Licensing the ALS FPGA Based Safety Related I&C Platform

Wolf Creek Nuclear Operating Corporation

CS Innovations, LLC

Regulatory Information Conference (RIC)
March 11th, 2009

Introduction

- Wolf Creek Nuclear Operating Corporation (WCNOC) to install first implementation of the Advanced Logic System (ALS) during fall 2009 refueling outage
- For WCNOC and CS Innovations (CSI), installation is culmination of five year development and 24 month licensing effort

Safety Related I&C Platform Study

- ALS project was born out of immediate need to solve reliability and obsolescence issues
  - WCNOC conducted study of challenges faced by all USNPPs replacing their existing safety related I&C systems.
  - Found that original manufacturers of existing equipment are in most cases out of business or no longer support the product lines.
  - Situation typically leads to two approaches, each with their own challenges:
    1. Reverse engineer existing system/maintain as obsolescence and failures occur
       - Short-term fix for long-term problem
       - Offers little benefit from advancements in system integrity, diagnostics, and testability
       - Updated version subject to same obsolescence problems, multiplied due to number of components required to replace or update all safety related I&C systems
       - Requires specific experts and specific training
    2. Replace the system with a Commercial-Off-The Shelf System (COTS)
       - Complex system, designed targeted for more complex industrial control apps
       - COTS platforms are rapidly advancing, thus shortening the obsolescence cycle. This creates a cost model the NPP is unable to justify
       - Cost and effort to upgrade physical and procedural infrastructure provides little benefit

Safety I&C Platform Goals

- Common Platform for Safety I&C Architecture
- Mitigate Impact of Future Obsolescence
- Increase Integrity
- Increase Reliability
- Minimize Cost and Effort to Retrofit
- Advanced Testing and Diagnostics
- No Additional Diverse Actuation Systems
- Approval for RPS/ESFAS Applications

NRR I&C Staff Interaction

- Early Interaction Produced Positive Feedback from NRR I&C Branch
  - July 2006 Face-to-Face Meeting, including NRR and Research
  - Several conference calls were held early in the process
- LAR Submitted in March 2007
  - Wolf Creek did not have a good understanding of what information needed to be submitted in the LAR
- Subsequent submittals were made from July 2007 to February 2009
- Face-to-Face meeting in July 2007 involving NRR and Research
  - The meeting was very beneficial in clarifying the details of the ALS architecture
- Two inspections were performed at CS Innovations
  - CS Innovations personnel provided immediate responses to reviewer questions
  - The inspections proved to be critical in helping progress the review process

Review Process

- FPGA based platform created difficulty due to “first of a kind”
- Final product delivered to Wolf Creek is a fixed hardware system
  - The design process utilizes software tools to achieve the final hardware
  - A robust design process must be employed
- FPGA design process is different than software design process
  - This created a misunderstanding for WCNOC and CSI as to the use of IEEE 7-4.3.2 and it’s applicability to the ALS
  - Final agreement resulted in use of applicable portions of IEEE 7-4.3.2 with the purpose of ensuring a robust design process
- Given the first of a kind nature of the review, all parties; WCNOC, CSI, and NRR I&C Staff kept an open mind and worked through the difficulties
  - Good communication was maintained throughout the review, particularly in the final stages

Status of Project

- All information has been provided to NRR I&C Staff
- NRC audits and visits complete
- No outstanding technical items
- SER in progress, very close to issue
- Overall Review Consisted of Multiple Reviews
  - Generic Topical
  - Applications Specific
  - Generic Application
- MSFIS Equipment Designed, Built, Qualified, Tested
- Install Fall 2009

Let's review the goals of the project and how they were met!

Meeting the Goals

Common Platform for Safety I&C

- ALS architecture is scalable, from single system replacement to full safety I&C replacement
- ALS is architected with dedicated and redundant control modules, which are designed for reliability and integrity attributes critical to safety systems

Mitigate Future Obsolescence

- Fewer components and common components – one FPGA per board incorporates all digital circuits, filters, and bus communication (no "chip set" ICs required)
- For the primary critical component (FPGA), obsolescence is mitigated by utilizing portable RTL design which supports targeting to a new technology if required in the future

Increase Integrity

- ALS is capable of detecting failures while the system is operational
- ALS performs corrective action upon detection of a failure
- The ALS utilizes redundancy and/or Digital BIST for all critical circuits
- ALS Incorporates dedicated integrity logic and provides run-time detection of a changed device and/or board behavior

Meeting the Goals - 2

Increase Reliability

- Increased reliability and robustness by implementing an appropriate level of design complexity, which results in fewer active components, and translates directly to a lower system failure rate
- ALS utilizes only proven design practices and methodologies for implementation of the hardware
- ALS utilizes distributed monitoring of the integrity and validity of signals, and provides the capability to take action on exceptions

Minimize Cost of Retrofit

- Installation is simplified due to reduced hardware and wiring, maintenance is simple, efficient, and reliable translating to lower on-going costs to maintain
- The ALS provides simple, efficient, and reliable maintenance with a high degree of visibility into the system, where all boards are easily replaceable, reusable, and hot-swappable
- Training for plant personnel is reduced due to simplicity of the system and the ability to implement multiple applications with a common platform

Advanced Testing and Diagnostics

- Provides deterministic testing, maintaining the same behavior
- A run-time test strategy provides exhaustive self-testing to validate system integrity
- Advanced diagnostics are provided utilizing the ASU and Built-in Self-test (BIST)

No Additional Diverse Actuation

ISG #2 – Diversity and defense in depth

- The ALS architecture implements key design attributes which are sufficient to eliminate the consideration of Common Cause Failure (CCF)
  - This conclusion is based on the guidance provided in U.S. NRC document DI&C-ISG-02 "Task Working Group #2: Diversity and Defense-in-Depth Issues", Revision 1, September 2007
- DI&C-ISG-02 states in section 5 "There are two design attributes that are sufficient to eliminate consideration of CCF:"
  - Staff position 1 states that if sufficient diversity exists in the protection system such common cause failures within channels can be considered to be fully addressed without further action, no additional diversity would be necessary in the safety system.
  - Since there is adequate diversity, no DAS or manual actions were necessary

Compliance with ISG #1 and #4

ISG #1 – Cyber Security

- There is no inbound communications, so there is no path for cyber attack
- Logic configuration can only be changed by removal of board while the channel is off-line, so no changes are possible while the channel is performing the safety function
- There is no operational software, so there can be no unintended functions within the software, and no operational software changes
- All hardware circuits are traced to state machines used by requirements. There are no unneeded circuits
- The design life cycle considered cyber security as required by RG 1.152

ISG #4 - Communications

- The only two-way communications with non-safety is with the ASU
- Section 1. There is no interdivisional communications
- Section 2. The command prioritizations is between automatic and manual safety related signals, and the command to isolate takes priority. All inputs are safety-related. There are no non-safety inputs during operation. Since the command is processed by a finite state machine, verification is simplified.
- Section 3. There are no multidivisional control and display stations

What's Next at Wolf Creek

Wolf Creek Safety I&C Replacement Plan

-**MSFIS (RF17, Fall 2009)**

-**LSELS (RF19, Fall 2012)**

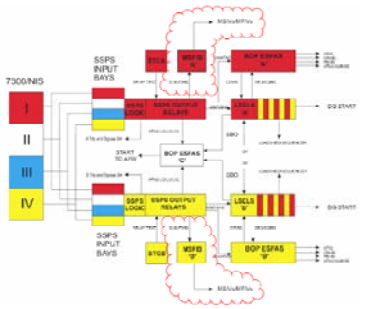
-**BOP ESFAS (RF19, Fall 2012)**

-**SSPS**

-**TC/CCM (On-line)**

-**RVLIS**

Wolf Creek Safety I&C Architecture (RPS/ESFAS)



Questions?

Gregg Clarkson
Project Manager, Safety I&C
Wolf Creek Nuclear Operating Corporation
(620) 364-8831 x4438
grclark@wcnoc.com

Steen Sorensen
President
CS Innovations, LLC
(480) 612-2040
steen@cs-innovation.com