DISTRIBUTED CONTROL SYSTEM APPLICATION TO CANDU PLANTS RECENT ACTIVITIES FOR ADAPTATION OF DCS PLATFORM TO IEC STANDARDS

K. Ishii, M. Kobayashi, M. Shiraishi, S. Masunaga, H. Harada
Hitachi, Ltd., Information & Control Systems Div.
2-1, Omika-cho 5-chome, Hitachi-shi, Japan

G. Raiskums, S. Tikku
Atomic Energy of Canada Limited
2251 Speakman Drive, Mississauga, Ontario, Canada, L5K 1B2

ABSTRACT

This paper describes the current activity status for IEC qualification of the Hitachi DCS platform with special focus on products that would be applicable to the new Enhanced CANDU 6 (EC6), Advanced CANDU Reactor (ACR) and existing CANDU reactors. Hitachi's product qualification goal is to be compliant with the IEC standards (61508, 61000), so as to allow it to offer suitable technology for use in projects that are adopting IEC 61226 and IEC 61513 for categorization of safety functions. Basic applicability of the existing Hitachi product for the ACR DCS platform has already been evaluated by AECL [1]. This paper discusses current developments of the enhanced version to address gaps identified in the existing product with regards to compliance to IEC 61508.

KEYWORDS

CANDU, EC6, ACR, IEC standards, IEC61513, IEC61508, DCS, Functional Safety, Certification, Qualification

CONTEXT AND OBJECTIVE FOR HITACHI

Construction plans of Nuclear power plants, in Canada, appear to be taking a concrete shape as electric demands increase. Since digital technology is widely used in the industry for measurement and control equipment, use of the IEC standards are gaining increased acceptance by the user and vendor community. In view of these trends, Hitachi Ltd, has undertaken the development of their I&C systems to be compliant with the requirements of these standards for use in safety applications.

GOVERNING STANDARDS

AECL considers compliance with IEC standards as an acceptable means to develop Safety Related computer systems for CANDU reactors [2]. In the case of DCC replacement, AECL has considered adaptation of framework and categorization methods of the IEC standards for Safety-Related I&C functions of CANDU reactor [3].

Two top level standards in the IEC series applicable to electronic programmable devices form the starting point for qualification of computer based systems: 61508 (for all industries) and 61513 (for the nuclear industry). There is a general consistency between the industry specific 61513 and non-industry-specific 61508 to the extent that the more detailed 61508 can be used for guidance when addressing less detailed requirements in 61513. For this reason, computer products are typically certified to the non-industry-specific 61508 allowing for a simplified qualification process when using the certified products in specific industries such as for nuclear, petro-chemical, transportation, etc..

The following framework illustrates the application of the IEC standards to the computer systems of new CANDU plants:

1) Entire project: IEC 61513
2) Application software design process:
    - IEC 61513 Class 2 and 3: IEC 62138
    - IEC 61513 Class 1: IEC 60880
3) DCS platform: Qualified as per IEC 61508 to meet project requirements defined by 61513.
    - Hardware
    - OS, Middleware
    - I/O, I/O communication buses

APPLICABILITY OF THE PRODUCTS INTO CANDU SYSTEMS

The computer system development philosophy for the ACR and for EC6 enhancements will make significant use of qualified products developed specifically for control and safety applications. Past traditional approaches involved much more customized development of software on general purpose computer platforms. The traditional approach had benefits in optimizing use of the limited computer performance of the time, but is generally expensive and requires long term maintenance with highly specialized knowledge of aging technology. The practices of the time did not facilitate porting the design to newer technology. Application details were not always clearly specified, requiring reverse engineering of the assembler code in some cases to determine certain critical behavior of the control application.

Considering the high rate of evolution in computer technology and the long life-times of nuclear power plants (e.g. 60 yrs for ACR), it is necessary to design for change-out of the control systems once or twice during the life of the plant. The development strategy using products specifically designed for control and safety applications and using "limited variability" block languages for the application software should minimize the effort for both the initial design and future change-out to more modern technology. An added benefit exists when the technology supplier is a large stable company with support commitments in the nuclear industry.

QUALIFICATION TARGET

Goals of Development for DCS core platform is shown as follows:

1) SIL2 certification of DCS for majority of control functions for reactor and plant control.
2) SIL3 certification for a safety controller for safety critical application of nuclear power plant.
3) Platform mentioned above, (1) and (2), must demonstrate capabilities compliant with IEC 61000 for electro-magnetic compatibility (EMC).

QUALIFICATION APPROACH & CERTIFICATION APPROACH

(1) Approach

Hitachi has been proceeding in the following way.

1) Gap analysis of existing product of the DCS core platform {HIACS-7000 (HISEC-04M/R700, HSC700)} with respect to IEC 61508.
2) IEC 61508 compliant Qualification for the existing product of the DCS core platform {HIACS-7000 (HISEC-04M/R700)} after plugging gaps found in Gap analysis.
3) IEC 61000 compliant EMC Test for the existing product of the DCS core platform {HIACS-7000 (HISEC-04M/R700)}.
4) Development of an enhanced version of DCS core platform and its certification to IEC 61508/IEC 61000 (Currently ongoing)
    - Enhanced version of HISEC-04M/R700 / HSC700: NuSAFE-HSC800
    - SIL3 controller: NuSAFE-FSM800
5) Qualification for other components of DCS platform.
    - Network between PDS (Plant Display System) and DCS (Ethernet based): Qualification with respect to IEC 61508.
    - Network among HSC800 (Dedicated optical link based)
    - HIACS middleware (Supporting Function Block Diagram (FBD), Structure Text (ST) and so on): Qualification with respect to IEC 61508.
        - Pre-existing portion: Software Criticality Impact Analysis, HAZOP analysis and code review in accordance with coding standard under the qualification plan (Done).

(2) Development Philosophy

Hitachi has established a development philosophy in order to meet new market needs. That is based on application design and operating experiences of I&C systems for nuclear power for over 30 years. The development philosophy is as follows.

1) To be based on the proven technologies, using reliable hardware and software.
2) To minimize overhead time needed for functional safety, and continue to meet the response time characteristics of the exiting platform.
3) To incorporate improvements to the existing platform required for Qualification.

DESIGN CONCEPT OF THE SOLUTIONS

The basic architecture, which is part of the scope of certification to demonstrate IEC 61508 compliance, is designed by combining two methods.

The black channel approach regards the communication path to be a black-box and does not care about the hardware structure of the communication path in detail.

The white channel approach is based on the evaluation of failure rate of each component.

White channel and black channel methods are described as follows:

No.	Items	White Channel Approach	Black Channel Approach
1	Safety Management (Top Layer)	Certified Safety Integrity and the Development Process (The V model applied to Software and LSI Design Process)	
2		Implementation	Implementation
3	Diagnostics by Software (Upper Layer)		
4		Patrol / Sequence Monitoring	Sequence Monitoring
5	Diagnostics by Hardware (Lower Layer)		
6		Patrol / Comparison of 2 ch. output	Monitoring and Correction
7	EUC(Equipment Under Control) to be diagnosed		
8	Feature	Small overhead of response time	Not necessarily require hardware diagnostic function

Figure-1: Approach to IEC 61508 SIL Certification

(1) Optimization of diagnostics between hardware and software

Figure-1 illustrates approaches for IEC 61508, SIL certification.

In order to realize functional safety, the development process for the safety management layer has to be qualified/certified with respect to IEC 61508.

The V&V process defined in IEC 61508 is applied to software and LSI development processes. Both the white channel approach and black channel approach can be used to achieve SIL certification. An optimum combination of the approaches, utilizing features of each approach, is considered during detailed implementation.

1) In the white channel approach, EUC (Equipment Under Control) is broken into component levels. The black channel approach is a method to evaluate failure rate with channel error rate as a single entity.
2) Diagnosis by software developed using V&V process for both approaches is considered for the

higher layer of diagnosis for both approaches.

3) Diagnosis function, in white channel approach, is provided in the following ways.

The tests consist of mainly three parts, that is, patrol, comparison of two channel output and sequence monitoring.

For patrol, test signals from the software test program are input to hardware diagnostic circuit and then to EUC. The calculation results are returned to the software test program, and compared to the predetermined results. This test is conducted under the periodical surveillance mode (when the general purpose control tasks are not executed) so that they do not interrupt the execution of general purpose control tasks, which has close relationship to response time of the system.

For comparison of two channel output, outputs of the dual element such as microprocessor, transmission path, etc. are compared with each other to detect the unconformity of the two outputs. This test is conducted with periodical surveillance mode by hardware.

For sequence monitoring, order of software logic operation is monitored in hardware diagnosis circuit.

Thus, diagnosis function in white channel approach is provided in the hierarchical manner, and as shown in Figure-1, EUC diagnosis is implemented directly by hardware.

4) In black channel approach, errors are monitored by safety layer communication software and rectified. And order of software logic operation is monitored in hardware diagnosis circuit in the same manner as white channel approach.

Figure-2 shows examples of task scheduling when the approach in Figure-1 is realized. The basic cycle is test program of diagnosis, diagnosis, and execution of control circuit, and it is repeated in this order, that is,

1) For diagnosis phase, test program for diagnostic function outputs the test signal to hardwired diagnostic function during the surveillance mode as shown in Figure-1.
2) Then, diagnostic function in the comparator mode implements the 2 channel output comparison.
3) 1) and 2) are the test functions realized by white channel approach.
4) Then, safety layer communication program at the both ends of the node to be implemented by black channel approach monitors the feasibility of the communication.
5) Comparator mode diagnostic function and safety layer communication program is interfacing with functional safety task which is provided by application program layer.
6) After the series of diagnostic test are conducted, the general purpose control tasks execute control functions.
7) 1) to 6) are periodically implemented at every execution cycle.

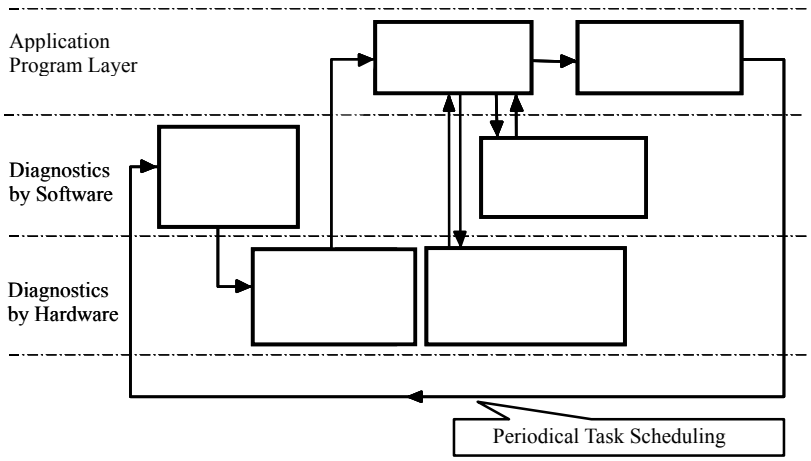
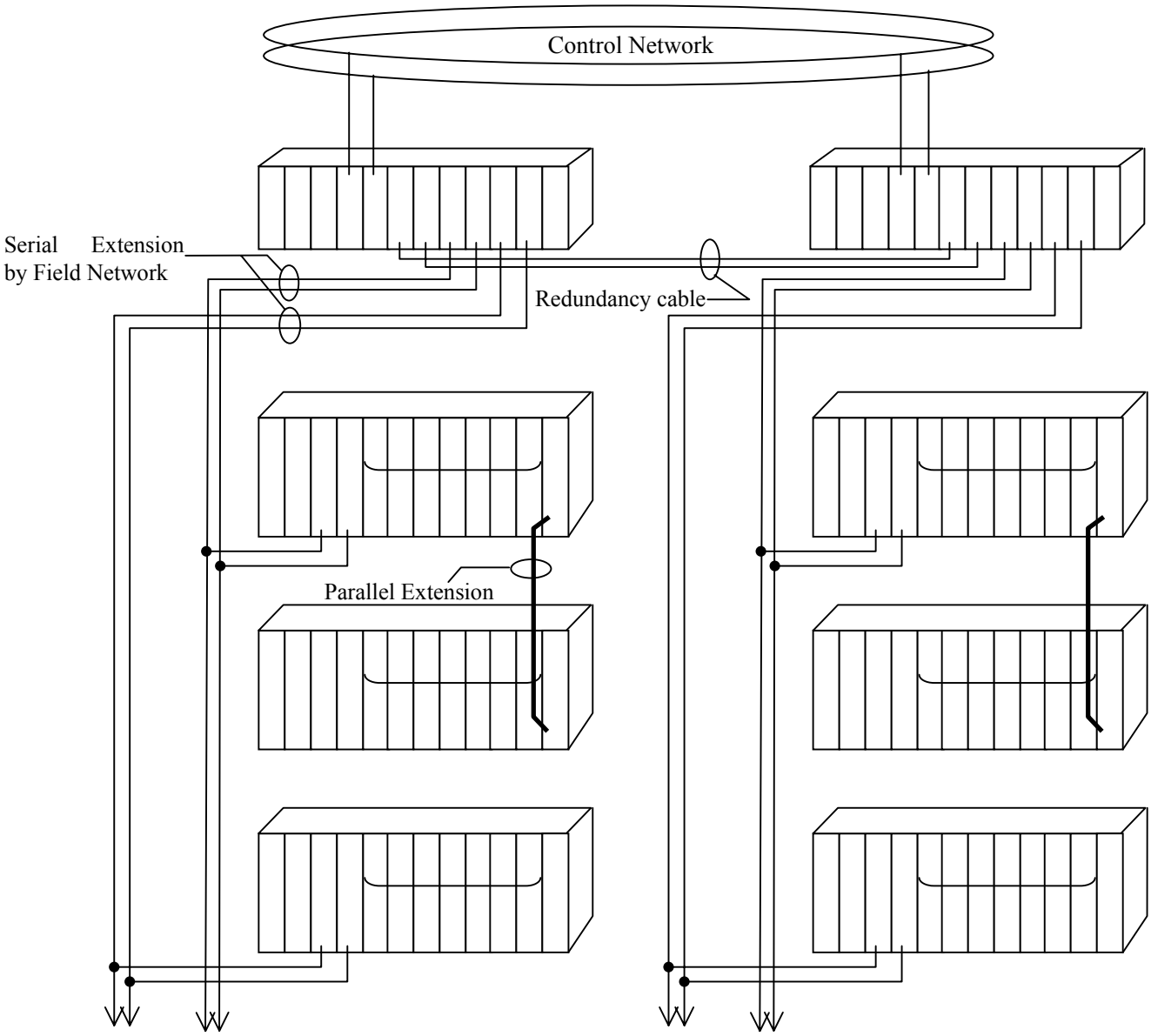


Figure-2: Task Scheduling of Hardware/Software Diagnosis Function

(2) Redundancy and the production availability

Figure-3 illustrates configuration example of DCS that achieves IEC 61513 Class 2/3. One set of duplicated system is shown as an example. CPU's, which perform control functions, are connected to PIO, which interface with plant process, via transmission line consisting of PIOP and ST. Each CPU is connected via PIOP with each other for status monitoring of the other CPU, etc. Components for transmission line, that is, PIOP and ST, are to be certified by black channel approach, and the other components will be certified by white channel approach. It is a configuration that realizes a higher safety (class) by potentially using lower safety class components in a redundant configuration. However, all software which is subject to common cause issues must still meet the higher class requirements. This technique is under consideration for EC6/ACR DCS.



Terms Used in the Figure

No.	Terms	Functions	Remarks
1	PS (Power Supply)	Supplying power to the components inserted in the same chassis	
2	CPU(Central Processing Unit)	Calculating control execution, diagnosis function, etc.	
3	PIOP(Process Input and Output Communication Processor)	Component which is mounted in CPU chassis and interfaces with the followings: 1) ST in the PIO chassis 2) The other PIOP in the different CPU chassis	
4	ST (STation)	Component which is mounted in PIO chassis and interfaces with PIOP in the CPU chassis	
5	CE (Chassis Extension)	Components for bus extension by interfacing with UD (mounted in upper flow chassis)	
6	UD (Unit Driver)	Components for bus extension by interfacing with CE (mounted in down flow chassis)	

Figure-3: Structure Example of Distributed Control System

－IEC 61513 Class 2 and Class 3 －

CONCLUSIONS

Hitachi is introducing evolutionary enhancements to the DCS products, in view of compliance with IEC 61508/IEC 61000.

The enhanced versions of R700 controller/HSC700 I/O are currently under development and will be christened NuSAFE-R800/NuSAFE-HSC800 (currently in process of registering brand name). Additionally, NuSAFE-FSM800 as a SIL3 controller is also under development. The applicability of NuSAFE-800 including its software development/maintenance environment is being assessed by AECL for use in ACR etc.

Hitachi is extremely hopeful that its applicability can be expanded to not only new construction EC6/ACR but also refurbishment of existing CANDU reactor I&C

LIST OF ACRONYMS

AECL	Atomic Energy of Canada Limited
CANDU	CANada Deuterium Uranium
CE	Chassis Extension
CPU	Control Processor Unit
DCS	Distributed Control System
EC6	Enhanced CANDU 6
EMC	Electro-Magnetic Compatibility
EUC	Equipment Under Control
FBD	Function Block Diagram
IEC	International Electrotechnical Commission
I&C	Instrumentation & Control
I/O	Input and Output
NCP	Network Communication Processor
OS	Operating System
PIO	Process Input and Output
PIOP	Process Input and Output Communication Processor
PDS	Plant Display System
SIL	Safety Integrity Level
ST	Structured Text (programming language)
ST	STation (Hitachi component)
UD	Unit Driver
V & V	Verification & Validation

REFERENCES

[1] R. Brown, R. Basso, "Advanced CANDU Reactor Distributed Control System Design", 25th Annual Conference of the Canadian Nuclear Society, Toronto, Ontario, Canada, 2004 June 6-9

[2] R. D. Fournier, "Applying IEC Standards to Categorizing Safety-Related I&C Functions in CANDU Plants", 26th Annual Conference of the Canadian Nuclear Society, Toronto, Ontario, Canada, 2005 June 12-15

[3] E. Harmer, G. Mitchel et al. , "DCC Replacement Initiative – System Design Process and Standards Framework", 24th Annual Conference of the Canadian Nuclear Society, Toronto, Ontario, Canada, 2003 June 8-11