Meeting 1:

1. Welcome
   1. Agenda/Objectives of the meeting
   2. Introductions of Consortium Members
      1. One representative from each utility to share the state of digital modernization at their utility 5-7 minutes. Here are some topics to consider:
         1. Digital Strategy
         2. Modernization Phased Approach
         3. Digital Organization – Who is contained (e.g. projects, design, maintenance, operations, training etc.)? Projects focused vs long-term asset management focused?
         4. Decision Making Framework for Digital Upgrades
         5. Standard Requirements for Digital Components
         6. Digital Design Change Process (Software/Hardware)
2. Consortium Framework
   1. Charter
      1. The purpose of this group is to network, problem-solve, and advocate for the strategic digital direction of the US nuclear fleet.
   2. Responses to Questionnaire
   3. Communication Plan – SharePoint
   4. Rules of Engagement
      1. Every topic: every utility will be called on to speak up
      2. For technical questions, consider posting in the SharePoint.
      3. 1 Communication Rep per company will respond to questions posed in the SharePoint based on their group consensus
3. Protection System Upgrades - Pablo
   1. Approach to Platform Decisions
   2. Approach to Procurement Spec Development
      1. Is effort put into a conceptual design first? How much detail?
      2. Competitive vs. non-competitive?
      3. LOE (Man-hours/Month)?
   3. What challenges has Peach Bottom’s LAR has faced with achieving NRC approval, specifically with regards to CCF and FPGA technology?
   4. What is your Safety Analysis role in licensing activities (Limerick, Peach Bottom)?
   5. Approach to contracts – lessons learned
4. Strategic Activities
   1. Understand efforts to capture control room modernization process within digital upgrade environment.
      1. DOR – Who leads the effort?
      2. Benchmarking Opportunities?
   2. What is your Project Group and Engineering Group Structure to support the design and implementation of your Digital mods?
   3. Do you have a digital support organization? In other words, what digital organization that will own future digital projects including any plans to create a new maintenance organization/model?
      1. Is it located at the site or is it a corporate entity with some site located support?
      2. How is the support team organized?
      3. How do you maintain cyber security information? At the site or corporate offices?
      4. Do you have a dedicated cyber secure test/warehouse area on site?
      5. Can you share an organization chart (no names)?
      6. Do you have a process (or planned process) where equipment data can be seen and analyzed at the corporate offices?
   4. Goals for Modernization
      1. Are your business operations teams involved in developing the modernization strategy?
      2. Has there been a consideration in aligning modernization efforts with business objectives to ensure a purpose-driven transformation?
      3. Does the current technological infrastructure of your legacy I&C systems influence your modernization plans (including architecture) to determine the scope and feasibility of your modernization initiatives?
      4. Do your current business operations, maintenance, engineering, procedures support the development process enabled by recent advances in industry procedures. For example, have project management procedures been updated to follow Agile methods vs traditional waterfall methods? This is also applicable to engineering.
      5. Have non-tangible benefits to the modernization program (e.g., improved employee morale, enhanced reputation) been considered in BCA?
   5. Enhancements
      1. How is the scope and priority of modernization efforts determined?
      2. What modernization approach will you take (e.g., re-platforming, re-architecting, re-building)?
      3. What are your governance and operating models for the modernization program?
   6. Risks/Benefits
      1. What are the potential risks and challenges that are seen in your organization? (e.g., resistance to change, security vulnerabilities, technical issues)
      2. How will these risks be identified and assessed? How is the potential impact and likelihood of each risk evaluated?
      3. How will these risks be mitigated? What contingency plans will be in place?
      4. How will issues be identified, tracked, and resolved?
      5. Can you share an example of a particularly complex digital project you managed and how you successfully navigated through challenges?
   7. Have you developed process/plans for system refreshes?
   8. Have the industry standard procedures increased or decreased efficiency for you?
5. Long Term Digital Asset Management
   1. How do you support the transition of system test/turnover to the station if you do not already have a digital maintenance organization in place?
   2. What are the roles and responsibilities for Testing for Digital Modifications, from FAT, SAT and PMT?  What high level activities do you perform at SAT and PMT?
   3. What is your training plan for digital modifications?
      1. Installation, testing, maintenance of the system
      2. Future design changes – Are internal resources trained to perform minor design changes? Tuning parameters
   4. Have you run into issues with vendor support capabilities after installation?
   5. Do you have a plan for training or building a team for the transformation?
   6. Do you have a plan for data migration and integration?
   7. Does the records retention system support modernization and parameter configuration control?
   8. Software Configuration Management / Digital Repository / Version Control
      1. How are software/program files handled throughout your fleet?
      2. What does Software Version Control look like?
         1. How frequently are backups taken and how are they stored?
      3. Have you adopted a standard for software configuration management?
      4. What does excellence look like? Where do we want to go with this in the future?
         1. DOR – internal or external control of software configuration?
   9. Software changes post commissioning
      1. DOR
         1. Develop the change
         2. Analyze the licensing aspect
         3. Perform testing
         4. Implement the change
      2. Licensing Process
      3. Role of the Secure Development Environment
      4. Graded approach for software changes – are there “minor” changes that can be handled in house? Do you want to handle them in-house?
         * 1. Tunable parameters?
           2. Graphic Interfaces?
           3. Administrative tasks – password changes, transferring files
      5. What are the scoping criteria for adjustments performed internally vs externally?
      6. How to handle “minor” software changes regarding protection systems
         1. Do you have/need a SDE?
         2. Do you have the proper QA processes in place? Would this fall under your current QA processes or would there need to be an update to them?
         3. What training and software do you need access to for the change development/implementation?
            1. Can we build this into the contract with the vendor?
         4. How is it different for safety vs non-safety system changes?
         5. Can we have a standard process across utilities for developing, testing, installing, and post-mod testing of software changes?
6. Action Items & Closeout

Future Meeting Topics:

1. Cyber Security
   1. Does your Cyber Security Plan allow 2-way (non-deterministic, firewall) communication between Level 4 and Level 3?
   2. Does your Cyber Security Plan allow 2-way (non-deterministic, firewall) communication between Level 3 and Level 2?
   3. Does your Cyber Security Plan allow 2-way (non-deterministic, firewall) communication between Non-Safety Control and Non-Safety Monitoring (e.g. would your plant computer be able to send digital communication to your turbine control system)?
      1. In what cyber defensive level would your turbine control system reside?
      2. In what cyber defensive level would your plant computer system reside?
   4. Has your cyber team ever made any changes to the Cyber Security Plan?
      1. Did they use LAR or 10CFR50.54p?
      2. If LAR, what was a summary of the change?
2. Human Factors
   1. High level description of HFE program and qualifications (if applicable) and integration into the design process, project lifecycle.  Specific example for graphic development.
3. AI/Smart Tech
4. Simulators
   1. What is your plan for integration of digital project into the Simulator. How would that be scheduled and implemented?  What groups, roles and responsibilities, are involved?
5. Project Management
   1. How will you handle multiple systems in an outage with respect to tagging?
      1. How do you align tagging with testing?
   2. Do you have a process to ensure attendance at meetings, i.e. 30%, etc.?
   3. What tools and methods do you used to ensure management, station and stakeholder communication, engagement, and support?
   4. How do you interact with your O&P groups? How far in advance do you engage them especially O&P/Operations to provide them with an indication of work being developed?