ANS 11th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies

NPIC HMIT 2019

Insights and Experience from the NRC Review of APR1400 I&C Design

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Dawnmathews Kalathiveettil

Electronics Engineer

Office of Nuclear Reactor Regulation

USNRC

ANS

Disclaimer

This presentation presents the personal opinions and viewpoints of the authors. Although the authors are employees of the NRC, the NRC expresses no opinion whatsoever either in support of, or in opposition to, the contents of this presentation. Reference to this presentation is not a sufficient basis for establishing the acceptability of any proposed system, and will not be accepted as an adequate justification or technical explanation in any licensing application.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ANS

Overview

- Background
- Overall I&C Architecture and Independence
- Deterministic Behavior and Platform Characteristics
- Diversity Strategies
- Lessons Learned
- Conclusion

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

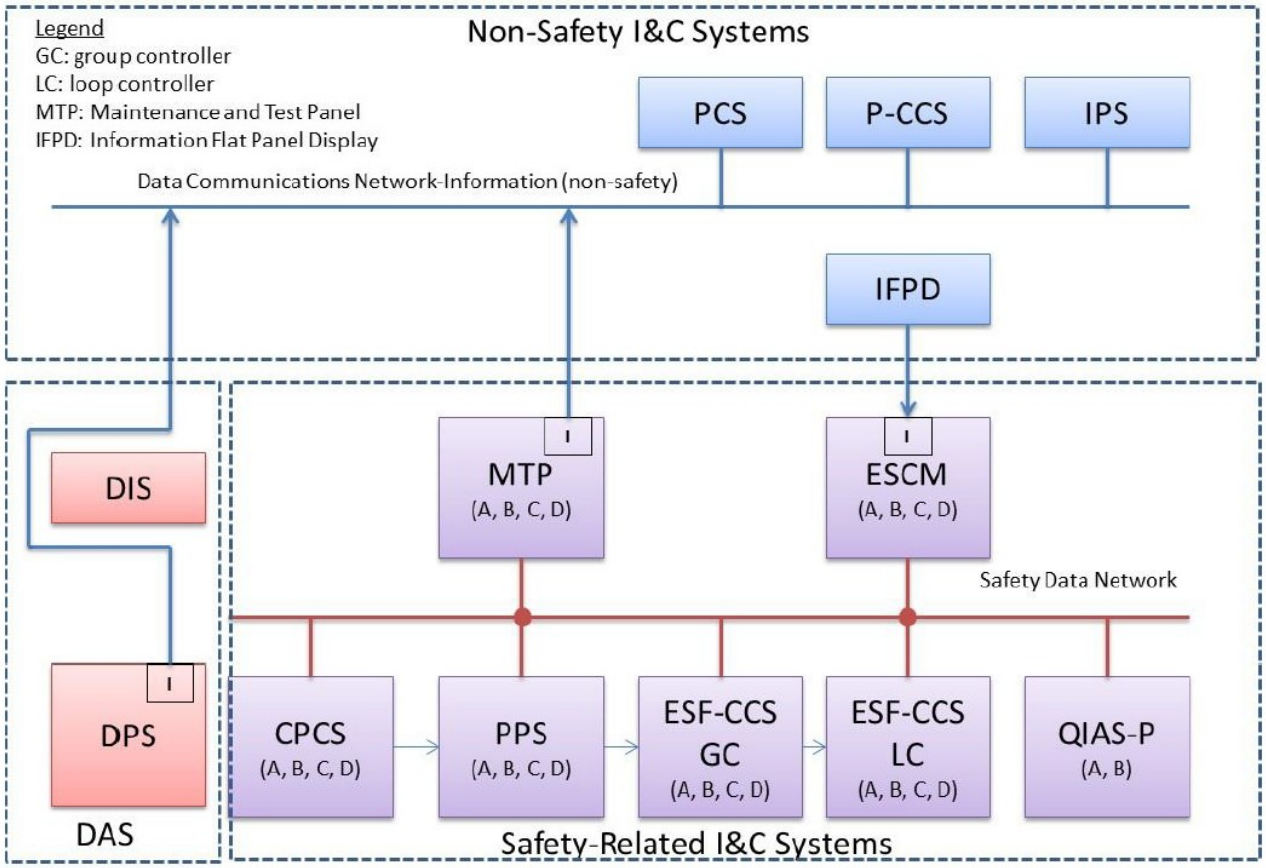
ANS

Background

The staff reviewed the design against the following:

- Title 10 of the Code of Federal Regulations (CFR) Section 50.55a, which incorporates by reference IEEE Std 603-1991, and other applicable regulatory requirements.
- 10 CFR Part 50, Appendix A, General Design Criteria applicable to I&C system.
- Chapter 7 of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," Revision 6.
- Applicable I&C regulatory guides and NUREGs.

Overall I&C Architecture



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ANS

Architecture and Independence

- NRC staff focused on the various interfaces and how independence is achieved between these interfaces
- Applicant needed to demonstrate:
  - that hazards associated with non-safety to safety data communication would not impact safety
  - how the non-safety to safety-related I&C system communications enhanced the performance of safety functions as specified in DI&C-ISG-4

Demonstrating Independence

- The applicant modified the ESF-CCS Soft Control Module (ESCM) that directly controls safety-related components to be divisionalized
- The applicant also provided an analysis that demonstrated an operational time reduction when using IFPD in conjunction with the ESCM to control safety-related equipment versus using the ESCM in a standalone manner

Deterministic Behavior And Platform Characteristics

- Common Q platform is a multitasking operating system
- It uses a scheduling technique and design restrictions to ensure that deterministic performance can be achieved
  - Specifically, this scheduling technique specifies shorter cycle duration tasks have higher job priority than longer duration tasks
- In order to ensure all tasks are completely, the Common Q Platform Topical Report specified that the platform's central processing unit load limit must be set to under a certain percentage

Diversity Strategies

- DAS is the independent and diverse system used by the APR1400 design to mitigate the effects of software CCFs
- DAS is credited to meet the NRC four point position on diversity and defense-in-depth established in Item II.Q of the Staff Requirements Memorandum to SECY-93-087
- The DPS is credited to meet the requirements of 10 CFR 50.62 regarding Anticipated Transient Without Scram mitigation

Diversity Strategies

- The actuation signals from the ESF-CCS, the DPS, and DMA switches converge at the Component Interface Module (CIM)
- The CIM is a non-software-based, nuclear safety grade module which does the signal prioritization and actuation of plant components
- The CIM priority logic is implemented using complementary metal-oxide-semiconductor or transistor-transistor logic devices
  - CIM is diverse enough such that the same CCF cannot affect both the CIM and the safety-related I&C system

Diversity Strategies

- The DPS uses shunt trip mechanism; PPS uses undervoltage trip mechanism – this provides functional diversity for meeting Anticipated Transient Without Scram requirements

- The DPS and DIS are both implemented on FPGA Logic Controller (FLC) technology while the safety-related I&C systems are implemented on the Common Q PLC-based platform – this provides design and equipment diversity

- Hardware Description Language is used for programming the FLC of the DPS and DIS. The Common Q PLC-based platform is programmed using software for microprocessor-based technologies – this provides software diversity

Lessons Learned

Pre-application Meetings

- Held several pre-application coordination meetings
- Meetings enabled applicant to present key aspects of the planned submittal and allowed staff the opportunity to provide feedback on any challenging areas of the design that require more focus
- Significant gains in efficiency of the APR1400 I&C systems review
  - decrease in the number of requests for additional information issued compared to previous design certification applications
  - decrease in review time and resources

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ANS

Lessons Learned

Phase Discipline

- Design certification application reviews typically have six phases
- During previous DCA reviews, the NRC staff spent a significant amount of resources during the Phase Four review in order to resolve the open items identified in Phase Two of the review process
- However, during the APR1400 I&C systems review, the staff used lessons learned from the previous design certification application reviews to ensure that all open items identified in Phase Two safety evaluation report had clear paths for resolution.

Conclusion

- Design decisions may have a significant impact on the safety and regulatory compliance demonstration
- Having pre-application meetings and discussions resolves many issues upfront
- Having phase discipline during the review ensures there are minimal unresolved open items during late stages of the review

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ANS

Acronyms

- CFR: code of federal regulations
- CIM: component interface module
- CPCS: core protection calculator system
- DAS: diverse actuation system
- DCS: non-safety distributed control system
- DI&C: digital instrumentation and controls
- DIS: diverse indication system
- DMA: diverse manual actuation switches
- DPS: diverse protection system
- ESF-CCS: engineered safety features – component control system
- ESCM: ESF-CCS soft control module

Acronyms

- I&C: instrumentation and controls
- IFPD: information flat panel display
- IPS: information processing system
- ISG: interim staff guidance
- NRC: United States Nuclear Regulatory Commission
- P-CCS: process component control system
- PCS: power control system
- PLC: programmable logic controller
- PPS: plant protection system
- QIAS-P: qualified indication and alarm system safety
- RMS: rate-monotonic scheduling
- SECY: NRC commission paper

Any Questions ?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

ANS