DEVELOPMENT OF FUNCTIONAL REQUIREMENTS SPECIFICATION FOR DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS UPGRADES USED AT NUCLEAR POWER PLANTS (NPPs)

Roger D. Wyatt and Richard W. Supler
Enercon Services, Inc.
500 Town Park Lane, Kennesaw, GA. 30144
rwyatt@enercon.com; rsupler@enercon.com

Digital I&C Engineering

ABSTRACT

Recent market conditions have driven the nuclear industry to become more innovative at reducing cost in order to remain competitive. Instrumentation and Control (I&C) systems used by many NPPs are based on outdated 1960s and 70s technology. Many of the components used in these digital systems are no longer supported by Original Equipment Manufacturers (OEMs) and are rapidly becoming obsolete. Coping with the high cost of replacing I&C equipment due to obsolescence adds to this economic challenge. While other industries have migrated from analog to modern digital I&C technology, implementation of digital I&C controls within the nuclear industry has been very slow. This is primarily due to the high capital cost related to implementation of digital I&C upgrades, which is compounded by regulatory uncertainties that present significant licensing risks. The Nuclear Regulatory Commission (NRC), Nuclear Energy Institute (NEI) and the industry's Digital I&C Working Group are working to address many of the regulatory barriers that adversely impacts implementation of digital upgrades at NPPs. The NRC has developed an "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ML16097A182), Reference 1. Once fully implemented, this plan is expected to help reduce regulatory uncertainties that affects project cost. Excluding regulatory uncertainty, most OEM's will concur that one of the most important factors in reducing project cost is assuring that all requirements are well defined and complete prior to starting the project. A detailed and high quality Functional Requirements Specification (FRS) is critical in documenting these requirements.

Key Words: Functional, Requirement, Specification, Digital, I&C

1 INTRODUCTION: FUNCTIONAL REQUIREMENTS SPECIFICATION

Excluding regulatory uncertainty, most OEM's will concur that one of the most important factors in reducing project cost is assuring that all requirements are well defined and complete prior to starting the project. Vendor uncertainty can be significantly reduced when a high quality Functional Requirements Specification (FRS) forms the basis for Request for Proposals (RFPs) and subsequent purchase contract(s).

When RFPs contain vague and ambiguous requirements, vendors assume a risk that additional equipment or engineering may be required. Large cost contingencies are often added to offset potential risks which can inflate the price and increase the overall project cost. Vague and ambiguous requirements also elevate the cost to develop and implement the engineering change package and may result in a design of a system that doesn't meet the needs of the end user.

Errors or omissions that occur due to vague or ambiguous requirements can have a significant impact on project cost and schedule since they often lead to change orders for better defining the requirements and implementing the correct solution. The process for developing digital I&C systems usually follow a waterfall or V-Model life cycle development process where requirements cascade down from higher tier specifications, based on FRS requirements, to lower tier documentation that implement the requirements. Therefore, lack of clarity, not correcting imbedded errors and/or omissions within the FRS can impact multiple downstream documents, as well as the owner's engineering change package. This increases the cost of verification and validation (V&V) and often requires additional regression testing. When these issues are not discovered until later life cycle phases they result in costly rework and schedule delays.

1.1 Digital versus Analog/Relay Based Systems

Digital I&C systems are fundamentally different from analog/relay based I&C systems. Analog base systems receive signals from field sensors which are processed by analog based instrument loops. System logic is often implemented using analog and relay based control circuits. However, digital systems process the signals via input/output modules using software based logic, field-programmable gate array (FPGA) or complex programmable logic device (CPLD) based logic.

Legacy documentation such as Design Basis Documents (DBDs) and/or Systems Descriptions (SDs) often provide a good general description of the logic implemented by the analog/relays based I&C system. However, DBDs and SDs can often lack complete detailed descriptions of all interlocks and functions implemented by the analog/relay based I&C system. Typically, these details can only be discovered by close examination of the logic depicted in the system's legacy elementary diagrams/schematics. Historically, system designers of legacy I&C systems often used logic diagrams to convey detailed design requirements to OEMs. However, many NPPs have transitioned to using elementary diagrams/schematics as the primary means of controlling detailed design logic. Since these documents may not clearly convey all of the specifics and requirements often involved with complex logic, an OEM providing a proposal often builds additional contingency dollars into the project to cover uncertainty and possible hidden requirements. Use of an FRS helps to minimize the uncertainty and the OEM(s) to reduce and/or eliminate contingency costs from their proposal.

1.2 Basis for an FRS

When an FRS is based solely on descriptions contained in DBDs and SDs, this presents a risk that important logic details contained in the analog/relay based elementary diagrams are inadvertently omitted. These omissions may not become evident until factory acceptance testing (FAT), site acceptance testing (SAT), or post modification testing (PMT) when plant personnel discover that the new digital I&C system does not behave the same as the system being replaced.

While it may be tempting to expedite the procurement process by simply stating that the new I&C system must meet the same functional requirements that apply to the legacy I&C system, this approach is strongly discouraged. Analog/relay based systems frequently contain interlocking logic provided to identify and address the effects of single failure of hardware components. Many of these interlocks can be eliminated since they are not applicable to a software based digital I&C system. Each functional requirement needs to be carefully evaluated to determine if it is applicable to the new digital I&C system. Functional descriptions contained in DBDs, SDs, as well as the Updated Final Safety Analysis Report (UFSAR) need to be compared to logic shown in legacy elementary diagrams/schematics to assure the functional requirements are complete, accurate, unambiguous, fully traceable and applicable to the scope of the project. This approach is required to support traceability requirements applicable to the digital system life cycle development process discussed in NUREG 0800, Chapter 7, Reference 2, and Appendix 7.0-A "Review Process for Digital Instrumentation and Control Systems of the NRC's Standard Review Plan" (ML070660258), Reference 3.

1.3 Scheduling of an FRS

Since a high quality FRS is critical to assuring that RFPs contain an appropriate level of detail required for OEMs to propose their most cost effective solutions, the development of the FRS should not be rushed. Adequate time, budget and resources must be provided early in the planning and initiation phase of the project to support the development of this critical document. FRS requirements should be independently verified to assure requirements are complete, accurate, unambiguous, fully traceable, and applicable to the scope of the project.

Adequate time, budget and resources must also be provided to collect all plant legacy documentation that is applicable to the system. The documents must be analyzed to ensure requirements are complete and clearly defined, and assemble the information in a format that eliminates vendor uncertainty regarding scope and breadth of the requirement. A well-defined FRS not only improves OEM performance and efficiency but also improves performance and efficiency of all groups responsible for: planning and scheduling, preparing engineering change packages, developing test procedures, preparing and implementing work orders, as well as changes to maintenance procedures, preparing and implementing changes to the plant simulator, preparing operating procedures and performing test activities.

1.4 Software Life Cycle V-Model

The purpose of IEEE Standard 1012, "Standard for System and Software Verification and Validation", References 4 and 5 (1998 Edition endorsed by the NRC), is to establish a common framework of the Verification & Validation (V&V) processes, activities and tasks in support of all system, software and hardware life cycle processes. The standard also defines the V&V tasks and required inputs and outputs for the process. Following this process ensures requirements are complete, clearly defined, and most importantly helps to ensure that the final design satisfies its intended use and the user's requirements. One tool that is critical for incorporating the V&V process through development of the Hardware and Software design, development and testing, is the Software Life Cycle V-Model as demonstrated in Figure 1. This model may be considered an extension of the waterfall model and demonstrates the relationship between each phase of the development life cycle and its associated testing phase.

As discussed above and shown in the first block of the V-Model, the first step in the process is development of the requirements of the system as collected, documented, verified and validated in a Functional Requirements Specification. This is an important and vital specification needed at the front end of the project and will be used as the procurement specification for the development of the I&C Digital system upgrade. Without this document, procurement specifications are generally vague and non-specific leaving the door wide open for the equipment/software supplier to make un-validated assumptions and to formulate their proposal on a design basis that may or may not meet the full requirements of the project and the end user's needs. As stated previously, use of an FRS helps to minimize the uncertainty and the OEM(s) to reduce and/or eliminate contingency costs from their proposal.

A well written FRS will generally progress through three steps when translating the various existing analog or relay logic requirements into useful software requirements. First the information from the various DBDs, SDs, schematics, elementary diagrams and relay logic diagrams are translated in their entirety into Instrument Society of America (ISA) based logic diagrams, terminology, symbols & descriptions. Then the logic is streamlined to eliminate the redundant logic and/or interlocks required when utilizing discrete relay logic but is not required when software performs the same function. The last step is to tailor the logic, descriptions and requirements to the platform that best fits the application.

Before utilizing the finished FRS for design purposes, it is vitally important at this stage to have the client's operations and design/system engineers to perform a thorough & detailed review to validate that the requirements exactly describe the functions that will meet the end user's needs. If designers and end users wait until after the software is developed and being tested to determine whether or not all functions are operating as needed, it will be very costly to make alterations at this point in the project especially when such changes could be wide sweeping throughout the software, design and documentation. This added cost and delay can be avoided and minimized by ensuring the requirements and logic is correct before the actual software design, programming and testing commences. Otherwise, the end result is a project hampered by ever increasing cost resulting from multiple change orders and rework of the design by the supplier to ultimately meet the client's requirements and end use.

Although the development of an upfront detailed and vetted FRS requires an investment of resources, financing and time, experience has proven that one of the hallmarks of a successful project that is completed on time and within the budget, is a project that has precise well defined requirements developed and specified on the front end. An FRS will help in reducing and/or eliminating the need for change orders, rework and schedule delays because the design will be based from the beginning on a firm verified and validated design basis.

As can be seen in the V-Model, Figure 1, at each phase of the process as the design progresses, the next step is based on a firm foundation that has been established, verified and validated in the previous step. This method allows for traceability of the requirements through the process. In addition, in parallel with the development of the design, testing criteria/instructions are being developed so that the end product can be tested to validate that the requirements have been satisfied. Thus, this provides and explains the V shape of the model.

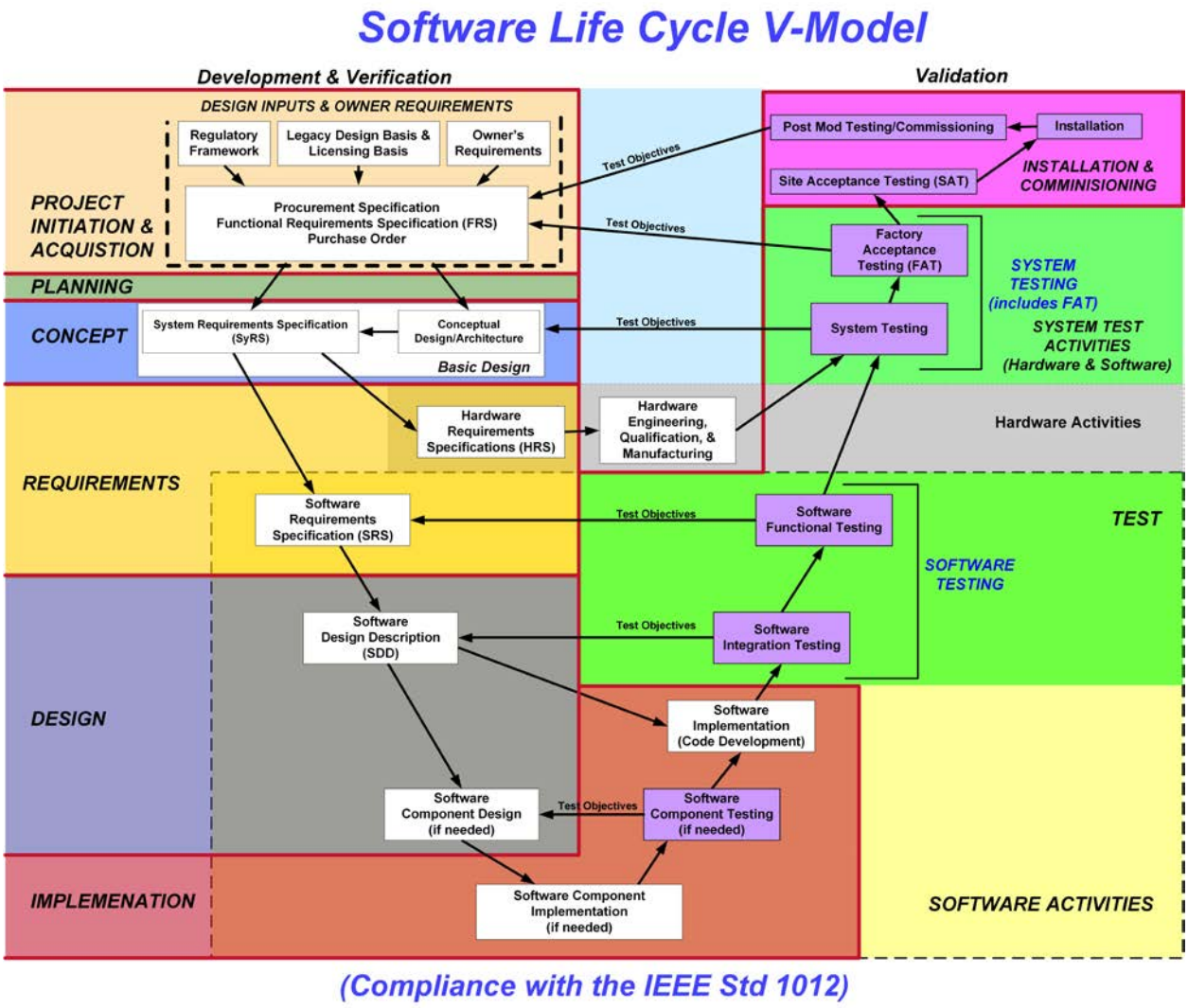

Figure 1. Software Life Cycle V-Model

2 CONCLUSIONS

The most important factors in reducing project cost is assuring that all requirements are well defined and complete in the front end of the project. A detailed and high quality Functional Requirements Specification (FRS) is critical in documenting these requirements and eliminates the need for inflated contingency funds. Since the waterfall or V-Model life cycle development process is used where requirements cascade down from higher tier specifications, based on FRS requirements, to lower tier documentation that implement the requirements, each functional requirement needs to be carefully evaluated to determine if it is applicable to the new digital I&C system. In addition, the follow-on testing instructions and procedures are developed to capture each requirement and to ensure that each requirement is validated via testing of the design. The FRS must include detailed functional descriptions contained in DBDs, SDs, as well as the Updated Final Safety Analysis Report (UFSAR) and must be compared to logic shown in legacy elementary diagrams/schematics to assure the functional requirements are complete, accurate, unambiguous, fully traceable and applicable to the scope of the project. Up front project planning needs to ensure the schedule and budget accounts for development of an FRS which will be vital for a successful implementation of digital upgrades at NPPs.

3 REFERENCES

1. "Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure" (ML16097A182)
2. NUREG 0800, Chapter 7
3. NUREG 0800, Appendix 7.0-A "Review Process for Digital Instrumentation and Control Systems of the NRC's Standard Review Plan" (ML070660258)
4. IEEE-1012, IEEE Approved Draft Standard for System and Software Verification and Validation, 2016 Edition, March 1, 2017
5. IEEE-1012, IEEE Standard for System and Software Verification and Validation, 1998 Edition