DOOSAN HF Controls

NPP CCS FPGA Controller Architecture

HOT STANDBY ARCHITECTURE WITH MESSAGE BASED REDUNDANCY

12/5/17

Innovation Leadership Service

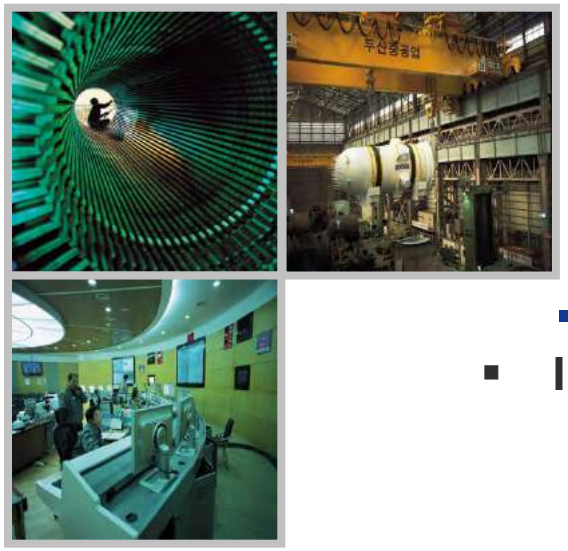


Table of Contents

MYSELF

- **FPGA DEVELOPMENT MANAGER AT HFC FOR THE LAST TWO YEARS**
  - BEEN WITH THE COMPANY FOR APPROXIMATELY 3 YEARS
  - ELECTRICAL ENGINEERING DEGREE WORKING IN THE INDUSTRY FOR > 30 YEARS
- **RESIDED IN NORTH TEXAS FOR LAST 32 YEARS**
  - NATIVE TEXAN?
- **BACK GROUND IS TELECOM – HIGH AVAILABILITY HARDWARE**
  - PCB, FPGA, RTL, AND TEST

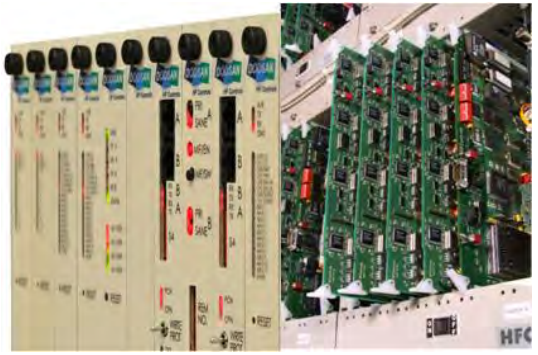
HFC INTRODUCTION

Overview

- Address : 1624, West Crosby Carrollton, TX 75006, USA
- Toll Free: 1-866-501-9954
- Fax: 469-568-6589
- Web www.HFControls.com

Business Line

- Designing and manufacturing **Nuclear Power Plant safety class 1E/** non-class 1E control systems
- Designing and manufacturing plant control system and boiler management system for fossil power plant
- Commercial digital control systems for several industries including water treatment, petrochemical, etc.



Accomplishments

- **Over 450+ plant control system installations worldwide**
  - Thousands of digital controllers and I/Os installed in nuclear power plant
  - Field proven plant control I&C product lines including both nuclear and non-nuclear applications

DOOSAN HF Controls

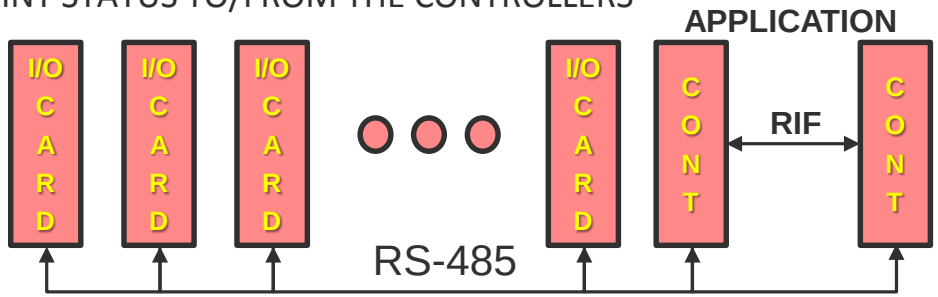
HFC ACCOMPLISHMENTS

HFC-6000 FPGA USAGE

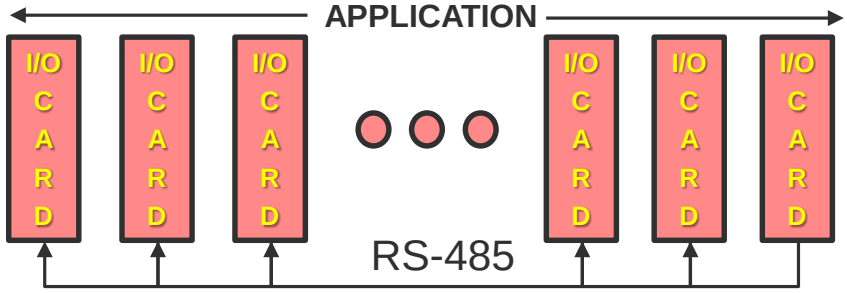
- **FPGA'S ARE USED TO IMPLEMENT FSM BASED APPLICATION CONTROL ALGORMITMS**
- **ROBUST CONTROL ARCHITECTURE - ALL CONTROLLER AND I/O CARDS ARE ARCHITECTED WITH TWO FPGA'S**
  - CONTROL FPGA – PERFORMS I/O AND/OR CONTROL PROCESSING
    - MONITORS HEALTH OF DIAGNOSTIC FPGA
  - DIAGNOSTIC FPGA – MONITORS CONTROL FPGA BY VERIFYING THE CONTROL FPGA PROCESSING OUTPUT
    - MONITORS HEALTH OF THE CONTROL FPGA
- **FPGA'S ALLOW RAPID CUSTOMIZATION OF CONTROL ALGORITHMS**
- **THREE PARTS TO THE DEVELOPMENT OF CCS APPLICATION – GENERATED BY HFC SOFTWARE TOOL FLOW**
  - PROCESSING ENGINE
    - CUSTOM CALCULATION BLOCK GENERATED BY HFC FOR ANALOG CALCULATION
  - CUSTOMER DEFINED APPLICATION ADDED TO PROCESSING ENGINE
    - APPLICATION DESCRIBED IN SCHEMATIC TYPE DRAWINGS
      - COMPILED WITH SOFTWARE TOOLS
      - AUTOMATIC RTL GENERATION ADDED TO PROCESSING ENGINE FOR FINAL PROGRAMMING FILE GENERATION
  - ALGORITHM CONTROL CONFIGURATION BINARY
    - ANALOG CALCULATION CONTROL SEQUENCE STORED OFF FPGA
    - LOADED AT POWER UP FROM EXTERNAL FLASH MEMORY
  - ALL PARTS ARE IDENTIFIED BY UNIQUE NUMBER ASSIGNED BY THE SOFTWARE FLOW
  - PROTECTED BY CRC'S AND CHECKED FOR ACCURACY BETWEEN THE DIAGNOSTIC AND CONTROL FPGA'S

HFC-6000 CCS VS DCS

- **HFC HAS DEVELOPED TWO TYPES OF NUCLEAR POWER PLANT CONTROLLERS USING FPGA BASED CARDS**
  - CENTRALIZED CONTROL SYSTEM (CCS)
    - LOOP CONTROL APPLICATION IS CENTRALIZED ON A REDUNDANT PAIR OF CONTROLLER CARDS
      - COMMUNICATION OCCURS BETWEEN CONTROLLERS OVER A PRIVATE REDUNDACY INTERFACE
    - I/O CARDS AND CONTROLLERS COMMUNICATE OVER A RS-485 BUS
    - I/O CARDS SEND/RECEIVE POINT STATUS TO/FROM THE CONTROLLERS

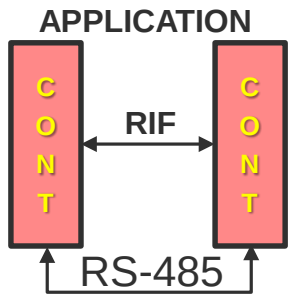


  - DISTRIBUTED CONTROL SYSTEM (DCS)
    - I/O CARDS BECOME THE CONTROLLER CARDS AND PROCESS LOOP CONTROL APPLICATION LOCALLY
      - LOOP CONTROL APPLICATION IS DIVIDED BETWEEN THE I/O CARDS
    - I/O CARDS COMMUNICATE WITH EACH OTHER OVER A RS-485 BUS
    - REDUNDANCY IS ACHIEVED THROUGH ARCHITECTURAL FUNCTION DUPLICATION AND VOTING



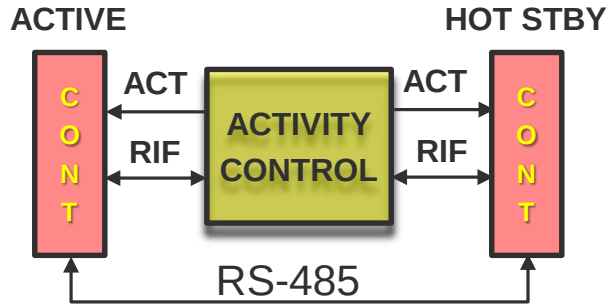
HFC-6000 CCS REDUNDANCY

- **PARALLEL REDUNDANCY – HFC EXPERIENCE**
  - IMPLEMENTATIONS IN MICROPROCESSOR AND FPGA BASED CARDS
  - BOTH CONTROLLERS ARE PROCESSING THE SAME APPLICATION AT THE SAME TIME
    - REQUIRES EQUALIZATION OF APPLICATION DATA BETWEEN CONTROLLERS
  - CHARACTERISTICS
    - NOT AS COMPLEX AS OTHER SCHEMES
    - BOTH CONTROLLERS ARE BEING FULLY TESTED 100% OF THE TIME
    - I/O CARDS HAVE TWO SETS OF DATA TO CHOOSE FROM
    - FAILSAFE REQUIRED TO GUARANTEE I/O CARDS USE DATA FROM A HEALTHY CONTROLLER
      - CONTROLLERS HAVE TO SELF DIAGNOSE ISSUES
    - I/O CARDS USE PRIORITIZATION – CONTROLLER A OVER CONTROLLER B
    - EQUALIZATION CAN BE COMPLEX AND TAKES TIME
      - BUMPLESS CONTROL
    - SUPPORTS MIGRATION TO HOT STANDBY CONTROLLER ARCHITECTURE



NPP CCS REDUNDANCY

- **HOT STANDBY REDUNDANCY**
  - HFC HAS IMPLEMENTATIONS IN MICROPROCESSOR AND FPGA BASED CARDS
  - INTRODUCES AN ACTIVITY CONTROL ELEMENT BETWEEN THE TWO CONTROLLERS
    - DETERMINES WHICH CONTROLLER IS ACTIVE AND WHICH IS HOT STANDBY
      - ACTIVE CONTROLLER PROCESSES THE APPLICATION
      - HOT STANDBY CONTROLLER RECEIVES APPLICATION EQUALIZATION DATA
    - SUPPORTS STATUS AND EQUALIZATION MESSAGING BETWEEN ACTIVE AND HOT STANDBY CONTROLLERS
      - EQUALIZATION BETWEEN THE CONTROLLERS IS REQUIRED TO ALLOW BUMPLESS CONTROL
    - PERFORMS AUTOMATIC FAILOVER FUNCTION
      - VERIFIES HEALTH OF THE ACTIVE CONTROLLER CARD
      - IF ACTIVE CARD FAILS, REMOVES ACTIVE ENABLE AND ENABLES HOT STANDBY CONTROLLER AS ACTIVE
    - PARTICIPATES IN MANUAL FAILOVER PROCESS
  - CHARACTERISTICS
    - I/O CARDS HAVE ONE SET OF DATA TO CHOOSE FROM
    - CENTRAL CONTROL ENTITY THAT VERIFIES CONTROLLER CARD FUNCTION
    - CONTROLS WHICH CONTROLLER IS ACTIVE WITH ACTIVITY (ACT) SIGNAL
    - MORE COMPLEX SYSTEM WITH SINGLE ELEMENT BETWEEN CONTROLLERS



CCS HOT STANDBY ARCHITECTURE OBJECTIVES

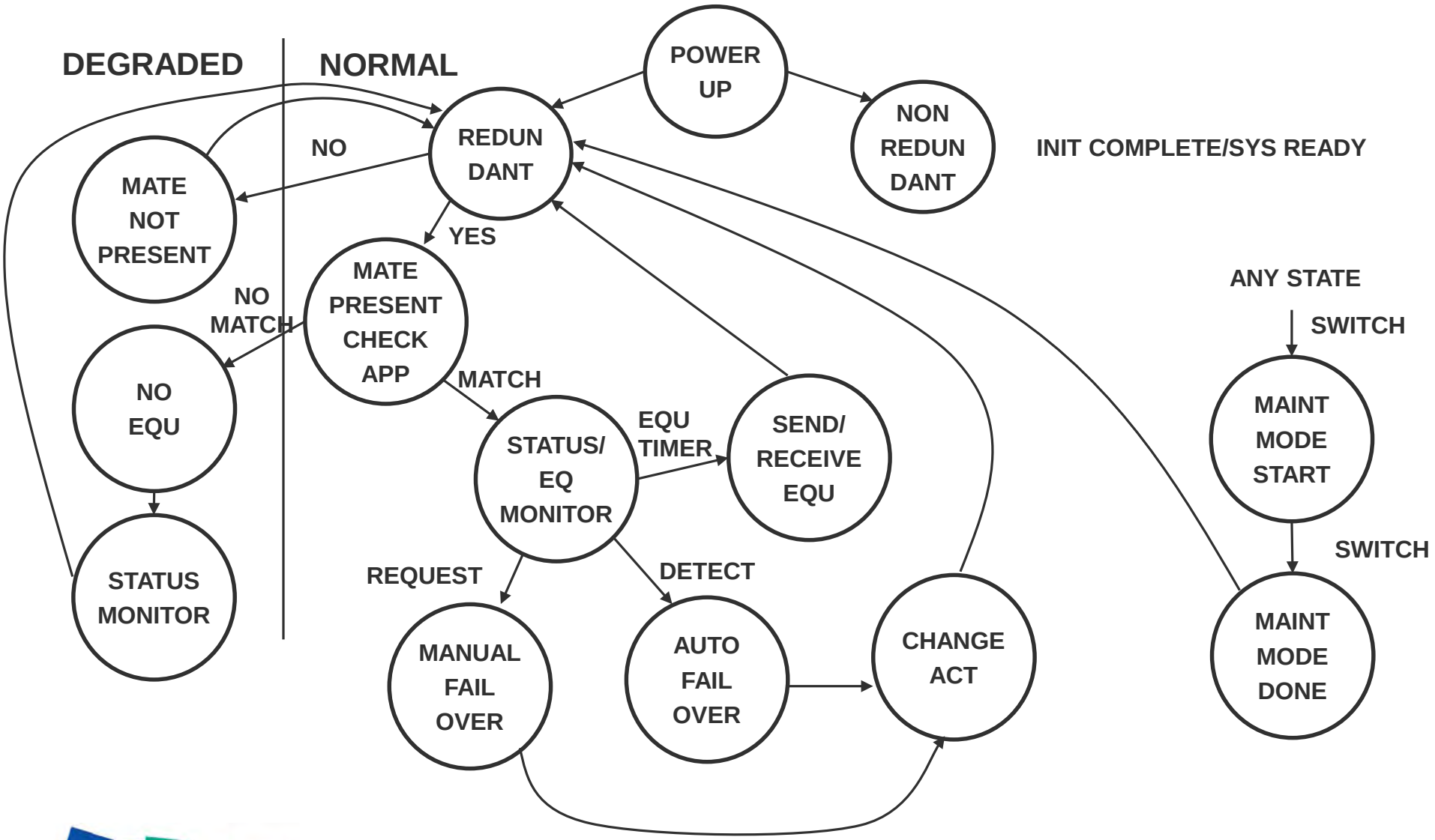
- SUPPORT NON REDUNDANT CONFIGURATIONS – NO ACTIVITY CONTROL
- USE HIGH SPEED SERIAL REDUNDANCY INTERFACE BETWEEN THE CONTROLLERS FOR COMMUNICATION
- FAILURE DETECTION OF ACTIVE CONTROLLER AND SWITCH TO HOT STANDBY
- CONTROLLERS COMMUNICATE HEALTH AND LAST RECEIVED STATUS INFORMATION REGULARLY
- ACTIVITY CONTROL ELEMENT RESPONDS TO CONTROLLER STATUS WITH SYSTEM STATUS
- CONTROLLERS CAPTURE STATE OF ACTIVITY CONTROL SIGNAL WHEN VALID SYSTEM STATUS RECEIVED
- ACTIVITY CONTROL ELEMENT SUPPORTS EQUALIZATION – ACTIVE TO HOT STANDBY
- ACTIVITY CONTROL ELEMENT SUPPORTS MAINTENANCE MODE FOR FIELD SERVICE
- CONTROLLERS SUPPORT MANUAL FAILOVER REQUEST
- SUPPORT DYNAMIC SYSTEM CHANGES

CCS HOT STANDBY MESSAGE TYPES

- **CONTROLLER MESSAGE TYPES**
  - INIT COMPLETE – CONTROLLER HAS COMPLETED INITIALIZATION TESTS AND ITS STATUS
  - CNTR STATUS – CONTROLLER STATUS UPDATE
  - EQU UPDATE – EQUALIZATION UPDATE FROM ACTIVE CONTROLLER
  - EQU TRANSMIT – HOT STANDBY REQUEST FOR ACTIVE CONTROL ELEMENT TO SEND NEW EQUALIZATION DATA
  - EQU ACK – HOT STANDBY ACKNOWLEDGES RECEPTION AND USAGE OF EQUALIZATION DATA
  - MAINT MODE ACK – MAINTENANCE MODE ACKNOWLEDGE FROM THE CONTROLLER

- **ACTIVITY CONTROL ELEMENT MESSAGE TYPES**
  - SYSTEM READY – INIT COMPLETE ACK FROM THE ACTIVITY CONTROL ELEMENT
  - SYSTEM STATUS – SYSTEM STATUS UPDATE
  - SYSTEM ERROR – GENERATED FOR AUTOMATIC FAILOVER UPON ERROR DETECTION
  - MAINT MODE INIT – MAINTENANCE MODE INITIATED FROM THE ACTIVITY CONTROL ELEMENT

ACTIVITY CONTROL SYSTEM STATES



CCS HOT STANDBY - MESSAGE FLOW

- **POWERUP**
  - CONTROLLERS BROADCAST "**INIT COMPLETE**" MESSAGE WITH HEALTH STATUS
  - AFTER RECEPTION OF THE "**SYSTEM READY**" RESPONSE FROM THE ACTIVITY CONTROL ELEMENT
    - CONTROLLER STORES THE STATE OF THE **ACT** AND ENTERS NORMAL OPERATION MODE

- **NON REDUNDANT MODE – NO MESSAGING REQUIRED**
  - SELECTABLE OPTION FOR CONTROLLER CARD
  - ACTIVITY CONTROL ELEMENT MESSAGING IS NOT ACTIVATED AND NOT REQUIRED TO BE INSTALLED
  - CONTROLLER ASSUMES ACTIVE CONTROLLER STATUS
    - SENDS APPROPRIATE SYSTEM CONFIGURATION INFORMATION TO OPERATOR POSITION

CCS HOT STANDBY - MESSAGE FLOW

- **NORMAL OPERATION MODE**
  - ACTIVE CONTROLLER – TWO CASES FOR THE ACTIVE CONTROLLER
    - MATE PRESENT – INFORMATION EXCHANGED THROUGH STATUS AND ERROR MESSASES AS DESCRIBED
      - **"SYSTEM STATUS"** MESSAGE FROM ACTIVITY CONTROL ELEMENT INDICATES MATE STATUS
        - » NO COMMUNICATION FROM MATE INDICATES DEGRADED STATUS - ALARM
      - APPLICATION COMPATIBILITY INFORMATION MUST BE CURRENT AND MATCH TO START EQUALIZATION
        - » STALE APPLICATION IDENTIFIER DATA IS SET TO DEFAULT TO IDENTIFY UNITIALIZED STATE
        - » MUST MATCH UNIQUE NUMBER ASSIGNED AT APPLICATION COMPILE TIME
        - » NO MATCH IS DEGRADED MODE
      - EQUALIZATION ENABLED
        - » REGULARLY SEND APPLICATION DATA STATUS TO THE HOT STANDBY CONTROLLER
        - » SET TIMER FOR ACKNOWLEDGE RECEPTION – TIMER EXPIRES BEFORE ACK RECEIVED, SETS ALARM
    - NO MATE PRESENT
      - CONTINUALLY CHECK FOR HOT STANDBY MATE TO BE INSTALLED
      - DEGRADED MODE
  - HOT STANDBY CONTROLLER
    - RECEIVES NOTIFICATION IN "**SYSTEM STATUS"** OF EQUALIZATION UPDATE STATUS
    - REQUESTS TRANSMISSION USING "**CONTROLLER STATUS"** MESSAGE AND STARTS RESPONSE TIMER
      - RECEIVES TIMELY RESPONSE, CHECKS DATA INTEGRITY, USES DATA TO UPDATE APPLIATION STATUS
      - DOES NOT RECEIVE TIMELY RESPONSE, GENERATES ALARMS SENT IN SYSTEM STATUS UPDATE

CCS HOT STANDBY - MESSAGE FLOW

- **AUTOMATIC FAILOVER**
  - ACTIVE CONTROLLER FAILURE HAS BEEN DETECTED BY THE ACTIVITY CONTROL ELEMENT
    - FAILURE IN MESSAGING FREQUENCY (STATUS, EQUALIZATION) OR REPORTED ERROR CONDITION
    - CONTROLLER IS REPORTING INTERNAL ERROR CONDITION OR OTHER ADVERSE HEALTH CONDITION
    - ACTIVITY ELEMENT SWITCHES ACTIVITY CONTROL AND UPDATES SYSTEM STATUS DATA
      - OUTPUTS **"SYSTEM ERROR"** STATUS MESSAGE TO BOTH CONTROLLERS
        - » CONTAINS ERROR CODE DETECTED FOR AUTOMATIC FAILOVER
        - » NEW ACTIVE CONTROLLER UPDATES STATUS FLAGS REPORTED TO OPERATOR POSITIONS

- **MANUAL FAILOVER**
  - INITIATED BY SWITCH ON THE FRONT BEZEL
    - ACTIVE CONTROLLER SENDS "**CONTROLLER STATUS**" MESSAGE WITH INDICATOR FOR FAILOVER REQUEST
    - ACTIVITY ELEMENT SENDS "**SYSTEM STATUS**" WITH FAILOVER REQUEST TO CURRENT HOT STANDBY CONTROLLER
    - HOT STANDBY CONTROLLER SENDS FAILOVER ACKNOWLEDGE STATUS IN "**CONTROLLER STATUS**"
      - SUCCESS – READY TO INITIATE FAILOVER
      - FAULT – ISSUE WITH BECOMING ACTIVE CONTROLLER
    - ACTIVE CONTROLLER UPDATES FAILOVER COMPLETION STATUS IN "**CONTROLLER STATUS**"
      - SUCCESS – FAILOVER COMPLETE
      - FAULT – ACKNOWLEDGE FAILURE TO MANUAL FAILOVER AND MAINTAIN ACTIVE CONTROLLER STATUS
        - » REPORT ERROR TO OPERATOR POSITION

CCS HOT STANDBY - MESSAGE FLOW

- **SYSTEM CHANGE**
  - CONTROLLER ADDITION – CONTROLLER INSERTION DETECTED
    - NO ACTIVE CONTROLLER – WAIT FOR RECEPTION OF “INIT COMPLETE” MESSAGE
    - ONE ACTIVE CONTROLLER – AFTER RECEPTION OF “INIT COMPLETE” MESSAGE
      - ASSIGN HOT STANDBY STATUS AND ENABLE EQUALIZATION IF APPLICATION PARAMETERS MATCH
  - CONTROLLER REMOVAL – CONTROLLER REMOVAL DETECTED, NORMAL AND ERROR CONDITION
    - HOT STANDBY CONTROL REMOVED - “**SYSTEM STATUS**” UPDATED WITH CONTROLLER
    - ACTIVE CONTROLLER REMOVED – NO MANUAL FAILOVER, ERROR CONDITION
      - IMMEDIATE SWITCH OF ACTIVITY CONTROL TO HOT STANDBY CONTROLLER
      - UPDATE OF “**SYSTEM STATUS**” TO SHOW ERROR INDICATOR IN FOLLOWING MAINTENANCE PROCEDURE
      - ERROR CONDITION REPORTED BY NOW ACTIVE CONTROLLER IN SYSTEM FLAGS
  - SYSTEM APPLICATION UPDATE
    - HOT STANDBY CARD REMOVED FROM THE SYSTEM
      - REMOVAL OF CONTROLLER DETECTED BY ACTIVITY CONTROL ELEMENT
        - » “**SYSTEM STATUS**” CHANGED TO REFLECT REMOVAL ACTION AND EQUALIZATION DISABLED
    - MANUAL FAILOVER INITIATED ON THE ACTIVE CONTROLLER TO MAKE SECONDARY
      - UPDATE TO THE SAME APPLICATION REVISION AS THE CURRENT ACTIVE CONTROLLER
      - RE-INSERT IN THE CHASSIS AND NOTE RESTORATION OF EQUALIZATION
      - “**SYSTEM STATUS**” MESSAGE NOTES NORMAL OPERATION OR INDICATES FAULT CONDITIONS

CCS HOT STANDBY - MESSAGE FLOW

- **MAINTENANCE MODE**
  - INITIATED VIA SWITCH SETTING ON THE ACTIVITY CONTROL ELEMENT
  - ACTIVITY CONTROL ELEMENT SENDS "**MAINT MODE INIT**" MESSAGE
    - TO ALL CONTROLLERS PRESENT WITH REGULAR STATUS
  - CONTROLLERS RECEIVE "**MAINT MODE INIT**" MESSAGE AND STORE STATE OF ACT SIGNAL
    - ENTER ACTIVITY HOLDOVER MODE – INDICATED ON FRONT BEZEL
    - CONTROLLERS ACKNOWLEDGE ACTIVITY HOLDOVER MODE COMPLETE WITH "**MAINT MODE ACK**" MESSAGE
  - WHEN ACTIVITY CONTROL ELEMENT RECEIVES "**MAINT MODE ACK**" - CONTROLLERS WITH REGULAR STATUS
    - MAINTENANCE MODE

- **TEST MODES**
  - LAB USE ONLY, NOT ACTIVE FOR NORMAL OPERATION

THANK YOU

THANK YOU FOR YOUR ATTENTION AND COMMENT