GE Energy
Nuclear

NEDO-33234
Revision 1
Class I
eDRF 0000-0048-8110
December 2005

LICENSING TOPICAL REPORT

REACTOR TRIP AND ISOLATION FUNCTION DIGITAL TRIP MODULE FUNCTION SOFTWARE DESIGN SPECIFICATION

NON PROPRIETARY INFORMATION NOTICE

This is a non proprietary version of the document NEDE-33234P, Revision 1, which has the proprietary information removed. Portions of the document that have been removed are indicated by an open and closed bracket as shown here [[ ]].

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

PLEASE READ CAREFULLY

The information contained in this document is furnished **for the purpose of supporting the NRC review of the certification of the ESBWR**, with the information here being used as ABWR supporting reference. The only undertakings of General Electric Company with respect to information in this document are contained in contracts between General Electric Company and any participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone other than that for which it is intended is not authorized; and with respect to **any unauthorized use**, General Electric Company makes no representation or warranty, and assumes no liability as to the completeness, accuracy, or usefulness of the information contained in this document.

TABLE OF CONTENTS

LIST OF TABLES

1. Introduction

The Software Design Specification (SDS) describes the high level design of the ABWR RTIF Digital Trip Module (DTM) Functional Controller software.

The intended audience for this document includes the following:

- Software Engineering
- Software V&V
- Quality Assurance
- System Engineer

1.1Objectives

The purpose of this document is threefold:

- Define the Functional software design in sufficient detail such that software implementation can be undertaken without need for major design decisions.
- Provide a means for understanding how the DTM Functional Controller Software fulfills the design input requirements.
- Identify safety concerns and mitigation provided by the design.

1.2 Definitions and Acronyms

See Appendix A.

1.3 Design Scope

The DTM Functional controller software is designed to timely collect all the sensor inputs necessary to perform setpoint comparison logic on the sensor inputs, and generate sensor trip outputs to the Trip Logic Units (TLU) of each safety division. The sensor inputs are collected by receiving sensor inputs from the RTIF Remote Multiplexing Unit (RMU), digitizing the thermocouple sensor inputs from the Turbine Building, and reading discrete inputs. The software converts the sensor input parameters to engineering units before the setpoint comparison and trip logic. Signals for the trip and alarm outputs are also provided to the Control Room Local Display Unit (LDU), and the Process Computer system via the Communications Interface Module (CIM) in the safety division. The DTM also provides Control Rod Drive (CRD) Charging Pressure Trip signal to Rod Control & Information System (RCIS A & B).

1.4 Applicable Documents

1.4.1 Supporting Documents

Supporting documents provide the design input requirements for this document. These include the system level documents, any instrument level documents and any external communication protocol documents.

1. RTIF DTM Performance Specification 26A5233
2. RTIF LDU User's Manual 26A6018

3. RTIF LDU Protocol Specification 26A5524
4. RTIF Local Display Unit Performance Specification 26A5998
5. RTIF FDDI Communication Protocol Specification 26A5267
6. RTIF Digital Trip Module Schematic Diagram 105E3564

1.4.2 Supplemental Documents

Supplemental documents are used along with this SDS to shape the implementation of the software. The RTIF FDDI Communication Protocol Specification is both a supporting document and a supplemental document, but will only be included in the supporting documents section for simplicity.

1. ABWR DCIS Software Configuration Management Plan 31113-0A51-4501
2. ABWR DCIS Software Management Plan 31113-0A51-4500
3. ABWR DCIS Software Verification and Validation Plan 31113-0A51-4502
4. Software Conventions and Guidelines 26A5410
5. EOP NEDE-21109, GE Energy Nuclear Engineering Operating Procedures.

1.4.3 Reference Documents

This SDS uses the following documents as references.

1. NM386 Operating System User's Guide

1.5 Platform Description

1.5.1 Target Platform Description

The DTM Functional Controller consists of the NUMAC 386SX Computer Module [[

]]

1.5.2 Design Platform Description

Development of the RTIF DTM Functional Controller software is to be done on a cluster of DEC VAXstation [[

]]

1.6Development Tools

1.6.1 Compiler

[[

]]

1.6.2 Emulator

The DTM functional software development activities will use the DTM prototype chassis in conjunction with an INTEL 80386 in-circuit emulator (ICE). [[

]]

1.6.3 NUMAC Build Utility

[[	
	]]

1.6.4 Supporting Software

[[	

	]]

2. DTM Functional Software Design Considerations

2.1 Introduction

DTM is part of the Reactor Trip and Isolation Function (RTIF) of the Safety System Logic and Control (SSLC) system and performs certain Reactor Protection System (RPS) functions and Main Steam Isolation Valve (MSIV) control functions of the Leak Detection & Isolation (LDI) system. The DTM software is designed to digitize sensor inputs from the Turbine Building and receive sensor inputs from the RTIF Remote Multiplexing Unit (RMU), convert the sensor input parameters to engineering units, perform setpoint comparison logic on the sensor inputs, and generate sensor trip outputs to the Trip Logic Units (TLU) of each safety division. [[

]]

2.2 DTM Software Architecture Overview

A software design must have an underlying architecture, which directs the interaction of the software components, the internal hardware resources, and the external interfaces including the user interfaces. The Digital Trip Module (DTM) functional software architecture design must meet a set of performance requirements set forth by the Instrument's Performance Specification including the array of timing restrictions and the control logics. Additionally, it must provide division between safety and non-safety functions and fault isolation between all functions. This section gives an overview the critical items that drive the design of the software

2.2.1 DTM Software Components

The DTM software is composed of three main components; the NM386 operating system, set of hardware module driver packages, and the DTM application software. [[

]]

[[.]]

2.2.1.1 OS

The NM386 Operating System is the backbone of the DTM software. It is responsible for operating all the resources on the CPU card, and scheduling software task execution. It is also responsible for providing access mechanisms to the system resources such as semaphore, queues, timer functions, and hooks for installing application specific interrupt service routines and assigning task priorities. [[

]]

2.2.1.2 Hardware Module Drivers

All types of the NUMAC hardware modules are equipped with various mechanisms to interface with the host software. The hardware module drivers provide the hardware module interface functions for the instrument specific application software. [[

]]

2.2.1.3 DTM Application Layer Software

The DTM application layer software utilizes the OS and the hardware drivers to implement the software requirements specified in the DTM Instrument Performance Specification. This component provides the division of the software tasks, body of the software tasks, task-supporting functions including the functions interfacing to the drivers and the OS. [[

]]

2.2.1.3.1 Dividing into Software Tasks

Each major function performed by the functional software will be designated a "task". Tasks are the highest level of procedures in the DTM functional software, and only they will be called directly from the operating system. [[

]]

[[

]]

2.2.1.3.2 Task Scheduling and Task Priority

[[

]]

2.2.2 External interfaces

With its two protocol based interfaces, the FDDI and the RS485 (LDU), the DTM instrument communicates with other RTIF instruments in order to collect data from the source instruments, process the collected data, and send out the processed data to the destination instruments. [[

]]

2.2.2.1 FDDI Protocol based external interfaces

The following subsections define the interfaces that utilize the FDDI protocol. Please note that while this document lists input and output rates of FDDI messages for convenience, it defers to the FDDI Protocol Specification [1.4.1(3)] for all of these rates. [[

]]

2.2.2.1.1 RMU Interfaces

2.2.2.1.1.1 Redundancy

The FDDI link between the RMU and the DTM is so critical that two fully redundant FDDI links, primary and secondary, are provided. The two instruments always communicate over both the primary link (A13-J1) and the secondary link (A13-J2). [[

]]

2.2.2.1.1.2 RMU and DTM messages

[[

]]

2.2.2.1.1.3 RMU and LDU communication

[[

]]

2.2.2.1.2 TLU Interfaces

[[

]]

2.2.2.1.3 CIM Interfaces

[[

]]

2.2.2.1.4 NMSCLI Interface

[[

]]

2.2.2.2 RS485 Protocol based interfaces

The DTM communicates with the control room LDU using the RS485 protocol based interface located in the CPU module. [[

]]

2.2.2.3 Digital I/O interface

The DTM software reads various discrete inputs such as contacts, and instrument's division ID, using the two Isolated Digital Input (IDI) Modules. The keylock switch and the interlock switch are read using the Open Drain I/O (ODIO) card. [[

]]

2.2.2.4 Analog I/O interface

The DTM software reads the Main Steam Line Turbine area temperature sensor inputs via the analog module after the input signals get pre-conditioned by the two Six-thermocouple Input Modules. [[

]]

2.2.3 DTM Software States

The DTM software is expected to operate in one of the predefined states below:

- OS initialization
- DTM software initialization
- DTM software functional Mode

2.2.3.1 OS Initialization

Before the DTM software can come into the context of execution following a power cycle or a reset, the OS completes its own initialization first and updates its data structure with the application software specific data such as the application task names, task priorities, and also the interrupt service routine addresses. Once that state is achieved, the OS continuously schedules the DTM software tasks upon the system timer interrupt. [[ ]]

2.2.3.2 DTM Software Initialization

Prior to the start of the DTM software initialization (and at every 50 ms thereafter), the watchdog task resets the watchdog timer so that the timer does not expire and generate the NMI (Non-Maskable Interrupt) to the CPU during the initialization. The trip monitor task upon its first scheduled run performs the DTM software initialization and transitions to its forever-loop state. Therefore, the initialization is called only once before the next reset, or power cycle. [[

]]

[[

]]

2.2.3.3 DTM Software Functional Mode

Following the initialization the DTM software is in the functional mode executing the software tasks each of which has a set of functions to perform. The OS schedules the DTM software tasks primarily based on the priority of each task. Once a task is scheduled by the OS, it completes its set of functions and suspends itself for its predefined period before the OS schedules it to run again inside the task's forever-loop. Since the Watchdog monitor has the highest priority, it runs first before any other tasks. [[

]]

2.2.3.3.1 OPERATE Mode

When the keylock switch is in the OPERATE position, the DTM software tasks perform their normal operations of collecting, processing and outputting data autonomously in the predefined ways. [[

]]

2.2.3.3.2 INOP Mode

When the keylock switch is in the INOP position, the DTM software continues calculating and outputting trips to the TLU and communicating with all partnering instruments. The DTM software also does not transition itself from the OPERATE mode to the INOP mode when it detects the RMU keylock position change to INOP as indicated by the RMU FDDI message. [[

]]

[[

]]

3. Software Safe Design Discussion

This section is a brief discussion of the manner in which the DTM software can directly impact the safety of the RTIF System with emphasis on mitigations and controls in place to allow the DTM to perform it's primary function. Further detail can be found in the design sections of this document, Appendix E and Appendix F. Note that this section provides an overview and basic design guidance. It does not trace directly to system requirements. [[

]]

3.1General

Software has several functions it must perform in the RTIF systems and failure to perform those functions correctly can directly impact the safety of the systems in several ways.

For the RTIF instruments, software is responsible for monitoring the state of the instrument itself; it's sensors and hardware. This monitoring takes two forms. The software is responsible for reading and processing of sensors and other inputs, processing the data received, determining the validity of that data and acting accordingly. Additionally, software must monitor the health of the instrument. This monitoring, called Surveillance, should allow the software to detect the majority of hardware failures in a timely fashion and react appropriately to mitigate the hazard, maintain the primary function of the system when possible and fail in a safe manner when continued operation is not possible or desirable. Failure of the software to properly handle potential fault conditions, bad data and inputs or hardware failure could result in a failure of the instrument in its primary function. In this document this is referred to as "Functional Safety" and is discussed further in this section and elsewhere in the document, where deemed most appropriate.

Additionally, software must be designed in such a way that it does not challenge the system, that is it must not introduce faults where none existed. Examples of this type of fault would be a data corruption caused by one task interfering with another or a task that takes control of the system and doesn't allow other critical tasks the opportunity to process. This type of fault; a "Software Design Fault"; is best mitigated by following good design practices and guidelines such as those described briefly here and in Reference [1.4.2(5)], "Software Conventions and Guidelines". In this document this is referred to as "Software Safety" and is discussed further in this section and elsewhere in the document, where deemed most appropriate.

[[

]]

3.2The Digital Trip Module

The DTM instrument is designed, manufactured, and qualified as Class 1E equipment. All of the functions performed by the DTM are classified as Nuclear Safety-Related.

3.3DTM Functional Safety Summary

The primary purpose of the DTM instrument is to perform its safety related functions. Whenever the instrument becomes incapable of performing its safety related function or the ability to perform the safety related function becomes adversely affected, the DTM will assert its INOP trip output in order to achieve a safe state.

The main consideration given to the DTM software architecture as described in section 2.0 is safety. The software is also designed to maintain simple orderly execution of tasks while providing robust fault detection and handling. Because it is not desirable to halt the continuous operation of the software for minor faults while the reactor is operating, the fault handling is well separated for critical errors and non-critical errors.

The DTM Functional Controller software has been designed such that data received from the division RMU, TLU, CIM, and NMSCLI is validated before applied. If any input is out of range Invalid Data Code is substituted for the input.

[[

]]

3.4 General DTM Software Safety

[[

]]

4. DTM Functional Controller Software Design

[[

]]

4.1Task Table

Each of the tasks comprising the DTM Functional Controller software is described in the table below. The table shows the operational characteristics of each task: its priority, how often it is executed, the method by which it suspends (remains inactive), and the manner in which it is invoked.

Table 1: Task Table

[[

]]

4.2 Assignment of Instrument Functions to Tasks

The following sections list the instrument functions assigned to each of the tasks listed in the task table in section 4.1. The functions are described in detail in section 4.3. [[

]]

4.2.1 Watchdog Task

The Watchdog task is responsible for monitoring software health by monitoring task execution time. See section 4.3.7 for details. This is a safety critical task. [[

]]

4.2.2 Trip Monitor Task

[[

]]

4.2.3 Temperature Monitor Task

[[

]]

4.2.4 FDDI Output Task

[[

]]

4.2.5 [Section Deleted]

4.2.6 Display Input Task

[[

]]

4.2.7 Display Output Task

[[

]]

4.2.8 Chassis Monitor Task

[[

]]

4.2.9 Calibrate Task

[[

]]

4.2.10 Self-Test

[[

]]

4.3 Description of Instrument Functions

The following sections provide a brief description of each instrument function performed by the DTM Functional Controller software:

- Software Initialization
- Trip and alarm calculations
- Digital Inputs
- Digital Outputs
- Communications
- Analog I/O
- Temperature Monitoring
- Instrument Watchdog
- Instrument Calibration
- Instrument Self-test
- User-Entered Parameters
- Miscellaneous Instrument Functions

4.3.1 Software Initialization

At instrument power-up, the Functional Controller software recalls non-volatile parameters and initializes instrument hardware and software. All DTM sensor input readings are zeroed out while all sensor inputs from the RMU are set to invalid. All DTM tasks (other than the Trip Monitor Task) when scheduled for the first time check to see if the "Software Initialized" flag is indicating the initialization of the software and hardware is complete. If a task finds the flag is not set, it will not go onto the next step. [[

]]

4.3.1.1 Recalling Non-Volatile Storage

[[

]]

4.3.1.2 Initializing Hardware Drivers

[[

]]

4.3.1.3 Instrument ID

[[

]]

4.3.1.4 ID-Dependent Instrument Configuration

[[

]]

4.3.1.5 Initializing the Instrument Time of Day Clock

[[ ]]

4.3.1.6 Initializing the Open Drain Outputs

[[

]]

4.3.1.7 Initializing Global Flags

[[

]]

4.3.2 Trip and Alarm Calculation

The trip calculations are defined in the DTM performance specification (1.4.1 (1)) and used to build the trip status for the TLU. If any value of sensor data from the RMU is out of operating range or the link is down, the DTM would substitute the value with Invalid Data Code. An invalid data value from the RMU for a 4-20 mA input will be bigger than the maximum range value used by the DTM software and will become invalid. An invalid thermocouple data value from the RMU will be smaller than the minimum range value used by the DTM software and will become invalid. An Invalid Data Code for a sensor would cause a sensor trip. If any of the trip setpoints have become unknown, the DTM will use default values. The DTM will substitute a default value for a setpoint input which is out of range. In case the dual redundant FDDI link between the RMU and the DTM is down all the sensor inputs from RMU will be assigned Invalid Data Code.

4.3.2.1 Conversion to Engineering Units

4.3.2.1.1 RPV Narrow Range Water Level (L3)

This is one of the filtered 4-20 mA inputs from the RMU. [[

]]

4.3.2.1.2 RPV Wide Range Water Level (1.5)

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.3 RPV Dome Pressure

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.4 Drywell Pressure

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.5 CRD Charging Pressure

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.6 TCV ETS Oil Pressure

This input is read directly from the DTM's own 4-20 mA card. [[

]]

4.3.2.1.7 Main Condenser Vacuum

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.8 MSL Turbine Inlet Pressure

This is one of the filtered 4-20 mA inputs from RMU. [[

]]

4.3.2.1.9 Main Steam Line Flow

There are four main steam line flow inputs (A, B, C, D) from the RMU. [[

]]

4.3.2.1.10 Reactor Building Accelerations

There are five Reactor Building Acceleration digital inputs embedded in the digital input word sent by RMU. [[

]]

4.3.2.1.11 MSL Tunnel Temperatures

There are two MSL tunnel temperature inputs. One input is from the Reactor Building side and the other from the Turbine Building side. [[

]]

4.3.2.1.12 Main Steam Line Turbine Area Temperatures

The Functional Computer reads the nine Main Steam Line (MSL) Turbine Area Temperature inputs via the Thermocouple and Analog I/O Module. The temperature monitor task converts the voltage signals read to degrees centigrade (°C) for Type E thermocouples. Cold junction reference compensation is added in the conversion process using ambient temperature data read from each thermocouple input and the user entered Cold Junction Reference Offset. [[

]]

[[

]]

[[

]]

4.3.2.1.13 Suppression Pool Bulk Average Temperature

The SP Bulk Average Temperature is sent to the DTM from the RMU over the FDDI interface in the RMU SP Temperature Monitor data update FDDI message. [[

]]

4.3.2.1.14 Turbine Stop Valve Positions

Two valve positions (TSV Open and TSV > 90 % Open) are read in from the Integrated Digital Input cards. [[

]]

4.3.2.1.15 Turbine Bypass Valve Positions

The bypass valve positions are read in from the Integrated Digital Input cards. [[

]]

4.3.2.1.16 MSIV Inboard & Outboard Positions

The Main Steam Isolation Valve (MSIV) positions are read in from the Integrated Digital Input cards. There are a total of four inputs; "Inboard MSIV >92% Open", "Outboard MSIV >92% Open", "Inboard MSIV >90% Open" and "Outboard MSIV >90% Open". [[

]]

4.3.2.1.17 APRM Simulated Thermal Power (STP)

[[

]]

4.3.2.1.18 TCV/TSV Trip Bypass Determination

[[

]]

4.3.2.2 Trip Equations

4.3.2.2.1 RPV Narrow Range Water Level Low Trip

[[

]]

[[

]]

[[

]]

4.3.2.2.2 RPV Wide Range Water Level Low Trip

[[

]]

4.3.2.2.3 RPV Dome Pressure High Trip

[[

]]

4.3.2.2.4 RPV Dome Pressure Low Trip

[[

]]

4.3.2.2.5 Drywell Pressure High Trip

[[

]]

[[

]]

4.3.2.2.6 CRD Charging Pressure Low Trip

[[

]]

4.3.2.2.8 TCV ETS Oil Pressure Low

[[

]]

4.3.2.2.9 TSV Closure Trip

[[

]]

4.3.2.2.10 Seismic Activity Trip

[[

]]

4.3.2.2.11 Suppression Pool (S/P) Temperature High Trip

[[

]]

4.3.2.2.12 Main Steam Line Isolation Trip

[[

]]

4.3.2.2.13 Main Condenser Vacuum Low Trip

[[

]]

4.3.2.2.14 MSL Turbine Inlet Pressure Low Trip

[[

]]

4.3.2.2.15 MSL Flow High Trips

[[

]]

4.3.2.2.16 MSL Tunnel Temperature High Trips

[[

]]

4.3.2.2.17 MSL Turbine Area Temperature High Trip

[[

]]

4.3.2.2.18 Inoperative Trip

[[

]]

4.3.2.2.18.1 Mutual Inop Indication

[[

]]

4.3.2.2.18.2 INOP Trip Output Suppression

[[ ]]

4.3.2.2.19 Trouble Alarm

[[

]]

4.3.2.2.20 RTIF Channel Bypass Indication

[[

]]

4.3.3 Instrument Trip and Alarm Outputs

Upon power up, the trip monitor task will assume all tripped condition and lit the Trip indicator LED before the completion of the first cycle of the self-test. Once the first cycle of the self-test completes, the trip monitor will start to calculate the trips. [[

]]

4.3.4 Digital Inputs and Outputs

4.3.4.1 Digital Inputs

[[
]]

4.3.4.1.1 Fast sampled Digital Inputs

[[

]]

Table 2: Digital Inputs

[[

]]

The trip monitor task accepts the readings from the IDI card when the IDI cards are initialized properly.

4.3.4.1.2 Slow Sampled Digital Inputs

[[

]]

Table 3: Digital Inputs Continued.

[[	
	]]

The digital inputs for mode switch is only accepted if two consecutive reads confirms the same states.

4.3.4.2 Digital Outputs

The digital outputs are changed due to various events detected throughout the DTM software, but the Trip Monitor Task refreshes the output every 100 msec in order not to default back to the default states. [[

]]

Table 4: Digital Outputs

[[	
	]]

4.3.5 Instrument Communications

The functional controller software sends and receives communication/control messages from the various RTIF and NMS instruments at various rates.

[[ ]]

Table 5: Input Messages to DTM

[[				

]]

[[ ]]

Table 6: Messages sent by DTM

[[				

]]

4.3.5.1 Communicating with the LDU

The communication between the RTIF LDU and the DTM Functional Controller Software is driven by the Display output task and the Display input task. However, any task can send a response message to the LDU.

[[

]]

4.3.5.1.1 CPU Module serial (RS485) Ports

The communication between the RTIF LDU and the DTM Functional Controller uses a serial (RS485) port on the CPU module and the fiber optics isolation module. [[

]]

4.3.5.1.2 DMA Operation

4.3.5.1.2.1 Receiver Operation

The DMA channel for the receive operation is initialized by the display input task before the task enters its forever-loop. For the receive operation a receive queue is provided for the incoming messages. Receiving process is multi-staged. Each stage is only responsible for a section of the incoming message. [[

]]

4.3.5.1.2.2 Transmitter Operation

The Transmitter DMA operation is initialized by the display output task before the task enters its forever-loop. [[

]]

4.3.5.2 FDDI Communications

The DTM instrument communicates with RMU, TLU, CIM, and NMSCLI using three FDDI Interface cards. Each card utilizes a 125MHz fiber direct data interface. Refer to the RTIF FDDI Protocol Specification (1.4.1 (3))for information regarding frequency of transmission and data content.

[[

]]

[[

]]

4.3.5.3 RMU to RTIF LDU communication

The DTM functional controller software relays RMU messages destined for the RTIF LDU since there is no direct link between the two.

4.3.6 Analog I/O

The analog I/O function digitizes the following analog inputs:

- low voltage power supplies voltage readings
- the Main Steam Line (MSL) Turbine temperature inputs (Six Thermocouple Inputs)
- TCV ETS Oil Pressure Input
- Test Monitor Outputs

[[
]]

4.3.6.1 Initialization of Analog Modules

[[

-]]

4.3.6.2 Initialization of 4-20 mA

During the power up initialization the DTM monitor task initializes the global variables used for the 4-20 mA processing. [[

]]

4.3.6.3 4-20 mA (Analog) Signal Processing

The Trip monitor task is responsible for acquiring and processing the 4-20 mA analog input data (Only one input - TCV ETS Oil Pressure). [[

]]

4.3.6.4 Initialization of ASP module

[[

]]

4.3.6.5 Initialization of Thermocouple Inputs

{[

]]

[[

]]

4.3.6.6 Thermocouple Input (Analog) Signal Processing

The thermocouple inputs are processed by the DTM instrument's Temperature Monitor Task that performs the Temperature Monitor function. [[

]]

The temperature monitor task Reads and filters the thermocouple inputs after muxing the signals to the Analog I/O module. The calibration gain and offset corrections of the isolation amplifiers are applied to each T/C input reading and converted to equivalent thermocouple microvolts (µV). The TC µV values are cold junction reference compensated, filtered using a single-pole IIR filter with a 3.0 second time constant. The cold junction reference are converted to °C and stored in global variables for used by the self-test.

[[

]]

Table 7: Thermocouple Inputs

[[				

]]

4.3.6.7 Monitor LVPS

[[

]]

4.3.6.8 Calibrating Analog I/O Module

Once the user requests the manual calibration the Calibration Task performs the following in sequence:

- Overwrite all calibration corrections in use on the Analog I/O modules so that the A/D and D/A can be calibrated.

[1] Refer to the Six Thermocouple Input Module Performance Specification (see section 2.3.1 (f).

- Verify the time base of the instrument upon the user request. [[

]]

- Determine the D/A gain and offset correction factors for the A/D modules. [[

]]

- Check the A/D outputs. For each A/D module, the user is requested to connect a voltmeter at the test point and verify the voltmeter reading against the expected voltage range values displayed. [[

]]

- If the operator erroneously inputs data, the calibration sequence does not stop with an error. The entire sequence is repeated in this case.

4.3.6.9 Calibrating 4-20 mA Card

[[

]]

4.3.6.10 Calibrating ASP Card

[[

]]

4.3.6.11 Calibrating Six-Thermocouple Input Card

[[

]]

4.3.6.12 Auto-Calibration

[[

]]

4.3.7 MSL Turbine Temperature Monitoring

A MSL turbine temperature input is selected by setting up the mux in one of the two thermocouple cards. Once a temperature input is selected, it is routed to the A/D card for conversion to digital value. An analog input is converted using the input_analog() function in the analog.c module. [[

]]

4.3.7.1 Cold Junction Reference Temperature Monitoring

The cold junction reference temperatures are important in making correct temperature measurements and checked regularly by the temperature monitor task to see if they are in range. [[

]]

4.3.8 Instrument Watchdog

The watchdog task prevents the hardware watchdog timer from expiring by periodically pulsing the one shot circuitry. [[

]]

4.3.8.1 Watchdog Reset Suppression

Before refreshing the memory-mapped I/O point, which suppresses the watchdog reset, the task periods and task delays of each of the tasks comprising the DTM Functional Controller software are evaluated and compared against a pre-defined limit. [[

]]

4.3.8.2 Task Period Calculation

The task period is a measure of the time interval between successive task starts. Each task start is indicated by time stamping its return to the top of the infinite executive loop. [[

]]

4.3.8.3 Task Delay Calculation

The task delay is a measure of the time interval between the time a task last finished (and time stamped its completion) and the current time. An unexpectedly long task delay indicates that a task is taking longer to begin execution than expected. [[

]]

4.3.8.4 Watchdog Bypass and Exception Management

Certain user-initiated, asynchronous events undertaken while the DTM is in INOP mode require time delays which exceed the pre-defined max-task-periods and max-task-delays of one or more tasks allowed under normal operation. To prevent watchdog reset due to known time-intensive events, one or more tasks may be exempt from watchdog evaluation (i.e., comparison of task period and delay against threshold values) for programmable intervals.

[[

]]

4.3.9 Instrument Self-Test

Whenever the DTM Functional Controller software is not performing one of the aforementioned functions, it performs an instrument self-test. Depending on the instrument mode, the self-test may cycle automatically or await operator requests. The following sections describe the different modes of self-test operation and the individual tests performed.

4.3.9.1 INOP Mode Operation

When the DTM mode is switched from OPERATE to INOP mode, the self-test function stops and awaits operator request from the RTIF LDU. There are three possibilities: START, SKIP and STOP (STOP is available only after a module self-test has been initiated). [[

]]

4.3.9.2 OPERATE Mode Operation

When the DTM is in OPERATE mode, self-testing continuously cycles whether faults are detected or not. A counter keeps track of the number of self-test cycles and another one is used to indicate the last cycle that detected an error. [[ ]]

4.3.9.3 Modules Tested

The following sections briefly describe the tests performed on the various modules.

4.3.9.3.1 Functional Controller Module

[[

]]

4.3.9.3.2 Analog I/O Module

[[

]]

4.3.9.3.3 4-20 mA Module

[[

-]]

4.3.9.3.4 ASP Module

[[

]]

4.3.9.3.5 Thermocouple Input Module

[[

]]

4.3.9.3.6 Isolated Digital Input Module

[[

]]

4.3.9.3.7 Low Voltage Power Supplies

[[

]]

4.3.9.3.8 Open Drain I/O Module

[[

]]

4.3.9.3.9 FDDI Module

[[

]]

4.3.9.4 Error Handling

Faults detected by module self-tests are encoded into a bit mapped word, which is parsed by the Self-Test task. The following sections describe actions taken upon self-test fault detection.

4.3.9.4.1 Critical and Non-Critical Self-Test Faults

Self-test faults detected and reported by the DTM Functional Controller software are classified as either critical or non-critical faults. Critical self-test faults result in assertion of both DTM INOP trip and DTM Trouble alarm while non-critical self-test faults result in assertion of Trouble alarm only. [[ ]]

4.3.9.4.1.1 Critical Fault Classification

[[

-]]

4.3.9.4.1.2 Non-Critical Faults

[[

-]]

4.3.9.4.2 Successive Error Requirement

When the error word returned by a module self-test function indicates a fault, the module is tested again. [[

]]

4.3.10User-Entered Parameters

All user-entered parameters are received from the RTIF LDU via special parameter-set communication sequences while the instrument is in the INOP-SET mode. [[

]]

4.3.10.1 Set Parameter Mode (INOP Set Mode)

The DTM only transitions to INOP Set mode only if the keylock switch is in INOP mode. To enter set-parameter mode whereby user-entered parameters may be updated, the user must enter a password (itself subject to change by the user) at the RTIF LDU. [[

]]

4.3.10.2 Non-Volatile Storage (NVRAM) Operation

[[

]]

{[

]]

4.3.11 Miscellaneous Instrument Functions

4.3.11.1 Trip/Output Check

While in the INOP mode, the user may:

- Generate any trips DTM calculates
- Change the state of digital outputs

[[

]]

4.4Interrupts and Exceptions

The interrupt signals and exceptions (traps) serviced by the DTM Functional Controller, along with their corresponding service routines are tabulated below:

Table 8: Interrupts and Exceptions

[[

]]

4.4.1 Exception Handling

All exceptions are handled by the NM386 Operating System. The OS calls an application level service which records the exception and the processor state in non-volatile storage. [[

]]

4.4.2 Interrupt Service Routines

4.4.2.1 NMI_int

The non-maskable interrupt (NMI) is asserted for one of two reasons:

- system power has been removed or
- the hardware watchdog timer has expired

[[

-]]

4.4.2.2 DMA_chain_hdr

[[

]]

4.4.2.3 Timer0_int

[[

]]

4.4.2.4 Bus_timeout_int

[[

]]

4.4.2.5 Tmrisr

[[

]]

4.4.2.6 DMA_tc_hdr

[[

]]

4.5 Timing analysis

The timing analysis is conducted based on the actual timing data from the ABWR NUMAC NMSCLI instrument. The primary goal of the timing analysis at this point is to close out the risks of not having enough CPU power or the bandwidth in the external interface hardware to carry out the design called out in this document. [[

]]

4.5.1 Worst Case CPU Loading

This analysis is based on the 20 msec cycle on which the trip monitor task runs. This cycle is the most important restriction on the system timing, because the task performs the most important safety related functions. [[ ]]

[[ ]]

Figure 1 – Task Timing Analysis

[[

]]

[[

]]

4.5.2 Worst Case FDDI Interface Loading

Each FDDI port will have varying amount of traffic load. The interface between the RMU and the DTM will carry the heaviest FDDI traffic load. The time to pack and place the data into the TX_Load buffer or to retrieve and unpack the data from RX_Read buffer has been included in the task execution time estimate.

[[

]]

4.5.3 Worst Case LDU (RS485) Interface Loading

[[

]]

4.5.4 DTM Functional Controller Software Sizing Analysis

The DTM functional controller sizing analysis is based on the DTM prototype software. [[

]]

[[

]]

4.6 Starting Configuration

The following sections describe the software packages from which this design is derived.

4.6.1 Library Packages

[[

]]

4.6.2 Application Specific Packages

[[

]]

5. Software Module Design

Figure 5-1: Data Flow Diagram

[[

]]

5.1 Software Module Architecture

The ABWR DTM Functional Controller software will be designed to be modular. The following main modules will be developed to implement the tasks and requirements described in previous sections.

Table 9: Application Component Breakdown

[[

]]

[[ ]]

Table 10: Driver Component Breakdown

[[

]]

[[ ]]

Table 11: Support Component Breakdown

[[

]]

5.2 Module Description

The source file headers and software procedure headers will be an extension of the SDS (this document). Each procedure header will document the procedure description and the design decision. This section describes some of the major modules in the Application component.

5.2.1 Display Input Module Description

This software package implements the Display Input task and the support procedures to receive and processes messages from the RTIF LDU. The messages are defined in the RTIF LDU Protocol specification (1.4.1 (3)). The procedures in this package configure the data structure and call the necessary procedures in the Serial package for the data reception.

5.2.2 Display Out Module Description

This software package implements the Display Output task and the procedures to build and transmit messages to the RTIF LDU. The messages are defined in the RTIF LDU Protocol specification (1.4.1 (3)). The procedures in this package configure the data structure and call the necessary procedures in the Serial package for the data transmission.

5.2.3 Monitor Module Description.

This software package implements the Trip Monitor task, Temperature Monitor Task, Chassis Monitor Task, and the procedures for initializing the DTM functional controller software and all the hardware modules.

5.2.4 FDDI Interface Module Description.

This software package implements the FDDI output task and the procedures to build and transmit messages and receive and decode messages. The FDDI messages are defined in the RTIF FDDI protocol specification (1.4.1 (3)). Procedures in this package call the necessary procedures in the NUMAC FDDI Software packages for data transmission and data reception.

5.2.5 Calibration Module Description

This software package implements the Calibrate task and the procedures to perform calibration functions for the Analog module, 4-20 mA and Thermocouple modules.

5.2.6 Self-Test Module Description

This software package implements the Self-Test task and the procedures to perform self test on all the hardware modules in the chassis.

5.2.7 Watchdog Module Description

This software package implements watchdog task and the procedures to perform watchdog related functions.

6. Appendix A: Requirements Traceability Matrix

[[

]]

7. Appendix B: Symbols, Abbreviations, and Acronyms

°C	Degrees Centigrade
Ω	Ohm
µA	MicroAmperes
µV	Microvolts
A/D	Analog-to-Digital (Converter)
ANSI	American National Standards Institute
ASP	Automatic Signal Processor
Auto	Automatic
BNC	British Naval Connector
cm	Centimeters
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CRD	Control Rod Drive
CRJ	Cold Junction Reference
D/A	Digital-to-Analog (Converter)
DCIS	Distributed Control & Information System
deg C	Degrees Centigrade
DSP	Digital Signal Processor
DTM	Digital Trip Module
EL	Electro-Luminescent
ELD	Electro-Luminescent Display

EMI	Electromagnetic Interference
EPRI	Electric Power Research Institute
EPROM	Erasable Programmable Read-Only Memory
FDDI	Fiber Direct Data Interface
F/O	Fiber Optic
GE	General Electric
Hz	Hertz
ICD	Interface Control Drawing
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
INOP	Inoperative
INOP-CAL	Inoperative-Calibrate
INOP-SET	Inoperative-Set Parameters
I/O	Input/Output
IPS	Instrument Performance Specification
ITS-90	International Temperature Scale of 1990
KHz	KiloHertz
LDI	Leak Detection & Isolation
LDU	Local Display Unit
LED	Light Emitting Diode
LVPS	Low Voltage Power Supply
mA	MilliAmperes
MIL-HDBK	Military Handbook

MIL-STD	Military Standard
msec	Milliseconds
MSIV	Main Steam Isolation Valve
MSL	Main Steam Line
MTBF	Mean Time Between Failure
MTTR	Mean Time to Repair
mV	Millivolt
N/A	Not Applicable
NR	Narrow Range
NRC	Nuclear Regulatory Commission
NUMAC	Nuclear Measurement Analysis and Control
NVRAM	Non-Volatile Random Access Memory
OK	Okay
OPER	Operate
PCB	Printed Circuit Board
RAM	Random Access Memory
ROM	Read Only Memory
RB	Reactor Building
RMU	Remote Multiplexing Unit
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RTIF	Reactor Trip and Isolation Function
RX	Receiver or Receive

SCRAM	Safety Control Rod Axe Man (Reactor Trip - Safety Control Rod Insertion)
S/P	Suppression Pool
SPT	Suppression Pool Temperature
SPTM	Suppression Pool Temperature Monitor
SSLC	Safety System Logic and Control
TB	Terminal Board or Turbine Building
T/C	Thermocouple
TLU	Trip Logic Unit
TTL	Transistor-Transistor Logic
TX	Transmitter or Transmit
V	Volts
Vdc	Volts Direct Current

8. Appendix C: ITS-90 Table for Type E Thermocouples

[[

]]

9. Appendix D: Self-Test Error Messages and Criticality

[[ ]]

10. Appendix E: Component and Module Level Fault Mode Analysis

[[

]]

11. Appendix F: Software Safe Design Guidelines

[[

]]

ENCLOSURE 3

MFN 05-151

Affidavits

(Quantity of three)

General Electric Company

AFFIDAVIT

I, George B. Stramback, state as follows:

(1) I am Manager, Regulatory Services, General Electric Company ("GE") and have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.

(2) The information sought to be withheld is contained in the GE proprietary report NEDE-33232P, *Safety System Logic and Control Reactor Trip and Isolation Function (SSLC/RTIF) - System Performance Specification*, Revision 1, Class III (GE Proprietary Information), dated December 2005. GE proprietary information is identified by a dark red font with double underlines inside double square brackets. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation {3} refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.

(3) In making this application for withholding of proprietary information of which it is the owner, GE relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).

(4) Some examples of categories of information, which fit into the definition of proprietary information, are:

a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by General Electric's competitors without license from General Electric constitutes a competitive economic advantage over other companies;

b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

c. Information, which reveals aspects of past, present, or future General Electric customer-funded development, plans and programs, resulting in potential products to General Electric;

d. Information, which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a., and (4)b, above.

(5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GE, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GE, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements, which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.

(6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GE is limited on a "need to know" basis.

(7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GE are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

(8) The information identified in paragraph (2), above, is classified as proprietary because it contains specific, detailed, and extensive safety I&C equipment design information, which implements the life cycle design process plan, regarding the safety SSLC/RTIF equipment hardware and software design applicable to the GE BWR, ABWR, and ESBWR safety I&C systems. This information is part of the multi-generational engineering design and development program, specifically for equipment hardware and software design utilizing digital I&C equipment technology, developed by GE for over 25 years, at a total cost in excess of ten million dollars.

The reporting, evaluation and interpretations of the results, as they relate to the ESBWR, was achieved at a significant cost to GE. The development of the evaluation process along with the interpretation and application of the analytical

results is derived from the extensive experience database that constitutes a major GE asset.

(9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GE's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GE's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GE.

The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GE's competitive advantage will be lost if its competitors are able to use the results of the GE experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GE would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GE of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 12th day of December 2005.

George B. Stramback

George B. Stramback
General Electric Company

General Electric Company

AFFIDAVIT

I, George B. Stramback, state as follows:

(1) I am Manager, Regulatory Services, General Electric Company ("GE") and have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.

(2) The information sought to be withheld is contained in the GE proprietary report NEDE-33233P, *Safety System Logic and Control Reactor Trip and Isolation Function (SSLC/RTIF) – Hardware and Software Specification*, Revision 1, Class III (GE Proprietary Information), dated December 2005. GE proprietary information is identified by a dark red font with double underlines inside double square brackets. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation {3} refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.

(3) In making this application for withholding of proprietary information of which it is the owner, GE relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).

(4) Some examples of categories of information, which fit into the definition of proprietary information, are:

a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by General Electric's competitors without license from General Electric constitutes a competitive economic advantage over other companies;

b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

c. Information, which reveals aspects of past, present, or future General Electric customer-funded development, plans and programs, resulting in potential products to General Electric;

d. Information, which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a., and (4)b, above.

(5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GE, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GE, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements, which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.

(6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GE is limited on a "need to know" basis.

(7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GE are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

(8) The information identified in paragraph (2), above, is classified as proprietary because it contains specific, detailed, and extensive safety I&C equipment design information, which implements the life cycle design process plan, regarding the safety SSLC/RTIF equipment hardware and software design applicable to the GE BWR, ABWR, and ESBWR safety I&C systems. This information is part of the multi-generational engineering design and development program, specifically for equipment hardware and software design utilizing digital I&C equipment technology, developed by GE for over 25 years, at a total cost in excess of ten million dollars.

The reporting, evaluation and interpretations of the results, as they relate to the ESBWR, was achieved at a significant cost to GE. The development of the evaluation process along with the interpretation and application of the analytical

results is derived from the extensive experience database that constitutes a major GE asset.

(9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GE's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GE's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GE.

The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GE's competitive advantage will be lost if its competitors are able to use the results of the GE experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GE would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GE of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 12th day of December 2005.

George B. Stramback
General Electric Company

General Electric Company

AFFIDAVIT

I, George B. Stramback, state as follows:

(1) I am Manager, Regulatory Services, General Electric Company ("GE") and have been delegated the function of reviewing the information described in paragraph (2) which is sought to be withheld, and have been authorized to apply for its withholding.

(2) The information sought to be withheld is contained in the GE proprietary report NEDE-33234P, ***Reactor Trip and Isolation Function Digital Trip Module Function Software Design Specification,*** Revision 1, Class III (GE Proprietary Information), dated December 2005. GE proprietary information is identified by a dark red font with double underlines inside double square brackets. Figures and large equation objects are identified with double square brackets before and after the object. In each case, the superscript notation {3} refers to Paragraph (3) of this affidavit, which provides the basis for the proprietary determination.

(3) In making this application for withholding of proprietary information of which it is the owner, GE relies upon the exemption from disclosure set forth in the Freedom of Information Act ("FOIA"), 5 USC Sec. 552(b)(4), and the Trade Secrets Act, 18 USC Sec. 1905, and NRC regulations 10 CFR 9.17(a)(4), and 2.390(a)(4) for "trade secrets" (Exemption 4). The material for which exemption from disclosure is here sought also qualify under the narrower definition of "trade secret", within the meanings assigned to those terms for purposes of FOIA Exemption 4 in, respectively, Critical Mass Energy Project v. Nuclear Regulatory Commission, 975F2d871 (DC Cir. 1992), and Public Citizen Health Research Group v. FDA, 704F2d1280 (DC Cir. 1983).

(4) Some examples of categories of information, which fit into the definition of proprietary information, are:

a. Information that discloses a process, method, or apparatus, including supporting data and analyses, where prevention of its use by General Electric's competitors without license from General Electric constitutes a competitive economic advantage over other companies;

b. Information which, if used by a competitor, would reduce his expenditure of resources or improve his competitive position in the design, manufacture, shipment, installation, assurance of quality, or licensing of a similar product;

c. Information, which reveals aspects of past, present, or future General Electric customer-funded development, plans and programs, resulting in potential products to General Electric;

d. Information, which discloses patentable subject matter for which it may be desirable to obtain patent protection.

The information sought to be withheld is considered to be proprietary for the reasons set forth in paragraphs (4)a., and (4)b, above.

(5) To address 10 CFR 2.390 (b) (4), the information sought to be withheld is being submitted to NRC in confidence. The information is of a sort customarily held in confidence by GE, and is in fact so held. The information sought to be withheld has, to the best of my knowledge and belief, consistently been held in confidence by GE, no public disclosure has been made, and it is not available in public sources. All disclosures to third parties including any required transmittals to NRC, have been made, or must be made, pursuant to regulatory provisions or proprietary agreements, which provide for maintenance of the information in confidence. Its initial designation as proprietary information, and the subsequent steps taken to prevent its unauthorized disclosure, are as set forth in paragraphs (6) and (7) following.

(6) Initial approval of proprietary treatment of a document is made by the manager of the originating component, the person most likely to be acquainted with the value and sensitivity of the information in relation to industry knowledge. Access to such documents within GE is limited on a "need to know" basis.

(7) The procedure for approval of external release of such a document typically requires review by the staff manager, project manager, principal scientist or other equivalent authority, by the manager of the cognizant marketing function (or his delegate), and by the Legal Operation, for technical content, competitive effect, and determination of the accuracy of the proprietary designation. Disclosures outside GE are limited to regulatory bodies, customers, and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and then only in accordance with appropriate regulatory provisions or proprietary agreements.

(8) The information identified in paragraph (2), above, is classified as proprietary because it contains specific, detailed, and extensive safety I&C equipment design information, which implements the life cycle design process plan, regarding the safety SSLC/RTIF equipment hardware and software design applicable to the GE BWR, ABWR, and ESBWR safety I&C systems. This information is part of the multi-generational engineering design and development program, specifically for equipment hardware and software design utilizing digital I&C equipment technology, developed by GE for over 25 years, at a total cost in excess of ten million dollars.

The reporting, evaluation and interpretations of the results, as they relate to the ESBWR, was achieved at a significant cost to GE. The development of the evaluation process along with the interpretation and application of the analytical

results is derived from the extensive experience database that constitutes a major GE asset.

(9) Public disclosure of the information sought to be withheld is likely to cause substantial harm to GE's competitive position and foreclose or reduce the availability of profit-making opportunities. The information is part of GE's comprehensive BWR safety and technology base, and its commercial value extends beyond the original development cost. The value of the technology base goes beyond the extensive physical database and analytical methodology and includes development of the expertise to determine and apply the appropriate evaluation process. In addition, the technology base includes the value derived from providing analyses done with NRC-approved methods.

The research, development, engineering, analytical and NRC review costs comprise a substantial investment of time and money by GE.

The precise value of the expertise to devise an evaluation process and apply the correct analytical methodology is difficult to quantify, but it clearly is substantial.

GE's competitive advantage will be lost if its competitors are able to use the results of the GE experience to normalize or verify their own process or if they are able to claim an equivalent understanding by demonstrating that they can arrive at the same or similar conclusions.

The value of this information to GE would be lost if the information were disclosed to the public. Making such information available to competitors without their having been required to undertake a similar expenditure of resources would unfairly provide competitors with a windfall, and deprive GE of the opportunity to exercise its competitive advantage to seek an adequate return on its large investment in developing these very valuable analytical tools.

I declare under penalty of perjury that the foregoing affidavit and the matters stated therein are true and correct to the best of my knowledge, information, and belief.

Executed on this 12th day of December 2005.

George B. Stramback

George B. Stramback
General Electric Company

ENCLOSURE 1

MFN 05-151

Contains GE Proprietary Information

Licensing Topical Reports

- NEDE-33232P, Revision 1, *Safety System Logic and Control Reactor Trip and Isolation Function (SSLC/RTIF) System Performance Specification*, December, 2005
- NEDE-33233P, Revision 1, *Safety System Logic and Control Reactor Trip and Isolation Function (SSLC/RTIF) – Hardware and Software Specification*, December, 2005
- NEDE-33234P, Revision 1, *Reactor Trip and Isolation Function Digital Trip Module Function Software Design Specification*, December, 2005