COMBATING OBSOLESCENCE – ACR DIGITAL CONTROL SYSTEMS DESIGN

Sunil Tikku, Gilbert Raiskums
Atomic Energy of Canada Limited

Abstract

The ever increasing use of digital technologies and products to meet the control, automation and monitoring needs of the nuclear power plant– even though justified by the benefits it provides – comes with an increased risk of technological obsolescence happening through the course of the plant life. Some well considered strategies are being employed in the ACR design process to minimise this risk and alleviate the consequence if it happens. These include application of a modular overall architecture, adoption of international widely accepted standards to harmonise equipment qualification and software practices, production of control functional specifications that are not influenced by target platform, and careful selection of technologies and products.

Introduction

AECL is recognised as an innovator in adopting computer control and monitoring systems in CANDU nuclear power plants. As with other superior CANDU features, the concepts used for digital control and monitoring in the installed plants have formed the basis for significant evolutionary enhancements being incorporated into ACR (Advanced CANDU Reactor) design. These enhancements are well justified by the increasing benefits drawn, some of which are:

- Smarter algorithms for real time control for enhanced safety and performance
- Functionally partitioned control
- Improved control room operator interfaces, including central overview displays
- Improved and operator friendly alarm annunciation strategies– CAMLS (Computerised Alarm message List System)
- Predictive Maintenance Strategies
- Automatic Start Up Sequences
- Centralized Safety System monitoring and automated testing
- Tighter Enterprise Integration
- Sophisticated Technical Support Centres/ Emergency Operation Facilities
- Smart CANDU features such as ChemAND, ThermAND, SPDS etc

The increased use of digital systems comes with an increased risk of technological obsolescence happening through the course of the plant life. This paper discusses the issues surrounding this risk, the strategies that can be employed to manage this risk and how ACR is incorporating each of these strategies early in the design stages.

Problem / Risk:

In 1965, Gordon Moore, the founder of Intel Corporation predicted the rapid pace of technology innovation. His prediction, known as the Moore's law, stated that the number of transistors on a chip roughly doubles every two years. As illustrated by the following

table, Moore's law has proved to be startlingly accurate and industry experts predict similar growth to continue for the next 15 to 20 years. What will happen after that is anyone's guess at this point in time.

Microprocessor	Year of Introduction	Transistors
4004	1971	2,300
8008	1972	2,500
8080	1974	4,500
8086	1978	29,000
Intel286	1982	134,000
Intel386™ processor	1985	275,000
Intel486™ processor	1989	1,200,000
Intel® Pentium® processor	1993	3,100,000
Intel® Pentium® II processor	1997	7,500,000
Intel® Pentium® III processor	1999	9,500,000
Intel® Pentium® 4 processor	2000	42,000,000
Intel® Itanium® processor	2001	25,000,000
Intel® Itanium® 2 processor	2003	220,000,000
Intel® Itanium® 2 processor (9MB cache)	2004	592,000,000

(source: http://www.intel.com/pressroom/kits/events/moores_law_40th)

As transistor counts have climbed so has the ability to increase device complexity and integrate many capabilities on a chip. While this has led to enormous growth in the applicability of digital systems – thus benefiting the industry and society as a whole, it has also posed the challenge of technology obsolescence as never before. The effect is especially pronounced in the area of control and automation system technology with its heavy modern day reliance on microprocessor based technology.

Strategies for Managing Obsolescence:

From the cumulative experience of past legacy systems, it is clear that carefully considered and well-defined strategies have to be employed early from the design phase onwards to effectively manage technology obsolescence expected to happen later during the life of the plant. The objective is to

a) Minimise the occurrence of technology obsolescence.

b) Be prepared if and when it happens, so that there is minimal pain when migration is really required.

There are differences between the strategies to minimize the likelihood and impact of obsolescence and maintenance strategies to effectively deal with it.

As with any industry, the control and automation objectives of a nuclear power plant should be well aligned with its business objectives. The business objectives of an NPP include both its performance (production economics) and safety targets. The automation

technology employed and work processes followed are means to meet these business objectives. Even if the technology changes, the business goals are expected to remain constant.

Review of past major enhancements of digital technologies at nuclear power plants has indicated that, even though in some cases there might be increased (or changed) requirements for information and automation necessitating system upgrades, the majority of upgrades are due to either aging or obsolescence. The hallmark of effective obsolescence management is to ensure that there is minimal impact on items shown in the area marked 'B' in Figure 1, even if the technologies shown in area 'C' face obsolescence and need replacement. This will keep the engineering and training cost components down and will minimise the lead-time required for both.

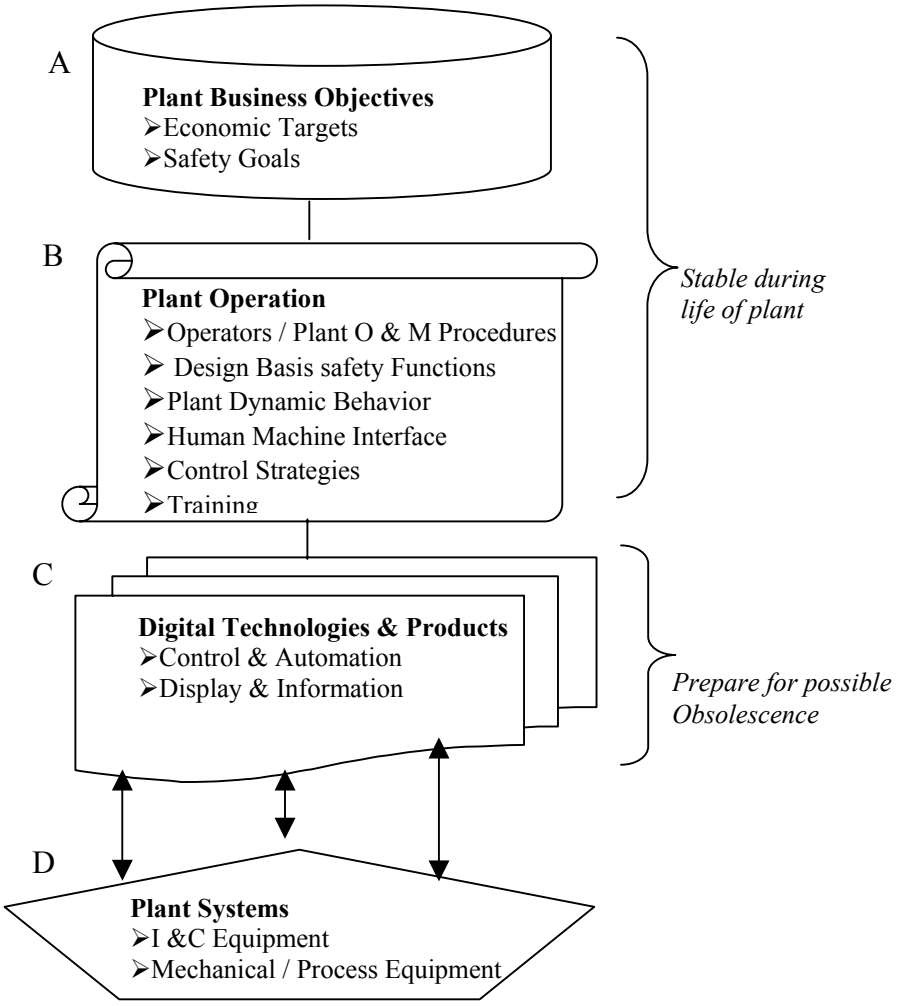

Figure 1 – Technology Obsolescence Perspective

The following strategies are key to effective obsolescence management. It should be noted that often a number of these strategies are closely interleaved and complement each other. However, in certain cases they can also be in conflict with each other, requiring careful judgement in deciding the best path forward:

- **Modular overall architecture:** An NPP typically contains multiple information and automation systems. Some of them have tightly coupled interfaces with each other whereas others might be largely standalone with none or only a few interfaces. The overall architecture should allow easy integration based on standards defining interoperability. A good architecture should allow the coexistence of old and new technologies and should smoothen the transition from old to new. In that respect, the architecture should be able to transcend technology. Different systems are likely to have different life cycle profiles and life spans and thus a stepwise or phased approach to migration, when required, can be planned. The individual products and applications are just building blocks that make up the systems that help to realise the overall plant architecture in line with the plant business (performance + safety) goals.
- **Compliance with modern standards**: Hardware and software solutions used in the nuclear domain have to be 'qualified' before they can be applied in target applications. Qualification, in general, establishes the suitability of a specific product to implement the safety functions of a particular level of safety significance. Therefore the two dynamics in any qualification exercise are, a) the understanding of the application that determines the safety significance of the function(s) being implemented, and, b) the understanding of the product attributes and how it is to be used in a particular architectural solution. The product attributes include the 'as designed' hardware and software components, and the quality assurance of the work processes used for software development and maintenance.

  Traditionally, different users and regulatory regimes have had varying guidelines and frameworks for addressing both of the above stated factors. This has led to very expensive qualification processes and ones that have been a big challenge for upgrades and replacements. Fortunately, modern standards have now emerged and have gained acceptance in the marketplace in terms of buy-in from all three major players involved, namely the vendors, the users and the regulators. IEC 61508 is now broadly used by the industry to certify products for use at any of the pre-defined safety integrity levels (SILs). Vendors across the spectrum (catering to both nuclear and non nuclear applications) are familiar with the standard. It provides a level playing field for the vendors and a harmonious application of the testing / qualification guidelines from the users'/ regulators' points of view. The onus is still on the user to qualify the product for use in an architectural configuration that meets the needs of a particular project, but that is now a less onerous process (i.e. qualification effort is reduced when using a certified safety product).Expectations of a nuclear renaissance coupled with the challenges faced in qualifying replacements for legacy systems has accelerated the adoption of the nuclear specific versions of the IEC standards by many countries. IEC 61513 provides the interpretation of IEC 61508 for the nuclear industry and defines the overall safety lifecycle and requirements for developing I&C systems for an NPP. IEC 61226 is the nuclear

industry standard for assigning the I&C application functions to various safety categories.

The use of the abovementioned standards ensures the proper capture, documentation and validation of functional requirements (including safety requirements), design details (including design constraints, assumptions and rationale) that form the detailed design basis for the system. This ensures that this knowledge is preserved. This will facilitate subsequent design modifications or system replacements far into the future as a result of obsolescence ad minimise the risk of design errors or oversight.

On the control application software development front, IEC 61131-3 provides a standard for industrial control programming that has been globally accepted and adopted. It specifies the syntax, semantics and program rules for a unified suite of programming languages for programmable controllers. These include textual languages, IL (Instruction List) and ST (Structured Text), and graphical languages, LD (Ladder Diagram), FBD (Function Block Diagram) and SFC (Sequence Function Chart). It allows programs to be decomposed into logical elements and modularised, increasing their reusability, enhancing software quality and development productivity.

- **Portability of Control Functional Specifications:** The specifications for the control and monitoring functions should not be influenced by the target hardware. The requirements of the application functions should be stated in functional terms rather than in terms of computer technology so that they are platform independent and are well understood by the process engineers, I&C functional engineers and plant operators. This ensures that in the event of need of migration, a top down approach can be applied to engineer a new solution based on the old specifications. It is thus easier to demonstrate compliance and traceability of the implemented solution to the original functional intent. Legacy code has often needed to be reverse engineered to get a requirement definition before a new solution could be implemented. In addition to being very cost ineffective and incurring long lead times, it often also has the very undesirable consequence of masking the real functional requirement; often the solution is treated as the requirement.

  Use of 61131-3 structure (discussed above) to generate software specifications for the control & automation applications also tremendously aids portability. The use of 61131-3 has helped to standardise the engineering environment thus increasing programming and user efficiency. A spec based on 61131-3 structure would also be portable (or near portable) to any other target hardware adhering to the standard.

- **Judicious technology (and product) selection:** Technological evolution (even though inevitable) should not act as a destabilizing force. The owner/ operators should be able to decide the time frame for making any technology migrations. Real obsolescence takes longer than is generally perceived. Although new product innovations may have desirable benefits, care should be taken to select a product technology that is proven and reliable and will be maintainable well into the future. (An aging system may sometimes be maintainable beyond the obsolescence of the underlying technology with proper pro-active maintenance strategy of parts management etc.)

It is wise, where possible, to base the solutions on technologies that are used widely rather than ones that are custom designed and don't have an extensive installed base. One off technologies - even if perfect for the application today – can be a recipe for early obsolescence tomorrow. Technologies should be chosen with appropriate knowledge of industry standards. Often technologies endorsed, across the industry, by companies are able to draw superior service, migration, upgrade and superior life cycle extension programs.

- **Judicious vendor selection**: The selected vendors should have a track record in nuclear business - thus having accumulated an application knowledge base - and should be committed to stay in the business. It is highly desirable for the vendors to supply the same or similar family of products to a broader market base outside the nuclear industry. This helps long-term sustainability of the vendors to continue supporting their safety products and also justifies investments that are required for backward compatible upgrades. It is also important to be watchful of the market alignments especially with mergers and buyouts being so commonplace. Market re-alignments have been known to cause major difficulties in receiving long term support or addressing migration needs.
- **Use of Open concepts**: Open technologies has been a somewhat misinterpreted and overused term in the past but holds a lot of potential if used wisely. Industry wide desire for standardisation and concerns of over-reliance on proprietary technologies has spawned many initiatives where a group of companies have come together to develop technologies based on a standard set of specifications. Open technologies are characterised by the attributes of interoperability, portability and scalability. Interoperability enables different systems from different vendors to communicate with each other through use of widely accepted standards in communication protocols. Portability allows application software to run on different platforms. Scalability means that systems that are based on current needs can be easily expanded to meet future needs. An 'open' system attains its attributes by adherence to widely used, publicly available standards. Although there are no guarantees that a popular 'open' technology of today will continue to remain so in future, the concept offers lot of promise of developing system integration solutions without overdependence on proprietary technologies. It also enables lower cost integration and makes the pain of a future migration less burdensome.

  Examples of open technologies are Fieldbus, Ethernet, PCs, ODBC, OPC etc. Caution has to be exercised since there are restrictions on how open each of these technologies really is. For example, Foundation Fieldbus and Profibus are two popular and widely used examples of fieldbus – however, field devices using Profibus will need to be supported by data server(s) that understands that protocol. Nevertheless, instead of each vendor having their own proprietary protocol, we are now down to a couple of options. This offers a lot of flexibility and good options for scalability.

  In the nuclear industry, the use of open technologies has to be further balanced with other requirements that may be overriding. In other words an 'open technology' can only be adopted if for that application it meets the requirements of reliability,

performance, environmental / seismic qualification, data security and safety integrity level (SIL) of the hardware / software in question.

Applicability to ACR Design

Overall Architecture

Figure 2 gives a context diagram for the ACR control and information systems.

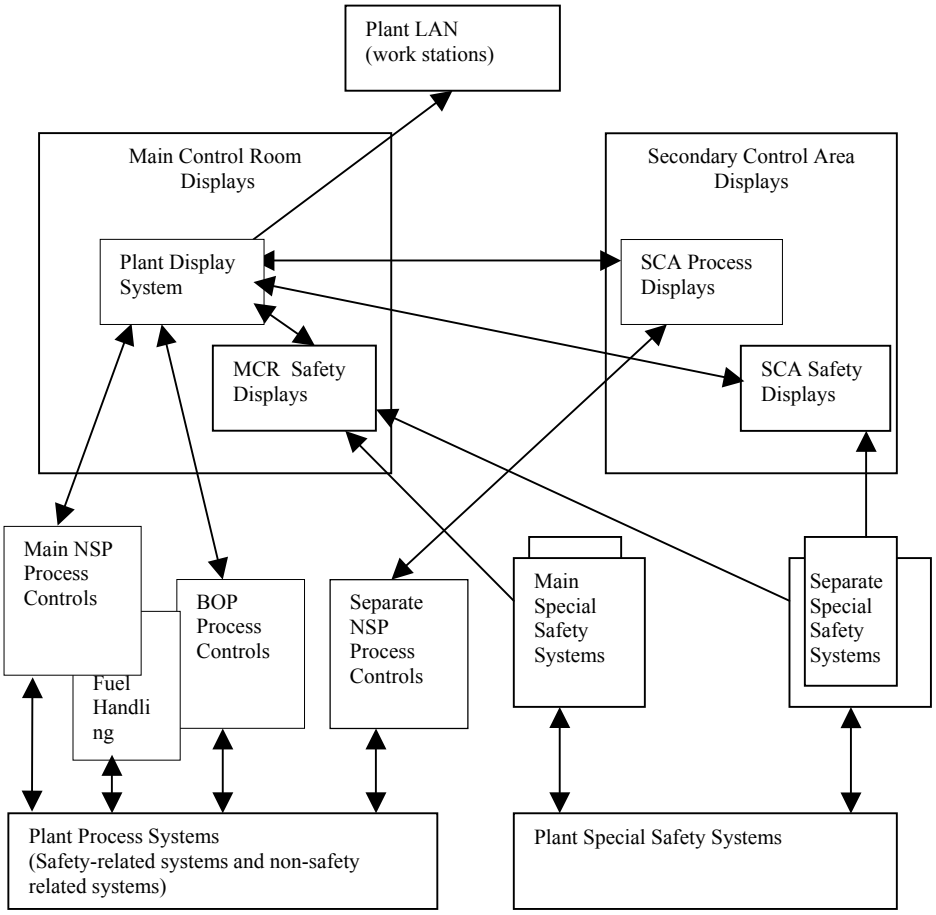

Figure 2 - Context diagram

The control system(s) are independent of the display systems. Each is based on technology suited to its effective implementation. The computing is by processors and operating systems suited to their roles and the communication links used to transmit control signals are independent from those used by display system for display or annunciation. No failure in any part of the display system is capable of interfering with the correct and continued operation of the controls. Each technology is expected to follow a different course of future evolution. If ever necessary in the future, migration

strategies can be separately formulated in independent time frames. The communication between the two systems is based on well defined specifications for interoperability. The selection of technologies is based on well thought out considerations for long term life cycle support.

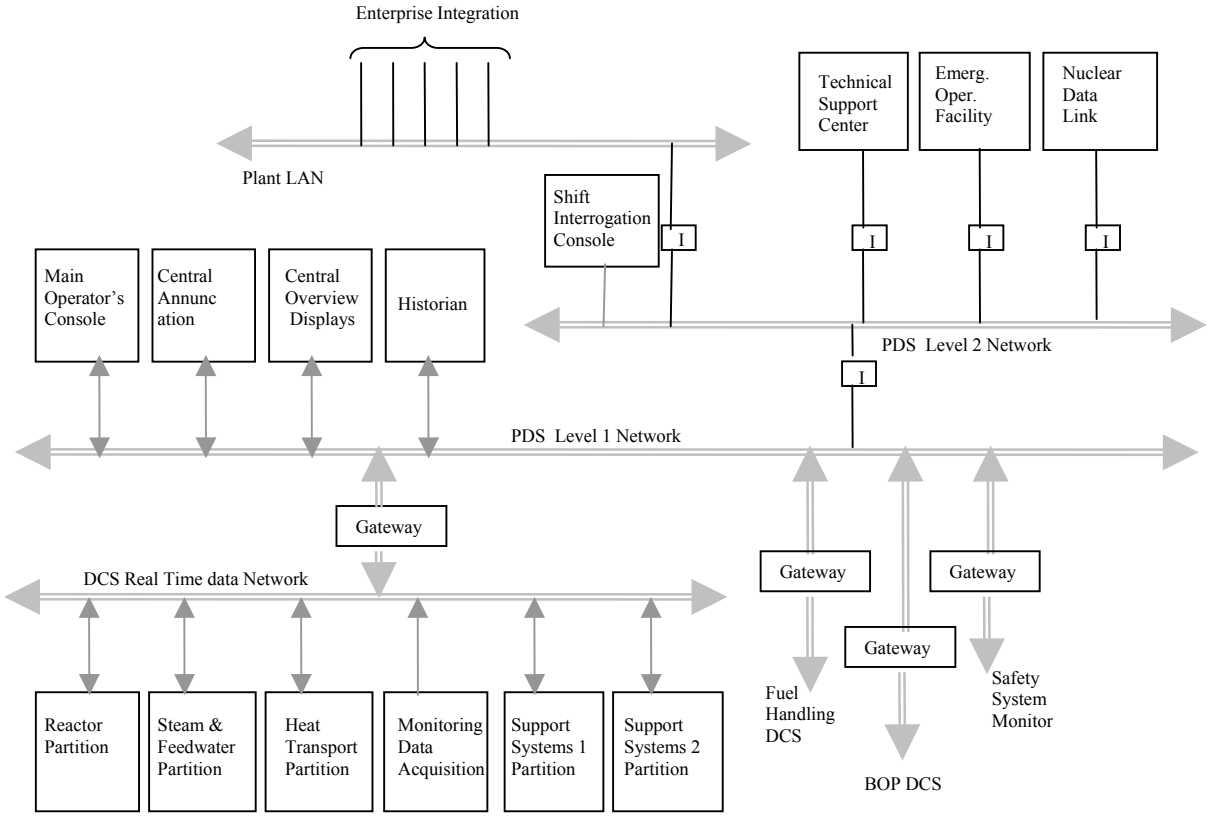

Figure 3 – Overall DCS / PDS High Level Architecture

Technologies

The ACR control system is based on 'distributed control system' technology The DCS is divided into a number of functional partitions – thus dividing the process control functions into different controllers logically and also separating the regular process control functions from their mitigating functions. To save wiring costs, the input / output terminations are remotely located. The partitions use a high speed network based on 'Ethernet' to have a bi-directional communication exchange between partitions and with the PDS. This network supports the open concepts of TCP/IP, UDP/IP and ensures real time communication as per IEEE 802.X protocols. The application software for control logic functions are implemented in IEC 61131 compliant/equivalent limited variability languages such as Functional Block Language and Structured Text. This allows encapsulation of logic chunks into macros for repeated use. Bearing very close mapping

to the way control functional requirements are written, it will permit easy migration when needed.

The PDS provides the primary human-systems interface (HSI) for plant annunciation and for plant monitoring and control. The PDS is based on AECL's human system interface product called Advanced Control Centre Information System (ACCIS). Based on substantial operating experience gathered over the past decades, ACCIS incorporates specific features, which are not commonly available in standard HMI products offered by major control system vendors. The notable examples are an enhanced alarm annunciation strategy (CAMLS), support for predictive maintenance and equipment maintenance status monitoring, and automated sequential control to facilitate start up / shutdown / fuel handling / testing tasks. ACCIS provides a collection of software services based on QNX, which is a Real Time, Message passing Microkernel operating System software. Communication among PDS components is by means of QNX's native communication protocol called Qnet. Communication between PDS and other systems (such as DCS & FDS and including other PDS type networks) is based on UDP/ IP or TCP/IP. PDS also talks to a number of other information systems on the plant LAN for enterprise integration, historical data storage, equipment status monitoring, and configuration tools. Internet technologies are used on the non-secure sections of the network for data access.

Standards Framework

ACR has adopted a standards framework, as shown in Figure 4, for systems development with safety implications. Hitachi and AECL are both in the process of qualifying the HIACS and ACCIS systems for use in safety applications as per the requirements of IEC 61508 / 61513. (In the past 'Centre of Excellence' standards jointly developed by AECL and OPG (formerly Ontario Hydro) were used for software qualification. A difficulty with that was the lack of widespread knowledge of those standards – causing huge hindrances in both new and migration projects.) The use of IEC standards is finding increasing acceptance with the regulator. Thus the product suitability assessment methodologies, and, design and engineering processes drawn out of these standards are in harmony with those increasingly being followed by design companies, vendors and regulators on a widespread basis.

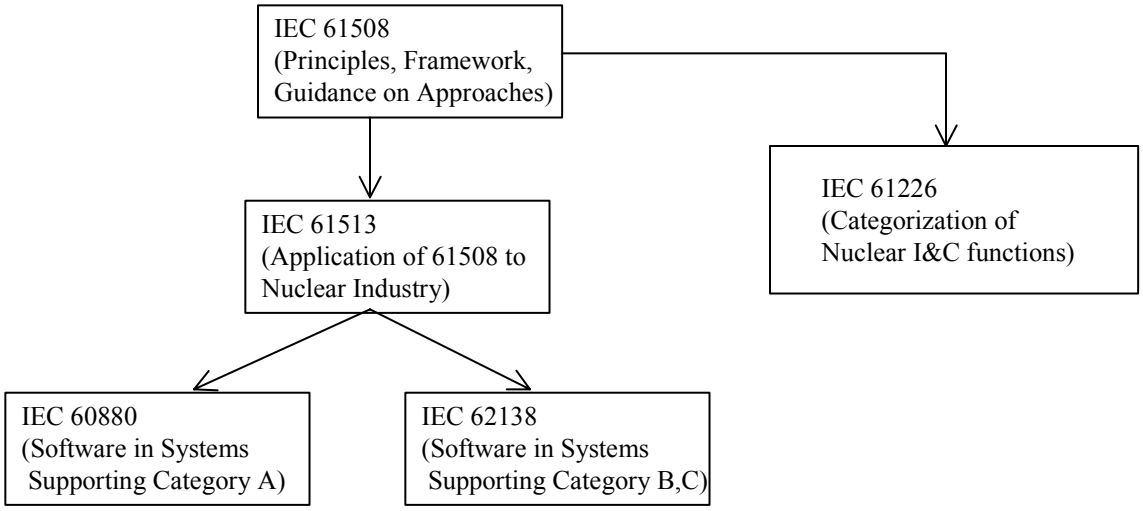

Figure 4 – Standards Framework

Control Functional Specifications

In the past, the design processes and work procedures have often been influenced by the choice of the target platform. Functionality for the various control systems used was documented in varied formats such as text based program specifications, logic diagrams, and other various specification documents. However, ACR's design is being realized in a manner consistent with latest international standards (e.g., IEC-61131 / 61513). It makes use of tools that allow the plant control system functional and performance requirements to be documented using graphical representations. The documents are arranged in a logical manner such that reviewers can systematically check their correctness and completeness. Requirements are specified in such a way that changes can be included later without introducing inconsistencies. Overview diagrams of system functionality provide a common understanding of the system boundaries and interfaces. Important requirements are readily traced through the development process to ensure consistency with the safety and economic significances of the system.

All functions are classified based on their importance to safety. Although the classification may not affect the way the functional requirements are defined, they are an important input in determining the specifications for the target platform and the software work practices to be followed for implementation. The functions with higher safety category requirements need to be traceable to the plant safety base.

The Control Functional Specification documents are used as an input into the functional validation of the control system design. This verifies the correctness of the control system functionality versus the plant performance and functional requirements. It is complementary to the system validation of the control system design that verifies the compliance of the system with the system (hardware and software) specifications.

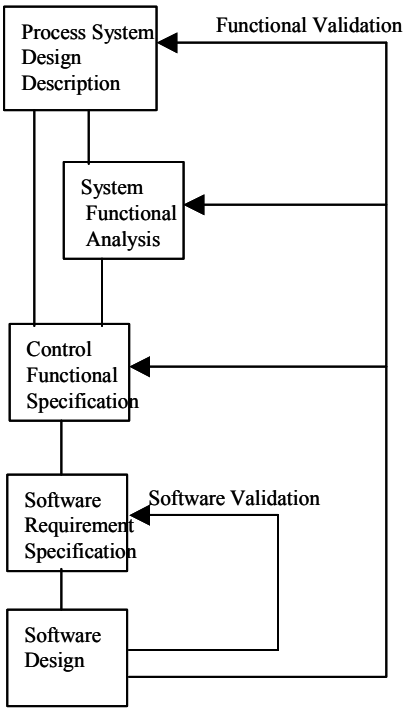

Figure 5 Simplified development and Verification Process

Conclusion:

The enhanced use of digital control and monitoring has clearly opened possibilities for smarter solutions that will tremendously serve to boost the plant performance and safety objectives. However, the rate of evolution of computer technology is bound to result in need for system migration(s) during the life of the plant. Therefore, these systems need to be designed for change to minimize the lead-time and costs of migration. Well-considered strategies - such as use of modular overall architecture, adoption of international widely accepted standards to harmonise equipment qualification and software practices, production of control functional specifications that are not influenced by target platform, careful selection of technology / products, and use of open concepts wherever possible - are being employed in the design of ACR control systems to effectively address these concerns.

Abbreviations:

ACR	Advanced CANDU Reactor
ACCIS	Advanced Control Centre Information System
AECL	Atomic Energy of Canada Limited
CAMLS	Computerised Alarm Message List System
ChemAND	Chemistry Monitoring, Analysis and Diagnostics
COG	CANDU Owners Group

DCS	Distributed Control System
EOF	Emergency Operation Facilities
FDS	Fuel Handling Display System
HMI	Human Machine Interface
IEC	International Electro Technical Commission
IEEE	Institute of Electrical and Electronic Engineers
NPP	Nuclear Power Plant
ODBC	Open Database Connectivity
OPC	OLE (Object Linking and Embedding) for Process Control
PC	Personal Computer
PDS	Plant Display System
SIL	Safety Integrity Level
SPDS	Safety Parameter Display System
TCP/IP	Transmission Control Protocol / Internet Protocol
TSC	Technical Support Centre
ThermAND	Thermo-mechanical Monitoring, Analysis and Diagnostics
UDP/IP	User Datagram Protocol / Internet Protocol

References:

[1] G.A. Raiskums, “Use of "Open" Systems Technology for Bruce A Safety System Monitoring Computer Rehabilitation”, International Conference on Control & Instrumentation in Nuclear Installations, University of Cambridge, UK, April 1995.

[2] E. Harmer, G. Mitchel, A. Hepburn, “DCC Replacement Initiative – System Design Process and Standards Framework”, CNS Conference, June 2003.

[3] J. Harber, M. Borairi, S. Tikku, A. Josefowicz, “Documenting Control System Functionality for Digital Control Systems”, IAEA Technical Meeting, September 2005.