands and necessary operational changes increasingly required to perform engineering interventions in the control system and PLC programming. However, since PLC configuration and programming software required an outdated proprietary platform to run and proprietary communication hardware, it was infeasible to configure the PLC using modern computer system interfaces and utilize the configuration software to make the desired modifications. Although, such an interface was eventually established, it was not sustainable in the future. Moreover, it was impractical to operate the configuration software, using this interface, since the original keyboard character map didn't match the modern, commonly used ASCII mapping. Another issue that limited implementing changes in the PLC programming was that the GE Fanuc Series One PLC was capable of only basic logic instructions. Absence of extensive instructions library, including calculations, math and control, prevented any complex control requirements implementation. The second issue, which complicated PLC program changes, was the lack of PLC logic documentation.

The existing PLC hardware is about thirty years old, and contradictory to the past reliable operations, some hardware modules had started to fail and needed to be replaced. As previously mentioned, the hardware and software are obsolete; therefore, no manufacturer support is provided, and replacement parts are only available in refurbished condition. Finally, the electrical operating panel, which consisted of pushbuttons and status indication lights, demanded frequent maintenance and parts replacements. The old control cabinet and junction box suffered from numerous undocumented changes over the years, resulting in tangled hard to trace, unlabeled wiring, which was difficult to maintain and troubleshoot. Some of the old control system electrical and operation panel components are shown in Figure 1.

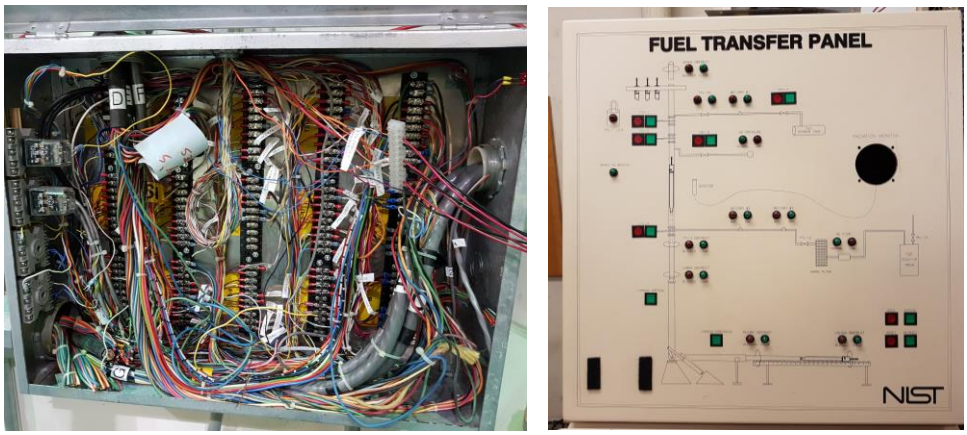

Figure 1. Old Control System Components – Electrical Junction Box (on the left) and Analog User Interface (on the right)

It was determined to upgrade the FTCS and install a modern industrial control system and a PC based HMI (Human Machine Interface). The system upgrade was designed to replace the old PLC and the physical operator panel (lights and switches) with modern, industrial grade PLC[3] and a digital high performance HMI[4]. The new equipment would lower maintenance demands by reducing the number of components (HMI PC and display instead of electrical pushbuttons and lights panel), along with manufacturer support and replacement parts. Modern PLC and HMI systems would, also, make it possible to enforce version control, implement any new operational requirements and allow modifications and additions to its logic and programming in the future. Electric junction box wiring, as shown in Figure 1 left, was also completely redesigned and replaced. The existing mechanical equipment and instrumentation of the system was interfaced to the new control system.

1.2 Challenges

Upgrading an aging system, such as described above, represents several significant challenges, mainly due to uncertainties it involves. We discuss most significant five, including documentation issues, wiring, scheduling, safety and field sensors.

First, the old system lacked detailed documentation. Although, some helpful electrical wiring documentation was available, no control logic description or diagrams could be found.

Secondly, after some investigation, undocumented changes and additions to electric wiring were identified. Thus, reverse engineering of the undocumented control logic and tracking the unlabeled wiring were essential for the success of the project. Fortunately, the reactor operators had extensive knowledge in the operations of the FTS, thereby providing invaluable information.

Third challenge was the scheduling around the reactor operations. Consequently, once the new system was ready for deployment in the field, the installation work must not interfere with reactor operation schedule. In our case, the refueling system is used in between the reactor operating cycles, limiting a working window for an upgrade. After a refueling was completed using the old system, the new system must be installed, tested and operational before the next scheduled refueling. Additional safety restrictions, such as restricted access to the reactor process room, due to high radiation during and sometime after reactor operation cycle, further limited the available installation time, which amounted to a period of about three weeks in total to dismantle the old equipment, then install and test the new control system.

Fourth issue was presented by operational safety considerations, which required that the three system valves, keeping irradiated primary reactor coolant/moderator D_2O from flowing to the storage pool, be sealed shut during reactor operation. These valves may only be open when the reactor vessel D2O level is

lowered during reactor shut down for a limited time (a day at most, typically for refueling). The planning and preparation imposed by this safety requirement, included mechanically sealing the valves shut during reactor operation and providing external light indications, verifying that the valves are shut, even after the old control system was dismantled. This restricted the installation work, and operator training preventing completing the wiring and testing of these components, even after the rest of the system was installed. Therefore, a temporary simulation mode was also implemented in the control system to allow functional testing and operator training.

Lastly, some uncertainties existed regarding a few system sensors. Their exact specifications, modes of operation, wiring diagrams and compatibility with the new control hardware were partially unknown, requiring a lot of field investigation and experimentation to fill in the missing information. These uncertainties affected "Wet/Dry" and Proximity sensors.

To overcome these challenges, a careful and detailed project plan, along with control system and deployment safety analysis, was necessary to ensure safe installation and operation. Extensive, planned and documented validation and verification process is crucial for safe and flawless operation after such an upgrade. Moreover, complete technical and operator instruction documentation and training are vital for successful system operation and maintenance.

The installation and testing process was planned in a way that could be completed in several stages: sealing the three valves shut and providing external indications, dismantling the old and installing the new control system, field wiring the instrumentation, except for the three sealed valves. Last, after the vessel level is lowered, finalizing the field wiring and testing the remaining three valves.

The following two sections presents our experience in upgrading an obsolete control system. Part 2 describes control system requirements and design process, including chosen architecture, safety analysis and reverse engineering of the existing control system, required as a basis for the new system design. Part 3 describes the implementation of the design, installation and validation of the new control system.

2 COTROL SYSTEM DESIGN

2.1 Requirements

A basis for the design of the new control system was founded on a set of requirements that would ensure sustainable operation and maintenance. PLC program must be well commented and comprehensible. The code must be modular, i.e. use of function blocks for repeating code for easy maintenance and future changes. The new system will be operated using digital HMI interface. The HMI must be developed in accordance to current industry standards for interfaces in industrial plants control systems[1,5]. Control system architecture details are provided in section 2.2. Additionally, HMI will allow paperless execution of the FTS operating procedures.

Engineering safety features, described in section 2.3, shall be introduced to define safe equipment operation in case of power failure or PLC power cycling and for the deactivated state of the system.

Control Logic Requirements are based on the original system control logic, which mainly consisted of complex conditions for equipment operation, triggered by operating panel pushbuttons. The new PLC logic is required to implement all conditions to precisely reflect the original logic. Essentially, this requirement translates into a set of Open/Close or ON/OFF conditions required for manual operation of the valves and hydraulic functions. Due to the lack of detailed logic documentation, reverse engineering of the original coding, described in section 2.4, was completed as one of the preliminary stages of this project.

2.2 Control System Architecture

Control system architecture is composed of an industrial PLC[6], and a PC providing HMI and OPC server functionalities[7]. The HMI is designed to allow manual operation of the system equipment (valves, hydraulics), to display the status of the field instrumentation and components, and to manage and log alarms, events and operator actions. In addition, the HMI provides convenient access to all project documentation in embedded digital format. The HMI communicates with the PLC using OPC protocol.

The FTCS may be considered a small-scale application; hence an appropriate PLC model and HMI software were selected. IO modules were selected to cover the system IO requirements and provide spare inputs and outputs for potential future upgrades and changes. The controller is programmed using a IEC 61131-3 standard compliant software[8]. In accordance with the IEC 61131-3 standard, this software supports five industrial control languages (LD, FBD, ST, IL, SFC), and the design of reusable function blocks and complex data structures.

Control system components, described above, are depicted in Figure 2, as a diagram that explains their relations and purposes. The PLC acts as a control and data acquisition center and is programmed using PLC programming software. HMI PC acts as an operator interface and OPC communication channel to the PLC.

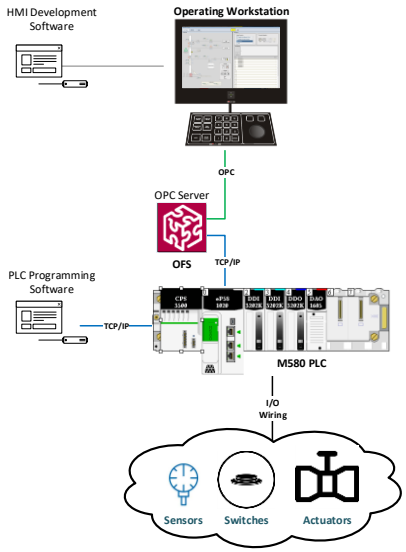

Figure 2. Control system Architecture

2.3 Safety Analysis

Control System Failsafe defines a safe state for the controlled equipment in case of the defined system failures – Power loss, PLC STOP and a manual Safe Mode. The Safe Mode is defined as a deactivated state of the FTS, while the control system functions normally, but system operation is logically deactivated by an operator using the control interface. Since the deenergized equipment state is established as the safe state of the system, all components must be retained in this state by the PLC when in deactivated Safe Mode.

To ensure smooth operation whenever the control system recovers from one of the failures and resumes normal operation, the control program needs to check for the actual state of the latched equipment and match the internal program states to prevent sudden and unpredicted changes in the equipment operation.

Additional safety operation features must include self-diagnostics that alarms if control system hardware faults, instrumentation operation faults or HMI-PLC communication errors are detected.

There are number of faults that can occur in the control system that could affect its safe operation. Those fault scenarios were analyzed below, and appropriate control system actions were implemented to assure safe system operation[7].

First scenario is simply loss of power, where the PLC will shut down. At this point, all the controller outputs will lose power as well, reverting all the controlled equipment to its default state. All latched components will retain their last state and the rest will revert to their deenergized state. Original system design already employed hardware that would ensure safe system state when deenergized.

Next Scenario is PLC or program runtime faults that may cause a halt in a normal program execution. As such the PLC will switch to STOP mode. The fallback states for the PLC outputs are configured to deenergize whenever the PLC enters STOP mode, similar to the power loss scenario, resulting in the same behavior. This ensures a single straightforward safe-system-state definition and appropriate recovery. Same mode of failure also simplifies operator training.

2.4 Reverse Engineering

One of the most significant project requirements was to replicate the original PLC logic precisely in the new system. This logic mainly represents equipment operation conditions and corresponding interlocks. Nevertheless, this logic depended on various process states in a complex and tangled way.

ASCII printouts of the old PLC program were analyzed and translated to visual logic diagrams, which precisely reflect different system states and conditions. This document serves as a reference for FTS operation and as a basic control requirement for the system upgrade project. Figure 3 shows an example of a logic diagram, summarizing the conditions for Cylinder Retract hydraulic function.

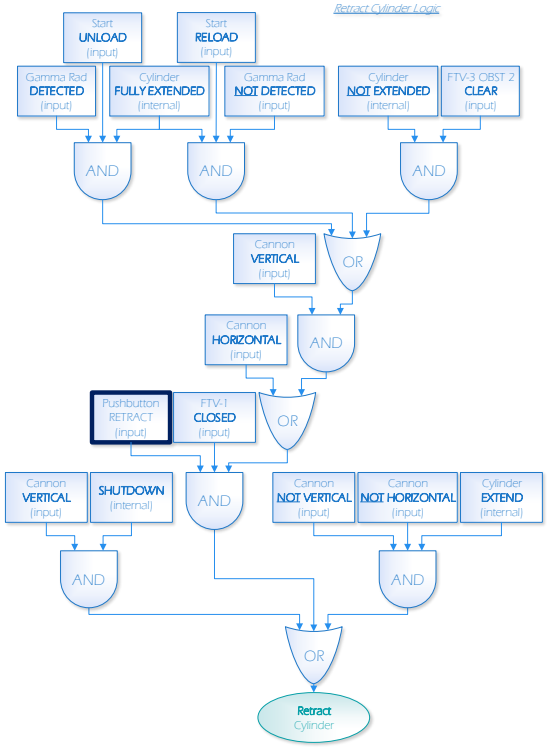

Figure 3. Example of Interlocks Logic

3 IMPLEMENTATION, INSTALLATION AND VALIDATION

3.1 Control System Implementation

The new PLC program and HMI application were developed based upon the previously described control requirements, and the outcomes of the control system architecture design, safety analysis and the reverse engineering stages.

The PLC program is well commented and structured. Repeating and reusable functions are implemented as function block objects with all the variables having meaningful aliases and detailed description. This resulted in a very clear, easy to understand program code and one that is simple to modify, expand or adapt to changing operational needs and requirements. Following the safety analysis that was performed during the design phase of the project, engineering safety features were introduced in addition to basic interlock logic and equipment operation. These features define and guarantee safe system state during power loss, PLC failures or planned deactivation. They also ensure detection, logging and alarming of control hardware, instrumentation and communication failures.

HMI, as shown in Figure 4, is also developed using a modular approach. Modular design leads to expedited development time and simple, straightforward modifications in the future. The HMI development platform is suited for small scale applications, however it provides versatile tools for quick and efficient application development, such as: class structure variables, multiuse custom symbols, ActiveX controls, scripts and subroutines.

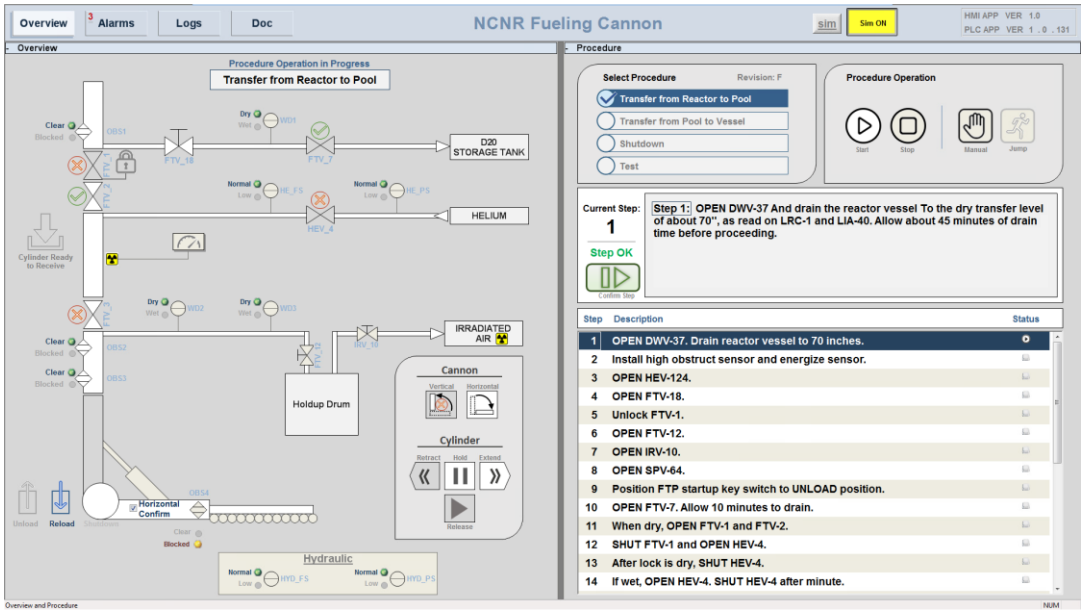

Figure 4. Main HMI Interface. Procedure Management on the Right Side of the Display.

Communication with PLC is facilitated by an OPC data server. It facilitates access to PLC variables directly by name, instead of numeric Modbus addresses. This way, all selected PLC variables are accessible in the HMI directly by name, including complex variables, such as arrays and structures.

In addition to regular operation, alarm and events logging, a procedure engine was developed, embedding all operational procedures in the HMI. This feature allows paperless execution of the procedure steps, which are clearly displayed on the main screen with detailed descriptions. The procedure execution is managed consecutively, preventing accidently skipping or repeating the steps. Necessary conditions to

complete the step are automatically tested, if possible, and the step may be confirmed only after the conditions are met. Another feature of the procedure engine, is to guide operators to appropriate action by highlighting the equipment or element (e.g. a valve) that should be operated in the current step as shown in. These features enable smooth operational flow and minimize possible errors and operator mistakes.

The example in Figure 5 illustrates a reusable graphic object for process valve operation and presents various visualization states of the valve, including a procedural highlighted state (state 4).

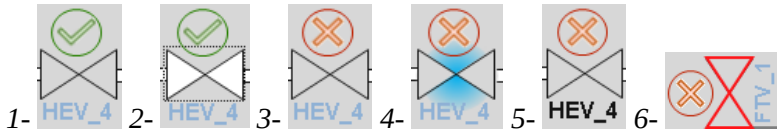

Figure 5. Example of Reusable Graphical Template for Process Valves

Essential states in Figure 5 are described below, from left to right:

1. Valve **Closed**, operation **permitted** (Green V symbol means no active interlocks).
2. Valve **Open**.
3. Operation is **not permitted** (Red X symbol means active operation interlock).
4. Blue blinking background circle acts as a **hint**, calling operators attention to operate the valve according to current procedure step instruction.
5. Black blinking valve label helps to **identify a valve** that is being operated – its operating screen is open.
6. Red blinking valve outline indicates a **mismatch alarm**.

3.2 Electrical Refurbishment Design and Implementation

The old control system was housed in an operating enclosure, which included the PLC, I/O hardware and wiring. The I/O signals were brought to the panel by five cables from the remote junction box (JB). The JB connected the wires from and to field equipment with the cables from the operating panel. It also included wiring for some unrelated equipment and even some unconnected, redundant wires. Modifications over the years made this panel tangled and difficult to maintain. The new FTCS required complete refurbishment and redesign of the operating panel and JB electrical wiring.

A new industrial operating panel cabinet was specified and acquired, housing the industrial PC and display for the HMI as displayed in Figure 6. The cabinet complies with NEMA-12 (IP54) and the display complies with NEMA-4X (IP65/IP66) standards. The original JB was completely striped of all the wiring. Unconnected and dead wires and cables were identified and removed. Unrelated equipment wiring was rerouted directly, so it wouldn't pass through the JB.

A new electrical control panel was designed and manufactured as shown in Figure 6. The panel includes PLC, I/O modules, power supply, contacts and internal wiring. The new panel was fitted in the JB, wired to the field instrumentation and connected to the operating panel by a single Ethernet communication cable.

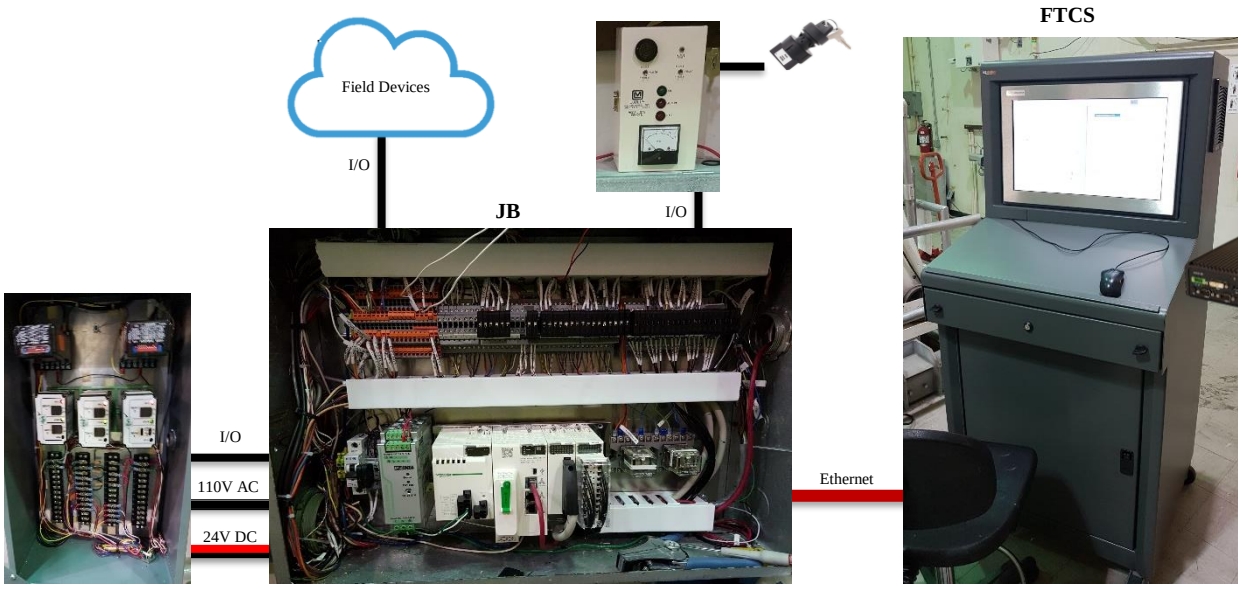

Figure 6. Physical System Layout after the Upgrade.

3.3 Installation and Testing

To avoid interfering with reactor operation schedule, the whole installation and testing of the new system was performed during one operation cycle, between the refueling operations. For operational safety reasons and due to inaccessibly of some working areas during reactor operation cycle, the net available time amounted to a three-week window. Therefore, the installation and testing stages were carefully planned and executed with some prerequisite stages complete prior to the installation period. First the controller program and HMI were tested in offline simulation mode. After the new control panel was manufactured, all internal PLC wiring was tested and verified.

During the installation stage, the old system was dismantled, and the new system was installed. Each element of the system (valves, sensors, etc.) were tested and its correct operation and indications were validated. Finally, the entire system operation tests were performed and the refueling procedures carried out and tested to eventually validate the complete system.

All tests were performed according previously prepared Validation and Verification (V&V) document[9]. Following the V&V tests, operators' trainings were carried out and finally, the system was successfully utilized to perform operational refueling procedure. It is worth noting, that the new system installation did not interfere with planned shutdown, refueling and consequent reactor start up schedule.

4 CONCLUSIONS

We presented our experience in safely upgrading an aging system which is part of operational reactor support systems. The replacement took place during routine reactor operation without any operational schedule disruptions. This upgrade presented challenges, such as lacking documentation, tight schedule, safety considerations and equipment uncertainties. We have shown that we were able to overcome these challenges with careful planning, system and safety analysis, design and documentation.

This upgrade resulted in numerous operational, safety and engineering enhancements. Before the upgrade, the system could be operated by experienced operators only. System maintenance was extremely difficult, and any control modifications were virtually impossible. The upgrade project addressed those

issues. The new interface is user friendly, informative and clearly displaying elements status and interlocks. A new embedded guided refueling procedure much simplified the operation. Detailed operating manual documentation enables novice operators to operate the system safely. Modern, up to date hardware and redesigned wiring makes system maintenance and addressing technical and electrical issues much easier. Modern software and sensible design practices allow simple and straightforward modifications. Implemented engineering safety features make the system reliable during shutdown, power failure and restoration. Extensive documentation was generated during the system design, development and deployment: Original system logic documentation, System design and Specifications report, Operators' Manual and V&V testing procedures. The documentation provides a fast learning curve for operating and engineering personal, with extensive technical and engineering information reference for the required system maintenance or modifications.

5 ACKNOWLEDGMENTS

Special thanks to the NBSR Reactor Operation and Engineering personnel for their contribution, support, valuable feedback and assistance provided during the development and installation of this project. Special thanks to Oscar Wiygul for his excellent technical assistance in the installation and the deployment of the new system.

6 DISCLAIMER

Certain commercial equipment, instruments, or materials are identified in this study to specify the experimental procedure adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the materials or equipment identified are necessarily the best available for the purpose.

7 REFERENCES

1. *GE Fanuc Series One Programmable Controllers User's Manual*, gek-90842 edition, GE FANUC AUTOMATION (1988).
2. "Series 90-70 PLC," GE Automation; 6 March 2015; http://www.geautomation.com/products/series-90-70-plc; (current as of Sep. 27, 2018).
3. *Modicon M580 Automation platform*, 5.0, Schneider Electric (2018).
4. B. HOLLIFIELD et al., *The High Performance HMI Handbook*, 1st edition, Plant Automation Services, Houston, Tex (2008).
5. ISA, *ISA 101.01-2015 Human Machine Interfaces for Process Automation Systems*.
6. *Modicon M580, Hardware Reference Manual | Schneider Electric*, 7.0, Schneider Electric (2017).
7. E. SHTEIMBERG, "Refueling Canon Control system design and specifications," National Institute of Standards and Technology (2018).
8. IEC, *IEC 61131-3 Programmable Controllers - Part 3: Programming Languages*, 3rd ed., International Electrotechnical Commission (IEC) (2013).
9. P. M. INSTITUTE, *A Guide to the Project Management Body of Knowledge (PMBOK Guide)–Sixth Edition*, 6 edition, Project Management Institute, Newtown Square, PA (2017).