DCS Innovation by SIL and Non-SIL Unified Architecture – Hitachi Approach on G-HIACS (R800FS/R900)

Yu Horikoshi, Toshiki Shimizu, Yusaku Otsuka, Masashi Suenaga, Sunao Masunaga
Hitachi Ltd., Infrastructure Systems Company
Information & Control Systems Division, Ibaraki, Japan

Abstract

In response to the demand for safe, secure and smart systems, Hitachi, Ltd. has been developing a new generation of DCS, the Global-Hitachi Integrated Autonomous Control System ("G-HIACS[1]"), based on its highly successful HIACS-7000 architecture. The G-HIACS product family comprises the SIL2-rated R800FS/HSC800FS νSAFE[2] (pronounced "nu-safe") Functional Safety Controller and the R900/HSC900 General Purpose Controller. This paper summarizes the ongoing technical development successes, presents the key results of Hitachi activities within the Canadian nuclear market, and maps out our medium-term goal of fully integrating the two platforms into a harmonized architecture (the G-HIACS "Unified Architecture").

1. Introduction

In the 1990s, the concept of "functional safety" was introduced to quantify the level of safety of safety-related systems and functions; based on probabilistic safety assessments covering function and system life cycle rather than deterministic rules. Demand for the functional safety approach and for functional safety compliant products has been increasing worldwide ever since. In response to this market shift, Hitachi has developed its latest Distributed Control System (DCS) product, the νSAFE R800FS/HSC800FS Functional Safety Controller (henceforth "νSAFE"), which has been certified by TÜV Rheinland as meeting Safety Integrity Level (SIL) 2 per IEC 61508, the international standard for functional safety. On the other hand, not all control systems require the application of functional safety (FS) certified hardware and software components. FS systems require extensive and rigorous diagnostics, fault-avoidance and fault-recovery. These unavoidably reduce performance as well as operational flexibility. In many cases, e.g., for critical infrastructure systems, this trade-off is appropriate and necessary; however, in some cases (e.g., in systems dealing with high volumes of data across large networks such as Smart City and Smart Grid or for high-speed systems such as turbine control systems (TCS)), loss of performance is fundamentally incompatible with system requirements. To support this type of application, the R900/HSC900 Controller DCS, Hitachi's next-generation non-SIL ("general purpose") DCS product will provide solutions with superior installation compatibility and system flexibility.

Finally, since the entire trend of modern IT and Control is towards integration and inter-compatibility, Hitachi is proceeding with the development of a "Unified Architecture"

[1] G-HIACS is a registered trademark of Hitachi, Ltd.
[2] νSAFE is a registered trademark of Hitachi, Ltd.

concept that will integrate both product lines under the single G-HIACS application development environment, in order to realize safe, secure and adaptable smart systems. This paper summarizes Hitachi's approach.

2. Introduction to Hitachi G-HIACS DCS Products

For over 40 years, Hitachi's Omika Works has been supplying DCS products integrating information and control technologies covering various applications such as power plants, chemical plants and steel plants as well as many types of general infrastructure such as water supply and treatment plants. In order to continue supporting a wide variety of applications, Hitachi is focusing on supplying and supporting for the global market the two G-HIACS DCS products introduced above.

2.1 R800FS/HSC800FS vSAFE Functional Safety Controller

Hitachi vSAFE is an evolutionary programmable controller designed for use in a DCS dedicated to safety-related applications. Figure 2-1 shows a basic vSAFE control system architecture example.

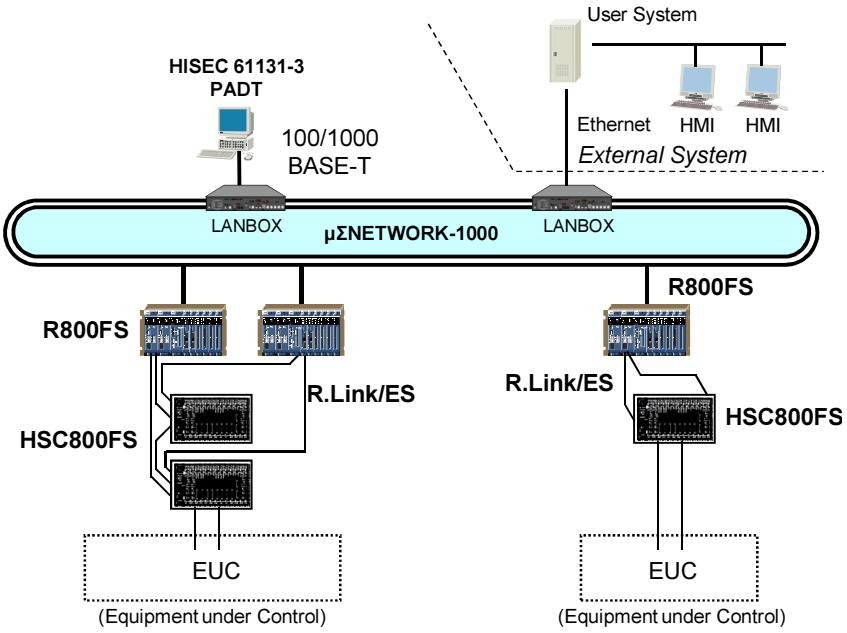

Figure 2-1 Example G-HIACS DCS Architecture based on vSAFE R800FS/HSC800FS

The vSAFE major hardware components (CPU, Remote Input/Output (RIO) modules and safety network) are designed to meet the requirements of the IEC 61508 functional safety standard, so that a single fault does not cause dangerous output to the plant, and was certified SIL2 in March, 2010 by TÜV Rheinland. Additionally, vSAFE meets the electrical safety

and EMC requirements per IEC 61131-2 international standards for programmable controllers.

CPU and RIO modules are connected together through R.Link/FS field bus (see Section 2.4), and multiple CPUs are connected to the HISEC 61131-3FS Programming and Debugging Tool (PADT) and other CPUs through the μΣNETWORK-1000 control network (μΣ1000, see Section 2.3). νSAFE supports full non-interfering CPU, RIO and network redundancy to improve availability while maintaining SIL2 functional safety.

While not designed to support extensive non-SIL applications, Hitachi created νSAFE with the ability to have safety related (SIL) and general-purpose (non-SIL) hardware and software co-exist in the same control system with 2 major types of HSC800FS RIO modules (SIL and general purpose) compatible with the R800FS CPU module. This dual hardware support is made possible by specially developed protection and diagnostic capabilities as well as R800FS CPU's unique capability of "dynamic switching of dual microprocessors" as shown in Figure 2-2.

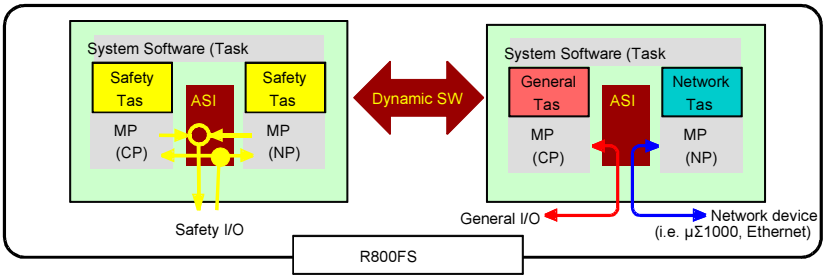

Figure 2-2 Dynamic Switching of Two Microprocessors

While providing the advantages of enabling coexistence of SIL and non-SIL components, νSAFE assures non-interference of the SIL components by non-SIL components. Hardware non-interference is realized by diagnostic functions to prevent or detect interference to SIL hardware by non-SIL hardware. Software non-interference is realized using two approaches: temporal separation and spatial separation. Temporal separation is realized by assigning higher execution priority levels to SIL software than to non-SIL software so that the SIL software is executed at the intended interval and is not interrupted by non-SIL software. Spatial separation is realized by separating the memory space with memory protection so that non-SIL software cannot alter the data (physical memory) used by SIL software. A special protocol is used to implement data sharing between SIL and non-SIL software, in order to prevent unintended change of data used by SIL software.

The R800FS/HSC800FS controller hardware is based on a 1oo1D architecture model. This architecture executes most of the diagnostic functions inside a single ASIC on each module and provides a cost-effective and high performance safety solution as compared to the 1oo2 or 2oo3 architectures used in many other safety DCS products.

2.2 R900/HSC900 General Purpose Controller

The R900/HSC900 is a high performance programmable controller designed specifically for use in general purpose (non-SIL) DCS. Based on Hitachi's highly successful HIACS-7000 controller architecture, the R900/HSC900 has been made easier to use than its predecessor by adding a number of enhancements (such as faster CPU, easier cabling and maintenance of PIO modules, and improved user interface), while still retaining the high reliability and performance of the previous controller system.

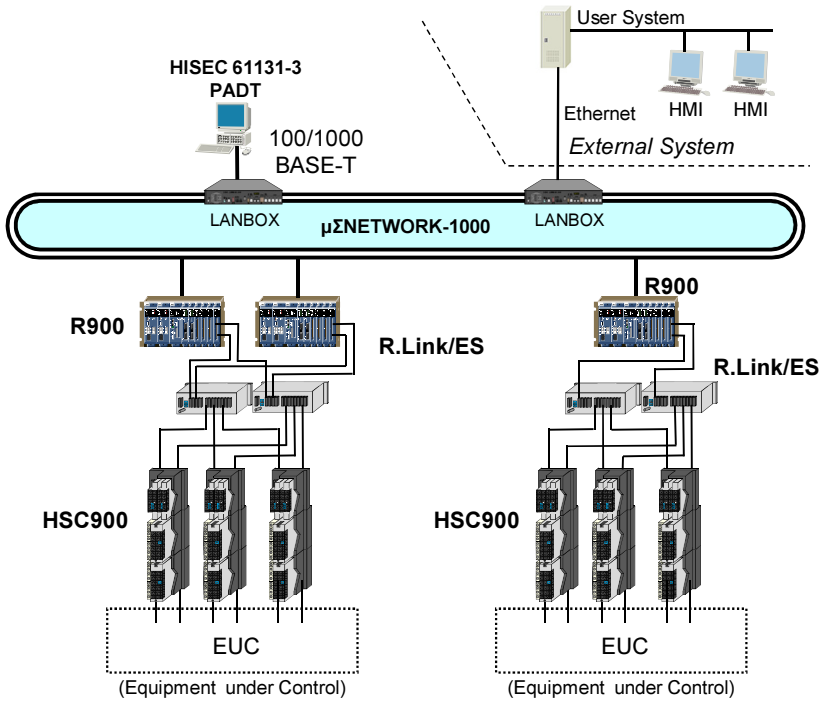

Figure 2-3 Example G-HIACS DCS Architecture based on R900/HSC900

Inter-CPU communication between redundant CPUs and communication between an R900 CPU and the HISEC 61131-PADT are carried out through the μΣ1000 network (same as νSAFE). R900 CPU and HSC900 Process Input/Output (PIO) modules are connected to each other via the R.Link/ES duplicated field bus. As with νSAFE, the R900/HSC900 Controller supports redundancy (CPUs, μΣ1000, PIO modules, and power supply) so that no single component failure can cause system shutdown. The R900/HSC900 covers a wide variety of modules; 30+ types are available (as of the time this paper was submitted) with more to be released in the future. The HSC900 PIO modules are designed with a base-mount structure with each module mounted to a base unit equipped with field wire terminals to which field wires can be connected directly. This design enables module replacement without disconnecting the field wires. This feature also makes wiring and cabling work easier, reduces the wiring and number of parts inside control cabinets, and improves serviceability.

2.3 μΣNETWORK-1000

The μΣ1000 network is designed for system applications integrating information and control communications. Based on Gigabit (1 Gbit/s) Ethernet[3] technology, μΣ1000 is an optical, ring-based network. The "LAN connection Box" (LANBOX) converts μΣ1000 to standard Ethernet enabling seamless communication with general purpose PCs (e.g., νSAFE PADT, user HMI) and all Ethernet-capable devices. The μΣ1000's 1-Gbit/s bandwidth can be allocated for control communication and information communication separately, so that real time and non-real-time communication can co-exist on a single physical network without real-time messages being delayed by non-real-time communication traffic. Fault tolerance is realized by the fully redundant dual-ring topology that compensates for single point failure by looping back along the ring. Cyclic memory transfer enables efficient communication between CPUs as if the CPUs shared a common memory. With the safety layer protocol implemented by the R800FS, μΣ1000 is capable of SIL2 compliant safety communications. Figure 2-4 summarizes these basic capabilities of μΣ1000.

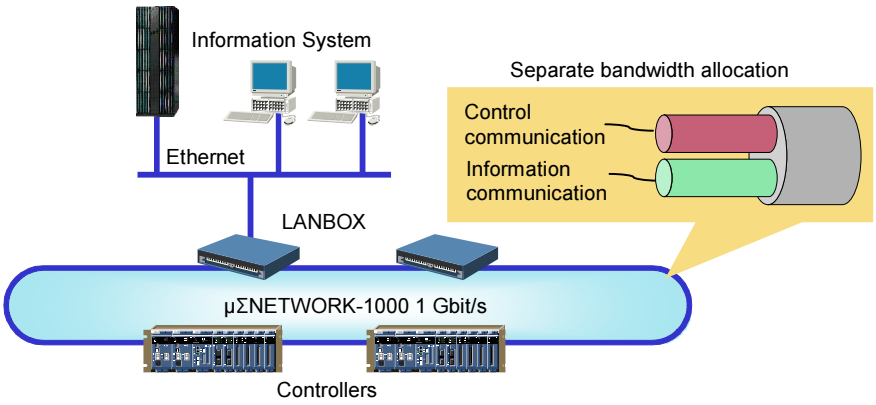

Figure 2-4 Example μΣNETWORK-1000 Configuration

2.4 R.Link Field Bus

Based on the RS-485 protocol, both R.Link I/O networks (R.Link/FS and R.Link/ES) are optical/electrical redundant serial field buses that connect a CPU to its Input/Output modules. The 20-Mbit/s bandwidth provides high speed and quick response as well as capacity for fault diagnostic information supporting high serviceability. R.Link/FS is the R800FS/HSC800FS CPU-RIO network, supporting high availability and safety with its ring-based network topology. Up to 252 RIO modules can be connected to a CPU module. With the safety layer protocol implemented, R.Link/FS supports SIL2 compliant safety communications. R.Link/ES is the R900/HSC900 CPU-PIO network, supporting high

[3] Ethernet is a registered trademark of the Xerox Corp.

scalability with its star-based topology and a wide variety of extension modules (e.g., HUB, optical-repeater,). Up to 1280 PIO modules can be connected to a CPU module.

3. HISEC 61131-3 PADT (Programming and Debugging Tool)

The HISEC 61131-3 PADT (Programming and Debugging Tool) series provides the programming and debugging environment for the R800FS and R900 controller systems. By using HISEC 61131-3 PADT series, the user can create application programs with three of the five IEC 61131-3 compliant languages, namely: Function Block Diagram (FBD), Structured Text (ST), and Sequential Function Chart (SFC). All FS programs are created within a functional safety task (FST) using the FBD language. Remote maintenance and system configuration are also performed using the HISEC 61131-3 PADT. Using the PADT allows the users to create the projects where SIL2 and non-SIL (General Purpose) applications can co-exist on a single R800FS CPU. Also, users can create non-SIL programs for the R900 CPU by using PADT. Some of the PADT key features are listed here:

1) IEC 61131-3 programming languages. All three available languages (FBD, ST and SFC) comply with the IEC 61131-3 standard on programming languages for programmable controllers including having the multi–language programming capability.
2) Intuitive interface system. The PADT is accessed by a graphical user interface whose ease of use and intuitiveness is supported by well–annotated command buttons, menu options, and intelligible command icons.
3) System Configuration
   - R800FS and R900 systems including configuration of multiple controllers, multiple I/O modules, and peer-to-peer networking.
   - I/O signal configuration including rationality limits and conversion from/to engineering units
   - I/O module configuration consistency checking
4) Security Features
   - Multi-level user access control via passwords with Read Only and Read and Write privileges
   - Password protection to prevent unauthorized users from writing to the CPU memory
5) Configuration Management
   - Version Tracking and Comparisons, Modification History
   - Import/Export capabilities with appropriate consistency controls
   - User defined function block (UDFB) library

6) User Program Testing Capabilities
   - Logic Emulator. The user can execute the user program logic on the PADT without needing a real controller.
   - Online monitor. In order to support user program testing and maintenance, the PADT includes live, online monitoring and such features as variable forcing, monitoring real-time data, trending real-time data, and manual controller state changes (i.e., online/offline run, stop).
   - Stimulator. The I/O Stimulator enables the user to run and test programs on the controller CPU without real field signals or physical I/O modules by simulating field data and responses. The Stimulator can also mimic CPU-to-CPU communications between a real controller and a virtual one in a full system simulation.
7) Import/Export capabilities based on XML files. System configuration and POU development are based on PLCOpen TC6 for XML (Extended Markup Language).
8) Online maintenance capabilities (for a real system)
   - Online software maintenance on standby controller while master controller is running
   - Online tuning
   - Online forcing

4. The Unified Architecture for R800FS (SIL DCS) and R900 (non-SIL DCS)

The Hitachi HISEC 61131-3 PADT series provides the programming and debugging environment for all G-HIACS (R800FS/HSC800FS νSAFE and R900/HSC900) controller systems. This is Hitachi's "Unified Architecture". This dual controller capability enables users to develop applications requiring safety, high performance and a wide variety of peripheral devices. Seamless and transparent access is possible from the same terminal regardless of the controller model or the location of the controllers on the control system network. The Hitachi HISEC 61131-3 PADT series provides cost savings and improved maintainability for the overall system. The following sections describe the main features of the "Unified Architecture", how to implement the "Unified Architecture", and the expected applications of the "Unified Architecture".

4.1 Key Features of the "Unified Architecture"

The key features of Hitachi's "Unified Architecture" are summarized below:

1) Project reusability

   Control program logic can be reused between R800FS and R900 CPUs and systems. This reduces workload in the programming phase.

2) Unified function library

The same operations and functions are supported independent of controller model. This reduces working hours for operator training for each controller model.

3) Master/Client PADT

The Master PADT for R800FS or R900 manages all the data related to each controller on the same μΣNETWORK-1000 while the Client PADT makes requests to execute the PADT functions to the Master PADT for both models of controllers. The Master PADT also allows the same access to different models of controllers as a Client PADT. Access transparency independent from controller model is implemented. This realizes unified access and improves maintainability. Up to 4 Master PADTs can be connected to a Client PADT.

4) Allowing Coexistence in the Same Network

Both R800FS and R900 can coexist in the same μΣ1000 loop, and they can send/receive the general transfer data to/from each other. Up to 63 non-SIL controllers can be connected to one μΣ1000 loop.

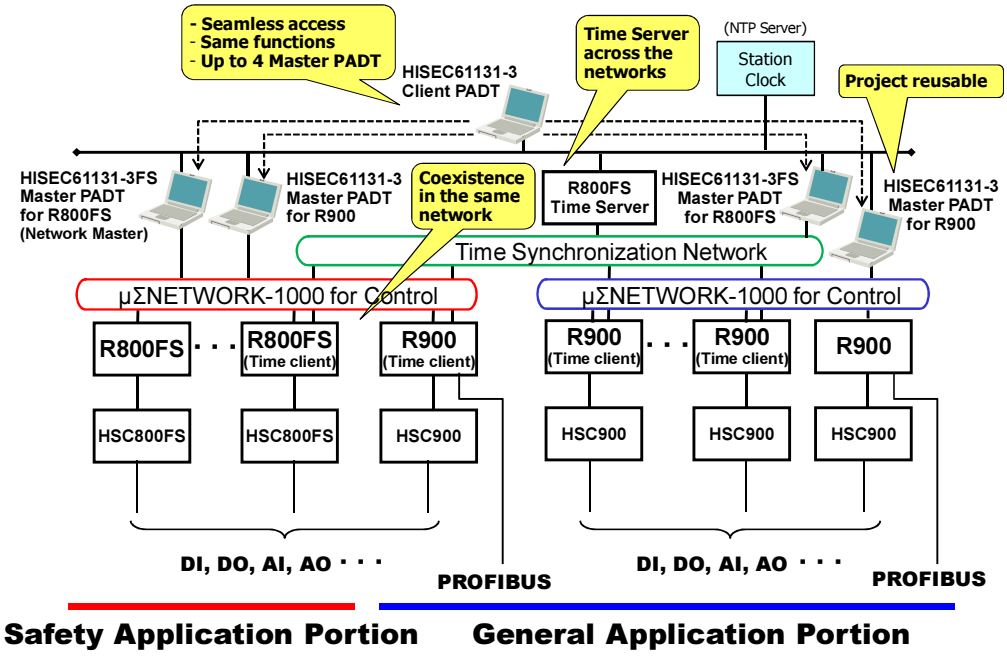

Figure 4-1 Hitachi G-HIACS DCS Unified Architecture Schematic

4.2 Implementation of the "Unified Architecture"

To implement the "Unified Architecture", Hitachi has overcome three technical challenges:

1) Non-Interference between SIL and non-SIL

Both the functional safety R800FS controller and the general-purpose R900 controller must be prevented from interfering with each other in order to allow one PADT to access both controllers. Achieving non-interference of the SIL portion by the non-SIL portion of the system is a significant technical challenge in the "Unified Architecture". Hitachi's G-HIACS assures non-interference through two measures:

➢ Separate Software Packages

The PADT is composed of two dedicated and independent software packages (one for each controller model, i.e., R800FS and R900) plus a common package to manage switching between the dedicated packages. The common package determines the start-up of the dedicated package depending on the controller model to be accessed thereby minimizing interaction between the packages. This means of configuration also allows the PADT to expand the number of supported controller models by adding on packages as necessary and as the overall G-HIACS product evolves over time.

➢ Access Control between Software Packages

Putting the PADT into a Master-Client configuration and restricting unintended access from the non-SIL Client Package to the SIL Master Package secures non-interference between the SIL and non-SIL portions.

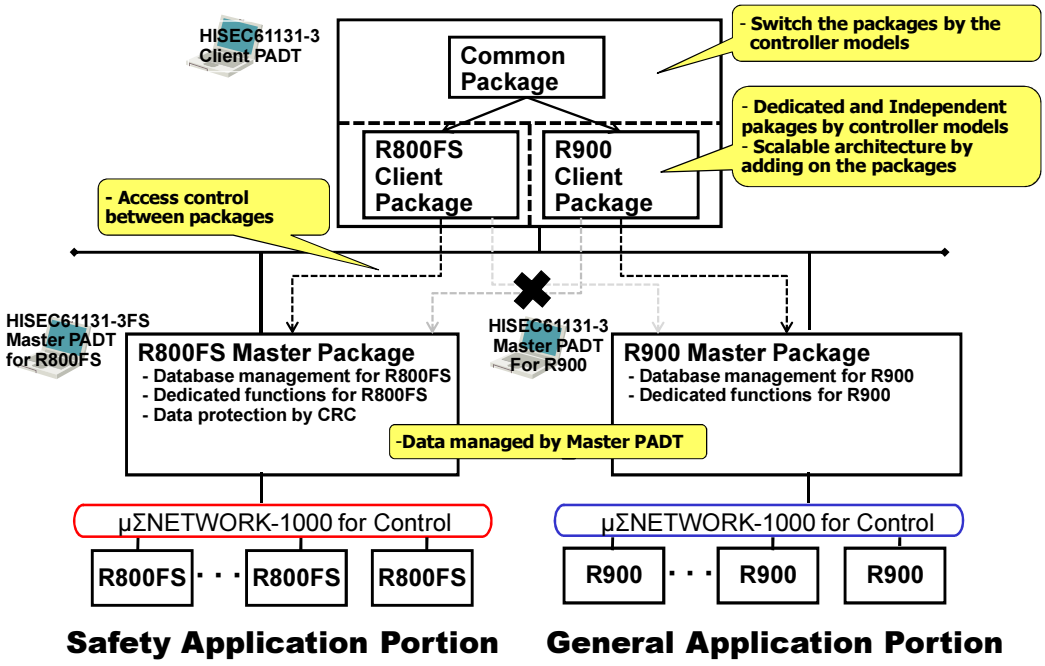

Figure 4-2 PADT Configuration for Realizing Non- Interfering

2) Plant-Wide Network Configuration

Using the Network Master PADT allows configuration of the plant-wide network shared by the Master PADTs. The Network Master PADT configures the plant-wide configuration items. This feature maintains the consistency of configuration and reduces costs for version control management.

3) High-Accuracy Software Clock Synchronization

High-accuracy synchronization of controller software clocks is required to allow for analysis of the failures of the plant system in chronological order.

The most common way to synchronize software clocks is to use the Network Time Protocol (NTP) or the Simple Network Time Protocol (SNTP). These protocols must wait for the response from the time server and compensate for the delay induced on the communication line in order to achieve high-accuracy time synchronization across their networks. In other words, these protocols are not really suited for real time control. The G-HIACS system achieves a good balance between high accuracy and real time control by using μΣ1000 (an excellent communication line in terms of response) and a proprietary Hitachi algorithm thereby requiring no waiting for a response from the time server. Up to 124 Time Client controllers can be connected to the Time Server via the Time Synchronization Network. This enables one Time Server to manage the time synchronization with the controllers connecting to different control networks. The Time Server can run without configuration from the PADT; the Time Client controllers will receive configuration information from the PADT on whether there is a Time Server or not. In addition, controllers connected to the Time Synchronization Network keep reliability, availability and serviceability (RAS) information such as “time synchronization failed”. The PADT error log and user application allow user access to this RAS information. Finally, costs for the time synchronization are reduced by enabling a single time source for all G-HIACS controllers.

4.3 Example Applications of the G-HIACS “Unified Architecture”

The G-HIACS “Unified Architecture” can cover safety-related applications using R800FS/HSC800FS νSAFE (designed to comply with functional safety standards) as well as large scale control applications using the scalable R900/HSC900 in a single unified system. This combination enables efficient monitoring and control of wide-range plant facilities. Accordingly, the G-HIACS “Unified Architecture” is well suited for large-scale safety-critical systems such as nuclear power plant applications. Specifically, a plan to apply the G-HIACS platform to new build CANDU®, [4] reactor designs is in progress [4]. Furthermore, the G-HIACS has been considered applicable to the Advanced Boiling Water Reactor (ABWR) worldwide.

[4] CANDU® is a registered trade mark of Atomic Energy of Canada Limited and used under license by Candu Energy Inc.

5. Conclusion

The Hitachi G-HIACS DCS "Unified Architecture" provides system configuration flexibility by permitting the combining of functional safety controller systems and conventional controller systems within a single application development environment and single user control system. This unified control system is suitable for a wide variety of DCS applications requiring safety, scalability, functionality, performance, and international standards compliance. A good example of such a demanding environment would be nuclear power plants with their main Balance of Plant (BOP) and Nuclear Steam Plant (NSP) split as well as several systems and sub-systems requiring high capability and safety but also, in some cases, performance and flexibility. For development and technical personnel, it reduces development and operational costs and complexity and increases inter-compatibility and re-usability. Hitachi's new generation G-HIACS DCS complies with the main international standards making it suitable for the Canadian nuclear market as well as any international market.

6. References

[1] S. Tikku, G. Raiskums, J. Harber and P. Foster, "Safety system and control system separation requirements for ACR-1000™ and operating CANDU® reactors", Proceedings of the 18th International Conference on Nuclear Engineering, ICONE18, Xi'an, China, 2010 May 17-21.

[2] CSA N290.14-07, "Qualification of pre-developed software for use in safety-related instrumentation and control applications in nuclear power plants".

[3] IEC 61508-Edition 1 and Edition 2, "Functional safety of electrical/electronic/programmable electronic safety-related systems".

[4] 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 νSAFE Platform", 32nd Annual Canadian Nuclear Society Conference, Niagara Falls, Ontario, Canada, 2011 June 5-8

[5] IEC 61131–3-2003, "Programmable controllers – Part 3: Programming languages".

[6] CAN/CSA-E61131-2-06, "Programmable Controllers – Part 2: Equipment Requirements and Tests".

[7] Technical Paper PLCopen Technical Committee 6 XML Formats for IEC 61131-3 Version 2.01 – Official Release