31310021R0046 Attachment No. 1
Statement of Work

Title: Assessment of Model-Based Systems Engineering Processes in a Regulatory Review Context for Digital Instrumentation and Controls of Existing Nuclear Power Plants

C.1 Background

Over the past 15 years, Model-Based Systems Engineering (MBSE) has emerged as powerful methodology and practice for realizing and verifying complex embedded systems while providing rigorous evidence of functional and safety compliance. The phrase "Model Based Systems Engineering" has been used in many different contexts to the point where its meaning and purpose is vague. For safety critical systems design, the definition from the systems engineering and the formal methods community is appropriate.

"Model-Based Systems Engineering (MBSE) is the formalized application of modeling to support system requirements, design, analysis, verification and validation activities beginning in the conceptual design phase and continuing throughout development and later life cycle."

Because of its capability to address the software and system complexity and productivity challenges of complex distributed embedded systems, MBSE is quickly becoming the preferred engineering paradigm for the development of such systems across a variety of application domains. However, MBSE has not been used in any significant degree in the nuclear industry.

The NRC's guidance for digital I&C has its origins in a document-based waterfall development model. Modern software (SW) engineering environments are increasingly using highly integrated ecosystems of SW and hardware (HW) development tools with less reliance on published documents during development. These approaches tend to view the model as a portable "executable specification." The NRC is investigating the potential utility and impacts of MBSE methods and tools to the established review process of I&C for nuclear power plants (NPPs).

Documents are created by and for people to use (in the nuclear I&C domain) and are mostly natural language descriptions. Electronic representations, such as models, can be statically and dynamically analyzed by electronic tools. Although a human can never be removed from the development process, certain analysis tasks can be performed more quickly and accurately by electronic tools. Such tools may be difficult to qualify using current NRC criteria, which is focused on whether defects in the tool or resulting software would not be detected by other verification and validation activities.

C.2 Objective

The objective of this contract/order is to obtain expert technical services in order to develop a better understanding of: (1) how Model-Based Systems Engineering (MBSE) methods and tools

can support regulatory reviews of adequate design and design assurance, (2) identify any barriers or gaps associated with MBSE in a regulatory review of Digital I&C for existing NPPs.

C.3 Scope of Work

The proposed research approach is for the implementation of a simple protection system using both: (1) highly integrated computer-based engineering development processes, and (2) MBSE. All the modules of the simple protection system would be modeled functionally, and one FPGA-based circuit card would be modeled/designed in detail. The level of detail in the design and supporting analysis should address independence of functions. Independence should address interfaces between functions and self-testing implemented on the circuit card, as well as voting between protection system elements.

The final product would be the design itself and the associated evidence to demonstrate its technical soundness. Then the NRC technical staff for I&C would review the "demonstration" material and identify additional information needed or material that is not needed for regulatory purposes.

Different parties have different ideas about what it means to use MBSE. This research is intended to identify and explore an existing state of the practice, and not to develop new engineering practices.

MBSE, with its inherent ability to analyze and simulate many different scenarios may be a superior approach for more complex systems, structures, and components (SSCs). Modern digital systems tend to be more complex because they are SW intensive and include more shared resources, more coupling of resources (e.g., digital communication, heterogeneous computing devices), and sometimes adaptive abilities. For these reasons, MBSE is often needed to design such systems to high levels of design assurance. Therefore, the regulator must be prepared for MBSE applications where non-document-based evidences are part of a safety evaluation.

For relatively simple applications, such as a reactor trip system, MBSE may support more robust analysis methods such as formal methods or model-based safety assurance.

This research is to explore the full scope of MBSE (i.e., it is not limited to simulation-based validation of I&C system designs). The use of models and simulations in the early design phases of new NPPs and validation of I&C system designs (e.g., confirm required behavior and identify unwanted or undesirable interactions) is one aspect of MBSE. For each aspect of MBSE, the kind of engineering artifacts should be identified and described to include their use as evidence of the soundness of the design. The alternate review process of DI&C-ISG-06, Rev. 2 (ML18269A259), could help to enable the use of MBSE.

Base System Architecture:

- Four redundant divisions of instrumentation, each containing identical designs:
  - Two instrumentation channels (Pressure and Temperature)
    - Sensor
    - Data acquisition and filtering
    - Setpoint comparison for trip generation
    - Trip output signal generation

- Two trains of actuation logic, each containing identical designs:
  - Two-out-of-four coincidence logic of like trip signals
  - Logic to actuate a first device based on an OR of two instrumentation coincidence signals
  - Logic to actuate a second device based on the remaining instrumentation coincidence signal

Functions to Be Implemented:

1. Trip on high pressure (sensor to actuation)
2. Trip on high temperature (sensor to actuation)
3. Trip on low saturation margin (sensors to actuation)
4. Vote on like trips using two-out-of-four coincidence
5. Automatically actuate devices
6. Manually actuate each device
7. Select mutually exclusive maintenance and normal operating modes on a per division basis
8. Perform setpoint adjustment in maintenance mode
9. Configure the system in maintenance mode to bypass an instrument channel (prevent it from generating a corresponding active trip output)
10. Configure the system in maintenance mode to force an instrument channel to an active trip output state
11. Display pressure, temperature and saturation margin
12. Display each trip output signal state
13. Display indication of each channel in bypass
14. Periodic continual self-test of safety signal path (e.g., overlapping from sensor input to actuation output)

Characteristics to be demonstrated (based on the requirements of IEEE Std 603-2018):

1. Completeness and consistency of requirements
2. Independence among the four divisions of instrumentation (inability for the behavior of one division to interfere or adversely affect the performance of another)
3. Independence among the two instrumentation channels within a division (inability for the behavior of one channel to interfere or adversely affect the performance of another)
4. Independence among the two trains of actuation logic (inability for the behavior of one train to interfere or adversely affect the performance another)
5. Completion of actuation whenever coincidence logic is satisfied or manual actuation is initiated
6. Independence between periodic self-test functions and trip functions (inability for the behavior of the self-testing to interfere or adversely affect the trip functions)

Task 1:

The Contractor shall implement the system described above using both: (1) highly integrated computer-based engineering development processes, and (2) MBSE. All the modules of the simple protection system would be modeled functionally, and one FPGA-based circuit card would be modeled/designed in detail. The deliverable will be the model-based design itself.

Task 2:

The Contractor shall perform preliminary V&V and testing of the design using model-based engineering and testing methods. The deliverable will be the artifacts as described in the proposal.

Task 3:

The Contractor shall participate in an evaluation of the artifacts produced in tasks 1 and 2 with NRC staff. This will consist of:

1. An initial kickoff meeting for this task with the NRC staff.
2. The NRC staff will then provide initial feedback on the artifacts produced and additional information that would be needed.
3. The Contractor shall then attempt to address any issues and provide the additional information within the time for this portion of task 3 (1 month).
4. A second meeting will be held to discuss the additional information provided.

Task 4:

The Contractor shall develop a one-day long virtual presentation on the results of this research that explains the MBSE approach used, the engineered development environment, the development products, and lessons learned from interacting with the regulator. The deliverable will be the presentation and associated materials.

Task 5:

The Contractor shall develop a final report describing the work summarizing the work performed and the results and conclusions derived. The final report shall include findings and recommendations for future research.

C.5 Deliverables and Delivery Schedule

Deliverable	Due Date	Format	Submit to
Task 1 design	4 months after start of work	As appropriate to the tools used.	COR
Task 2 artifacts	6 months after start of work	As appropriate to the tools used.	COR
Task 3	The initial kickoff meeting for task 3 will be held within two weeks of delivery of the artifacts and should be scheduled ahead of time. The NRC will provide input within one month of the kickoff meeting. The Contractor response is to be	As appropriate to the tools used.	COR

	provided within one month of receipt of NRC input. The NRC will provide input and hold the second meeting within one month of receipt of the Contractor responses.		
Task 4	The presentation is to be provided within 11 months of the start of work.	Slides (PowerPoint or Adobe Portable Document Format (PDF)) Training session	COR
Task 5 final report	Within 11 months of the start of work.	Word Document	COR

C.7 Section 508 – Information and Communication Technology Accessibility

C.7.1 Introduction

In December 2000, the Architectural and Transportation Barriers Compliance Board (Access Board) pursuant to Section 508(2)(A) of the Rehabilitation Act Amendments of 1998, established electronic and information technology (EIT) accessibility standards for the federal government.

The Standards for Section 508 of the Rehabilitation Act (codified at 36 CFR § 1194) were revised by the Access Board, published on January 18, 2017 and minor corrections were made on January 22, 2018, effective March 23, 2018.

The revised 508 standards have replaced the term EIT with ICT (Information and Communication Technology). ICT is information technology (as defined in *40 U.S.C. 11101(6)*) and other equipment, systems, technologies, or processes, for which the principal function is the creation, manipulation, storage, display, receipt, or transmission of electronic data and information, as well as any associated content. Examples of ICT include, but are not limited to: Computers and peripheral equipment; information kiosks and transaction machines; telecommunications equipment; customer premises equipment; multifunction office machines; software; applications; Web sites; videos; electronic documents, and email messages.

Note: The following electronic content is covered by the standards:

- Public facing content
- Non-public-facing content that is communicated through one or more of the following:
    - An emergency notification;
    - An initial or final decision adjudicating an administrative claim or proceeding;
    - An internal or external program or policy announcement;
    - A notice of benefits, program eligibility, employment opportunity, or personnel action;
    - A formal acknowledgement of receipt;
    - A survey questionnaire;
    - A template or form;
    - Educational or training materials; or
    - Intranet content designed as a Web page.

The text of the Standards for Section 508 of the Rehabilitation Act can be found in 36 CFR § 1194.1 and in Appendices A, C and D to Part 1194 (https://www.ecfr.gov/cgi-bin/text-idx?SID=caeb8ddcea26ba5002c2eea047698e85&mc=true&tpl=/ecfrbrowse/Title36/36cfr1194_main_02.tpl).

C.7.2 General Requirements

To help the NRC comply with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794d) (Section 508), the Contractor shall ensure that its deliverables (both products and services) within the scope of this contract/order are

1. in conformance with, and
2. support the requirements of the Standards for Section 508 of the Rehabilitation Act, as set forth in 36 CFR § 1194.1 and in Appendices A, C and D to Part 1194.

However, the Contractor's deliverables for tasks 1, 2, and 3, shall only be required to be conformant to the extent supported by the Contractor's existing acquired MBSE tools and their existing MBSE methodology, models, and processes.

As the Contractor's existing knowledge, experience, and the state of their MBSE practice allows, the Contractor shall support the NRC is obtaining insight into how the Contractor's existing acquired MBSE tools and their existing MBSE methodology, models, and processes can support Section 508 conformance for use of the MBSE tools and can support use of the tools to create Section 508 conformant MBSE artifacts.

C.7.3 Applicable Provisions of the Standards for Section 508 of the Rehabilitation Act

The following is an outline of the standards that identifies what provisions are always applicable and which ones may be applicable.

Applicable to the Contract/Order?	Provision of 36 CFR Part 1194
Yes	1) Revised 508 Standards
Yes	a) Appendix A to Part 1194 – Section 508 of the Rehabilitation Act: Application and Scoping Requirements
Yes	i) 508 Chapter 1: Application and Administration - *sets forth general application and administration provisions*
Yes	ii) 508 Chapter 2: Scoping Requirements - *containing scoping requirements (which, in turn, prescribe which ICT – and, in some cases, how many – must comply with the technical specifications)*
*See the **Exceptions** section below*	(1) E202 General Exceptions
No	(2) E203.2 User Needs

Applicable to the Contract/Order?	Provision of 36 CFR Part 1194
Yes	(3) E205 Electronic Content
See below	a) Appendix C to Part 1194 – Functional Performance Criteria and Technical Requirements
Yes	i) Chapter 3: Functional Performance Criteria – *applies to ICT where required by 508 Chapter 2 (Scoping Requirements) and where otherwise referenced in any other chapter of the Revised 508 Standards*
No	ii) Chapter 4: Hardware
Yes	iii) Chapter 5: Software
Yes	iv) Chapter 6: Support Documentation and Services *(applicable to, but not limited to, help desks, call centers, training services, and automated self-service technical support)*
Yes	v) Chapter 7: Referenced Standards - *the standards referenced here apply to ICT where required by Section 508 Chapter 2 (Scoping Requirements) and where referenced in any other chapter of the Revised 508 Standards*
No	2) Appendix D to Part 1194 – Electronic and Information Technology Accessibility Standards as Originally Published on December 21, 2000

Refer to 508 Chapter 2 (Scoping Requirements) first to confirm what provisions in Appendix C apply in a particular case.

C.8 Incremental Development for Software

The Contractor shall use an incremental build model for software development. The Agency defines an incremental build model as a method of software development where the product is designed, implemented, and tested incrementally, with increasing functionality and/or capability added in each increment until the product is finished.

C.9 Place of Performance

Contractor's site.

C.10 Contractor Travel

None. The training will be virtual.