DIGITAL I&C IN NUCLEAR POWER PLANT - ISSUES AND CHALLENGES

Neeraj Agrawal, **Ravi Parkash**
Nuclear Power Corporation of India Limited, Mumbai

ABSTRACT

The use of digital I&C in nuclear power plants may result in significant technical and economical benefits, but it poses unique technical challenges. In this paper various issues and challenges for use of digital I&C in Nuclear Power Plant are discussed.

KEYWORDS

Communication Independence, Common Cause Failure, Cyber Security, Documentation, Human Machine Interface, Nuclear Power Plant, Obsolescence, Verification & Validation

INTRODUCTION

Nuclear Power Plant (NPP) can be broadly divided into three main parts namely: Nuclear Island (NI), Conventional Island (CI) and Balance of Plant (BOP). Nuclear Island mainly consists of Nuclear Steam Supply System and associated systems. Conventional Island mainly consists of Turbine-Generator system and Secondary Cycle systems. Balance of Plant consists of various auxiliaries like D.M. water plant, Compressed air system, Chilled water system, etc. Traditionally for control of systems located in nuclear island, custom built systems either hardwired or computer based systems are used. These systems are designed, developed and manufactured for a specific application by NPCIL and other constituent units of DAE (Department of Atomic Energy). For control of systems located in conventional island, PLCs/Controllers/Distributed control systems (DCS) available in market are qualified for use in nuclear power plants and are used. For control of balance of plant systems, standard PLCs/controllers available in market are used.

TYPICAL I&C ARCHITECTURE OF A NPP

The I&C architecture in Indian NPP is engineered based on design, safety, operational criteria and above philosophy. Proper selection of I&C architecture at a NPP enables and ensures safe, reliable operation and helps in economic power generation. A hierarchical architecture is used for plant control. These hierarchies are designed such that failure of upper level does not affect the operation of lower level.

This I&C architecture is distributed among four levels of hierarchy:

Level 0: Process Interface: This level comprises field instrumentation and actuators.

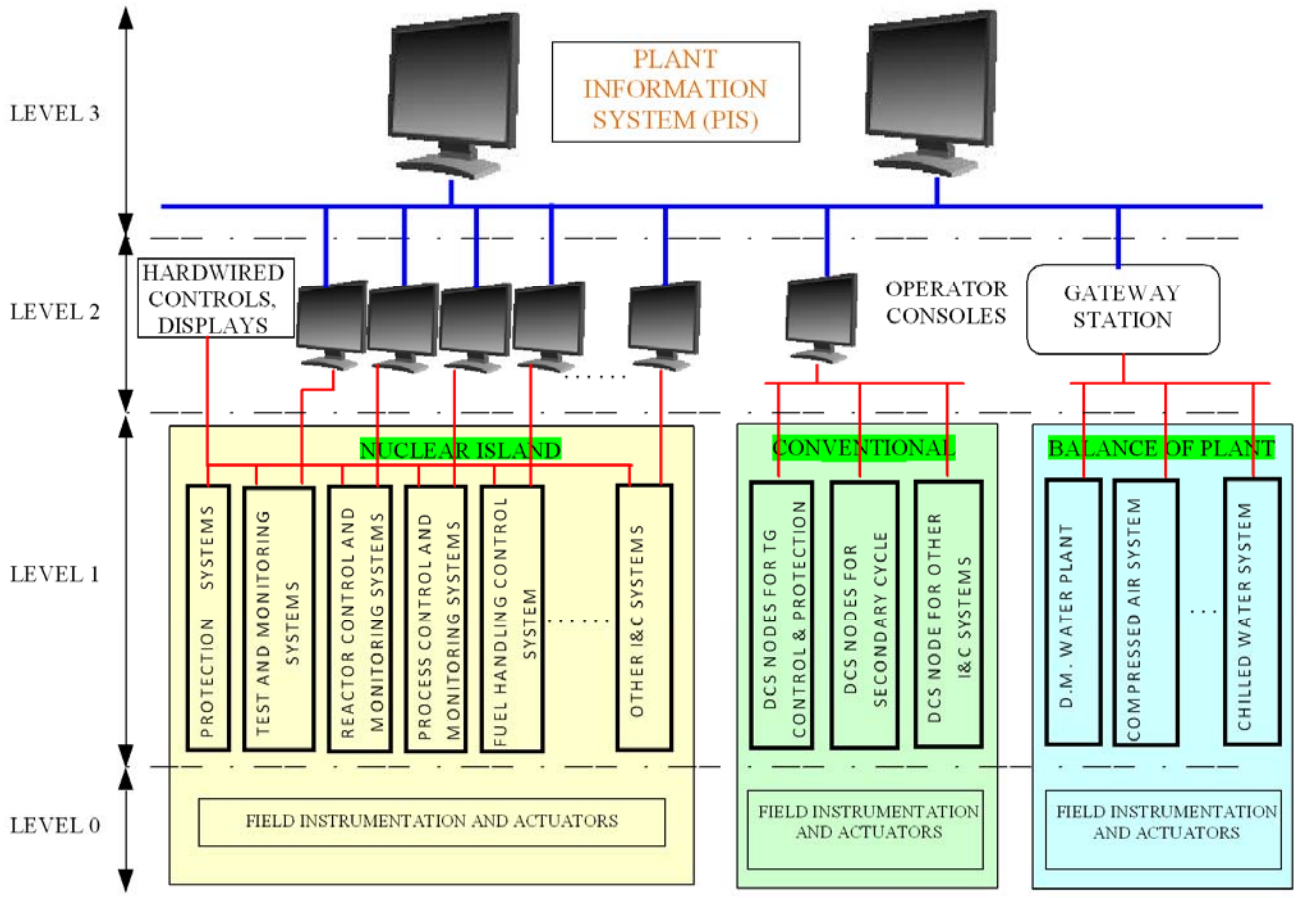

Figure-1

Level 1: System Automation: This level consists of processor based systems or analog systems or relay based systems. This level covers data acquisition, signal conditioning, signal processing, algorithms for controls and generation of output for actuator control.

Level 2: Unit Control and Supervision level: This level comprises of human machine interface and associated data processing functions.

Level 3: Site Management level: This level provides entire plant information for management.

Typical I&C architecture of a NPP is schematically shown in figure-1:

In Indian NPP due to safety concerns and reliability issues functionally distributed and independent I&C architecture is still in use. This division of I&C architecture is done based on **safety classification** of the I&C functions and systems. To take care of various safety issues at level 1, I&C architecture is divided into various computer based systems (CBS)/relay based system depending on their importance to nuclear safety. The design and engineering of computer based systems follow a diverse and independent philosophy. CBS of nuclear island are specifically designed and developed for the specified functions and these

systems employ only matured and well proven technologies. Each of these computer based systems is designed for maximum functional cohesivity and minimum connectivity with other CBS. For example all field instrumentation and signals required for reactor control and monitoring functions are directly wired to a dedicated CBS. All algorithms are processed in this system and field outputs are directly given from this CBS. In other words, each of this CBS is self-sufficient and failure of any computer based system does not have any effect or have minimal effect on operation of other I&C systems. In other power industry functionally distributed but interlinked I&C architecture with common hardware and software is used. Use of such functionally integrated, interlinked I&C architecture raises various issues in NPP.

INTEGRATION OF HUMAN MACHINE INTERFACE

In Nuclear Power Plant, Human Machine interface (HMI) is provided to operator through a combination of Video Display Units, hardwired indicators and annunciators. HMI systems are designed for optimal performance of the operator. Human factor engineering practices are applied to provide operator friendly operation and maintenance of systems so as to minimise the possibility of human error.

In the architecture for NPP an attempt needs to be made to provide uniform HMI. Since each digital I&C system is provided with its own operator interface this result in a variety of operator interfaces. This is not conducive to stress free operation by operator. Hence providing an integrated and identical HMI in NPP meeting the diversity concerns poses the biggest challenge to the I&C designers. For achieving uniform HMI meeting the diversity concerns following needs to be done:

a) Provide uniform HMI for various systems of nuclear Island and integrate them in to common HMI. While doing this it must be ensured that diversity is maintained and protection against common-cause failure is provided.
b) Provide uniform HMI for “Conventional Island systems”, “BOP systems” and nuclear Island systems. But systems for “conventional Island” and “BOP” are commercial systems with well proven HMI. Hence providing common HMI is at times difficult and poses great challenge.
c) After integration of plant processes next step is integration of “I&C systems” with “electrical SCADA systems”.

COMMON-CAUSE FAILURE OF SOFTWARE IN DIGITAL SYSTEMS

To improve the reliability of hardwired systems redundancy is generally employed. In digital I&C systems use of multiple channels does not always result in increased reliability. This is due to presence of identical software in multiple channels. In such cases potential software common cause failure becomes an important issue. Hence for increased reliability in safety critical systems, not only multiple channels should be used, but in these channels diverse software should also be used. This itself would increase the development, engineering, V&V and regulatory efforts multifold.

COMMUNICATION INDEPENDENCE

In NPP occasionally there is a need to share information and data between systems of various safety classes. During communication it is to be ensured that a malfunction in lower safety class systems does not degrade the performance of higher safety class systems. In conventional I&C systems it is sufficient to provide electrical, physical and functional isolation to ensure independence between connected systems. In integrated digital I&C systems Local Area Network (LAN) are used for communication between various systems. These communication networks handle a large number of signals which may involve handshaking between different systems and data of different safety class at times will pass through the same network. This feature increases interdependence between different systems. This introduces new modes of failure increasing the chance of failure. Hence provision must exist to preclude unsafe and incorrect operation of digital I&C systems. This unsafe and incorrect operation may take place due to following reasons:

- Signals causing software executions to hang.
- Invalid signals being sent and incorrectly acted upon by receiver.
- Corruption of valid signals during transmission and operation by receiver based on this incorrect signal.
- Operation by receiver based on unauthentic signals (i. e. signals originating from an unplanned source).

Technical solutions are available to counter these issues but since operating experience in integrated digital I&C systems at present are limited, failures resulting from non-conformance to communication independence are still issues of concern.

VERIFICATION AND VALIDATION

I&C architecture is increasingly relying on digital I&C system which employ software. Use of software in various digital systems results in additional issues. Small error in software may cause serious consequence. Further they are more difficult to test, because concepts like continuity and interpolation are much more difficult to apply to them as compared to traditional electronic systems. Hence the software in these systems must be demonstrated to be safe and have high level of integrity. Integrity is defined as quality of completeness, dependability and freedom from defects. Software faults always result from errors in requirements, design or implementation. Hence digital I&C systems must be developed using stringent development standards and appropriate development methodology. Further qualification of the system and manufacturing processes must follow applicable nuclear standards.

In order to ensure that these systems have high integrity, techniques like verification and validation (V&V) are used to demonstrate that I&C system is correct (with respect to specifications), safe and completely implements the requirements. This V&V must co-exist with development process right from the beginning of development cycle. In V&V, depending on the safety classification of the I&C system it is subjected to “walkthroughs”, “inspection”, ”Static analysis”, “Dynamic analysis” , “formal verification” and “various tests”. “System software”, “application software” and “source code” are also subjected to vigorous V&V.

Further development, V&V and manufacturing should be supplemented with adequate documentation. These documents, test reports and V&V reports are subjected to regulatory

review/audit by regulatory authorities before the system is accepted for use in Indian NPP.

This process involves enormous efforts on part of designer, developers and manufacturers.

Since most of the digital I&C systems available in Indian industry are designed and developed abroad, it is quite often difficult to get the information. In this scenario, a due credit is accounted for IV&V done by the vendor in the country of origin. Operating experience in similar application is also analysed. Subsequently only incremental V&V for application software and hardware configuration/customization is done to ensure that it correctly implements all the system requirements.

CYBER SECURITY

In case digital I&C is used in complete plant right from smart sensors to smart final control elements with LAN running in the field, possibility of unauthorised access to I&C system becomes quite high. Such I&C systems needs to be protected from unauthorised access and disruption of its functions.

To protect the I&C system it becomes essential to analyse the potential security threats and take this into account in relevant phases of the system and software development, engineering, installation, commissioning, operation and maintenance. This should also include counter measures including recovery procedures in case of loss of system due to any security related incident. As a minimum it includes:

a) Procedures related to the interface between administrative and technical security, access to systems, security aspects of data handling and storage, security aspects of modification and maintenance, security auditing and reporting, and security training
b) Security procedures are to be prepared and applied during operation for periodic audits, resolution of anomalies observed during operation, assessment of safety system changes and their impact on safety system security so as to ensure that modifications do not introduce any security vulnerabilities.

OBSOLESCENCE

In NPPs, only proven technologies are used, because even a small failure can have large radiological consequences to the plant personnel and to the public. Hence a lead time exists between introduction of new technology and its use in NPP.

In today's fast changing technological era and a shorter life span of the technologies, by the time new technology is introduced in NPP, it is quite often already old from the industry prospective. Hence a need arises to manage obsolescence of current technology and address reliability concerns of nuclear industry. Considering the normal life span of 40 to 60 years for the NPP, industrial support of minimum 10 to 15 years is required before upgrade of the I&C system is considered. Hence there is a need for the industry to support the technology for this period.

However at present stocking adequate spares is one of the options used for managing obsolescence.

DOCUMENTATION

Documentation is required for installation, commissioning, operation and maintenance of

the I&C system. In addition documentation plays following roles:

- In today's world rapid advancements in electronics, computer technologies, communication technology and information technology is taking place. Hence I&C systems available in market have shorter life span. NPP I&C are designed for longer life span and these systems have to be operated for a longer period. Hence these systems may require incremental upgrades several times during a plant life. Therefore documentation containing "know-how" and "know-why" of the system are essential for long term life cycle management of I&C systems.
- Documentation provide evidence that system development cycle has followed a well structured engineering process and final product conforms to relevant standards and codes and meets all the system requirements.

CONCLUSION

Adequate means and ways will emerge over a period of time to establish the performance of digital I&C and make it possible to use the same in Nuclear Power Plant in a wider fashion.

ACRONYMS

AERB	Atomic Energy Regulatory Board
BOP	Balance of Plant
CBS	Computer Based System
DCS	Distributed Control System
HMI	Human Machine Interface
I&C	Instrumentation and Control
LAN	Local Area Network
LVS	Large Video Screen
NPP	Nuclear Power Plant
V&V	Verification & Validation

REFERENCES

AERB-SG-D25: Computer based systems of Pressurised Heavy Water Reactors

IAEA TECDOC-952: Advanced Control systems to improve Nuclear Power Plant reliability and efficiency

IAEA TECDOC-1327: Harmonization of the licensing process for digital instrumentation and control systems in nuclear power plants

ACKNOWLEDGEMENTS

Relevant standards, codes and guides of AERB (Atomic Energy Regulatory Board) and IAEA (International Atomic Energy Agency) have been used.

BIOGRAPHIES

Sh. Neeraj Agrawal was born in Nainital, India in the year 1963. He graduated in Electrical engineering from Delhi College of Engineering. He joined Department of Atomic energy, in 1984. At present he is working as an Additional Chief Engineer and associated with design, engineering and procurement of I&C of Indian PHWR plants and imported Light water reactors. He was conferred with "Homi Bhabha Award" by BARC, "Special contribution award for the year 2006" and "Group achievement award for the year 2007" by NPCIL.

Sh. Ravi Prakash was born in Delhi, India in the year 1950. He graduated in Electrical engineering from Delhi College of Engineering. He joined Department of Atomic Energy in 1972. During his career he has been associated with design, engineering, procurement and various development related activities for the I&C of Reactor Protection Systems and Reactor Process Systems. At present he is working as Associate Director (Control & Instrumentation) in Nuclear Power Corporation of India Limited