Non-Proprietary

Technical Part 1: RadICS Digital I&C Platform Topical Report

RadICS Digital I&C Platform

(Closed Session)

August 30, 2017, Rockville, Maryland

Agenda

- RadICS Platform Overview
- RadICS Platform System Interfaces
- RadICS Platform Modules
- RadICS Platform Safety Features

RadICS Platform Overview

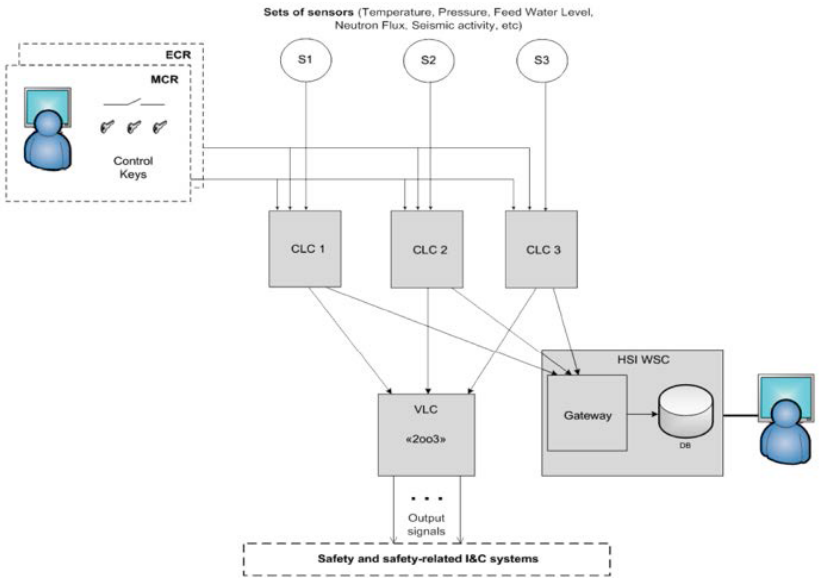
RadICS Platform Overview

Product Highlights

Typical System Configurations

Configuration Flexibility:

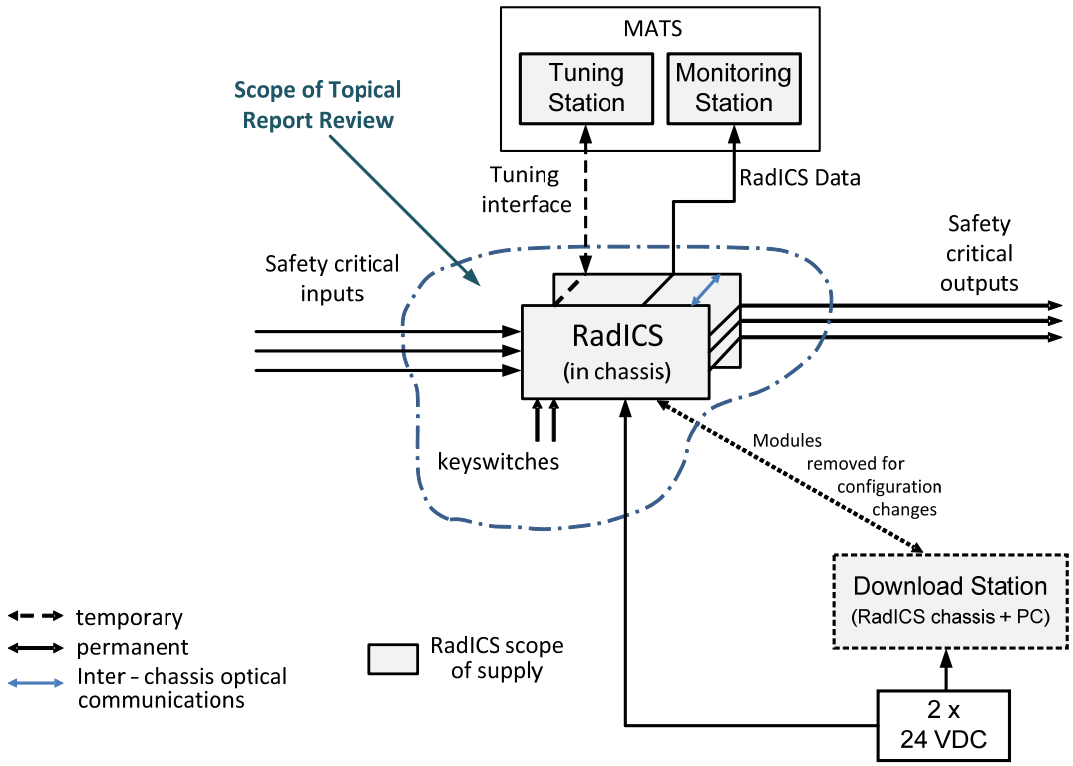
- 2, 3, or 4 channel systems
- Separate trip processing and voting layers



Used for Safety I&C Systems:

- Reactor Trip System
- Engineered Safety Feature Actuation System
- Reactor Power Control and Limitation System
- Rod Control System

RadICS Platform Context



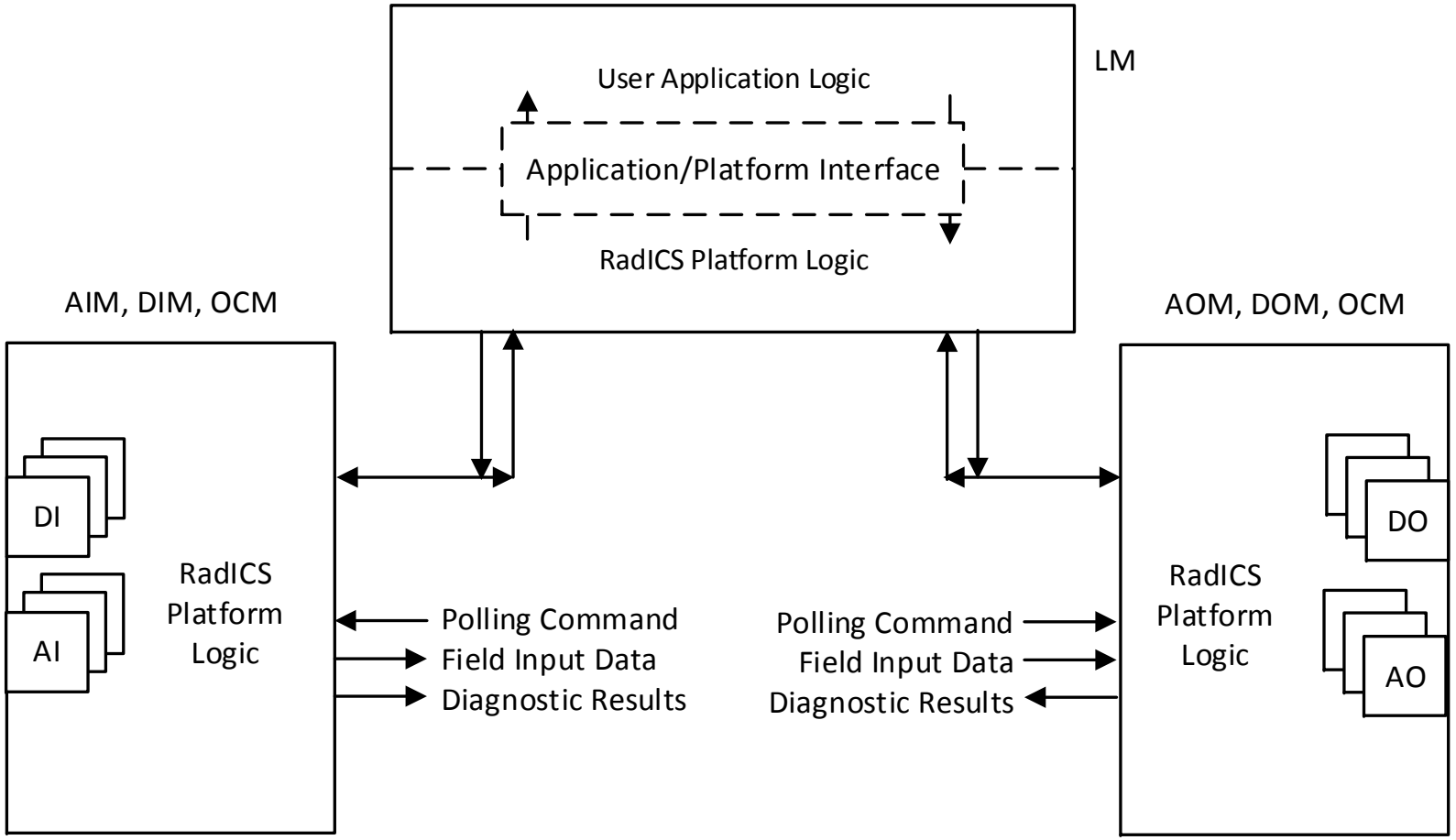
Modules FPGAs:

- Platform Electronic Design for all modules (i.e., standard programmable logic)
- Application Electronic Design for Logic Modules (i.e., project-specific programmable logic)

Radiy Product Configuration Toolset:

- Functional Block Library
- Separate libraries for platform and application

RadICS Platform Architecture



RadICS Platform General Attributes

- Fail-safe
- Fault-tolerance
- Diversity Capability
- Functional Isolation
- Determinism
- Self-diagnostic Testing
- Ease of Use
- Flexibility
- Modularity
- Scalability
- High Quality Development Process
- Secure Development and Operational Environment
- Maintenance Friendly

RadICS Platform Fundamental Safety Approach

- De-energize to trip
- Automatic Transitions to the Safe State
- Human Action to Leave the Safe State
- Safety Modules Only
- IEC SIL 3 Capacity by Design
- Application Logic Functionality
- Controlled Scope and Interfaces

RadICS Platform Maintainability and Operability

- On-line Monitoring
- Operational Parameter Tuning Capability
- Minimized Maintenance Error (e.g., Coding Pegs, I/O Cables Are Rear-connected)
- Hardware Protection
- Checking of User Configuration and Tuning Values
- User Safety Override
- Hot Swappable Modules (optional)
- Authentication of the RadICS Module Version

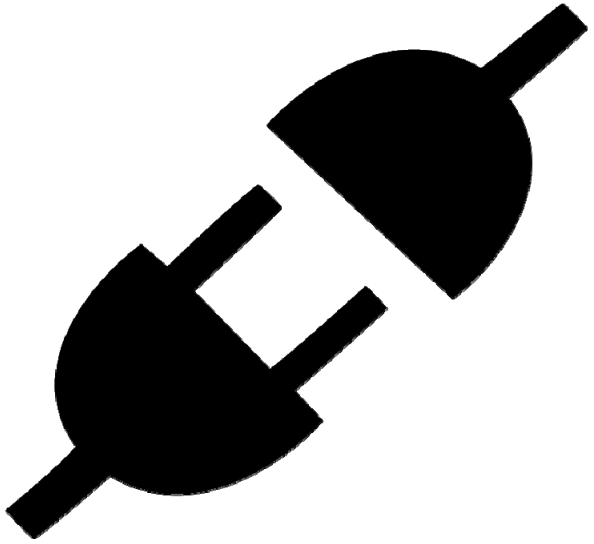
RadICS Module Architecture

- Modular Design
- 20 Standardized HW Units Used
- FPGA Executes Platform and Application Logic (Diagnostic)
- CPLD as Watchdog
- 2 Redundant 24 VDC Power Supply
- 3 Clock Domains
- LVDS Communication Lines
- Local Comprehensive Display System
- Safety Override Unit on Output Modules

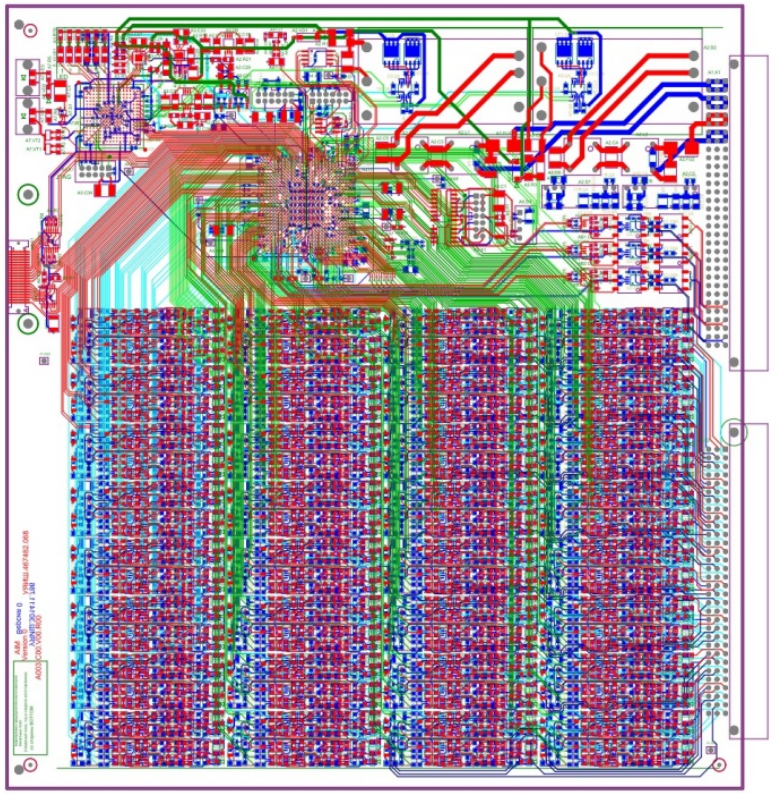
Hardware Design Principles

- Use components intended for safety applications or proven in use components (FPGAs qualified for SIL3)
- Operation experience and vendor safety recommendations are used in the process of components selection
- Use principle of sufficiency for the chips selection (plan required capacity, avoid unnecessary embedded features)
- More than 3 years on the market (without topology changes)
- Local HMI to provide details on current HW status

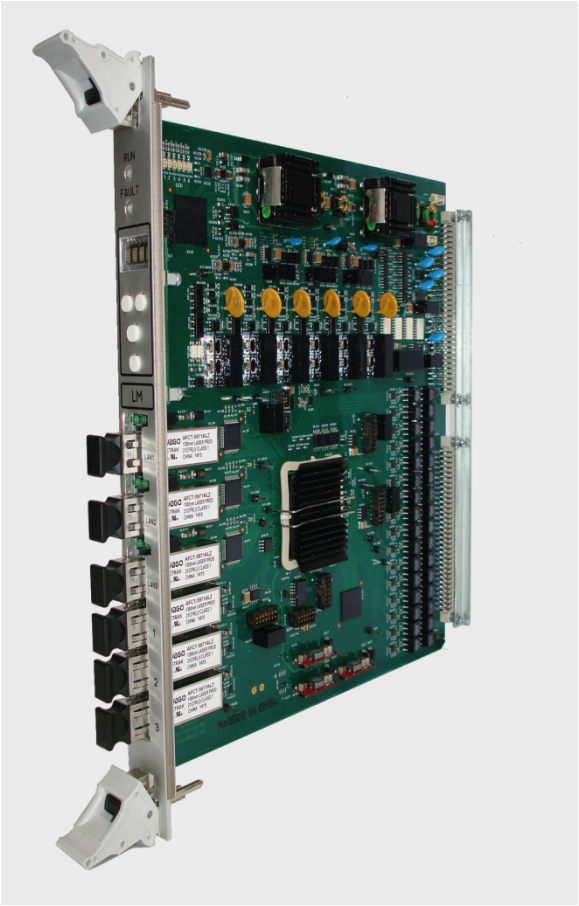
RadICS Platform System Interfaces



RadICS Modules



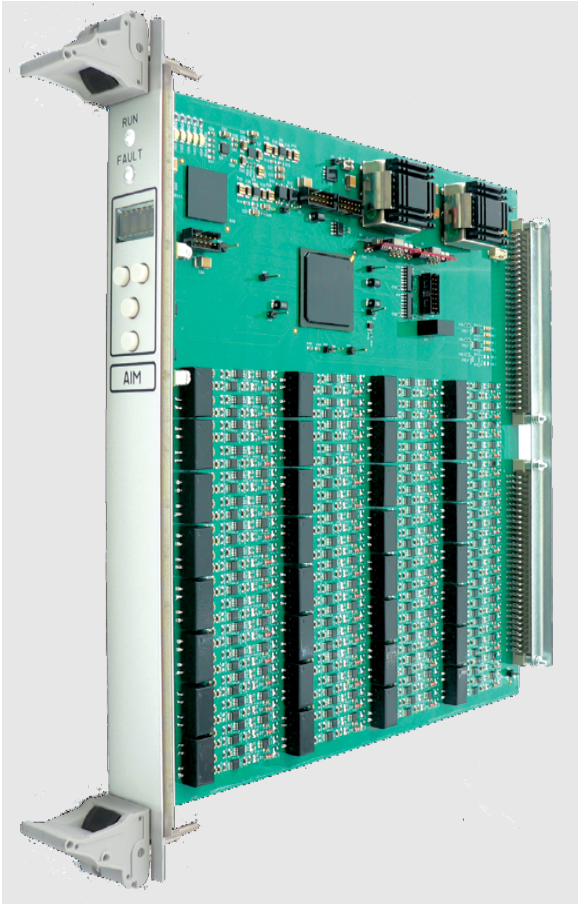
RadICS Modules (1/6)



Logic Module (LM)

- Dedicated SRAM FPGA chip for user configurable control logic
- Integrity checks on each communication line
- 14 LVDS full duplex lines for communication with OCM and I/O modules
- 3 galvanic-isolated discrete inputs (2 available, 1 reserved)
- 6 fast discrete outputs with embedded diagnostics of the outputs state
- 3 fiber optical lines for internal system communications
- 1 input for Tuning PC programming access key signal
- 3 Fast Ethernet (100 BASE-FX) optical communication lines

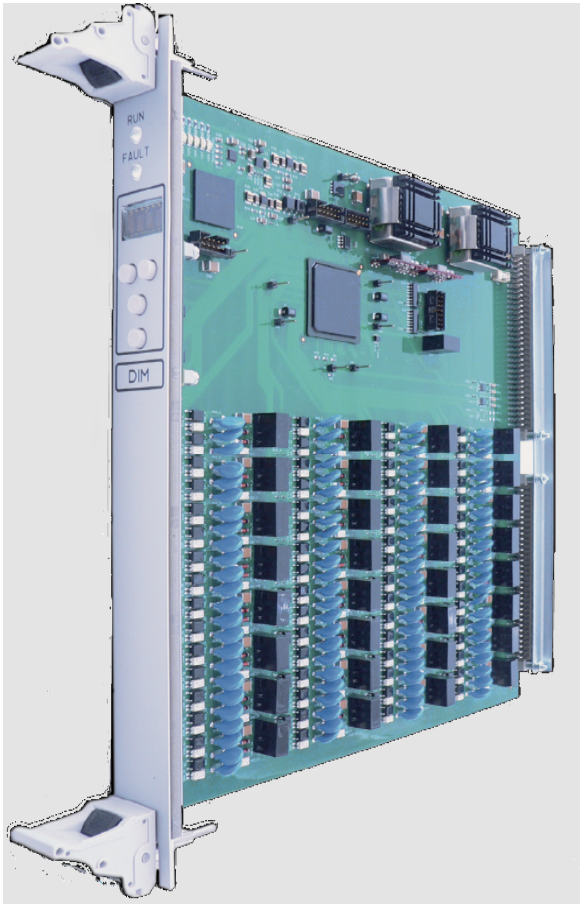
RadICS Modules (2/6)



Analog Inputs Module (AIM)

- Enhanced I/O diagnostics
- 32 independent analog input channels
- 18-bit analog/digital (A/D) conversion in each analog input channel
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Signal value accuracy – 0.15%
- Built-in calibration

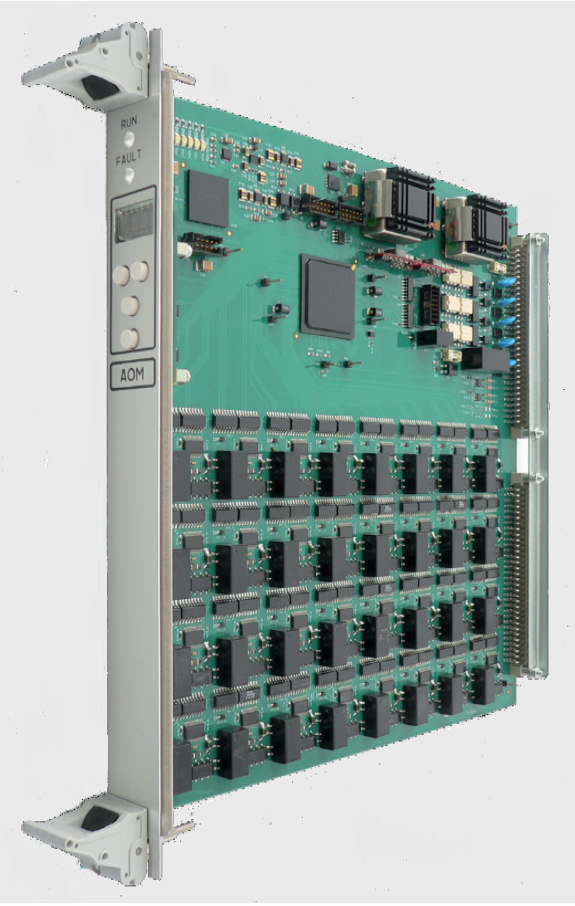
RadICS Modules (3/6)



Digital Inputs Module (DIM)

- Enhanced input diagnostics (i.e., shorted or broken load circuit detection)
- 32 independent discrete input channels (“dry” contact type)
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line

RadICS Modules (5/6)



Analog Outputs Module (AOM)

- Enhanced diagnostics of output channels
- 32 independent analog output channels
- 16-bit analog/digital (A/D) conversion in each channel
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Built-in calibration

RadICS Modules (5/6)

Digital Outputs Module (DOM)

- Enhanced active output diagnostics
- 32 independent digital form-A optic-relay isolated output channels (switching up to 48 V DC / 0.5 amp)
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Fuse and Overvoltage protected outputs

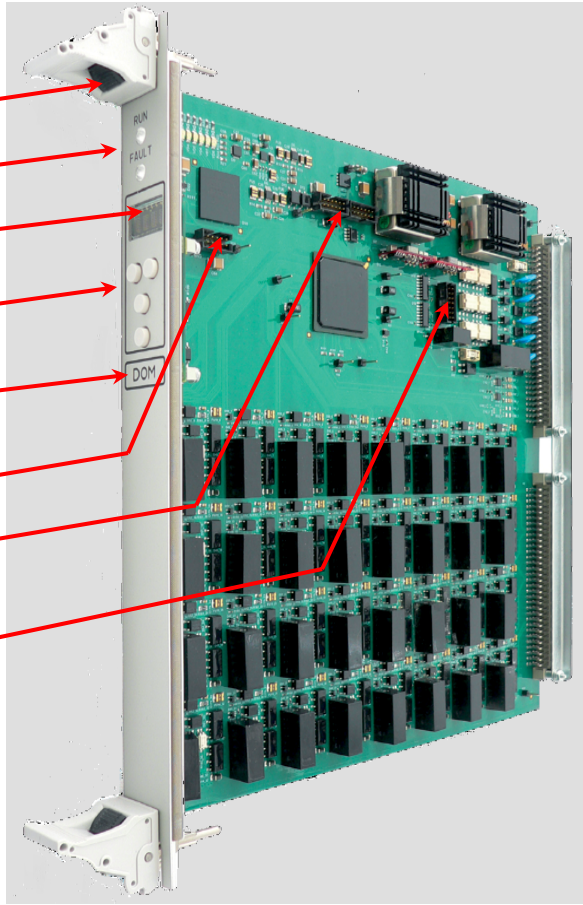
RadICS Modules (6/6)

Optical Communication Module (OCM)

- 5 fiber optical lines
- 2 Low-Voltage Differential Signaling (LVDS) lines (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- 5 RS-232 or RS-485 serial communication interfaces

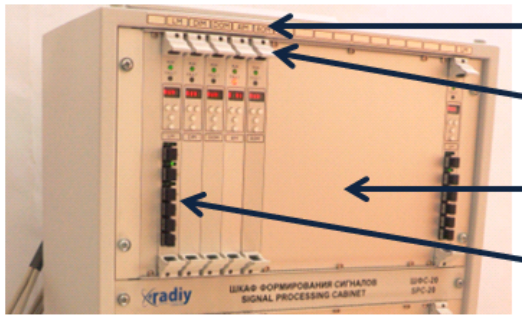
RadICS Modules Maintenance Features (1/2)

- Hold-down latches
- Status lights
- Display
- Pushbuttons
- Module type
- JTAG connector
- ASPI connector
- SPI connector



RadICS Modules Maintenance Features (2/2)

Maintenance Friendly Features



- Full insertion and complete clamp-down are visually verifiable
- All I/O cables are rear-connected

- Non-interfering local status display on every module
- Comprehensive diagnostics relayed to MATS
- Detection of some maintenance errors (e.g., wrong module in a slot)
- Hot-swap capability
- Validated maintenance documentation
- User Safety-Override

RadICS Platform Electronic Design Features

Non-Proprietary

Standardized Module Electronic Design

Electronic Design Architecture

- High level safety concept for Hardware Modules employed to meet target Safety Integrity Level (from IEC 61508)
  - No matter what configuration of modules is used, an individual module is designed such that failures that are both dangerous and undetected are limited to less than 10 percent
- RadICS design target is to meet same target for each Unit
- Units that are used on more than one module are standardized
  - Design strategy maximizes reuse of proven components and simplifies inter-operation of modules
- Electronic Design of each module performs self-diagnostics of the Units on the Module

Standardized Module Modes of Operation

LM Modes of Operation

Standardized Module Work Cycle

RadICS Platform Safety Features

RadICS Module Safety Features (1/3)

RadICS Module Safety Features (2/3)

RadICS Module Safety Features (3/3)

Tuning Mode Access Control

RadICS Platform Self-Diagnostic Features (1/5)

RadICS Platform Self-Diagnostic Features (2/5)

RadICS Platform Self-Diagnostic Features (3/5)

RadICS Platform Self-Diagnostic Features (4/5)

RadICS Platform Self-Diagnostic Features (5/5)

RadICS Platform Internal Diversity

- Functional Diversity
  - Segmentation of Hardware Units in Electronic Design
  - Separate Clock Domain for Self-Diagnostic Features
  - Separate Startup Checks
  - Independent Watchdog
- Technology Diversity
  - FPGA versus CPLD

Thank you for your attention!

Research & Production Corporation Radiy
29, Geroyiv Stalingrada Street, Kropyvnytskyi 25006, Ukraine
e-mail: a.andrashov@radiy.com
http://www.radiy.com