HF Controls

SOFTWARE SECURITY

WORK INSTRUCTION-ENGINEERING DEPARTMENT

Work Instruction No: **WI-ENG-020** Revision: **B**

Effective Date: **9/22/2009**

Prepared By: Jonathan Taylor

Reviewed By: Ivan Chow

Approved By: Charles McKinney

Software Security

Revision History

Date	Revision	Author	Description
8/18/09	A	I. Chow	Revised to current practice
8/20/09	A1	I Chow	Revised Merchant Tracker to Merant Tracker
9/22/09	B	J Taylor	Scope modified to cover software security requirements of USNRC RG 1.152

Table of Contents

Section **Description** **Page**

1.0 PURPOSE AND SCOPE

1.1 The purpose of this work instruction is to define the processes used to protect HFC software products from unauthorized access, corruption, or cyber attack. The scope of coverage includes three different aspects:

- Measures for software security during program development.
- Measures provided to prevent program corruption in customer systems during online operation.
- Measure to prevent corruption of standard HFC software products during product maintenance/enhancement.

2.0 ORGANIZATIONAL RESPONSIBILITIES

2.1 The Director of Engineering has the responsibility for ensuring that HFC software products remain protected from corruption or contamination with undocumented code or any malware. The primary mechanism for achieving this is by controlling user access rights to the software development tools and to the software libraries.

2.2 The Director of Engineering is responsible for ensuring that the anti virus software installed on all HFC servers and workstation PCs is kept up to date and that virus scans are executed on a regular basis.

2.3 The Software Engineering Manager has the responsibility for controlling object code created or purchased by HFC. The scope of this authority includes PC-based programs, and system code installed in PROM or flash memories.

2.4 The Hardware Engineering Manager has the responsibility for controlling source code for CPLD/FPGA programs.

2.5 The Project Engineering Manager has the responsibility for controlling logic diagrams and application program code.

2.6 The HFC LAN administrator is responsible for ensuring that the HFC LAN servers and all PCs on the HFC LAN remain free of malware.

3.0 REFERENCES

3.1 QPP3.1, "Design Control"
3.2 WI-ENG-001, "Design Verification & Review"
3.3 WI-ENG-003, "Configuration Management"
3.4 WI-ENG-206, "CMS Library – Software Source Code"
3.5 WI-ENG-207, "CPLD – Source Code Control and Rebuilding"
3.6 WI-ENG-209, "System Controller Firmware"
3.7 WI-ENG-213, "Saving Backup Data"
3.8 WI-ENG-704, "Engineering Catalog Part Number entry and Update"
3.9 WI-ENG-708, "Application Software Archiving"
3.10 WI-ENG-806, "Design Control Logic Procedure"
3.11 WI-ENG-811, "Backup Drawing and Documents"

3.12 USNRC Regulatory Guide 1.152 Revision 2, January 2006

4.0 GENERAL INFORMATION

4.1 DEFINITIONS

Malware – A collective term for all types of computer program designed to infiltrate a computer without the owner's consent.

Risk – The combination of the probability of occurrence of an undesirable event and the consequences that might be produced by that event.

Security. (A) The protection of computer hardware or software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations. (B) The protection of information and data so that unauthorized persons or systems cannot read or modify them and authorized persons are not denied access to them.

System Configuration Management (SCM) - The process of identifying and controlling the components of a computer system throughout the project life cycle. This includes release and change, recording and reporting of status, and verifying completeness and correctness of items such as V & V plans, drawings, code, manuals, design documentation, etc.

Virus – A computer program that is capable of copying itself and infecting a computer without the owner's consent.

4.2 ACRONYMS

BOM	Bill of Materials
CM	Configuration Management
COTS	Commercial off-the-Shelf Software
CPLD	Complex Programmable Logic Device
FPGA	Field Programmable Gate Array
LAN	Local Area Network
PCB	Printed Circuit Board
PDS	Previously Designed Software

5.0 PROCEDURE

5.1 DEVELOPMENT TOOLS

5.1.1 Hardware

The table lists the tools HFC uses to support development of hardware designs for PCB assemblies and control system components.

AutoCAD 2006	To generate detailed drawing; HFC hardware design engineers use it to generate detailed drawings for any newly developed PCB.
CAM350	To convert Gerber file to DXF format file
Power Logic 5.0.1	To generate schematic drawings.
Merant Tracker 8.0.3.0	For Change Request Control
Serena Version Manager 8.1.3	Configuration management tool for BOMs and AutoCAD graphic files.
Macola 7.6.4	For generating BOM

HFC uses Version Manager to control V&V records, drawings, documents, and source code for individual projects. HFC uses Tracker to control the change process.

5.1.2 Software/Firmware

The following table lists tools HFC uses to support creation/maintenance of system-level program code and PC application programs.

Microsoft SourceSafe 6.0 Microsoft Visual Studio 6.0	For firmware development
Serena Version Manager 8.0	Configuration management tool for logic diagrams, source code files, and project-related documentation.

Refer to the following Work Instructions for details of specific use:

- WI-ENG-206, “CMS Library – software source Code
- WI-ENG-207, “CPLD – Source Code Control and Rebuilding”
- WI-ENG-209, “System Controller Firmware”
- WI-ENG-213, “Saving Backup Data”

5.1.3 Application Program Code

The following table lists the tools HFC uses during development of application program code.

Software Security

AutoCAD 2006	HFC application engineers use AutoCAD to generate loop schematic drawings and system assembling drawings.
Promis*e - AutoCAD version 5.06	Promis*e is the drawing configuration tool to generate linkages between symbols. The extracted information can be used as system configuration for database, IO, and even programming data.
One-Step	HFC proprietary software tool used for generating application program code.

Refer to the following Work Instructions for details of specific use:

- WI-ENG-704, "Engineering Catalog Part Number entry and Update"
- WI-ENG-708, "Application Software Archiving"
- WI-ENG-806, "Design Control Logic Procedure"
- WI-ENG-811, "Backup Drawing and Documents"

5.2 SOFTWARE/FIRMWARE DEVELOPMENT ENVIROMENT

5.2.1 [

]

5.2.2 [

]

5.2.3 The Director of Engineering shall authorize eligible users for PVCS Version Manager.

- [

  ]
- [

  ]
- [

  ]

5.2.4 All software development work is conducted on line via the HFC LAN.

- Each project will have its own project directory. (Refer to WI-ENG-206 and WI-ENG-209.)
- A software engineer assigned to a particular task or project shall check out the software modules to be modified and check them in again when preliminary testing is complete. Software modules shall not remain checked out longer than necessary to accomplish the changes.

- Source code files associated with projects and/or released software shall not be kept in personal directories.
- The LAN administrator is responsible for ensuring that the LAN server and all work computers remain free from infection by malware.

5.3 SOFTWARE SECURITY DURING DEVELOPMENT

HFC develops and maintains the following types of software components:

- System software for microprocessor-based control systems.
- CPLD/FPGA firmware for PCB assemblies
- Software tools for internal used to support product development
- Windows application programs for workstation PCs
- Application programs for industrial control systems.

HFC has developed processes and safeguards to protect both system software and application programs from cyber threats. The scope of these processes include provisions for each lifecycle phase of the software components.

5.3.1 Concept Phase

5.3.1.1 During development of a new design for an existing product line or creation of a completely new product line system developers shall consider the following:

- [   ]
- [   ]

5.3.1.2 [

]

5.3.2 Requirements Phase

5.3.2.1 Security requirements shall be considered along with the functional requirements for the new program code. Security requirements shall be subject to the same level of V&V evaluation as all other functional requirements.

5.3.2.2 If PDS or COTS will be included in the new design, potential vulternabilities of this software shall be explicitly considered and evaluated.

5.3.3 Design Phase

5.3.3.1 Security requirements shall be translated into specific design configuration items. These items should include:

- [ ]
- [ ]
- [ ]

5.3.3.2 [ ]

5.3.4 Implementation Phase

5.3.4.1 Implementation encompasses development of hardware, coding of software, integration and testing. As a minimum:

- [ ]
- [ ]
- [ ]
- [ ]

5.3.4.2 The finally accepted version of object code shall be released for production.

- [ ]
- [ ]
- [ ]
- [ ]

5.3.5 Testing Phase

5.3.5.1 For an integrated control system, each security design feature shall be validated by one or more specific test cases.

Software Security

5.3.5.2 For a new/modified HFC product, the function and effectiveness of security elements shall be verified and evaluated as part of final testing.

5.3.6 Installation/Checkout Phase

5.3.6.1 This phase applies only to a complete system.

- All safety features shall be specifically tested and verified.
- All communication interfaces between this system and external equipment shall be tested/examined for potential security vulnerability.

5.3.7 Operation/Maintenance Phase

5.3.7.1 Following final customer acceptance of a complete system the customer takes over responsibility for operation and maintenance of that system. HFC remains responsible for 10 CFR Part 21 reporting and for warranty issues.

5.3.7.2 The maintenance phase applies to all HFC standard products.

- All hardware and software products remain under configuration management following initial development.
- Only qualified software engineers shall have access to or make changes to source code files. All such changes shal be authorized in advance and validated by review before being checked back into the standard libraries.

6.0 QA RECORDS

None

7.0 ATTACHMENTS

None