HF Controls

Reliability and Availability Report of the Fast Performance Controller of HFC-6000 Safety Platform

RR901-003-04

Rev. B

Effective Date 8/30/2012

Prepared By: Yang Lu

Reviewed By: Terry Roberts

Approved By: Ivan Chow

[ ]

Revision History

Date	Revision	Author	Changes
08/27/2012	A	Y. Lu	Initial Revision
08/30/2012	B	Y. Lu	Revised per comments

TABLE OF CONTENTS

List of Tables

List of Figures

1.0 PURPOSE AND SCOPE

This document provides reliability and availability analysis report for the Enhanced Equipment of the HFC-6000 Safety Platform. The overall analysis is based on methods described in IEEE Std 352 and in IEC 61508-6. Failure rate calculations are based on mathematical models developed in MIL-HDBK-217F. Utilities of the Relex® software were used to perform the actual failure rate calculations for each assembly.

This document contains the results of a reliability analysis covering all functional components of the HFC-FPC08 controllers and additional equipment of HFC-6000 Safety Platform and an availability analysis based on those calculations. The reliability analysis calculated separate failure rate parameters based on reliability models, failure rate data for individual components, assembly design characteristics, and assumed environmental conditions. The resulting failure rate parameters can be used for calculating the expected availability data for a safety system utilizing these additional equipment and HFC-FPC08 as the controllers.

2.0 REFERENCES

EPRI TR-107330	Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants, 1996
IEC 61508-6	Functional Safety of Electronic/Electrical/Programmable Electronic Safety-Related systems
IEEE Std 352	IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems, 1987
MIL-HDBK-217F	Reliability Prediction of Electronic Equipment
Relex®	Visual Reliability Software Reference Manual
RR901-003-03	FMEA Report for the Enhanced Equipment of HFC-6000 Safety Platform

3.0 SPECIAL TERMS AND ABBREVIATIONS

AI	Analog Input
AO	Analog Output
β	Correction parameter for common cause failures
CPLD	Complex Programmable Logic Device
DC	Diagnostic Coverage
DI	Digital Input
DO	Digital Output
ESFAS	Engineered Safety Function Actuation System
FMEA	Failure Modes and Effects Analysis
HFC	HF Controls Corporation
IC	Integrated Circuit
I/O	Input/Output
λ	Failure Rate (failures/10^6 hours)
λ_U	Unsafe Failure Rate
λ_S	Safe Failure rate
λ_{DU}	Undetected Dangerous Failure Rate
λ_{DD}	Detected Dangerous Failure Rate
λ_{SU}	Undetected Safe Failure Rate
λ_{SD}	Detected Safe Failure Rate
MFT	Master Fuel Trip
MMI	Man-Machine Interface
MTBF	Mean Time Between Failures
MTTR	Mean Time to Repair
PC	Personal Computer
PFD	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PSH	Probability of Success per Hour
R	Reliability
RSP	Remote Shutdown Panel
1oo2	One-out-of-two

4.0 OVERVIEW OF ANALYSIS

The Relex® software was used to calculate failure rates for each functional module as a stand-alone component based on estimated power loads and assumed environmental conditions.

4.1 ANALYSIS DESCRIPTION

4.1.1 Approach

HFC-6000 Safety Platform can be configured to provide plant monitoring and control systems distributed over more than 400 separate controllers. These systems can be composed of individual controller modules, I/O modules, communication modules, power supply modules, and man-machine interfaces (MMI). Since there can be any number of configurations for a control loop or a control remote using a combination of the components of the HFC-6000 safety platform, the sample system configuration required by 4.2.3.2 in EPRI TR-107330 is used to perform the availability analysis for a sample control loop.

Both EPRI TR-107330 and IEEE Standard 352 have been extensively used as guidelines in performing this reliability analysis. EPRI TR-107330 was written to specify generic requirements for qualifying PLCs for safety related applications in nuclear plants. IEEE Standard 352 provides guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems. In addition, IEC 61508-6 provides specific methods and examples for performing reliability calculations on complex control system equipment.

Military specification MIL-HDBK-217F was used as the basis for the mathematical models used to predict the failure rate data. A software tool, Relex®, was used to perform most of the initial calculations. The Relex® software is one of the leading software tools for reliability and maintainability analysis. It provides software solutions for reliability predictions and MTBF calculations.

For the availability of redundant modules configured using HFC-6000 safety platform, that calculation was based on the guidelines described in IEEE Standard 352 and in IEC 61508-6.

4.1.2 Assumptions

The Relex® software was configured to calculate reliability for functional modules used to make up the typical Class 1E safety system based on reliability models defined in MIL-HDBK-217F The following paragraphs provide a detailed summary of the assumptions and parameters used to configure the system model for the failure rate calculations.

4.1.3 Environmental Assumptions

a.	Location	On ground, fixed
b.	Operating Life	40 years
c.	Temperature	25° C (77° F) for Class 1E;
d.	Relative Humidity	7% – 95% (Non-condensing)
e.	Pressure	0 psig (ambient)
f.	Radiation	1.0 Gy Total Integrated Dose

These parameters correspond to those for the Ground, Fixed environment in MIL-HDBK-217F.

4.1.4 System-Level Assumptions

A sample Clas1E safety system used for the calculation is composed of different channels communicating through HFC-6000 Gateway Controller on safety C-Link. See Figure 1.

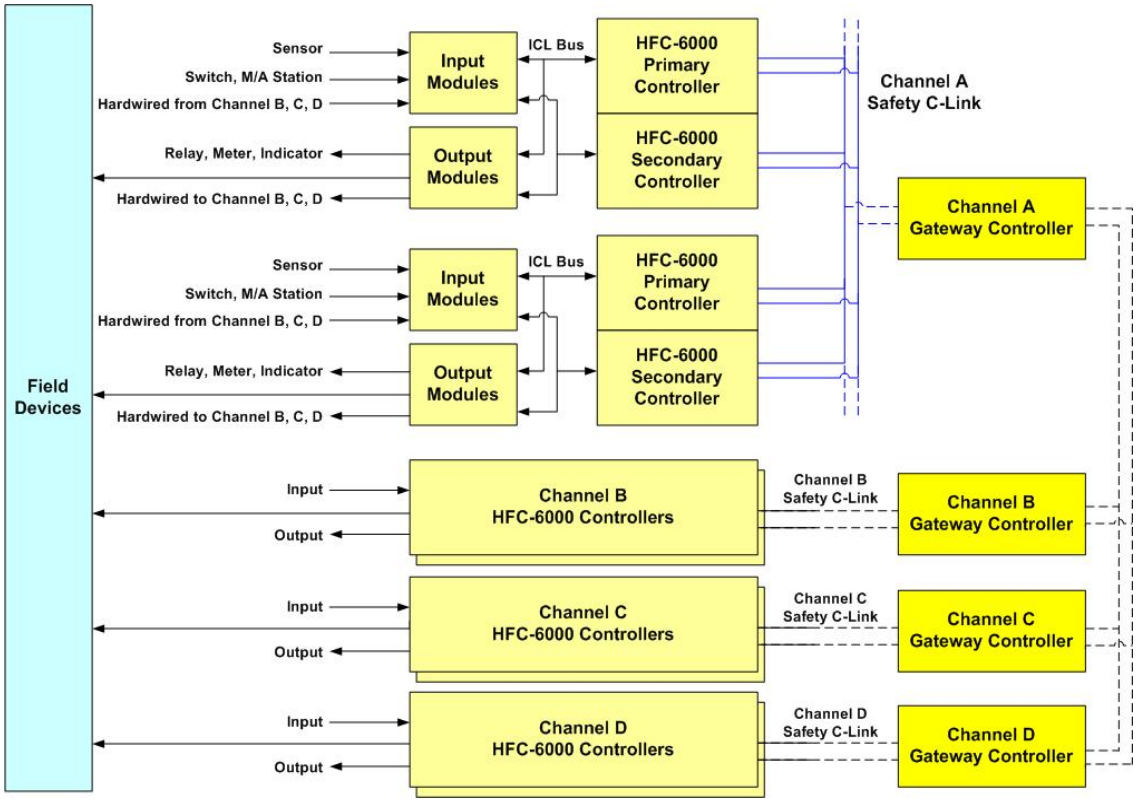

Figure 1 – Safety Class 1E Safety System General Arrangement

The sample safety system is assumed to remain in continuous operation between successive outages and that the temperature in the equipment room would remain at 77º F under normal conditions.

In addition, the following assumptions have been employed throughout this reliability analysis:

- Field repair of the assemblies is limited to removal and replacement of socket or clip-mounted components. Such components may include fuses, certain ICs, and relays. Soldered components will not be removed and replaced in the field.
- Modular items such as network hubs, relays, meters and M/A stations etc. will be replaced as a unit and not repaired in the field. All of the programmable modules are assumed to have the current revision of their software installed.
- All spare modules requiring calibration or alignment are assumed to have been properly calibrated by the manufacturer prior to delivery to site. Consequently, such components will not require calibration following installation in the safety system.
- Sufficient spares will be maintained on site to provide immediate access to critical

replacement modules. Repairs may be accomplished on any single bay without disrupting normal system operation.

- None of the spares will require mechanical alignment following installation. Proper installation of jumper straps and adjustment of configuration switches are assumed as part of the normal process for installation of replacement assemblies.
- The MTTR of 4 hours during normal system operation will be assumed for a safety system.
- Diagnostic coverage is assumed to be greater than 75% as a whole.
- The surveillance interval is the time period between executions of successive proof tests. During this interval, a typical safety system is assumed to be operating online continuously. System availability will be calculated for surveillance intervals of 6, 12, 18, 24, and 30 months.

4.2 HARDWARE MODULES

4.2.1 HFC-FPC08 Controller Modules

Table 1 provides a list of HFC-FPC08 Controller Modules and additional equipment.

Table 1 – HFC-FPC08 Controller Modules and Additional Equipment

Part Number	Module Name	Summary Description
40103827Q	HFC-FPC08 (C-Link)	HFC-6000 Fast Performance Redundant Controller
40103823Q	HFC-FPC08 (MTP)	HFC-6000 Fast Performance MTP Controller
40103824Q	HFC-FPC08 (SDL)	HFC-6000 Fast Performance Serial Data Link Controller
40108621Q	HFC-HSIM	HFC-6000 High Speed Interface Module
70085301Q	HFC-ILR06T	HFC-6000 Fiber-Optic Transmitter/ Digital Input
40031281Q	AFS-CSM-01	AFS-1000 Control Switch Module
40040222Q	HFC-ILR06R	HFC-6000 Fiber-Optic Receiver/ Digital Output
70050001	Control Module Type 1 (HS-121A)	HFC-6000 AFS-CSM-01 Control Module Type 1
70050101	Control Module Type 2 (HS-043A)	HFC-6000 AFS-CSM-01 Control Module Type 2
70050401	Control Module Type 3 (HS-138)	HFC-6000 AFS-CSM-01 Control Module Type 3
70051101	Control Module Type 4 (HS-035)	HFC-6000 AFS-CSM-01 Control Module Type 4
70052305	Control Module Type 6	HFC-6000 AFS-CSM-01 Control Module Type 6

4.2.2 Field Terminations

The HFC-6000 Safety Platform supports a set of termination board assemblies. Each of these assemblies includes the specific terminal hardware needed to interface with a particular type of field signal. These modules may also include relays, fuses, configuration switches/jumpers associated with the field interface. The TB modules can be installed in the rear bays directly behind the bay that contains the corresponding functional I/O module. As a result, the cabling between the TB module and its functional module remains completely enclosed within a cabinet assembly.

4.2.3 System Surveillance

RR901-003-03 contains a detailed FMEA for the enhanced equipment. This analysis evaluated the effects of various failure conditions on system performance and assessed available mechanisms for failure detection. In general, two methods are available for detecting an equipment failure before it adversely affects the capability of a typical plant control system to perform its safety functions.

4.3 SYSTEM DIAGNOSTICS CAPABILITIES

The HFC-FPC08 controllers support the following diagnostic capabilities:

- Comprehensive power-up diagnostic and validation tests
- Run-time hardware watchdog functions (all modules)
- Run-time software watchdog functions (controller modules only)
- Run-time detection of input channel failures (all input modules)
- Run-time detection of data corruption (all modules)
- Run-time detection of power faults (all modules)

All failures detected by diagnostic utilities are indicated locally by LEDs on the equipment affected. In addition, the main processor maintains a detailed log of system status that is available for display on the operator workstation and can be accessed to facilitate troubleshooting and fault isolation.

4.3.1 Diagnostic Coverage

The diagnostic coverage parameter for a system is defined as the ratio of the number of failure states detected by the diagnostics to the total number of possible failure states. The Relex® software was used to calculate failure rates for the various assemblies that make up a safety system based on standard mathematical modules, and the results of these calculations are summarized in section 7.0. The percentage of failure states detected by diagnostics within any complex system is more difficult to assess. A standard statistical analysis of system performance divides the calculated failure rate into safe and hazardous failure conditions. When a system includes diagnostic algorithms, these failure rates are further divided between those detected by the diagnostics and those that are not detected until the system enters a failure state. This provides the mathematical basis for calculating the diagnostic coverage parameter.

4.3.2 Failsafe Capability and Safe Fail Fraction

The fundamental concept behind 'failsafe' is that when some portion of a system is no longer capable of performing its safety function, it enters a state that does not degrade performance of the remaining system components. Failure modes for any one controller are naturally categorized into I/O module failures and controller failures. The following failsafe transitions are built into the HFC-FPC08 controllers:

Controller [

]

Power Fault [

]

A diagnostic coverage level of 75% has been assumed for a safety system composed with the enhanced equipment. This implies that 75% of all failure states will be detected and alarmed by the system. It is assumed that all detected failures result in a failsafe state for the portion of the system affected.

5.0 COMPONENT FAILURE RATE AND AVAILABILITY PARAMETERS

5.1 FAILURE RATES

Every functional component has a finite probability of failure throughout its operating life. The failure probability for any integrated system then becomes a composite of the failure probabilities of its components. A 'bathtub-shaped' failure rate model (Figure 2) is considered to be applicable to many types of device and many systems. This model assumes a relatively large early-life failure rate that diminishes to a relatively low constant value during normal operation and then increases as the component or system ages.

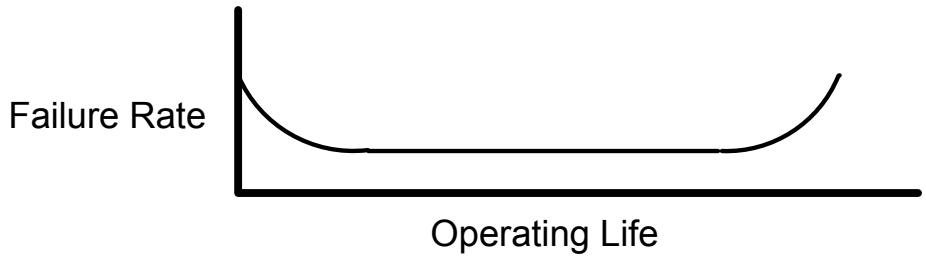

Figure 2 – Bathtub Failure Rate Model

The major aging factors for electronic components are heat generation, humidity, and vibration. MIL-HDBK-217F assumes that the failure probability function for most components can be represented by an exponential function of time, and it provides different algorithms for calculating failure rates for different types of devices. The Relex® software uses the mathematical models defined by MIL-HDBK-217F as the basis for its failure rate calculations. The overall aging analysis consisted of importing the parts list for a particular assembly into the Relex® database and then entering parameters for component category and subcategory, thermal resistance, power load, etc. Once all parameters for a particular assembly have been entered, the Relex® software will perform the detailed calculations. These results are contained in section 7.0. Table 2 lists a summary of the failure rate and MTBF values for the enhanced equipment.

Table 2 – Failure Rate Summary of Enhanced Equipment Components

Equipment	Unit λ	MTBF (hours)
HFC-FPC08	10.695714	93,495
HFC-HSIM	1.772363	564,219
HFC-ILR06R	0.447278	2,235,745
HFC-ILR06T	0.214828	4,654,889
AFS-CSM-01	0.521515	1,917,491

5.2 PROBABILITY OF FAILURE PER HOUR CALCULATIONS

A safety system and its associated controller may have one of two different operating

modes – low demand or high demand. The low demand mode can be quantified as an operation that is required at a frequency of once per year or less but not greater than twice the surveillance test interval. The high demand mode refers to any function that is in continuous or regular operation. Generally, a safety shutdown system is categorized as low demand, and those used to monitor/control real-time operations are categorized as high demand. The distinction between low and high demand systems determines the type of parameter needed to evaluate the reliability of a system and its component parts:

- The Probability of Failure on Demand (PFD) is the average probability that a safety system or one of its components will fail to perform its intended function on demand.

- The Probability of Failure per Hour (PFH) is the average probability that a dangerous failure will occur per hour of safety system operation. (This parameter is directly related to the system failure rate (λ), which is frequently listed in component specifications as the probability of failure per 10^6 hours.)

Most system functions operate with field hardware that requires continuous status monitoring throughout online operation. However, the RSP function remains completely inactive except when an emergency requires transfer of system control to the RSP or when this emergency backup function is being tested. Similarly, the ESFAS and Load Sequencer test functions are exercised at periodic intervals only, and between successive executions they remain inactive. Consequently, these functions could be viewed as low demand operations, but all other functions of a safety system must be viewed as high demand. Consequently, the PFH parameter provides the more significant value for evaluating the reliability and availability of the safety system.

Figure 3 is a reliability block diagram for a simple process that might be controlled by the safety system. The complete loop consists of the following elements:

- Field process. This element represents the process that is being controlled. Typically it includes some equipment that is being controlled directly by the safety system and one or more sensors to detect process status.
- Input Module. This element typically includes one or more DI and/or AI channels for each signal generated by the field sensors.
- FPC08 Controller. This element reads the input status, executes an application program that defines the intended process, and generates the digital image for one or more output signals.
- Output module. This element includes one or more DO and/or AO channels. It receives output images from the controller and then sets its output signals to the appropriate level.

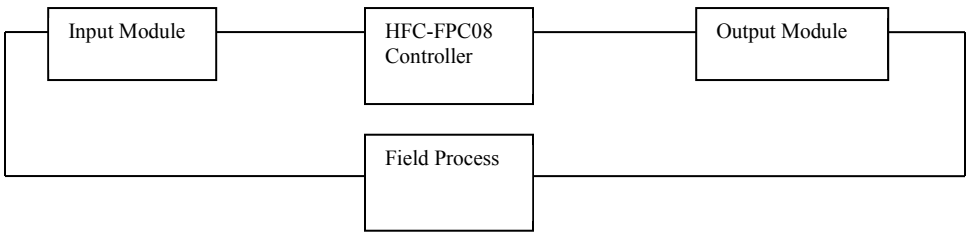

Figure 3 – Simple Process Reliability Block Diagram

Each element in Figure 3 (including signal cables) has a finite probability of failure. Calculating the overall reliability of the entire process would require evaluating the PFH for each element and then calculating a failure rate for the entire loop. The complete power plant installation will include many simple processes like that illustrated above. Some of these processes will be interrelated with one another, and some will be completely independent. The present analysis does not consider any of the field processes, any element external to the safety system itself, or any architectural redundancy to be built into the application.

Standard reliability calculations produce a value for the failure rate of a component based either on a mathematical model or actual field experience, but this failure rate does not differentiate between safe and dangerous failures. IEC 61508-6 Annex B expands this to consider diagnostic coverage within a system as well as the distinction between safe and dangerous failures. The following definitions are employed for the following analysis:

λ	Failure Rate
λ_D	Dangerous Failure Rate
λ_S	Safe Failure Rate
DC	Diagnostic Coverage
λ_{DU}	Undetected Dangerous Failure Rate
λ_{DD}	Detected Dangerous Failure Rate
λ_{SU}	Undetected Safe Failure Rate
λ_{SD}	Detected Safe Failure Rate
T_1	Surveillance interval in hours
t_{CE}	Average system down time in hours

Since no reliable method exists for differentiating between safe and dangerous failures in a complex electrical component, the following relations have been assumed:

$$\lambda_S = ½\,\lambda \qquad (1)$$
$$\lambda_D = ½\,\lambda$$
$$\lambda_{DU} = ½\,\lambda(1\text{-}DC)$$
$$\lambda_{DD} = \lambda_U - \lambda_{DU} = ½\,\lambda\,DC$$
$$\lambda_{SD} = \lambda_S\,DC$$

For a typical safety system, the average diagnostic coverage for safety-all components (both safety critical and non-safety critical) of the system is assumed to be approximately 75%. The failure rate parameters obtained from the Relex® software and those defined by equation (1) represent the PFH value for a single component. When a system includes more complex architecture, the failure rate for each element must be calculated from the failure rates for its constituent components. The following relations are used for that purpose:

$$t_{CE} = [\lambda_{DU} / \lambda_D]*[½\,T_1 + MTTR] + [\lambda_{DD} / \lambda_D] * MTTR \quad \text{Average down time} \qquad (2)$$

$$PFH = \lambda_{DU} \quad \text{Single channel PFH} \qquad (3)$$

$$PFH = 2\,[\lambda_{DD} + \lambda_{DU}]^2\, t_{CE} \qquad \text{1oo2 configuration PFH} \quad (4)$$

When a control loop includes a combination of simple and redundant elements, the total failure rate for the loop cannot be obtained merely by calculating the sum of the component failure rates. The average down time and the probability of failure per hour (PFH) for the redundant elements are defined by equations (2) through (4) above. Once these parameters have been established for a given surveillance interval, the probability that the module will operate successfully at any given point in time is given by

$$PSH = 1\text{-}PFH \quad (5)$$

Such a value exists for each module or element of the control loop. Since the application is completely undefined at this point, we will assume that every element must operate successfully to obtain the required control function. The probability that this will be achieved is given by

$$PSH_G = PSH_1 * PSH_2 * PSH_3 * \ldots * PSH_n \quad (6)$$

PSH_G represents the probability of successful operation of the composite group, and the combined probability of failure for the composite control loop is give by

$$PFH_G = 1 - PSH_G \quad (7)$$

Since we have assumed that the failure probability is described by an exponential function having a constant failure rate, the total failure rate is equal to the sum of the failure rates. If $\lambda << 1$, this sum is approximately equal to the group probability of failure per hour.

The percent availability parameter for a system is defined by the total up time divided by the total operating time for the system, or

$$A = [UP/(UP + DOWN)] * 100\% \quad (8)$$

However, for a system that is in continuous operation it is more convenient to calculate this parameter in terms of the failure rate, surveillance interval, and mean time to repair:

$$A = [1/(1 + \lambda * MTTR)]*100\% \quad (9)$$

6.0 CONCLUSIONS

The above calculations indicate an availability value greater than 99.99% for a hypothetical control loop composed of HFC-6000 modules and availability values greater than 99% for a typical safety system. These values were obtained based on standard failure rate modeling and an assumed diagnostic coverage of 75% for the system as a whole.

The methods used for calculating these results are known to be relatively pessimistic with

respect to hardware failure rates. In addition, the overall architecture of the application will be based on redundant control loops throughout the plant. Since none of these architectural redundancies have been considered by the present analysis, the actual performance of a typical safety system is likely to be significantly better than that predicted in the above tables.

7.0 ATTACHMENTS – RELIABILITY CALCULATIONS

The attachments contain the Reliability Prediction Report tables generated by the Relex® software. Each module has its own separate calculations with a detailed listing of the parts for each component assembly. Because the reports have been incorporated into this appendix just as they were obtained from the Relex® software, they contain a Relex® report number.

Attachment 7.1 – Relex® Report for HFC-FPC08
Attachment 7.2 – Relex® Report for HFC-HSIM
Attachment 7.3 – Relex® Report for HFC-ILR06R
Attachment 7.4 – Relex® Report for HFC-ILR06T
Attachment 7.5 – Relex® Report for AFS-CSM-01