Hitachi's Proposed DCS Solution for New Build CANDU® EC6® using the G-HIACS® Unified Platform

D. Tan[1], K. Ishii[1], Y. Otsuka[1], K. Uemura[1] and P.E. Marko[2]
[1] Hitachi Ltd., Infrastructure Systems Company, Ibaraki, Japan
(E-mail: daisuke.tan.ye@hitachi.com)
[2] Hitachi Power Systems Canada Ltd., Power & Industry Division, Ontario, Canada

Abstract

Hitachi Ltd. has developed the safe and secure functional safety DCS controller for potential new build NPP projects in the global market. Hitachi has improved the availability, maintainability, and reliability for its latest DCS systems named G-HIACS®, [1]. In this latest paper on its DCS product development program, Hitachi would like to report a proposed DCS solution for new build CANDU®, [2] NSP and BOP based on the G-HIACS Unified Architecture (R800FS/HSC800FS νSAFE Functional Safety Controller and R900/HSC900 General Purpose Controller) hybrid control system.

1. Introduction

Hitachi, Ltd. introduced its first true HIACS (Hitachi Integrated Autonomous Control System) DCS (HIACS-3000) to the market in 1985. As a turn-key supplier of social infrastructure systems, Hitachi's focus has principally been system integration and performance. As such, DCS has been usually considered a part of the "overall machine" rather than a stand-alone / off-the-shelf commodity product. The last 2 decades have seen a steady move (even rush) toward standardization in all fields to ensure product technological compatibility independent of the commercial and/or corporate changes (e.g., mergers, acquisitions, bankruptcies) that may affect their original creators and provide a certain level of resistance to obsolescence. Hitachi's decision to evolve its successful HIACS® series DCS into a programmable controller family based around compliance with well-accepted international standards such as IEC 61131 and IEC 61508 was partly motivated by this clear market trend and partly motivated by its world-wide presence as a power generation systems (especially thermal and nuclear) supplier in its own right and potential partner in the CANDU® new build business. As previously reported (Gomez *et al*., 2011 [7]), new build CANDU® reactor control design has embraced this evolution toward standardization:

> "Design of EC6® Instrumentation and Control (I&C) architecture is driven by functional categorization. Control functions are categorized based upon their importance to safety following project design guidelines. These categories are - in order of decreasing safety importance – "A", "B", "C" and "D". Each computer system – comprised of hardware, embedded and system software, and the software application – is assigned a safety classification of Class 1, 2, 3 or as per applicable industry standards, determined by the category of the most significant safety function that it implements.

[1] G-HIACS is a registered trademark of Hitachi, Ltd.
[2] CANDU is a registered trademark of Atomic Energy of Canada Limited and used under license by Candu Energy Inc.

"The EC6® [3] DCS implements the bulk of the control logic for the plant process control systems and performs data acquisition functions for these systems; therefore, the DCS requires a qualified Programmable Electronic System (PES) platform for implementing these functions. To that end, portions of the DCS are qualified as IEC 61513 nuclear class 2 and class 3, as appropriate. Essential safety functions are implemented using dedicated class 1 control systems which are functionally and physically independent of the DCS.

"The qualification process of PES products is based on standards IEC 61513 and IEC 62138 as appropriate to the system class, which is also consistent with CAN N290.14. This qualification process is applicable to the PES product used to implement the mitigating, control, monitoring and testing roles in class 2 or 3 systems such as the DCS. The objective of the PES qualification is to establish the following:

- "Adequate suitability of the product for the intended application, with an emphasis on functional and operational safety over the product's in-service life;
- "Adequate documentation that specifies how the product can be safely used for applications important to safety; and
- "Adequate evidence of correctness of the PES product design. "

Hitachi has continually interfaced with Candu Energy to ensure that the requirements for the EC6® DCS are fully incorporated into the development of the (G-HIACS®) νSAFE®, [4] product

The following sections describe the product repertoire of Hitachi's DCS and the salient features of the Hitachi product which support its applicability to the DCS as well as summarize Hitachi's latest product design activities conducted as part of the proposed Enhanced CANDU 6® (EC6®,) DCS implementation plan and for ensuring suitability as a COTS product.

2. The Repertoire of Hitachi's DCS Products

Hitachi has regularly reported the progress of our DCS development at past CNS conference as follows:

1. Adapting our DCS technology to IEC standards (CNS 2006) [1]
2. Description of our project management experience for implementation of DCS in NPP (CNS 2007) [2]
3. Description of our BOP I&C and DCS experience and new developments (CNS2008) [3]
4. Description of our DCS Emulator development (CNS 2009) [4]
5. Description of our DCS Emulator development for the ACR-1000® simulator (CNS2010) [5]
6. Description of our DCS Emulator support for NPP Simulator design (CNS 2011) [6]
7. Joint AECL/Hitachi description of application of Hitachi DCS to new build CANDU® (CNS 2011) [7]
8. Description of expanding DCS family and compatibility developments (CNS 2012) [8]

[3] Enhanced CANDU 6 (EC6) is a registered trade mark of Atomic Energy of Canada Limited and used under license by Candu Energy Inc.

[4] νSAFE is a registered trademark of Hitachi, Ltd.

In this paper, Hitachi will report our latest achievements, specifically:

1. Improvement of availability of the latest Hitachi DCS Platform.
2. Improvement of maintainability of the latest Hitachi DCS Platform.
3. Improvement of performance of the latest Hitachi DCS Platform.
4. DCS architecture for new build CANDU® EC6® proposed and developed by Hitachi based on technical specifications and feedback from Candu Energy (previously AECL®), using the latest Hitachi DCS Platform.

At first, Hitachi would like to briefly describe its repertoire of G-HIACS® DCS products. More details may be found elsewhere ([5], [6], [7] and [8]).

2.1 G-HIACS® R800FS/HSC800FS νSAFE® Functional Safety Controller

The Hitachi νSAFE® controller system, certified compliant with IEC61508 SIL2 by TÜV Rheinland, was designed specifically with safety-related applications in mind. Additionally, the R800FS controller design is such that both functional safety-related (SIL) tasks and general purpose (non-SIL) tasks. Figure 1 illustrates a typical νSAFE® DCS configuration.

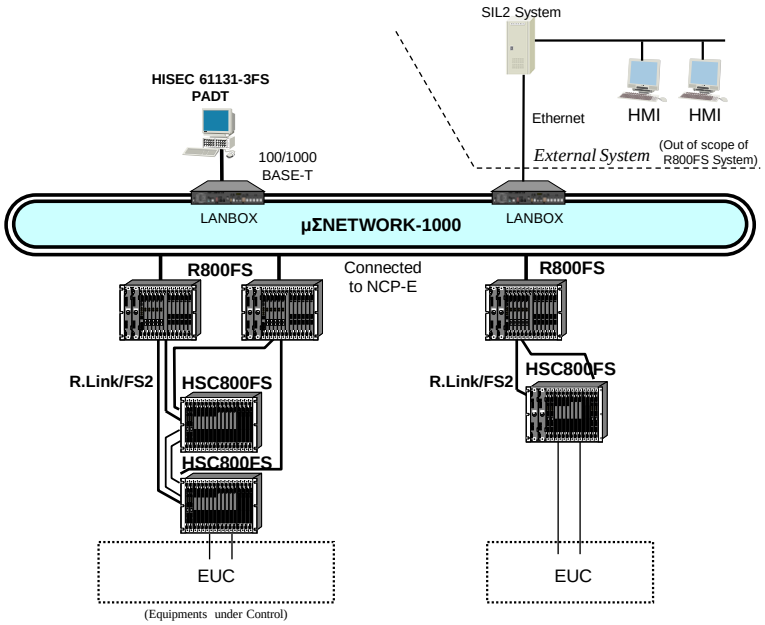


Figure 1 Typical DCS Configuration based on R800FS/HSC800FS

Except for any external systems and 3rd party EUC and open-source network equipment, all νSAFE hardware and software are COTS products designed and built by Hitachi.

2.2 G-HIACS® R900/HSC900 General Purpose Controller

The Hitachi R900/HSC900 controller system is designed mainly for high performance, compactness and general use applications where IEC61508 Functional Safety is not a central requirement. The

R900/HSC900 is the latest successor of the HIACS series which Hitachi has applied and developed since the 1980s. DCS systems provided by Hitachi have a proven record of high reliability and availability; this latest generation adds to this traditional characteristic improved performance as well as improved maintainability achieved by decreasing the number of parts and I/O modularisation. Figure 2 illustrates a typical R900/HSC900 DCS configuration.

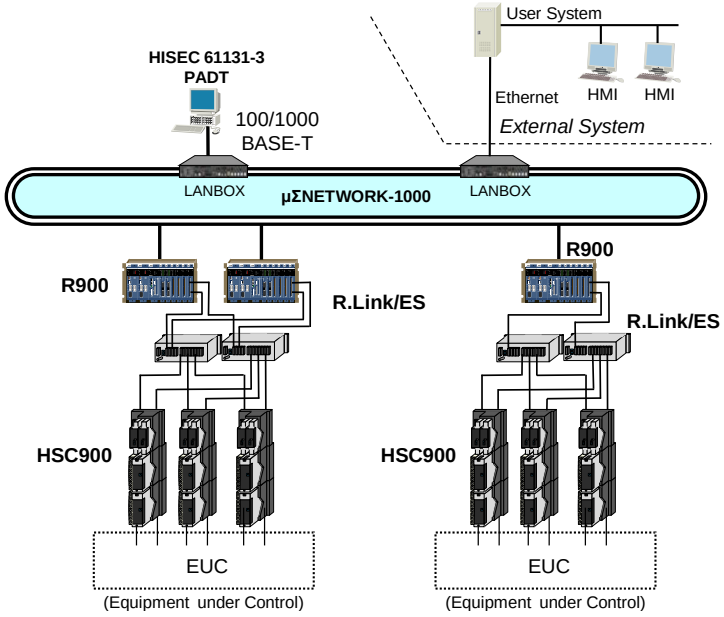


Figure 2 Typical DCS Configuration based on R900/HSC900

Similarly to νSAFE®, all R900/HSC900 hardware and software are COTS products designed and built by Hitachi.

2.3 HISEC61131-3 Programming And Debugging Tool (PADT)

The HISEC61131-3FS PADT is the interface that provides the programming and debugging environment for the configuration and application development of the G-HIACS® R800FS/HSC800FS νSAFE and R900/HSC900 controller systems, having the basic features listed in Table 1. The PADT consists of a Master/Client structure (the Master/Client definition is part of the initial setting) with different capabilities available for each with different functions and capabilities set for each. The master PADT can be configured for both SIL2 environments (R800FS) and non-SIL environments (R800FS and R900). Similarly, the client PADT connected to its Master via network can be used for both SIL2 environments and non-interfering general purpose (non-SIL, general purpose) environments. The client PADT can be used as a principal programming and debugging tool in the G-HIACS® "Unified Architecture" (see additional details below and [8]).

Table 1 Main Features of Hitachi G-HIACS DCS

Items	R800FS/HSC800FS νSAFE	R900/HSC900
IEC61508 Functional Safety	SIL2 (single/duplicated system)	N/A
Supported I/O Types	FS: DI, DO, AI, AO (4 types) Non-FS: DI, DO, AI, AO, etc. (8 types)	DI, DO, AI, AO, RTD, THC, PTI, LVDT, etc. (13 types)
System	Single (SIL2) Duplicated (SIL2,high availability) 2oo3/2oo4 (improved PFD*)	Single Duplicated Triple (only for HIACS)
Programming Languages	FBD, SFC, ST (IEC61131-3)	FBD, SFC, ST (IEC61131-3) FBD (Lyra HIACS†-type)

*Probability of Failure on Demand

†Hitachi in-house programming language interface used in previous HIACS series; supported by R900/HSC900 for legacy customers.

2.4 The G-HIACS® Unified Architecture for R800FS/HSC800FS and R900/HSC900

The Hitachi HISEC61131-3FS PADT programming and debugging environment is compatible with both the νSAFE® and 900-series DCS making it the central point of the G-HIACS® "Unified Architecture" system. Individual NPP sub-systems are specified a certain safety level/category depending on the requirements and a DCS which accords with that safety level/category must be installed. Systems with different safety levels must be divided physically and separated logically, so the programming environment and debugging environment is not shared. Thanks to the HISEC61131-3FS PADT's inherent capabilities, seamless and transparent access is possible from any authorized client PADTs regardless of the safety level or the location of the controllers on the control system network. In addition, thanks to the capability of multi-user access, effective maintenance work is available, and further maintenance improvement is possible by using shared files between each sub-system.

2.5 Example DCS Architectures proposed NPP New Builds

The DCS Architecture proposed by Hitachi for new build NPPs in the global market is based on the Unified Architecture. The architecture is based on the implementation of the specific controller and development of the applications according to the safety level of each sub-system, along with the use of the PADT as the central point connecting all NSP and BOP systems (excluding shutdown systems) seamlessly (see Figure 3).

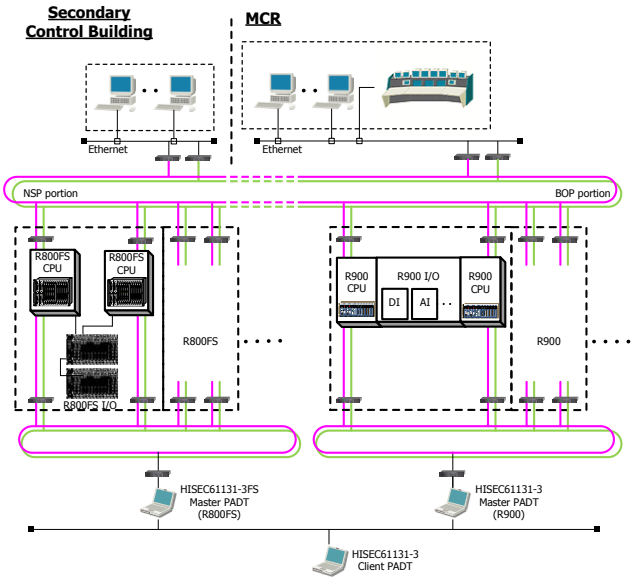


Figure 3 NPP (Total) DCS Based on the G-HIACS® Unified Architecture

Thanks to this "hybrid" architecture, SIL and non-SIL environments can be separated physically and systematically, and the plant can be managed securely and conveniently. A "Unified Architecture" based system concept can also be developed for a multi-unit generation station as shown in the following architecture, which assumes the existence of a common systems area for each unit in a two-unit plant (see Figure 4). There is also the ability to further sub-divide the "functional safety" area of the architecture thanks to the νSAFE® inherent capability to manage a hybrid SIL and general purpose (non-SIL) application within the same R800FS CPU with non-FS (HSC800) and FS (HSC800FS) I/O within the same architecture.

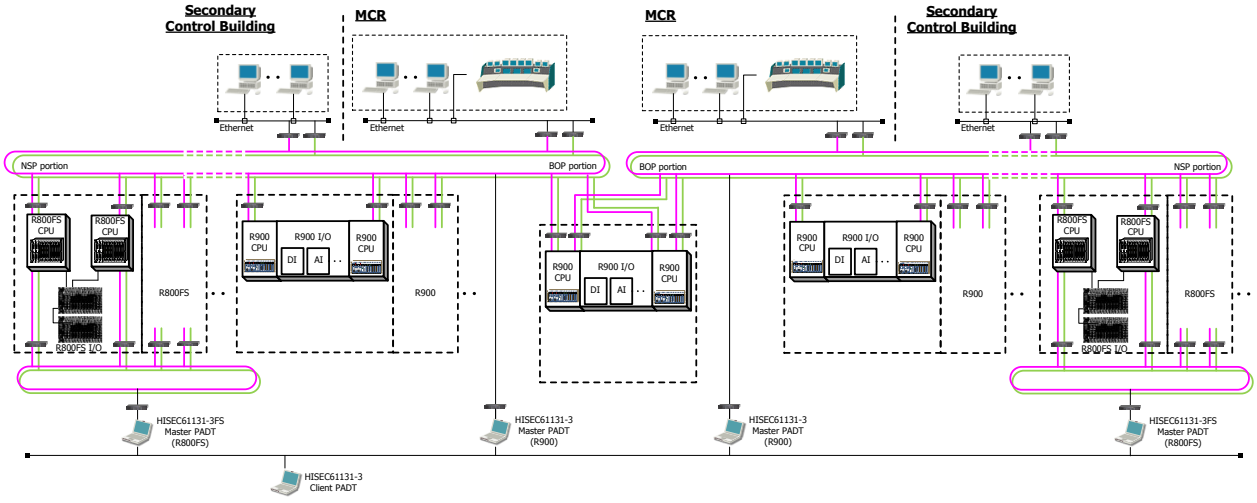


Figure 4 Twin-Unit NGS DCS Based on the G-HIACS Unified Architecture

In this architecture, we can access both units' CPU from one client regardless of this client's location in the plant. By using this common client, maintenance between units can be improved in this configuration using system control across the plant units.

3. Latest Improvements to the G-HIACS® Platform

Hitachi's latest improvements to its G-HIACS® product are focused on improving its availability, maintainability, and reliability through the following functionality.

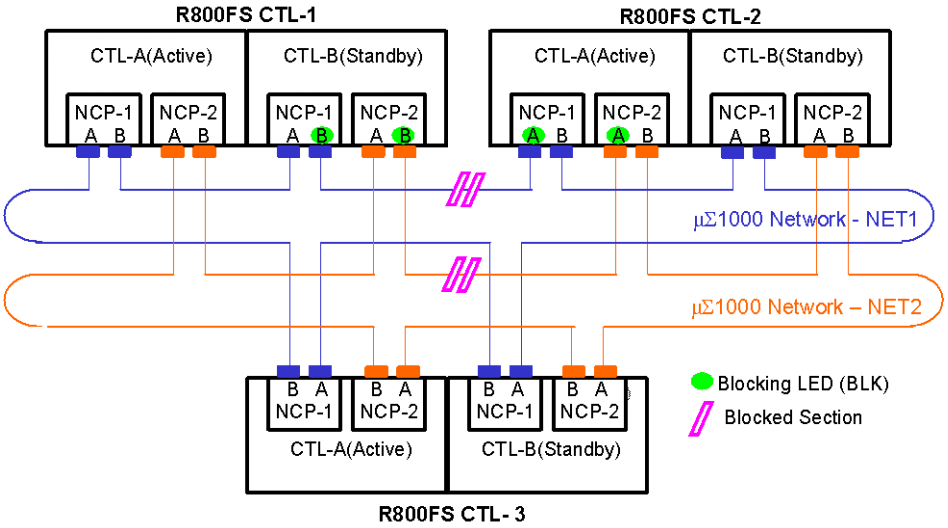
3.1 Hitachi G-HIACS® Availability

To improve the availability of G-HIACS® (as stated previously in [7] and [8]), Hitachi implemented integral dual redundancy for the three main systems: (1) LAN (peer-to-peer), (2) field network (CPU-to-I/O), and (3) CPU and RIO.

3.1.1 Circuit Redundancy of μΣ1000 Network

The μΣ1000 network (μΣ1000) is duplicated. This duplication improves the response to failures. Figure 5 shows example failure responses (countermeasures) in the case of a single break in the μΣ1000 network.

[Normal operation]



[See Figure 6 for Failure Mode]

Figure 5 Example of Normal Operation– pre-Optical Connector Failure

[Optical Connector Failure]

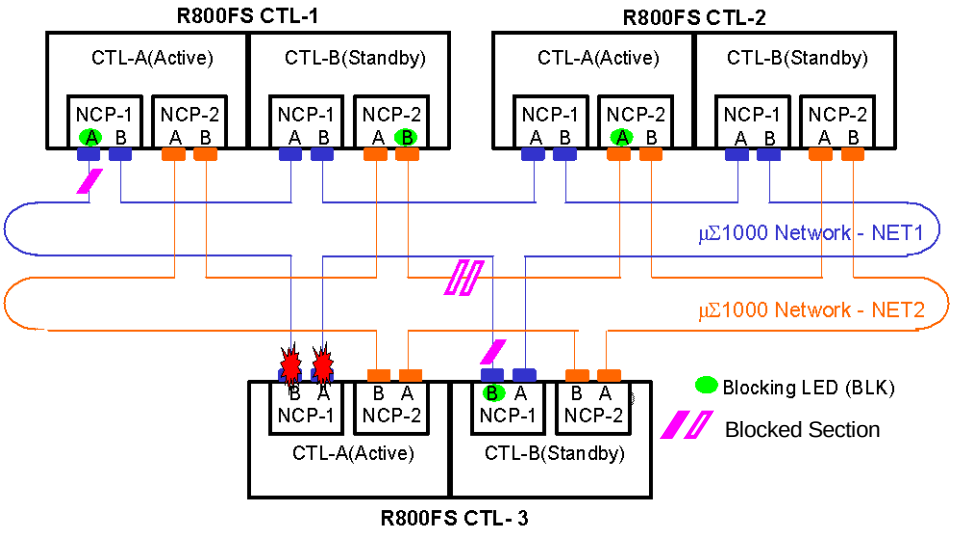


Figure 6 Example of Failure Mode – Optical Connector Failure

Figure 6 shows some countermeasures for failure of an optical connector of the μΣ1000 network connection. Although parts of NET1 are blocked by this failure, control operations continue by using NET2. Even if another failure were to occur in another part of the network (whether in NET1 or NET2), there would be no influence on the communications between the all controllers and the operations would continue because both NET1 and NET2 are also (inherently) redundant. G-HIACS® has this advantage of being able to continue operation under a single network failure without needing Controller switchover. From an operations point of view, network status is easily grasped by alarm and status signals sent to the PDS; and from a maintenance point of view, network system isolation (essentially duplicating a network break) can be manually initiated to maintain any faulty systems (such as field signal or I/O module) problems before more serious failure(s) causing plant or system shut down can occur.

3.1.2 Redundant R.Link/FS2 Network and Isolation of Branch RIO Chassis

R.Link/FS2 network is duplicated based on a redundant ring design. RIO chassis are connected to their controller(s) (CPUs) through multiple (1 to 6) electrically isolated "branches" each linked to the CPU chassis by an RIOSW (RIO switch) module. This redundancy and multi-branch capability of R.Link/FS2 improves failure response through redundancy and diversity. Two simple RIO system configurations (for R800FS/HSC800FS vSAFE) are shown in Figure 7.

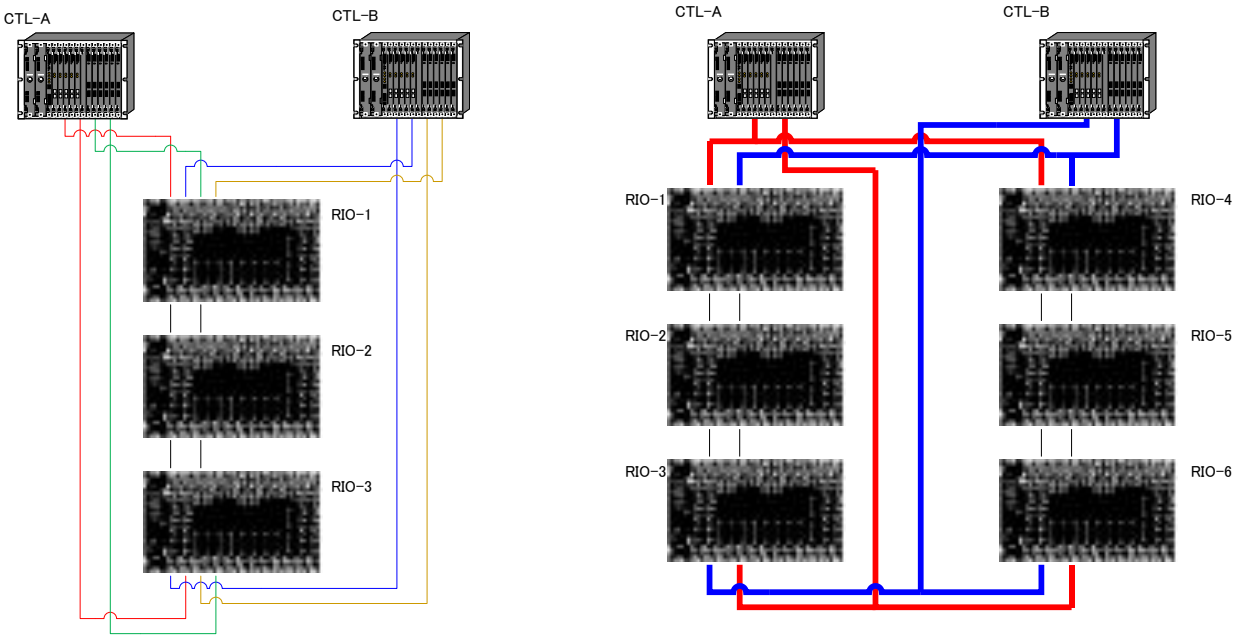


Figure 7 R.Link/FS2 Ring Duplication and Branch Architecture (using νSAFE)

The left diagram in Figure 7 highlights the R.Link/FS2 ring redundancy lines. The right diagram simplifies the left diagram and adds the configuration of two branched RIOs. In addition to this configuration's inherent properties, systematic and physically separate redundant configuration can be achieved by installing duplicated signals (modules) in separate branches and linked to redundant CPUs. These multiple supporting layers of redundancy increase both reliability and availability. Maintainability is also improved because failed parts can be isolated during failure for replacement.

3.1.3 Redundant CPU

In a fully redundant system as described above, even if one system should severely or completely fail, operations can continue supported by the redundant CPU. In addition, one system can be completely isolated physically by using the redundant capabilities of the networks and the RIO as shown in Figure 5, Figure 6 and Figure 7. For (redundant CPU)_functional safety systems, loss of a single CPU does not degrade SIL2 since νSAFE® SIL2 rating does not depend on redundancy. Thanks to these inherent capabilities, online hardware and software maintenance is possible even for functional safety systems by executing hot swapping of modules or switch over of CPUs.

3.2 Functional Safety for Hitachi G-HIACS vSAFE

To improve G-HIACS® functional safety (SIL2) capability, Hitachi implemented the following internal architecture features.

3.2.1 High Performance SIL2 System Architecture through 1oo1D Logic

Hitachi is using 1oo1D (1-out-of-1 diagnostic) logic by separating the functions in each module to achieve SIL2 without performance reduction. In a 1oo1D logic system, one of the functions in the module is dedicated to diagnosis for ensuring of data integrity and message reliability and the other ensures the actual function. Figure 8 outlines of this capability.

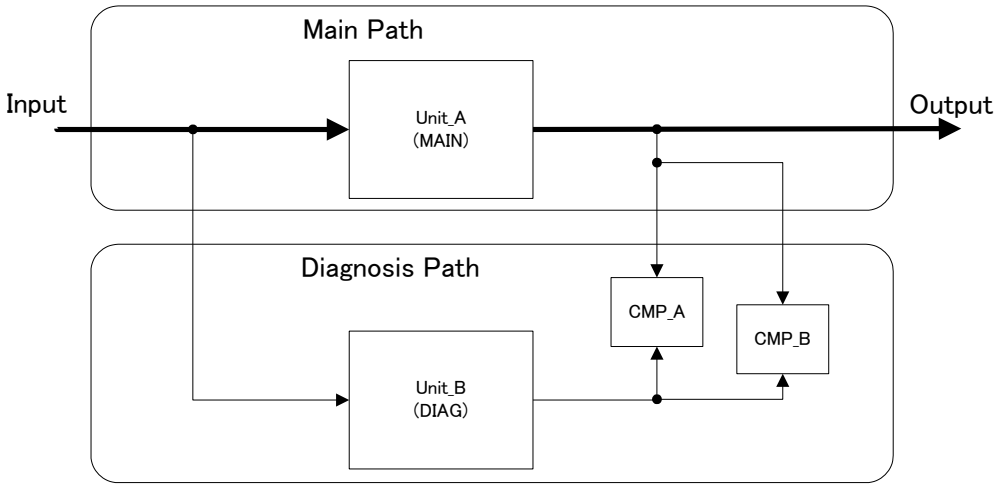


Figure 8 1oo1D Concept

As shown in Figure 8, the input signal is distributed to both the main path and the diagnosis path, while the output signal comes from the main path only. The output from the diagnosis unit (Unit_B) will be compared (in and by the diagnosis path) with the signal from the main unit (Unit_A) In short, the main path is dedicated to operations without the diagnostic burden; as a result, in spite of having a diagnosis function, performance does not decrease significantly. One should note that using the 1oo1D logic shown in Figure 8 does degrade the performance of SIL2 programs as compared to that of non-SIL (general purpose) programs due to the additional required overhead such as synchronization between units. Some performance issues related to SIL2 (FBD) programs vs. the equivalent program logic implemented in a non-FS system have been mitigated during the latest round of product development (2011-2013). The following specific countermeasures reduced the difference of the performance of such programs to 10%: (1) optimisation of frequency of use for 1oo1D, (2) optimisation of target for use, and (3) optimisation of the FBD operating environment.

3.2.2 Test-less Diagnosis using 1oo2 Logic

Hitachi has devised test-less diagnosis by using 1oo2 logic in the diagnosis function (i.e., the function for error detection) and the DI input area. Hitachi's system prevents a failure from affecting other systems and ensures the safety by shutting off the CPU or RIO modules power supply when the redundant system detects the failure. Figure 9 shows the concept of 1oo2.

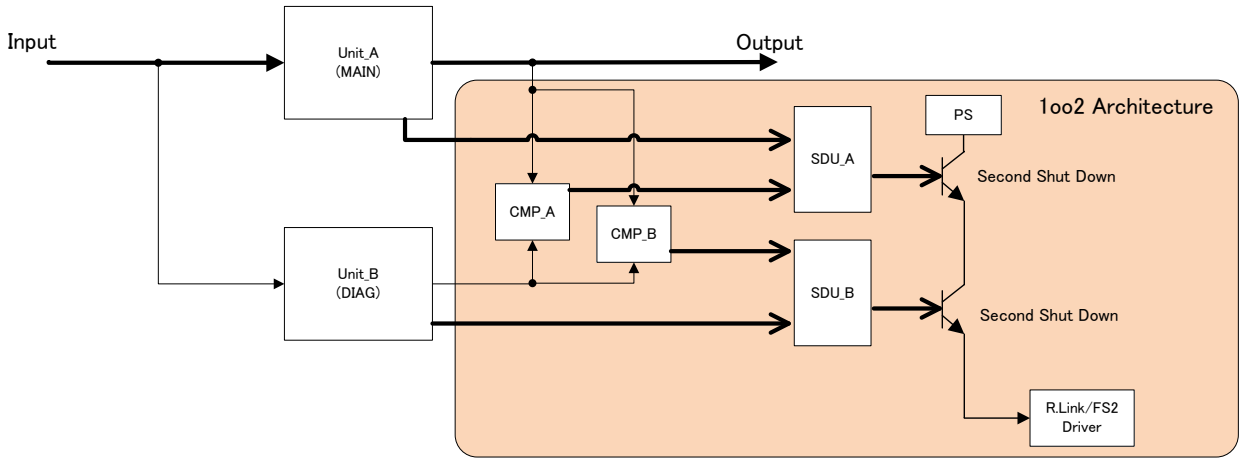


Figure 9 1oo2 Concept

3.3 G-HIACS® Maintainability

To improve G-HIACS® maintainability, Hitachi implemented the RAS concept as follows.

3.3.1 The RAS Concept

Hitachi divides the RAS concept into 4 parts: (1) RAS for control, (2) RAS for maintenance, (3) RAS for preventive maintenance, and (4) RAS for analysis. Functional safety considerations belong to (1) RAS for control. Table 2 shows the RAS separation and the purpose of each.

Table 2 RAS Concept for G-HIACS

Separation		Purpose
1	Safety	Supporting the behaviour for maintaining under an acceptable level the hazard to people and danger to materials or equipment.
	Reliability	Keeping items of equipment or devices usable per the stipulated terms and conditions and system requirements.
	Availability	Maintaining normal control mode under failure or transient failure conditions, or operating in a degraded way (e.g., switching to secondary CPU in case of primary failure) to prevent system shut down due to single or minor failures.
2	Serviceability	Allowing detection of failure point(s) and changing the failed portion of the system.
3	Integrity	Identifying in a timely way any degraded systems or module failures over the plant life cycle thus supporting preventive maintenance programs (i.e., repair or replacement prior to plant system failure or shutdown).
4	Analyticity	Allowing identification of the failed part at the site or after return of the part back to the factory.

3.3.2 Detailed RAS Functionality

Following the concept above, Hitachi has developed the following RAS functions (among others):

- Redundant architecture: the DCS fulfils 1oo1D with the Main path + Diagnosis path architecture for SIL2 certification with high performance (section 3.2.1), and 1oo2 logic for diagnosis function (section 3.2.2).
- Hardware safety layer of R.Link/FS2: The DCS can reduce the processing load of software.
- Function of RAS freeze and clear: The system acquires the statistical information on failures simultaneously (sampling interval of 10 minutes), to analyse failure trends for the preventive maintenance RAS function.

Depending on the requirements of the RAS concept, Hitachi's decision on the timing of data acquisition will vary. For example, data needed for control will be acquired in real time; data needed for preventive maintenance is acquired periodically (every 10 minutes).

4. Conclusion

In this report, Hitachi has further expanded on the G-HIACS® Unified Architecture platform and its capabilities to cover the integrated architecture (hardware, software, application and networks). For control systems with complex requirements and multi-levels of safety, diagnostics and categorization (modern NPPs such as the CANDU® EC6®, for example), the Hitachi G-HIACS® Unified Architecture is an integrated and elegant solution balancing the competing need for diversity of application and capabilities with the need for operational and maintenance uniformity. Hitachi continues to enhance its platform with Candu Energy's system development in mind as well as looking at applications to future ABWR and other I&C projects in the global market.

5. References

[1] K. Ishii, M. Kobayashi, M. Shiraishi, S. Masunaga, H. Harada, G. Raiskums and S. Tikku, "Distributed Control System Application to CANDU Plants Recent Activities for Adaptation of DCS Platform to IEC Standards", 27th Annual Conference of the Canadian Nuclear Society (2006)

[2] K. Ishii, H. Harada, S. Masunaga and P.E. Marko, "Hitachi's Project Management Experience on Distributed Control Systems (DCS) in Nuclear Power Plants", 28th Annual Conference of the Canadian Nuclear Society (2007)

[3] K. Ishii, H. Harada, T. Yamamori, K. Igarashi and T. Arakida, "Fundamental BOP I&C Systems Structure in Nuclear Power Plants", 29th Annual Conference of the Canadian Nuclear Society (2008)

[4] Y. Nakashima, K. Ishii and D. Chiba, "DCS Emulator Development for Nuclear Power Plants", 30th Annual Conference of the Canadian Nuclear Society, Calgary, Alberta, Canada, June 3, 2009.

[5] Y. Nakashima, R. Trueman and K. Ishii, "DCS Emulator Development for the ACR-1000® Simulator", 31st Annual Conference of the Canadian Nuclear Society, Montreal, Quebec, Canada, May 24, 2010.

[6] Y. Nakashima and K. Ishii, "Hitachi DCS Emulator Design to Support NPP Simulator

Implementation", 32nd Annual Canadian Nuclear Society Conference, Niagara Falls, Ontario, Canada, 2011 June 5-8

[7] V. Gomez, R. Zurek, S. Masunaga, K. Ishii, P. E. Marko, D. Tan, "Application of DCS to New Build CANDU Designs using the G-HIACS ,SAFE Platform", 32nd Annual Canadian Nuclear Society Conference, Niagara Falls, Ontario, Canada, 2011 June 5-8

[8] Y. Horikoshi, T. Shimizu, Y. Otsuka, M. Suenaga and S. Masunaga, "DCS Innovation by SIL and Non-SIL Unified Architecture – Hitachi Approach on G-HIACS (R800FS/R900)", 33rd Annual Canadian Nuclear Society Conference, Saskatoon, Saskatchewan, Canada, 2012 June 10-13

[9] K. Akagi, K. Morita, R. Miyahara, K. Murayama, C. Deir and S. Akahori, "The latest Application of Hitachi's State-of-the-art Construction Technology and Further Evolution Towards New Build NPP Projects", 29th Annual Conference of the Canadian Nuclear Society (2008)

[10] S. Asakura, N. Akane, J. Byrne, B. Canas, S. Kereliuk and S. Akahori, "New Build CANDU in Canada – Development and Application of Information Management Systems for Latest Construction Technology", 28th Annual Conference of the Canadian Nuclear Society (2007)