
DIABLO CANYON POWER PLANT PROCESS PROTECTION SYSTEM REPLACEMENT LESSONS LEARNED USING ISG 6 NRC Digital I&C Workshop Meeting July 1, 2015



Ken Schrader, MS
Principal Engineer PG&E
Vice Chairman, PWROG

kjse@pge.com
805-545-4328

Agenda

- ISG 6 (*Licensing Process for Digital I&C System Modifications*) Pilot Application and Status
- PG&E ISG 6 Positive Experiences
- PG&E ISG 6 Lessons Learned

ISG 6 Pilot Application

- Diablo Canyon is pilot plant for use of ISG 6
 - PG&E participated in ISG 6 working group
- PG&E submitted pilot application 10/26/11 (ML11307A331)
- Process Protection System replacement
 - Invensys Tricon V10
(PLC based, triple redundancy)
 - Westinghouse Advanced Logic System
- (FPGA based, redundancy and diversity)



ISG 6 Pilot Application

Current Status

- Invensys - Factory Acceptance Testing (FAT) completed and equipment delivered
- Westinghouse – Factory Acceptance Testing (FAT) in progress
- Initial ACRS meetings completed with no requested changes, additional ACRS presentations expected
- Completing final documentation to be submitted and will need to respond to final set of RAIs
- NRC approval expected early 2016

ISG 6 Pilot Application

- NRC support of application has been excellent
 - Resources
 - Knowledgeable personnel
 - Use of sharepoint site to view documentation
 - Efficient resolution of open items
 - Identifying lessons learned from Oconee project
 - ACRS presentations/meetings

ISG-06 Positive Experiences

- ISG 6 Pre-submittal (Phase 0) Meetings
 - NRC feedback critical to completing initial design that did not require any subsequent significant changes
 - PG&E decided to not use cross channel communications, two-way safety communications, or signal voting in the design
 - Meetings very beneficial to confirm understanding of requirements, reduce licensing and financial risk

ISG-06 Positive Experiences

- Phase 0 Meetings Topics, PG&E Meetings
 - ❑ Design redundancy and diversity
 - ❑ Diversity and Defense-in-Depth (D3) assessment
 - ❑ Communications
 - ❑ Software development requirements
 - ❑ System connections to non-safety systems, maintenance and plant computer, control systems
 - ❑ Cyber security controls
 - ❑ LAR contents (figures, level of detail, documents)

ISG-06 Positive Experiences

- ISG 6 Process for use of Approved Vendor Topical Reports (Tier 1, “fast-track”)
 - Significantly simplifies LAR (5-10 times smaller)
 - Can largely reference topical report for compliance with ISG-4, IEEE-603, IEEE 7-4.3.2
 - Eliminate need for large project team (utility and vendor)
 - NRC will have prior experience with platform

ISG-06 Positive Experiences

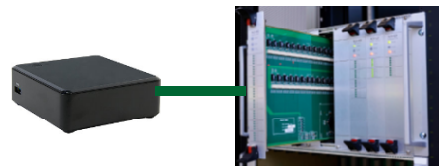
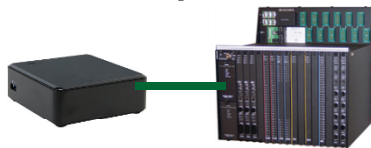
- ISG 6 Allowance for Open Items List and Public Phone Calls
 - NRC Open Items emailed, public calls held to discuss items, Open Items contained in NRC teleconference summary letter
 - Allowed efficient resolution of questions
 - Use of Open Items list
 - Limits Requests for Additional Information that require docket responses
 - Allows NRC feedback on responses during calls

ISG-06 Positive Experiences

- Use of Internet Sharepoint Website for Documents
 - Allowed documents to be viewed by NRC staff
 - Facilitated efficient response to questions
 - Limited the number of documents and information that needed to be submitted

ISG-06 Lessons Learned

- PG&E original design used single non-safety maintenance workstation for both Tricon and ALS subsystems in each of four divisions
- Testing and software requirements following software changes were not considered, became NRC issue
- PG&E changed design to use separate maintenance computer for each subsystem in each division
 - Simplifies factory acceptance testing requirements and eliminates potential software interaction issues



ISG-06 Lessons Learned

- PG&E issued single Functional Requirements Specification for project (applied to both vendors)
 - ❑ All functional requirements were not applicable to each vendor
 - ❑ Resulted in unnecessary difficulty for vendor design, vendor documentation, and NRC review
 - ❑ Contributed to vendors not meeting all applicable requirements during detailed design
 - ❑ Vendor verification personnel and NRC identified issues during vendor audits
 - ❑ Required redesign, extended vendor schedules, complicated NRC review
-

ISG-06 Lessons Learned

- PG&E did not incorporate I&C maintenance personnel expectations to support troubleshooting and maintenance into initial Functional Requirements Specifications
 - ❑ Required revision to Functional Requirements Specification to include maintenance personnel needs
 - ❑ Caused vendors to have to redesign to meet a few new functional requirements

ISG-06 Lessons Learned

- Vendors did not fully understand meaning of some functional requirements
 - ❑ Nuclear requirements and terminology are unique
 - ❑ Some vendor design personnel did not have prior nuclear project experience (most PLC and FPGA business is non-nuclear)
 - ❑ Clarifying questions on requirements from vendors occurred late in detailed design, required some redesign
 - ❑ Utilities need to proactively ensure vendor design and IV&V personnel have correct understanding of all requirements

ISG-06 Lessons Learned

- Vendors underestimated effort for detailed design
 - ❑ First-of-Its-Kind large scope application of each vendor platform to US nuclear plant protection system
 - ❑ Nuclear requirements and processes are more complex
 - ❑ Vendor document revisions required to address ISG 6 requirements
- Two year delay occurred in LAR review schedule to address combined aspects of functional requirements specification changes, redesign, and First-of-its-Kind engineering

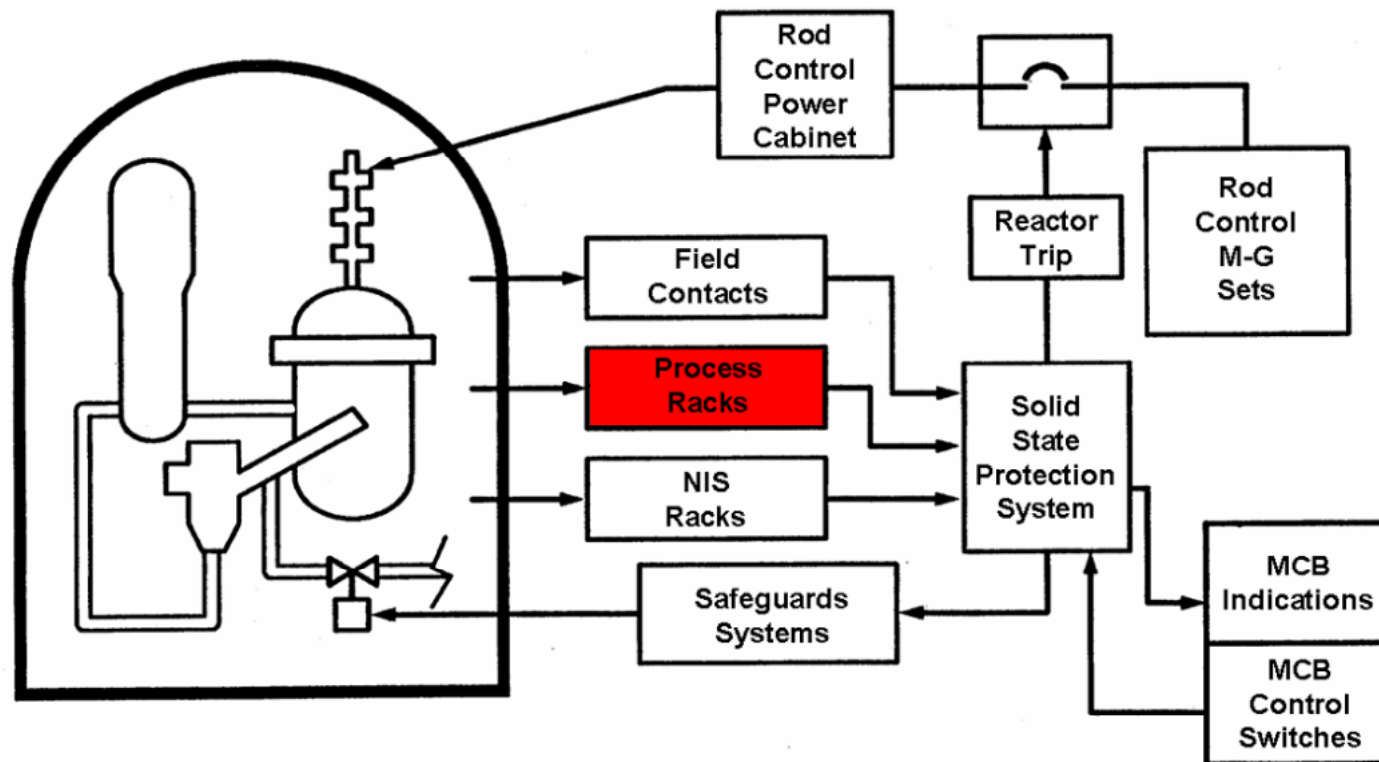
Summary

■ ISG 6

- ❑ Roadmap to success to develop acceptable License Amendment Request (LAR)
- ❑ ISG 6 process will reduce licensing uncertainty and effort for future licensees/vendors
- ❑ Utilities should strongly consider designs with approved Vendor Topical Reports
- ❑ LARs following ISG 6 and incorporating lesson learned from initial plant applications can be approved in timely manner

ISG 6 Pilot Application

■ Project Scope



ISG 6 Pilot Application

■ Process Protection System Replacement Architecture

