HFC-6000 FPGA Platform

JORDAN MOTT

2018 FPGA Conference
10/8~10/11

Innovation Leadership Service
Table of Contents

- HFC-6000 I&C DEVELOPMENT
  - GOALS AND OBJECTIVES
  - APPLICABLE REGULATORY STANDARDS AND GUIDANCE
  - EVOLUTION OF HFC-6000 TO HFC-FPGA SYSTEM

- HFC-FPGA - SYSTEM DESCRIPTION
  - HFC-FPGA PLATFORM CONFIGURATIONS
  - BASIC BUILDING BLOCKS - FPU, FCPU, GW

- HFC-FPGA – CARD LINEUP
  - CHARACTERISTICS AND FEATURES

- HFC-FPGA – APPLICATION DEVELOPMENT

- HFC-FPGA – DESIGN PROCESS

- HFC-FPGA – SUMMARY

- HFC-FPGA – Q & A
HFC I&C DEVELOPMENT

• HFC-6000 PLATFORM IS A COMBINATION OF ADVANCED MICROPROCESSORS, DSP, AND FPGA
  – RECEIVED US NRC SE REPORT IN APRIL, 2011 AND TUV SIL3 IN 2010/2013/2018

• HFC-FPGA PLATFORM IS SUITABLE FOR SOME SAFETY CONTROL APPLICATIONS IN NUCLEAR POWER PLANT DUE TO THE DETERMINISTIC NATURE OF FPGA FSM BASED DESIGNS

• THE DEVELOPMENT OF A GENERIC FPGA SAFETY I&C PLATFORM DEPENDS UPON THE MATURITY AND ENHANCEMENT OF FPGA TECHNOLOGY IN ORDER TO IMPROVE THE CALCULATION DENSITY AND NETWORKING CAPABILITY.

• HFC TREATS FPGA DESIGNS AS A MIX OF SOFTWARE AND HARDWARE
  – DEVELOPMENT FOR FPGA APPLICATIONS FOLLOWS SYSTEM, SOFTWARE, AND HARDWARE DEVELOPMENT LIFECYCLE PROCESSES.

• DEVELOPMENT GOALS AND OBJECTIVES
  – HFC ‘S GENERIC FPGA NUCLEAR SAFETY I&C PLATFORM IS BASED UPON THE FOUNDATION OF CURRENT HFC-6000 TECHNOLOGY.
  
  – HFC HAS FILED FPGA HFC-6000 DESIGN AS AN AMENDMENT TO CURRENT SER.
  – TO ACQUIRE US NRC SE REPORT FOR THE HFC-6000 FPGA AMENDMENT.
• THE NUREG/CR-7006 IS THE CURRENT NRC REGULATORY GUIDANCE FOR THE FPGA.
• OTHER APPLICABLE REGULATORY GUIDANCE AND INDUSTRY STANDARDS INCLUDE
  – NUREG-0800 BTP 7-14,
  – NRC RG 1.152, 1.168, 1.169, 1.170, 1.171, 1.172, 1.173
  – DO-254 (DESIGN ASSURANCE),
  – IEEE STD 603
  – IEEE STD 1012-2004 AND 2012 (V&V),
  – IEC 61508 (FUNCTIONAL SAFETY - TUV)
  – IEEE STD 7-4.3.2 (SAFETY DIGITAL SYSTEMS).

• THE INTENT OF HFC’S FPGA DESIGN AND DEVELOPMENT PROCESS IS TO MEET RELEVANT REGULATORY REQUIREMENTS AND INDUSTRY STANDARDS.
HFC-6000 PLATFORM

**Features**

- Nuclear safety class 1E qualified
- Modular Packaging (19”/23” Rack)
- Redundant and Triple Redundant
- DCS and Loop application
- Dedicated CSM & M/A stations
- Nuclear qualified Flat Panel Display
- Superior Response time
- Thousands controllers installed in Nuclear Power Plants

**Application**

- Nuclear Power Plant Safety
- Turbine Control
- Mission Critical Control
- TÜV SIL-3 Certified

- **HFC-FPGA I&C SYSTEM TO USE THESE HFC-6000 SAFETY QUALIFIED FEATURES**
  - MECHANICAL
    - CARD FORM FACTOR, 19 INCH 5U CHASSIS, FIELD CONNECTIVITY, SEISMIC CHASSIS/CABINET
  - ELECTRICAL – REDUNDANT POWER AND COMMUNICATION INTERFACES
  - APPLICATION DEVELOPMENT
    - SHARES HFC-6000 TOOLS FOR DEVELOPING APPLICATIONS AND HMI GRAPHICS
  - REDUNDANCY – CENTRALIZED CONTROLLER TO IMPLEMENT REDUNDANCY
  - I/O MODULE LINEUP – MICROPROCESSOR I/O MODULES AVAILABLE IN FPGA IMPLEMENTATIONS
✓ HFC’s nuclear safety class cabinet
✓ Three(3) racks of FPGA PCB modules for typical parameterized safety and protection functions; the Test Specimen Application Program (TSAP) includes the following:
  o Functional Diesel Generator Load Sequencer
  o Functional Diverse Protection System (DPS) – 2 Ch
✓ 5U Racks – up to 8 per cabinet
✓ Termination boards, Connection cards, cables
✓ A rack mounted Personal Computer (PC) with Flat Panel Device (FPD) and Human Machine Interface (HMI) utility software
✓ Network Hubs and Fans
✓ Rack mounted power supply set - 40ms withhold time, 24VDC
✓ Power distribution and a set of circuit breakers
DUAL FPGA ARCHITECTURE REPLACES THE MICROPROCESSOR FOR CONTROL

- CONTROL FPGA – F-LINK TX/RX TO COMMUNICATE WITH OTHER CARDS IN THE RACK
  - MAIN APPLICATION/PROCESSING ELEMENT DOING APPLICATION AND/OR I/O PROCESSING
- DIAGNOSTIC FPGA – F-LINK RX VERIFIES ACTIVITY AND PROCESSING RESULTS OF THE CONTROL FPGA
  - DISABLES CONTROL FPGA WHEN A FAULT IS DETECTED
    - FAULTS CAN BE HARDWARE OR APPLICATION/I/O PROCESSING RELATED
  - FPGAS COMMUNICATE STATUS AND PROCESSING RESULTS OVER A INTRA-FPGA DATA BUS
  - EXCHANGE HEART BEAT MESSAGES TO VERIFY HEALTH
  - CONTROL FPGA MONITORS FOR POWER FAULTS IN THE DIAGNOSTIC FPGA AND VICE VERSA
  - EACH FPGA HAS APPLICATION DATA STORED IN A NON VOLATILE MEMORY
    - READ AT POWER UP AND USED TO INITIALIZE I/O AND CONTROLLER CARD FPGA MEMORIES

ALL C CODE CONTROL FUNCTIONS REPLACED WITH FPGA FSM BASED PROCESSES

- HFC HAS A LARGE LIBRARY OF C FUNCTIONS THAT CAN BE IMPLEMENTED IN THE HFC-FPGA SYSTEM
HFC-FPGA SYSTEM DESCRIPTION

• TWO ARCHITECTURE OPTIONS FOR THE HFC-FPGA SYSTEM
  – DISTRIBUTED – NO CENTRALIZED CONTROLLER, EACH I/O CARD DOES APPLICATION PROCESSING
    • I/O CARDS (FPU) EXCHANGE POINT INFORMATION DIRECTLY
      – FILTERING ELIMINATES UNDESIRED VALUES
      – APPLICATION DISTRIBUTED, FPU RUN PORTIONS OF THE APPLICATION
  – CENTRALIZED – APPLICATION PROCESSING IN THE FCPUX ONLY
    • I/O CARDS (FPU) DO MINIMAL PROCESSING AND SEND/RECEIVE RESULTS TO/FROM THE CONTROLLER

• FPGA NODE – 1 TO 2 RACKS
  – EACH RACK CAN CONTAIN UP TO 14 CARDS (FPU I/O, FPGA CONTROLLERS, OR GATEWAYS)
  – RACKS ARE INTERCONNECTED WITH RS-485 CABLING (EXTENSION OF F-LINK)
  – FPGA LINK (F-LINK) IS A TOKEN PASSING PROTOCOL
    • OPERATES WITHIN THE FPGA NODE WITH A PERIOD OF 6.8 MSEC.
    • SUPPORTS UP TO 26 FPGA PROCESSING UNITS AND 2 CONTROLLERS
HFC-FPGA SYSTEM DESCRIPTION

• FPGA PROCESSING UNITS (FPU)
  – CAPABLE OF HANDLING BOTH DIGITAL AND ANALOG ALGORITHMS.
  – CONFIGURED AS SINGLE, REDUNDANT OR TRIPLE MODULAR REDUNDANT (TMR) SET.
  – COMMUNICATE WITH OTHER FPU AND CONTROLLERS VIA REDUNDANT F-LINK
     • TOKEN-PASSING PROTOCOL (SIMILAR TO HFC’S QUALIFIED C-LINK PROTOCOL)
     • 12.5 MBPS LINK ALLOWS FPUS TO EXCHANGE THEIR I/O STATUS AND INTERNAL DATABASE

• FPGA CONTROLLER PROCESSING UNIT (FCPUX)
  – FPGA BASED CONTROLLER CENTRALIZES APPLICATION IN ONE MODULE
  – CAN BE USED IN REDUNDANT CONFIGURATIONS
  – PERFORMS ANALOG AND DIGITAL PROCESSING ON INPUT FPU DATA
  – COMMUNICATES APPLICATION RESULTS TO OUTPUT FPU
  – COMMUNICATES APPLICATION STATUS WITH THE FPGA GATEWAY
     • USES A PRIVATE LINK TO THE GATEWAY CALLED G-LINK
  – FCPU – REDUCED CAPACITY FPGA CONTROLLER PROCESSOR UNIT WITH ONBOARD DI/DO
HFC-FPGA SYSTEM DESCRIPTION

- FPGA GATEWAY
  - TERMINATES G-LINK DATA FROM FPGA CONTROLLER
  - RE-BROADCASTS CONTROLLER DATA USING THE QUALIFIED ETHERNET BASED C-LINK PROTOCOL
  - CAN BE USED IN REDUNDANT CONFIGURATIONS
Typical HFC-FPGA system configuration that implements a control system in a Distributed Loop Control Scheme

- Two (2) or more FPU I/O Modules and redundant Gateway Controller communicate with:
  - Safety C-Link to other FPGA Nodes
  - F-Link within the FPGA Node

- Each HFC-6000 FPGA Node is capable of connecting up to 26 FPU Control Modules in two (2) racks. All FPUs are connected via 12.5MBPS F-Link.

- Accessories (i.e. Power Supply, Hubs,...)
This diagram illustrates the system configuration of HFC-6000 FPGA Load Sequencer for NPP application:

- The Load Sequencer logic for NPP can be programmed into four (4) HFC-6000 FPGA Processing Units.
- The system can be configured in one of the following cases:
  - **Non-Redundant**
  - **Dual Modular Redundant (DMR) with 1oo2D voting**
  - **Triple Modular Redundant (TMR) with 2oo3D voting**
- Voting in DMR and TMR on input signals, controller execution and output signals.
Typical HFC-FPGA system configuration that implements a control system in a Centralized Control Scheme

- Redundant FCPUX and its FPU I/O Modules with redundant Gateway Controller with:
  - Safety C-Link to other controllers
  - G-Link to Gateway Controller
  - F-Link to its FPU I/O Modules

- Each redundant FCPU is capable of connecting up to 24 FPU I/O Modules in two (2) racks via 12.5MB F-Link.

- Accessories (i.e. Power Supply, Hubs,...)
HFC-FPGA I/O AND CONTROLLER CARD LINEUP

- HFC-FCPUX – FPGA CONTROL PROCESSOR UNIT – USED ONLY IN CENTRALIZED CONTROL SYSTEM
  - APPLICATION PROCESSOR CONTROL MODULE USING DATA RECEIVED FROM SYSTEM I/O CARDS
  - REDUNDANCY INTERFACE TO MATE FCPUX
    - SUPPORTS REDUNDANCY OVER REDUNDANCY INTERFACE
  - SEPARATE G-LINK INTERFACE TO EWS GATEWAY CARDS

- HFC-FPUD – FPGA PROCESSOR UNIT – DIGITAL TYPE
  - FPUD01 – FPUD I/O CARD WITH 16 CHANNELS DI (COMMON OR ISOLATED) AND 16 CHANNELS DO (C-FORM RELAY)
  - FPUD02 – FPUD I/O CARD WITH 32 CHANNELS DI (COMMON OR ISOLATED MODE)

- HFC-FPUA – FPGA PROCESSOR UNIT – ANALOG TYPE (COMMON OR ISOLATED MODE)
  - FPUA01 – FPUA ANALOG I/O CARD WITH 16 CHANNELS AI – 4 TO 20 MA
  - FPUA02 – FPUA ANALOG I/O CARD WITH 16 CHANNELS AI – 0 TO 10 V
HFC-FPGA I/O AND CONTROLLER CARD LINEUP

• HFC-FPUAO – FPGA PROCESSOR UNIT – ANALOG OUTPUT TYPE
  – FPUAO01 – FPUAO ANALOG I/O CARD WITH 8 CHANNELS AO – 4 TO 20 MA
  – FPUAO02 – FPUAO ANALOG I/O CARD WITH 8 CHANNELS AO – 0 TO 10 V

• HFC-FPUM – FPGA PROCESSOR UNIT – M TYPE (SUPPORTS 3 RANGES TO 200 C AND 2000 OHM RTD)
  – ANALOG I/O CARD WITH 8 CHANNELS OF TYPE M 100 OHM PLATINUM RTD INPUTS

• HFC-FPUL – FPGA PROCESSOR UNIT – E TYPE (SUPPORTS 3 RANGES TO 500 C)
  – ANALOG I/O CARD WITH 8 CHANNELS OF TYPE E THERMOCOUPLE INPUTS

• HFC-HSIM – HIGH SPEED INTERFACE MODULE
  – FPGA BASED INTRA-SAFETY SYSTEM FIBER OPTIC COMMUNICATION LINK
  – 2 OPTICAL CHANNELS CONFIGURABLE AS EITHER TRANSMIT OR RECEIVE
**HFC-FPU FPGA Based I/O Modules**

**HFC-FPU DI/DO/AI/AO/RTD/TC**

**Product Features**

❖ FPGA based intelligent module diagnostics and self checking capabilities
❖ Power on reset circuitry with onboard watchdog timer
❖ Redundant power feeds with onboard diode auctioneering and fuse protection
❖ Redundant communications interfaces
❖ Onboard status LED indications

**Functional Description**

✓ All HFC-FPU are FPGA based intelligent I/O modules to perform these functions: sampling of input data and/or transmit to FCPUX or receive output data from the FCPUX and drive output devices.

✓ The two FPGAs on the HFC-FPU I/O modules are the Control FPGA and Diagnostic FPGA. They are intended to work in tandem, processing the same input and/or output data and comparing the results to detect faults.

✓ The dual FPGA structure is designed to protect final output data from Single Event Upset and single component failure that may impact safety function.

✓ The HFC-FPU circuit structure includes multiple layers of safety function protection circuitry/logic to enforce the I/O channel verification and communication data acquisition/verification.

✓ The diagnostic FPGA controls the F-Link RS485 transmit enable signal. The diagnostic FPGA also monitors all I/O activities. For any diagnostic non-conformance, the diagnostic FPGA can invalidate the FPU function or mark channel data as questionable.
Product Features

❖ FPGA based controller with diagnostics capabilities
❖ Intelligent module diagnostics and self checking capabilities
❖ Power on reset circuitry with onboard watchdog timer
❖ Redundant power feeds with onboard diode auctioneering
❖ Redundant communications interfaces
❖ Onboard status LED indications

Functional Description

✓ The HFC-FCPUX is a central control unit designed for use in the HFC-FPGA product line.
✓ The HFC-FCPUX supports communications with FPGA FPU I/O modules via F-Link, Gateway Controller via G-Link, and its redundant controller via the RIF.
✓ The two FPGAs on the HFC-FCPU is partitioned into Control FPGA and Diagnostic FPGA. They are intended to work in tandem, processing the same input to compare and validate output data.
✓ The dual FPGA structure is designed to protect final output data from Single Event Upset, and single component failure that may impact safety function.
✓ The HFC-FCPU circuit structure includes multiple layers of function safety protection circuitry/logic to enforce the DI/DO channel verification and communication data acquisition/verification.
HFC-FPGA I&C APPLICATION UTILITY – ONESTEP

- USES SIMILAR METHOD OF ENTRY TO HFC-6000 MICROPROCESSOR SYSTEM
• APPLICATION IS DEFINED BY THE GENERATION OF A SET OF CAD DRAWINGS
  – PROMISE CURRENTLY SUPPORTED
  – SCHEMATIC TYPE REPRESENTATION OF THE APPLICATION
  – PROCESSING OF THE DRAWING SET CREATES APPLICATION DATA BASE REPORT

• DRAWING SET IS PROCESSED BY ONESTEP
  – ONESTEP IS A NRC QUALIFIED TOOL DEVELOPED BY HFC
HFC-FPGA AUTOMATED LOGIC GENERATION

- INVOKING ONESTEP GENERATES PROGRAMMING FILES THAT CUSTOMIZE THE HFC-6000 FPGA SYSTEM
  - PARSES DRAWING DATABASE
    - DETERMINES THE ORDER OF ANALOG PROCESSING (IF REQUIRED)
    - REQUIRED APPLICATION LOGIC RTL
    - ANALOG PROCESSING (CQ4) REQUIREMENTS
    - F-LINK FILTERING
    - MEMORY INITIALIZATION
  - INVOKES LIBERO (MICROSEMI FPGA SOC TOOL) TO GENERATE FPGA PROGRAMMING FILES USING THE FOLLOWING INPUTS
    - PUBLISHED PLATFORM BLOCKS
    - APPLICATION LOGIC RTL
    - BUILD SCRIPTS GENERATE PROGRAMMING FILES FOR THE DIAGNOSTIC AND CONTROL FPGA’S
  - HFC BUILDFLASH TOOL GENERATES BINARY FLASH PROGRAMMING FILE
**HFC-FPGA AUTOMATED LOGIC GENERATION**

- **FLASH PRO (MICROSEMI TOOL)**
  - USES ONESTEP GENERATED FPGA PROGRAMMING FILES TO CONFIGURE THE FCPUX CONTROL AND DIAGNOSTIC FPGA’S

- **QSFLASH**
  - HFC UTILITY USED TO PROGRAM CONTROL AND DIAGNOSTIC SPI FLASH WITH A PC USB PORT
  - REQUIRES THE HFC 40134221Q SPI FLASH PROGRAMMER
FPGA DESIGN PROCESS

✓ DESIGN PHASE INPUT
  ✓ APPROVED SW REQUIREMENT SPECIFICATION

✓ DESIGN ACTIVITIES
  ✓ PARTITIONING AND DETAILED DESIGN
  ✓ OUTPUT – APPROVED DESIGN SPECIFICATION

✓ IMPLEMENTATION PHASE INPUT
  ✓ APPROVED DESIGN SPECIFICATION

✓ IMPLEMENTATION ACTIVITIES
  ✓ CODING, SYNTHESIS, PLACE AND ROUTE
  ✓ FORMAL VERIFICATION – VALIDATE SYNTHESIS, P&R
  ✓ OUTPUT - VALIDATED P&R NETLIST, PROGRAMMING FILES

✓ TEST PHASE INPUT
  ✓ PROGRAMMING FILE GENERATED FROM IMPLEMENTATION

✓ TEST ACTIVITIES
  ✓ DEVICE VALIDATION
  ✓ FUNCTIONAL VERIFICATION
HFC-FPGA PRODUCT SUMMARY

- **HFC-FPGA IS AN EVOLUTION OF THE HFC-6000 PRODUCT THAT REMOVES MICROPROCESSOR CONTROL ELEMENTS**
  - Shares important and necessary qualities of the HFC-6000 system
  - Builds on this platform by adding deterministic state machine processing and redundancy
  - Replace ICL protocol (master/slave) with a token passing protocol called F-LINK
  - Control FPGA – Main Control Element
  - Diagnostic FPGA – Verifies activity and processing results of the Control FPGA
  - Shares HFC-6000 tools for developing applications
  - Implements redundancy over a separate redundancy interface

- **TWO SYSTEM CONFIGURATION OPTIONS – DISTRIBUTED AND CENTRALIZED**
  - Distributed, I/O FPU run a portion of the application
  - Centralized, FCPUX runs application with input and output provided by the FPU

- **CONTROL APPLICATION STORAGE**
  - FPGA configuration and redundant non-volatile memory elements
  - FPGA’s validate application at powerup using intra-FPGA bus
THANK YOU