

HF Controls

Doosan HF Controls Corporation

HFC-6000 Safety Control System

Security Concept

RR901-000-23

Rev A

Effective Date 11/19/2009
Author/Title William Luo
Reviewer/Title Charles McKinney
Approval/Title Allen Hsu

Copyright© 2009 HF Controls Corporation

HFC-6000 Security Concept

Revision History

Date	Revision	Author	Changes
11/19/09	A	W. Luo	First Release

HFC-6000 Security Concept

Table of Contents

<u>Section</u>	<u>Title</u>	<u>Page</u>
SECTION 1		5
SYSTEM OVERVIEW		5
1.1	HFC-6000 Safety Control System	5
SECTION 2		6
SECURITY CONCEPT – HFC-6000 SAFETY CONTROL SYSTEM		6
2.1	Hardware Concept	6
2.1.1	<i>HFC-6000 Redundant Configuration</i>	6
2.1.2	<i>Block Diagrams</i>	7
2.2	Software Concept	12
2.2.1	<i>Overall Software Structure</i>	12
2.2.2	<i>HFC-6000 Controller Redundancy and EquAlization Software</i>	13
2.2.3	<i>ICL Communication Related Redundncy Software</i>	13
2.2.4	<i>Communication Link (Safety C-Link) Software</i>	16
2.2.5	<i>Application Program</i>	17
2.3	Development concept	18
2.3.1	<i>Methods, Tools</i>	18
2.3.2	<i>Quality Assurance</i>	19
2.3.3	<i>Documentation Control</i>	21
2.4	Definition of Faults to be considered	21
2.5	Measures for detection of these faults	22
2.5.1	<i>Online Diagnostic</i>	22
2.5.2	<i>The Quality of Database</i>	22
2.5.3	<i>Remote Status Broadcast</i>	23
2.5.4	<i>Dynamic Database (DDB) Broadcast</i>	23
2.5.5	<i>Communication Status</i>	23
2.5.6	<i>Summary of System Fault Measurement</i>	23
2.6	Reaction in case of Faults	24
2.7	List of the tests run after power-up or reset	24
2.8	Tests run during operation	25
2.8.1	<i>Mailboxes Test</i>	25
2.8.2	<i>ICL Communication Link Test</i>	25
2.8.3	<i>Maintenance Failover Test</i>	25

List of Figures

<u>Number</u>	<u>Title</u>	<u>Page</u>
Figure 1 - Redundant HFC-6000 Control System Architecture		5
Figure 2 - HFC-6000 System Arrangement Diagram.....		8
Figure 3 - HFC-SBC06 controller I/O interface		8
Figure 4 - Public Memory Data Stored.....		10
Figure 5 - Safety Communication Link (C-Link) Configuration.....		12
Figure 6 - Secondary Loop Back Test		16

List of Tables

<u>Number</u>	<u>Title</u>	<u>Page</u>
Table 1 - Redundant HFC-6000 control system hardware security structure.....		6
Table 2 - HFC-6000 software development and maintenance tools.....		18
Table 3 - HFC-6000 Application development and maintenance tools.....		19
Table 4 - HFC-6000 redundant safety system faults detection.....		23

Section 1

System Overview

1.1 HFC-6000 SAFETY CONTROL SYSTEM

The HF Controls (HFC) HFC-6000 Safety Control System is designed for the process function of any mission critical control application such as Nuclear Class 1E equipment control, Turbine Excitation Control, Main Fuel Trip (MFT) in a Burner Management System (BMS) application, and Safety Instrument System (SIS) in a Petrochemical process, etc. The configuration of the HFC-6000 redundant controller shall be capable of distributing safety functions, control algorithms, and information systems that form a base to meet the requirements for industrial plant process applications. The design of HFC-6000 system architecture shall be totally modular in order to operate either in a single cabinet or separated cabinets.

The hardware configuration of a redundant HFC-6000 control system resides in the controller and/or I/O racks. Figure 1 illustrates the process flow of a HFC-6000 redundant control system.

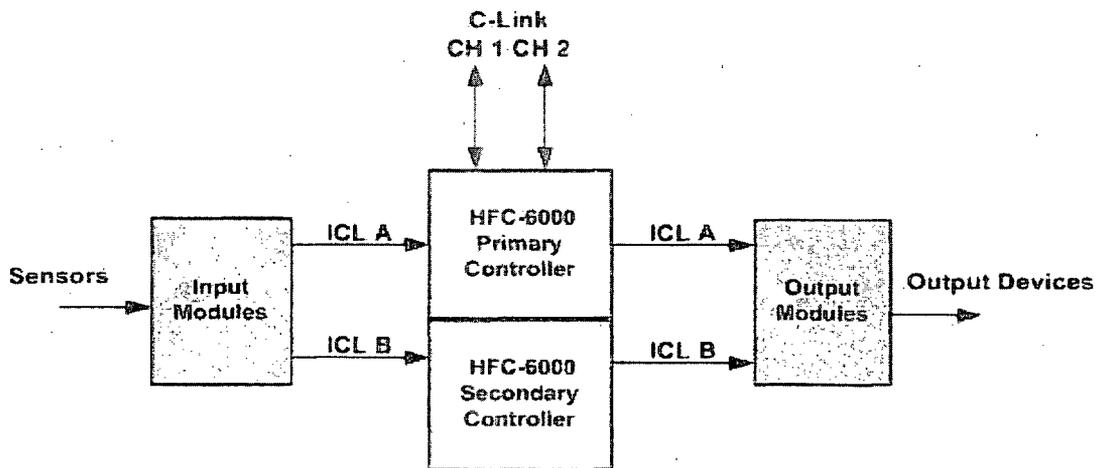


Figure 1 - Redundant HFC-6000 Control System Architecture

The purpose of this document is to perform a security assessment to identify potential security vulnerabilities in the concepts phase of the development of the HFC-6000 safety system. The proposed HFC-6000 safety control system shall disallow any remote access to its control function and the communication pathway from safety control system shall be designed as one-way broadcast out (by design, broadcast in the “in” direction is prohibited).

The scope of the HFC cyber security concept includes the description and concepts of security functions, diagnostic coverage, block diagrams, and the cyber security aspects for development phases of HFC’s safety projects.

Section 2

Security Concept – HFC-6000 Safety Control System

2.1 HARDWARE CONCEPT

2.1.1 HFC-6000 REDUNDANT CONFIGURATION

HFC-6000 Safety Control System shall consist of sets of redundant controllers and their modular I/O hardware. All redundant controllers shall be communicated over a safety Communication Link (C-Link) with token-passing Protocol by broadcasting a Dynamic Database (DDB) for exchanging information. A proposed gateway device shall be connected to the safety C-Link as a network node for providing one way communication to the outside of the system. In the operational mode, the peer to peer communication shall be prohibited over this safety C-Link. Within the controller, all field signals shall be updated by Peripheral Communication (PCN) processor (i.e. SAP processor, SAP is the code name for PCN firmware) of the primary controller. The secondary controller shall be equalized with the updated signals/images via Dual Port Memory (DPM). The following table illustrates the hardware security structure of the HFC-6000 Redundant Safety Control System. The control logic execution functions shall be prohibited from being accessed remotely.

Table 1 - Redundant HFC-6000 control system hardware security structure

Level	Description	Security Notes	Hardware Scope
Input Signal	Each input card has a redundant interface with the ICL, which provides separate hardware links to primary and secondary controllers	- Proprietary Master Slave polling protocol with error checking to prove the Communication integrity	Field Devices
Input Process	The Primary Controller access the input images and equalize to the Secondary controller	- Secondary loopback checking and backup - Redundant ICL link	The Primary Controller
Logic Execution	The primary controller perform logic execution and equalize the dynamic data to the secondary controller	- The result of executed logic as Digital Output & Analog Output images (DOs & AOs) - Equalize to Secondary	The Primary & Secondary Controllers
Output Process	The Primary Controller access the output images and equalize to the Secondary controller	- Secondary loopback checking and backup - Redundant ICL Link	Field Devices

HFC-6000 Security Concept

Safety Communication Link (C-Link)	Redundant safety C-Link with dedicated NIC chips and transmission and receiving buffer ring. Protected by gateway device and firewall software.	<ul style="list-style-type: none"> - Proprietary Token Passing protocol - Gateway and firewall protection & isolation - Hardware CRC32 - Broadcast data only (No peer to peer message) - Redundant C-Link timing measurement against replay attack 	Restricted to HFC Safety C-Link
------------------------------------	---	---	---------------------------------

2.1.2 BLOCK DIAGRAMS

The redundant HFC-6000 safety control system shall be designed to meet the following regulatory requirement (the overall requirements and guidance that the HFC-6000 digital platform is designed to meet is presented in the Licensing Topical Report) for safety system and critical mission function control applications:

RG 1.152 Rev. 2 Criteria for use of computer in safety system of nuclear power plants

Regulatory Guide 1.152 defines a set of life cycle phases with cyber security implementation throughout a digital safety I&C system. The life cycle phases begin at the concepts phase and continue through retirement. For HFC, the responsibility is with different people as the software life cycle progresses. However, the Quality Assurance group has the overall lead for all cyber concerns and interfaces with both the design group and the verification and validation group throughout the systems life cycle to ensure that the HFC-6000 software design meets the guidance contain in Section 2 of this Regulatory Guide.

The scope includes component quality, hardware and software qualification, redundancy, fault tolerance, deterministic performance, isolation, and independence. The overall architecture of HFC-6000 control and information systems forms the bases to meet the requirements for nuclear power plant applications.

The primary CPU Module (CPUM) in HFC-6000 controller unit is the system controller (HFC-SBC06), which supports the execution of control logic programs, I/O scan cycles, and safety C-Link communication. All functions shall be handled by dedicated 64/32 bit microprocessors. A redundant configuration of system controllers shall include two HFC-SBC06 controller boards and one HFC-DPM06 dual ported memory board.

Figure 2 illustrates a proposed system arrangement for modules of an HFC-6000 redundant safety system. The Input/Output Modules (IOM) provide the hardware interface to field sensors and controlled field devices and shall be implemented by different types of I/O printed circuit boards. Each I/O module shall have a redundant RS-485 serial interface to the controllers. This interface shall employ a proprietary poll-response inter-communication link (ICL) protocol for communication between the I/O modules and the system controllers. With a redundant controller configuration, each ICL shall be connected with one system controller. The ICL may be implemented with differential pair trace (or cable) for non-isolated communication or with fiber-optics cables for a electrically isolated chassis.

HFC-6000 Security Concept

The Power Supply Module (PSM) represents the redundant rack mounted power supply set. This hot swappable redundant power shall supply 24 vdc for both controllers and I/O modules. The interrogation supply voltage for DI inputs can be either 24vdc or 48vdc.

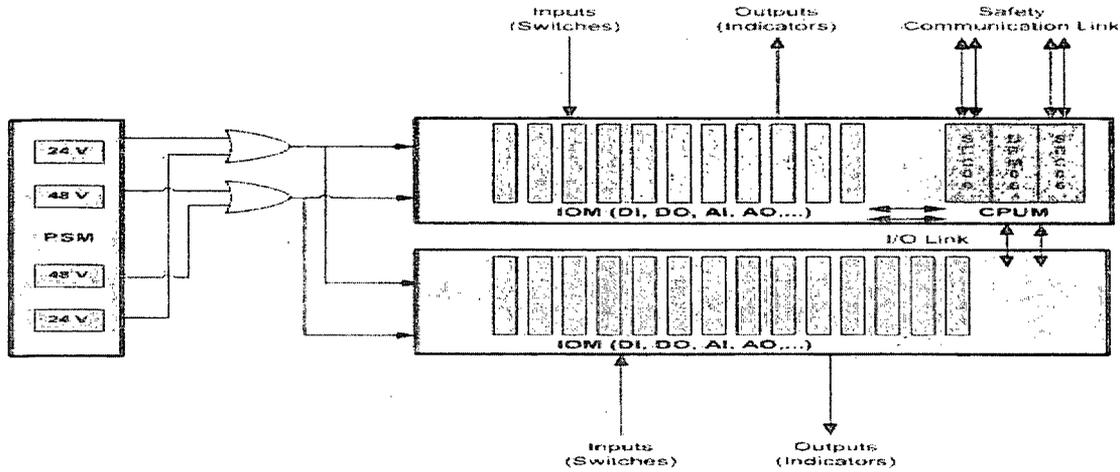


Figure 2 - HFC-6000 System Arrangement Diagram

2.1.2.1 Hardware Block Diagram

The redundant HFC-6000 safety system shall provide plant monitoring and control capabilities. The HFC-SBC06 System Controller (SC) shall be the logic execution module used for implementing plant safety functions. The HFC-SBC06 controller board with its I/O modules shall provide the signal-level interface to the equipment and devices under monitoring or control. Figure 3 shows the proposed interface function for a HFC-SBC06 controller board between its onboard system processor and its subordinate processors.

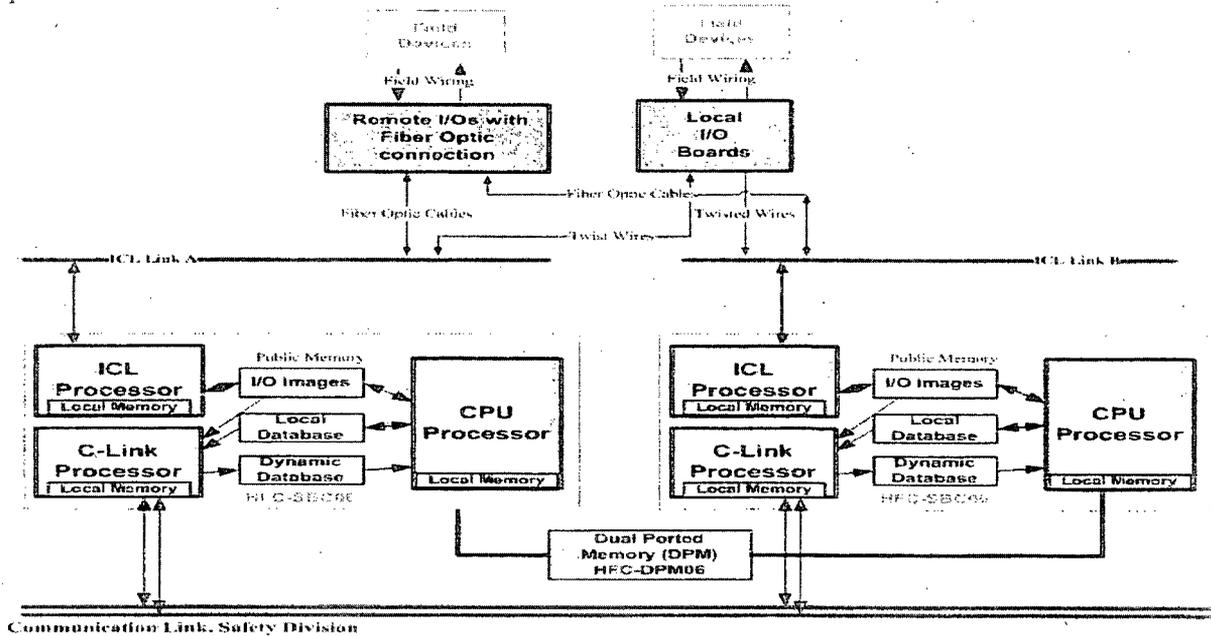


Figure 3 - HFC-SBC06 controller I/O interface

HFC-6000 Security Concept

The principal functions performed by any redundant HFC-6000 controller shall be:

- Redundant controller operation, system diagnostic, failure detection and failover
- Execution of application control programs for the specific safety system
- Communication with I/O modules through the ICL
- Broadcast status data over the redundant safety C-Link

[

]

HFC-6000 Security Concept

The HFC-SBC06 module shall contain three separate microprocessor sections: the SYS microprocessor (SC) section, the ICL microprocessor (SAP) section, and the C-Link microprocessor (SEP is the coded name of the firmware of the safety C-Link processor) section. Each microprocessor section shall be dedicated to a specific set of functional responsibilities, with the SYS processor being the main processor for the whole controller and the communication processors acting as subordinate processors. The SC processor section shall be implemented with an Intel Pentium processor. It shall execute application programs, coordinate operation of the other processor, and monitor the collective status. The SAP processor section shall be based on an Intel 386EX processor. It shall support communication with the I/O modules through the ICL. The SEP processor section shall also be based on an Intel 386EX or later processor. It shall support safety C-Link broadcasting. The SEP processor not requires communication handshaking or accepts any interrupt from a device outside of the HFC-6000 platform.

[

]



Figure 4 - []

[

]

[

]

[

]

2.1.2.2 Power Supply and Power Distribution

The HFC-6000 safety system shall be qualified with a plug-in type rack mounted power supply set that provides 24VDC source. An on-board regulator shall supply the operating voltages to the microprocessor circuitry of the controllers and I/O modules (5VDC in general and 3.3VDC for Pentium microprocessor). An onboard voltage supervisor shall verify that the controller power remains within ± 0.5 VDC and will:

- Halt and restart an out of control microprocessor
- Hold the microprocessor in check during power transients
- Restart microprocessor after power failure and restoration

2.1.2.3 HFC's Communication Gateway Device

[

]

Figure 5 illustrates the network architecture of Safety C-Link, CM-Link and TCP/IP IDH. The Safety C-Link shall be restricted to connect safety controllers within a safety division only.

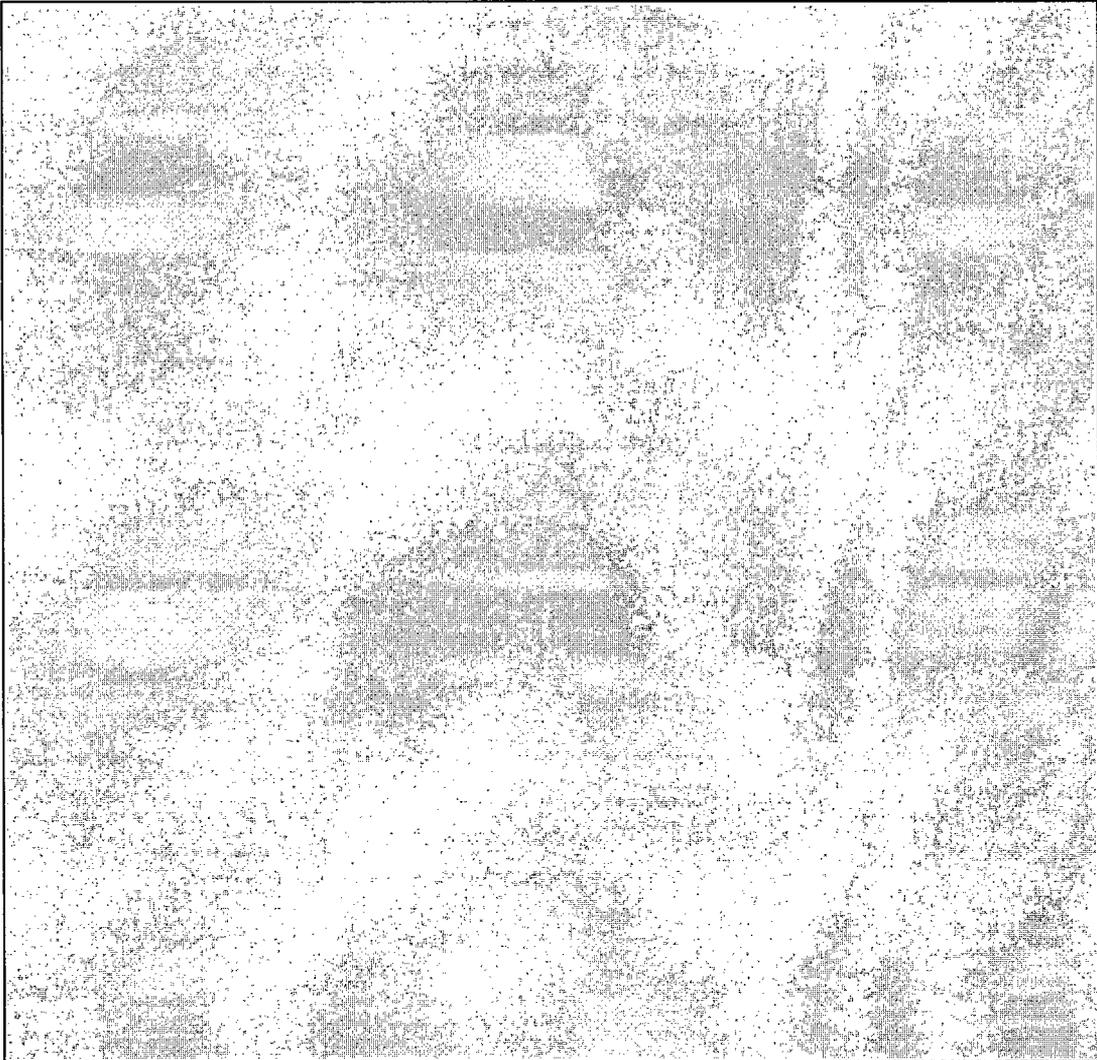


Figure 5 - Safety Communication Link (C-Link) Configuration

2.2 SOFTWARE CONCEPT

2.2.1 OVERALL SOFTWARE STRUCTURE

The redundant HFC-6000 safety system shall consist of system firmware (software) and a project-specified Application Program. The HFC-6000 shall contain the equalization software modules for controller and I/O redundant functions. The following list illustrates the proprietary software of HFC-6000 redundant controller configurations.

[

]

2.2.2 HFC-6000 CONTROLLER REDUNDANCY AND EQUALIZATION SOFTWARE

[

]

2.2.3 ICL COMMUNICATION RELATED REDUNDANCY SOFTWARE

The dual ICL shall provide the path to allow I/O modules to communicate with both the Primary controller and the secondary controller simultaneously.

2.2.3.1 Inter-Communication Link (ICL) Software

The ICL protocol shall be an HFC proprietary design used for general communications between a controller module and its configured I/O modules or interface modules.

[

]

2.2.3.2 Input/Output Module Software

Each of the I/O modules in the HFC-6000 product line includes an onboard microprocessor, with local firmware installed in PROM. The firmware code shall control initialization, diagnostics, ICL communication, I/O scan and data processing functions.

The initialization, diagnostics and ICL communication functions are essentially identical for all I/O module types. The characteristics of the I/O scan and data processing functions shall be uniquely configured for each module type and the program code shall be designed to operate with the specific hardware components that make up that module.

The program algorithm for each I/O module shall automatically access the initialization routine immediately following power-up. This routine shall perform hardware and firmware validation checks and then transfer control to the initialization routine. The initialization routine shall configure the interrupt service routines, RAM partitions, and initializes the ICL interface. After initialization is complete, control shall be passed to the main program. For most of the I/O module types, the main program shall run a single task: the I/O scan routine. This I/O scan routine shall run at regular intervals to read all input channels, write the current image from memory to all output channels, and execute any data processing required for newly received data. Between successive I/O scan cycles, the main program shall run diagnostic checks as a background operation.

All I/O modules shall be configured as slave stations on the ICL. After ICL initialization has been completed, the ICL communication routine shall remain inactive until the first byte of a new message has been received from the controller. At that time, the communication routine shall compare the content of the first message byte with the station address for its present rack and slot position. If the address does not match, the routine shall return control to the main program. If the station address does match, the program shall receive the entire message and validate the message data. If the data is not valid, the routine shall return an error message to the controller and return control to the main program. If the data is valid, the routine shall return the message in the current response buffer, transfers any message data received from the controller to memory, and then return control to the main program.

Each I/O module's software shall be composed of a set of programs that handles hardware and software initialization, I/O scan process, communication with the HFC-6000 controllers, and self-diagnostic tests functions.

The software shall have two types of interrupts: timer interrupt and serial communication interrupt. When an interrupt occurs, the program control shall be transferred to the configured Interrupt Service Routine. After the interrupt has been handled, program control shall be transferred back to the routine that was running when the interrupt occurred.

When a receive interrupt occurs, indicating that a message is received from the ICL, the Receive Interrupt Service Routine shall validate the message and then call a Process Command Routine to process the message and to store any output images contained in the message in the I/O image buffer in RAM. Then a communication routine shall fetch the response message from the Communication Message buffer and transmit it to the HFC-6000 controller via the ICL link.

Timers shall be used to control I/O scan intervals, communication response time out, etc. When a timer interrupt occurs, the configured Timer Interrupt Service Routine handles the interrupt.

2.2.3.3 Redundant Serial Link

Each HFC-6000 controller shall include a hardware interface for one or more ICL channels to provide the hardware link with configured I/O modules. All I/O modules

shall include a redundant ICL interface to permit communication with the redundant controllers. During initialization, one controller shall become Primary, and the other become Secondary. Immediately after completing its internal initialization, the Primary controller shall begin polling its configured I/O modules. After receiving its first message from one of its interfaces, it shall monitor that one as the primary ICL channel for communication with the controller. Throughout subsequent operations, the primary controller shall initiate all exchanges with the configured I/O modules, but the secondary controller shall remain available to support secondary loopback and secondary scanning.

2.2.3.4 Polling Operation

The ICL shall employ a poll-response communication protocol to control message exchanges between the controller and its configured I/O modules. The ICL controller shall initiate scan cycles at regular intervals throughout normal operation. During each scan cycle, the ICL controller shall transmit a poll message to each I/O module in the station address sequence as listed in an I/O configuration table. Each entry in this configuration table shall identify the I/O module address, the type of I/O channels present at that address, the starting point number, and the total number of I/O points present. This information shall enable the ICL controller to construct a message with a structure that is appropriate for the particular I/O to be polled. After transmitting a poll message, the controller shall enable its serial receiver and wait for the response from the station that was polled. If the response is received within a programmed timeout interval, the ICL controller shall process the response and continue the scan cycle with the next station in sequence. If the timeout interval expires, the ICL controller shall log an error for this I/O module and continue the scan operation with the next station address in sequence.

2.2.3.5 Secondary Loopback Test

The ICL protocol supports secondary loopback shall test whether the HFC-6000 controllers operating in a redundant configuration. The purpose of these tests is to verify the functional operation of the secondary link with each station. The Primary controller shall send a secondary loopback request message to one slave station during each scan cycle in a round-robin sequence. After an I/O module receives and validates a secondary loopback request message, it shall transmit that complete message back to the ICL and then enable the receiver on the secondary link. Because every I/O module always transmits over both ICL channels, the Secondary controller shall receive the message over the secondary ICL. If the message has been received without error, the Secondary controller shall transmit an ACK response to the station that transmitted the secondary loopback request. If this ACK message was received within a programmed timeout interval, the I/O module shall transmit a secondary loopback response message that indicates a successful exchange. If any portion of the exchange was unsuccessful, the I/O module shall either return a NACK response or no response to indicate secondary loopback failure.

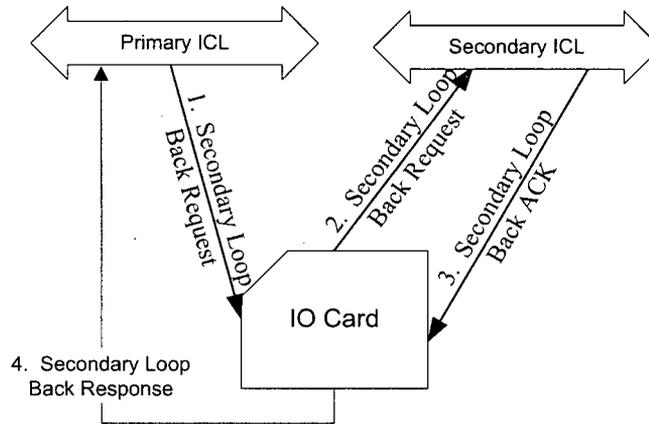


Figure 6 - Secondary Loop Back Test

2.2.3.6 Secondary Polling Function

If an I/O module does not respond to a regular poll message, the Primary controller shall request the Secondary controller to poll the same I/O module. This request is transferred via the Dual Port Memory (DPM) that is shared between the controllers. During this period while the primary channel on the I/O module is not operational, redundancy in the serial link is temporarily lost. The Primary controller shall continue to poll all other I/O modules, but the Secondary controller shall be responsible for polling only the particular module(s) in question. If the I/O module responds to the Secondary controller, that data shall be passed back to the Primary controller via the DPM. An alarm shall be set to indicate the status of the primary I/O link down. This shall continue until the primary link to the I/O module is once again functional.

While operating under the secondary polling procedure, the Secondary controller shall also be responsible for conducting the loopback test for that particular I/O module. If the test determines that the primary ICL is functioning properly, the Primary controller shall resume polling this I/O module in its normal sequence.

2.2.4 COMMUNICATION LINK (SAFETY C-LINK) SOFTWARE

The safety C-Link communication connects all HFC-6000 safety controllers (within the same safety division) together for status exchange. [

]

2.2.5 APPLICATION PROGRAM

The application program for the safety system controller shall consist of an equations file, an I/O configuration list, a Block Request (BLRQ) table, a block list and a block data file. These program components shall consist of the following:

- The equations file contains a sequential list of program statements (Boolean or arithmetic operations) and block calls for analog (called CQ4) algorithms. Each statement in the file either performs a specific operation or calls the software subroutine for a particular analog function (block). These statements constitute the functional algorithm to be executed by the controller.
- The I/O configuration table is a sequential list of each ICL link and each slave station on each link. In a HFC-6000 control system, each ICL processor controls from 2 serial channels that constitute one logical link having a maximum of 64 slave station addresses. The ICL processor uses the data in this table to identify the number of slave devices installed on its link and the type of data associated with each station.
- The BLRQ table determines the specific content of the data that a remote will broadcast to the C-Link, and it controls mapping of data received from the C-Link to specific areas in public memory.
- When an application includes analog data, the block list identifies the specific combination of analog database points (called CQ4 blocks) that are included in the application. The static data for each block is included in the block data file. This static data identifies the type of algorithm to be called and the internal configuration parameters to be used by that algorithm.

The four structures associated with the application program shall be generated using utilities installed on an offline station. After the files have been created, they shall be compiled into a binary format file. The successful compiled object file shall be downloaded into Flash memory (with a write enable switch protection) of the controller module via an offline tester.

HFC Application Programming Tools shall include the complete set of the PC workstation utility software and the One-Step utility programming tool under CAD environment. The PC workstation utility software shall include control programs editors, database editors, and simulator software. The One-Step utility shall be considered to be

HFC-6000 Security Concept

the ideal auto-documentation tool because it provides a single documentation source of the entire application programs.

2.3 DEVELOPMENT CONCEPT

Both system software and application programs shall be developed through HFC internal quality procedures and work instructions in accordance with the requirement of HFC software development quality guidance.

2.3.1 METHODS, TOOLS

2.3.1.1 System Firmware Development Tools

The system firmware for the controllers and I/Os of HFC-6000 safety platform software were written in Intel Assembly language. The Pre-Developed Software (PDS) were developed under Intel x86 Cross Assembler, Linker and Locater on Digital VAX computer and PC environment. HFC uses PC workstation as terminals.

The configuration management of PDS source codes and configuration files were under the VAX Code Management System (CMS) and Module Management System (MMS) control. A dedicated DEC3100 Digital Micro VAX computer was used to edit, compile, and configure the sources and executable codes.

Table 2 illustrates current HFC-6000 software development and maintenance tools. The code management shall be implemented through Version Manager utility and Microsoft SourceSafe utility software.

Table 2 - HFC-6000 software development and maintenance tools

Category	Description	Development Tool	Remark
Firmware for Controllers, I/O modules it includes source codes, linked files and executable codes	Files Editing	Microsoft Visual Studio	The code management software shall control the revisions of each software module and provide the version of downloadable HEX files for each processor.
	Assembler	Intel x86 Cross Assembler	
	Linker/Locater	Intel x86 Linker and Locater	
	Compiler/Linker	Intel ASM86 Intel LINK86	
	Configuration Management	Version control with Microsoft SourceSafe and Version Manager	

Only the assigned development managers or engineers shall be eligible to access the software files directories, documents directories and software development utilities. The development tools shall be protected by logged name and password control.

2.3.1.2 Application Programs Development Tools

The plant control application program is created or modified from an offline PC station which connects to a tester in accordance with pre-established software development

HFC-6000 Security Concept

processes. The new or modified software will be downloaded into the controller via tester.

HFC Application Programming Tools shall be used to generate application logic. HFC's proprietary "One-Step" utility under CAD environment is a logic programming and drawing making tool. The tool shall include embedded CAD drawing making Promise utility and HFC's proprietary macro assembler. The One-Step utility shall provide a single documentation source of the entire application programs. As the result of this programming tool, it shall generate executable application object code for controller, master database of configured system, and operator interface graphics.

Table 3 - HFC-6000 Application development and maintenance tools

Category	Description	Development Tool	Remark
Application drawings, database files and executable codes	Files Editing	PromisE with CAD environment	The single source (i.e. drawing) application codes shall be controlled by drawing number with revision.
	Compiling	HFC's proprietary One-Step Utility software	
	Configuration Management	Hard copies in Document Control	

Only the assigned project managers or engineers shall be eligible to access the application files directories, documents directories and development utilities. The development tools shall be protected by logged name and password control.

2.3.2 QUALITY ASSURANCE

The HFC QA Program covers the design, implementation and commissioning of the HFC-6000 safety control system. Requirements of this program shall apply to all activities (systematic and planned actions) affecting the quality of products and services provided and performed by HFC. All of essential prerequisites for an effective quality assurance program shall be incorporated into the QA program. These are:

- Clear delineations of authority and responsibility
- Employment of proven methods of management and work
- Good working conditions
- Personnel sense of responsibility and familiarity with duties they perform
- Procedures in place to assure systematic reporting of quality related issues
- Additional measures taken to assure the maintenance of records

The QA Program shall include procedures for managing the multidisciplinary interfaces within the HFC design effort and clearly delineates the responsibilities for quality functions in the respective organizations. To assure that the documentation reflects current design, the QA Program shall include procedures and methods that ensure the correctness and completeness of the documentation at the end of each phase of the HFC-6000 development project. The ultimate objective is to eliminate all design errors as early as possible and ensure that the design basis, safety, operational and maintenance requirements were properly considered. This ensured that the resulting HFC-6000 safety

HFC-6000 Security Concept

control system meets the highest standards of technical quality while eliminating the time-consuming “redo’s” that might otherwise plague the design effort.

To assure that the QA Program was being rigorously adhered to the Programs mandated an independent verification effort to assess compliance with the QA Program and to provide on-going assessment of the adequacy of the measures is undertaken to ensure technical correctness of the QA processes.

The Director of Quality has the responsibility for establishing the Quality Assurance Program and verifying that activities affecting the quality of deliverables are performed in accordance with this program. The performance of the group, that the manager represents, shall be assessed independent from the costs and schedule impacts of the group’s mandated quality assurance measures. By reporting directly to the President of HFC, the Quality Director shall be afforded sufficient authority and organizational freedom to identify quality problems; to initiate, recommend, or provide solutions to quality problems; and to verify implementation of solutions to quality problems. Per the HFC QA Program, all employees share the same responsibility and authority as the Quality Director to identify quality problems; to initiate and provide solutions to quality problems; to verify implementation; and to resolve deficiencies that affect quality.

At a minimum, a formal management review of the quality system shall be performed annually, to ensure its continuing appropriateness and effectiveness in satisfying HFC’s business policies and objectives. Records of the management review meeting and associated completed action items shall be maintained in accordance with documented procedures.

HFC has established and maintains documented procedures to ensure that applicable regulations, codes, standards, and customer requirements are translated into design documents, procedures, and/or instructions. These documents shall include provisions to assure that appropriate quality standards are specified and included in design documents and that deviations from defined requirements are controlled.

As noted earlier, organizational and technical interfaces between different design group disciplines shall be defined by the Project Quality Plan. All design information communicated between the respective disciplines necessary to ensure satisfaction of these interface requirements shall be documented and regularly reviewed.

The design control program shall be established and implemented to assure that the activities associated with the design of systems, components, structures, and equipment and modifications thereto, are executed in a planned, controlled, and orderly manner. The program shall include provisions to control design inputs, processes, outputs, changes, interfaces, records, and organizational interfaces. Major elements of this program shall include the following measures:

- Design input requirements, relating to the HFC products, are established, documented and their selection reviewed and approved for adequacy.
- Design outputs are documented and expressed in terms that can be verified against design input requirements and validated.
- Individuals or groups other than those that performed the original design review and design output documents.

HFC-6000 Security Concept

- Independent design reviews occur at prescribed stages within the design process. Participants at each design review include, when necessary, representatives of all functions concerned with the design stage being reviewed.
- Records of design reviews are maintained.

Design verification shall include design reviews, alternate calculations, qualification tests or a combination of methods executed in accordance with approved procedures. Design verifications shall be performed in accordance with approved procedures, performed prior to release for procurement, manufacturing, or to another organization for use to ensure that the design output meets the design input requirements. Independent design validations shall ensure that developed products conform to the specified requirements.

Design Analysis shall be performed in a planned, controlled and documented manner. They shall be sufficiently detailed as to purpose, method, assumptions, design input, references and units. Methods such as computer programs and calculations are described and controlled. Qualification testing shall demonstrate adequacy of performance under conditions that simulate the most adverse design conditions.

Design changes shall be subjected to design control measures identical to those applied to the original design. Design documents, including revisions, are reviewed, approved, released, distributed, and controlled in accordance with prescribed procedures and/or instructions. The HFC Software Configuration Management Program shall provide a method to track all past, current and future software configurations.

2.3.3 DOCUMENTATION CONTROL

[

]

2.4 DEFINITION OF FAULTS TO BE CONSIDERED

The HFC-6000 redundant safety system shall be designed and structured to perform safety and protection functions for the process of safety functions. The architecture shall be based on the redundant configuration of the controllers, I/O modules, power supply and all communication links. The design objective of this architecture shall prevent any single point of failure from disabling the function of the redundant configuration. In order to assure that this design objective is actually realized in any particular configured application, the possibility of postulated failures should be assessed. Any failure that defeats the safety performance shall be considered as fatal. The following list illustrates the considered critical faults for this system.

- Loss of redundant controller safety system (fatal fault)
 - The detected failure of both sets of controllers
 - The detected failure of critical input signals

HFC-6000 Security Concept

- The detected failure of critical output signals
- The detected communication failure of redundant links

- Loss of one controller (non-fatal fault)
 - The detected failure of one set of redundant controllers
 - The detected failure of non-critical input signals
 - The detected failure of non-critical output signals
 - The detected failure of one channel of redundant links

- Loss of partial function of controller (non-fatal fault)
 - The detected failure of hardware components of one controller
 - The detected errors of C-link communication
 - The detected errors of ICL link communication

2.5 MEASURES FOR DETECTION OF THESE FAULTS

The system fault detection shall be performed through online diagnostic software periodically throughout the process. The measured criteria are determined by either good/failure status or as cumulated error counts.

2.5.1 ONLINE DIAGNOSTIC

[

]

2.5.2 THE QUALITY OF DATABASE

[

]

2.5.3 REMOTE STATUS BROADCAST

[

]

2.5.4 DYNAMIC DATABASE (DDB) BROADCAST

[

]

2.5.5 COMMUNICATION STATUS

[

]

2.5.6 SUMMARY OF SYSTEM FAULT MEASUREMENT

All listed methods of fault measurement shall be built into HFC redundant safety system. As a summary, Table 4 illustrates the measures of different faults detections.

Table 4 - HFC-6000 redundant safety system faults detection

Fault	Description	Category
Fatal	Loss of redundant safety system	1. Loss of entire redundant control C-link 2. Loss of redundant controllers 3. Loss of particular critical output signals 4. Loss of particular critical input signal (For the case 3&4, the redundant I/O is required)
Non-Fatal	Loss of one controller	1. Loss of communication of one controller <ul style="list-style-type: none"> - Hardware and application failures detected by online diagnostic software - Communication failure on remote status and/or DDB 2. Loss of one of redundant controller <ul style="list-style-type: none"> - Hardware and application failures

HFC-6000 Security Concept

		<p>detected by online diagnostic software</p> <ul style="list-style-type: none"> - Failure to receive Remote Status data - Failure to receive DDB data <p>3. Loss of non-critical output signals</p> <ul style="list-style-type: none"> - Failure detected by application logic through quality words of database - Failure detected through ICL communication <p>4. Loss of non-critical input signal</p> <ul style="list-style-type: none"> - Failure detected through quality words of database - Failure detected through ICL communication
	Loss of partial function of one controller	<p>1. Failure of part of Peripheral, communication or I/O circuitry</p> <p>2. Error count of C-link communication</p> <p>3. Error count of ICL link communication</p>

2.6 REACTION IN CASE OF FAULTS

For fatal fault to loss a controller, the trouble shooting process with a hardware reset shall be required to bring controller back. For a non-fatal fault detected during operation, redundant safety system shall continue to operate normally after the loss of one controller or some components of one controller. An alarm shall be activated and transmitted to alarm reporting devices over the information data highway

2.7 LIST OF THE TESTS RUN AFTER POWER-UP OR RESET

During the power up initialization process, the software of each processor in an HFC-6000 Safety System shall check the following hardware components and their functions.

- Microprocessor Hardware Initialization Test
 - CPU processor
 - SAP processor
 - SEP processor
- Memory Test performed by CPU processor
 - Validate PROM and FLASH by reading the signature.
 - Validate RAM addressing for private, public and Dual Ported Memory
 - Validate RAM data recall and persistence.
 - Memory speed test.
- Hardware Diagnostic Report

All processors updated their own diagnostic status array, and the system processor validated the status of all configured microprocessors through access to the dedicated diagnostic memory area for each processor.
- Software test

The system processor validates the firmware and application code between PROM and Flash.
- System Go

At the completion of successful system initialization, the system processor shall synchronize the control process of all processors by issuing the system-wide "GO" flag.

2.8 TESTS RUN DURING OPERATION

2.8.1 MAILBOXES TEST

After the completion of power up initialization, all microprocessors shall report their operating status to the System Processor continuously by updating the dedicated "mailbox". A mailbox is a dedicated memory for each processor to communicate its status with system processor interactively. Each processor shall load a preset value into its mailbox area at the rate of every 100 MS. The system processor shall be responsible to monitor these mailboxes in order to determine the operating status of the entire controller. Upon the failure of any microprocessor, the hardware watchdog timer shall halt and the controller shall stop the function.

2.8.2 ICL COMMUNICATION LINK TEST

The ICL protocol software shall record communication status with all configured I/O modules in the ICL communication status array. An ICL link diagnostic function shall provide the path to validate all I/O communication related hardware components. The failure of any hardware shall be reported as I/O loopback error alarm or I/O card alarm.

The communication over C-Link with token passing protocol shall provide on-line diagnostic information for all C-Link related hardware that shall include C-Link Processor, NIC chips and its transmission/receiving buffer circuitry. The failure of any hardware component shall result in a safety C-Link channel error, Communication error, or remote down alarm.

2.8.3 MAINTENANCE FAILOVER TEST

The maintenance failover software shall provide the operational indicator of a HFC-6000 second controller. If the secondary controller is operating properly, the maintenance failover switch shall be enabled to switch the function of the primary controller and secondary controller.