RadICS Digital I&C Platform

Anton Andrashov

Director, Radics LLC

Head of International Projects Division, RPC Radiy

2018 Plant Performance Symposium
August 15-16, 2018, Grand Targhee Resort, Alta, Wyoming




Agenda

- About “Radiy”
- Nuclear Organization
- Manufacturing and Qualification Test Facility
- Products for Nuclear Power Plants
- Product/Project Experience
- FPGA Technology
- RadICS Platform Overview
- RadICS Platform System Interfaces
- RadICS Platform Modules
- RadICS Platform Safety Features

About “Radiy”

- Main profile: FPGA-based I&C systems for NPPs, headquartered in Kropyvnytskyi, Ukraine
- 1250 employees, 350 engineers
- 23 years servicing the nuclear industry
- All internal processes: R&D, design, manufacturing, V&V, testing, EQ, training
- Supplies I&C equipment to: Argentina, Brazil, Bulgaria, Canada, France, Ukraine

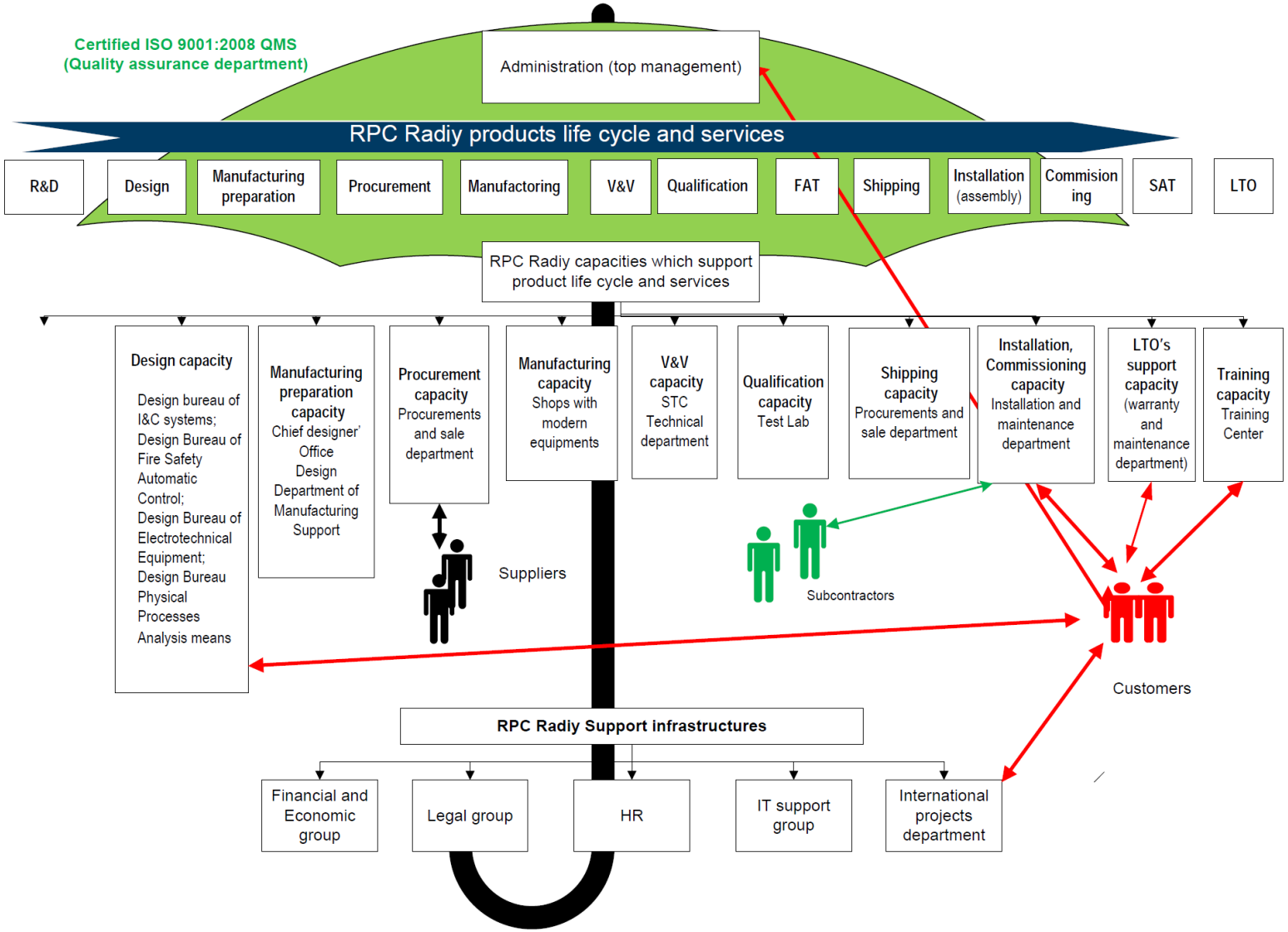
About “Radiy”

- 1954 – Company’s foundation. The main area of activity was connected with manufacturing of loudspeakers and electrical household products for consumers.
- 1976 – manufacturing of the equipment for television complexes, that provided television and radio broadcasting of the 1980 Olympic Games in Moscow.

About “Radiy”

- 1980 – Radiy participated in space exploration program “Buran - Energiya” (design and supply of the equipment for launch complex and Flight-Control Center).

Nuclear Organization



Manufacturing Test Facility

- Manufacturing and inspection facilities comply with Company Quality Management System (QMS) based on ISO 9001:2008 and applicable IEC and IPC Standards

Automated production line for PCB surface mounting

X-ray inspection system for real time inspection of solder joints

Qualification Test Laboratory

Qualification Test Laboratory

- Radiy Qualification Test Facility certified to ISO/IEC 17025:2005
  - Environmental and Seismic Capabilities

Electrodynamic Vibration Table V875-440 HBT Combo, LVD

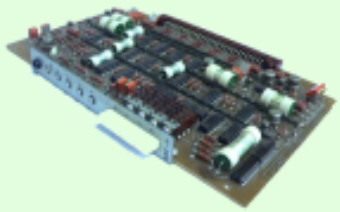
Climatic thermal pressure chamber KTBV 8 1

- Kinectrics test laboratory was used for RadICS Platform qualification testing

Radiy Product Evolution

1995

Started development and supply of the equipment for NPP I&C systems



Replacement of obsolete NPP I&C modules

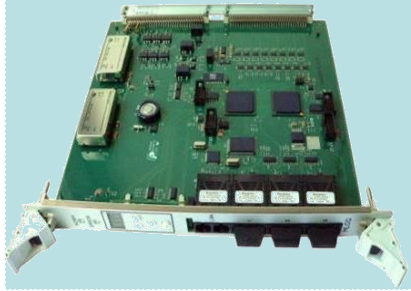
1998

First generation of equipment for NPP I&C systems

FPGA-based I&C systems for NPP

2002

Second generation of equipment for NPP I&C systems



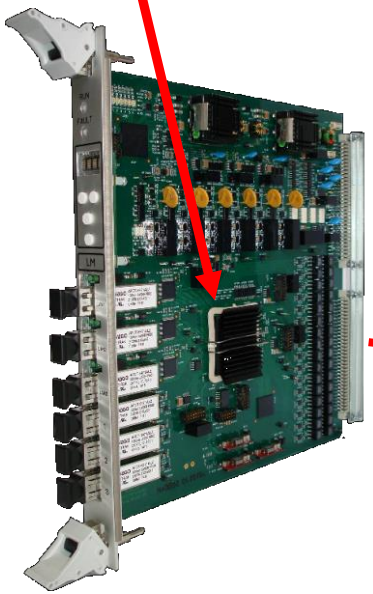
FPGA-based I&C platform for NPP

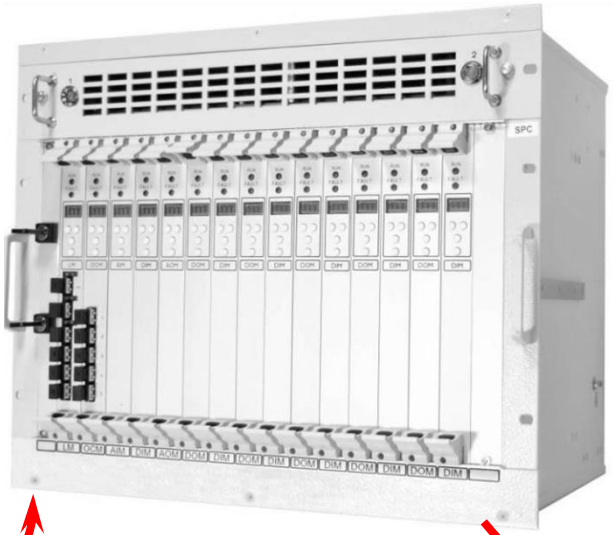
2014

Third generation of equipment for NPP I&C systems

SIL3 certified FPGA-based I&C platform for NPP

RadICS Platform Equipment





Modernization experience

Radiy implemented > 100 digital I&C modernization projects

NPP I&C before upgrade by Radiy

NPP I&C after upgrade by Radiy

Modernization of Ukrainian NPPs

Total Gross Capacity: 13,835 MW
4 sites
15 units
2 units under construction

Top 5 of Europe
Top 10 of the World
About 50% of national power generation
One utility: National company NNEGC "Energoatom"
http://www.energoatom.kiev.ua/
Regulatory Authority: State Nuclear Regulatory Inspectorate of Ukraine
http://www.snrc.gov.ua/nuclear

Product/Project Experience

Systems Supplied	Nuclear Power Plant	Number of Installed Systems	Installation Years
Reactor Trip System	Zaporozhye NPP; South-Ukraine NPP; Rivne NPP; Khmelnitski NPP	30	2004-2015
Reactor Power Control and Limitation System	Zaporozhye NPP; South-Ukraine NPP; Rivne NPP; Khmelnitski NPP	12	2004-2018
Engineered Safety Feature Actuation System	South-Ukraine NPP, Rivne NPP, Kozloduy NPP, Bulgaria	21	2005-2018

exida

The manufacturer may use the mark:

exida CERTIFIED IEC 61508 SIL 3 CAPABLE

Revision 1.4 May 18, 2016
Surveillance Audit Due
February 1 , 2019

ANSI

ANSI Accredited Program
PRODUCT CERTIFICATION
#1004

Certificate / Certificat
Zertifikat / 合格証

RAD 1406037 C001

exida hereby confirms that the:

FPGA-Based Safety Controller (FSC) RadICS
produced by **RPC Radiy**
29 Geroyiv Stalingrada Street
Kirovograd, Ukraine

Has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT=0; Route 1_H

PFD_{AVG}, PFH and Architecture Constraints must be verified for each application

Safety Function:
The FSC will read input signals, perform user-defined application layer logic and write results to the output signals within the stated response time.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

Evaluating Assessor

Certifying Assessor

Page 1 of 2

FPGA-Based Safety Controller (FSC) RadICS

exida

64 N Main St
Sellersville, PA 18960

T-002, V3R9

Certificate / Certificat / Zertifikat / 合格証

RAD 1406037 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT=0; Route 1_H

PFD_{AVG}, PFH and Architecture Constraints must be verified for each application

Systematic Capability :

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

For failure rates, see the Safety Manual.

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD_{AVG} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

SIL3 in single channel configuration

Note: IEC SIL is different than IEEE Std 1012 SIL

The following documents are a mandatory part of certification:
Assessment Report: RAD 14-06-037 R002 V1R4 61508 Assessment - FSC
Safety Manual: D11.1 – Radiy FSC Product Safety Manual

Page 2 of 2

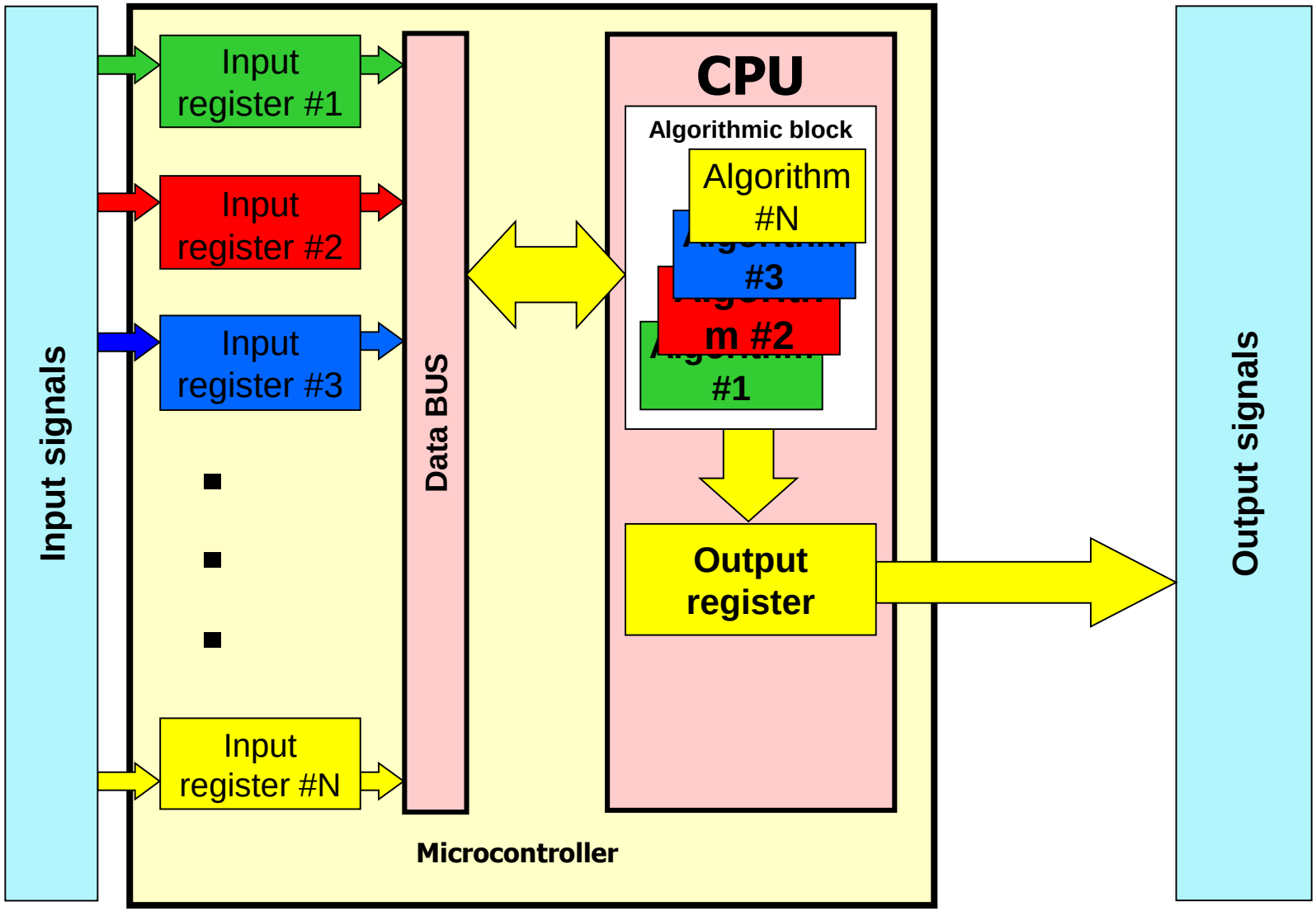
Development and Certification of FPGA-based Safety Platform RadICS (SIL 3 Requirements)

FPGA Technology

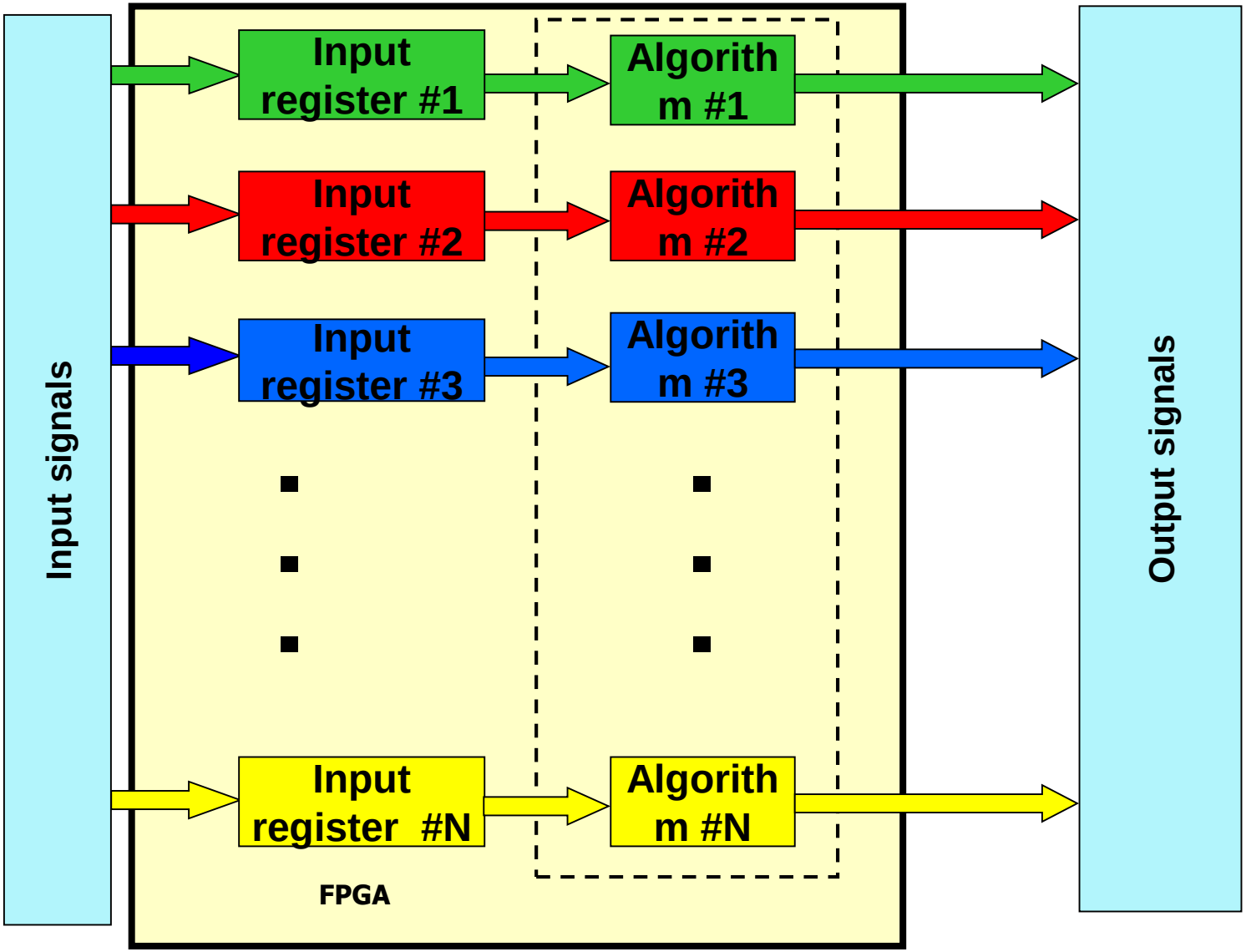
FPGA (Field Programmable Gate Array) is a semiconductor device that can be programmed after manufacturing

- FPGA integrated circuit is a hardware
- features and functions of this hardware are programmed i.e. configured by means of hardware description language (HDL)
- configuration (FPGA electronic design) can be updated even after the product has been installed

FPGA Technology (CPU based PLC)



FPGA Technology (FPGA based PLC)

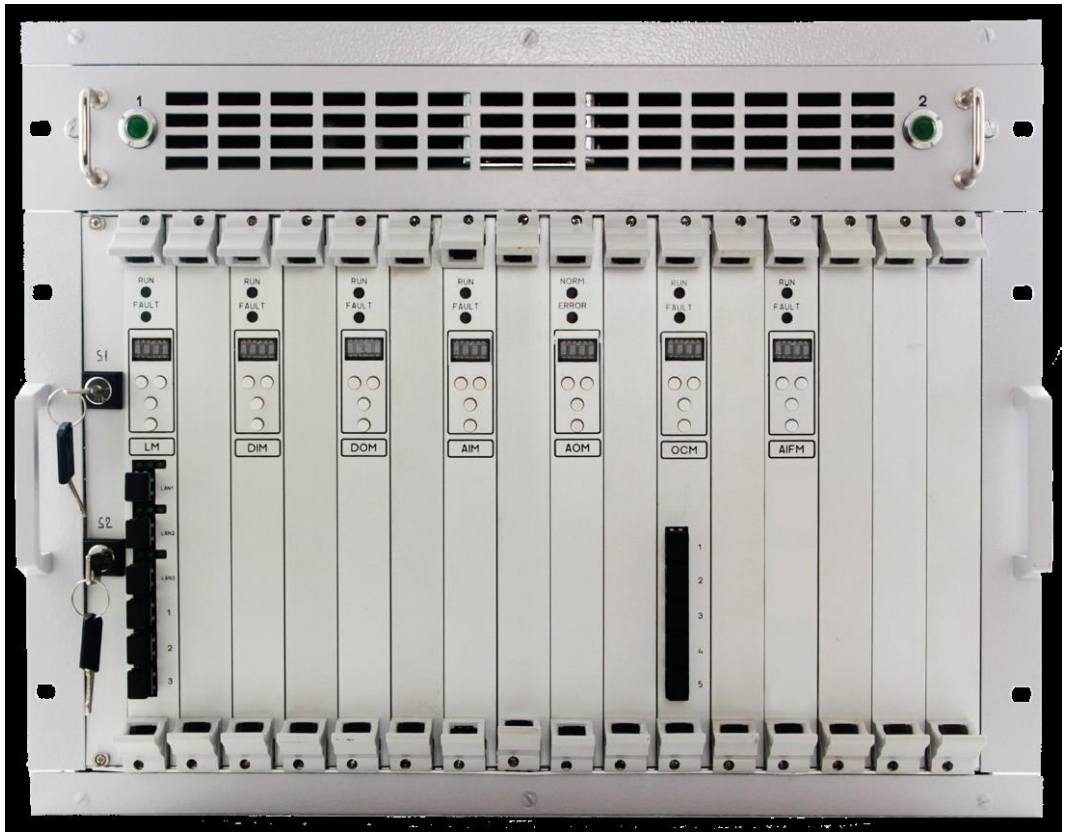


FPGA Technology benefits

- No Operating System
  - Less complexity (Radiy uses flat HW logic)
  - Less footprint for cyber attracts
- Parallel data processing
  - Faster response time (up to 5 ms)
  - Functional separation (Safety functions v.s. Diagnostic functions)
- Design portability

RadICS Platform Overview

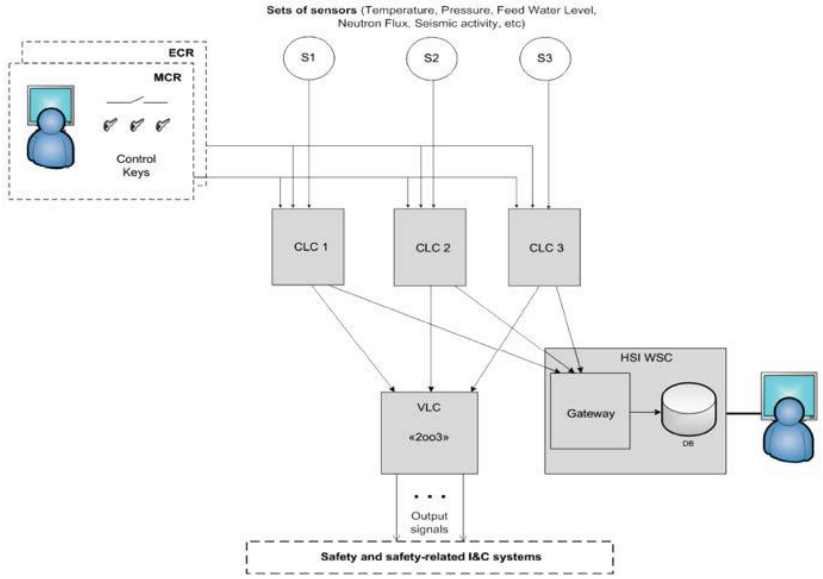
- Equipment fully qualified to NRC requirements for use in US safety related applications
- Flexible and scalable system design architecture for any size and type of I&C system
- Fast and deterministic performance using modern FPGA technology. Response times as fast as 5 milliseconds!
- Comprehensive self-diagnostics ensure safety-critical functions, with fail safe design features



Typical System Configurations

Configuration Flexibility:

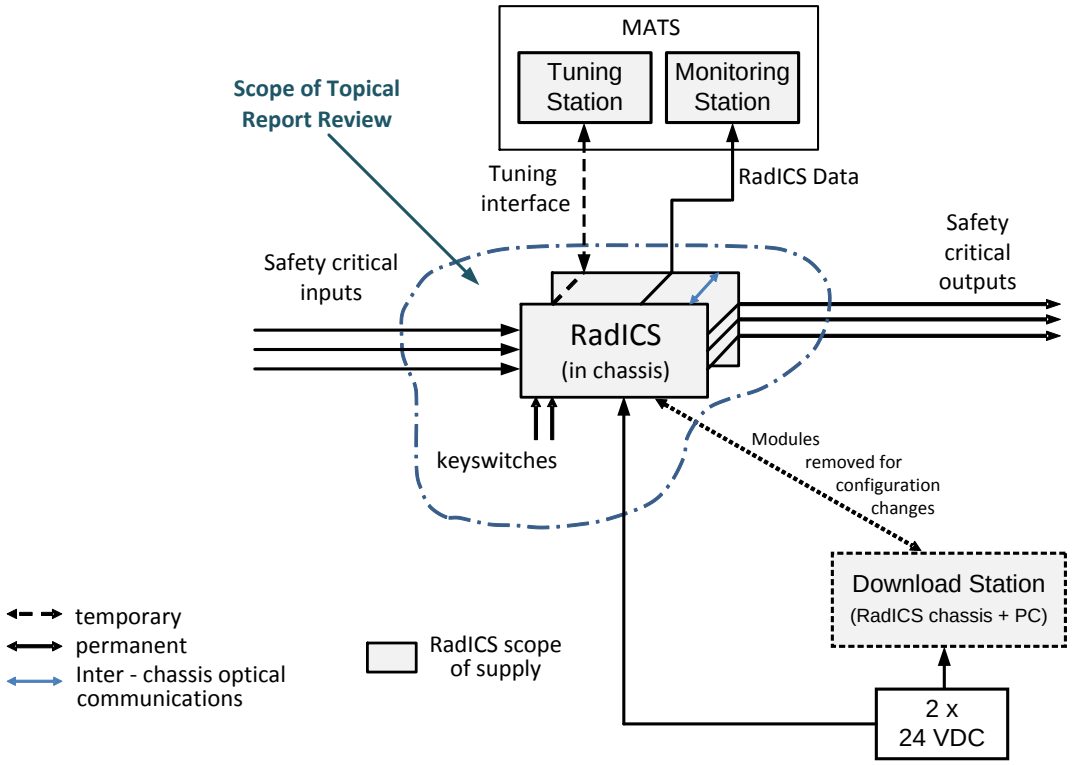
- 2, 3, or 4 channel systems
- Separate trip processing and voting layers



Used for Safety I&C Systems:

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

RadICS Platform Context



Modules FPGAs:

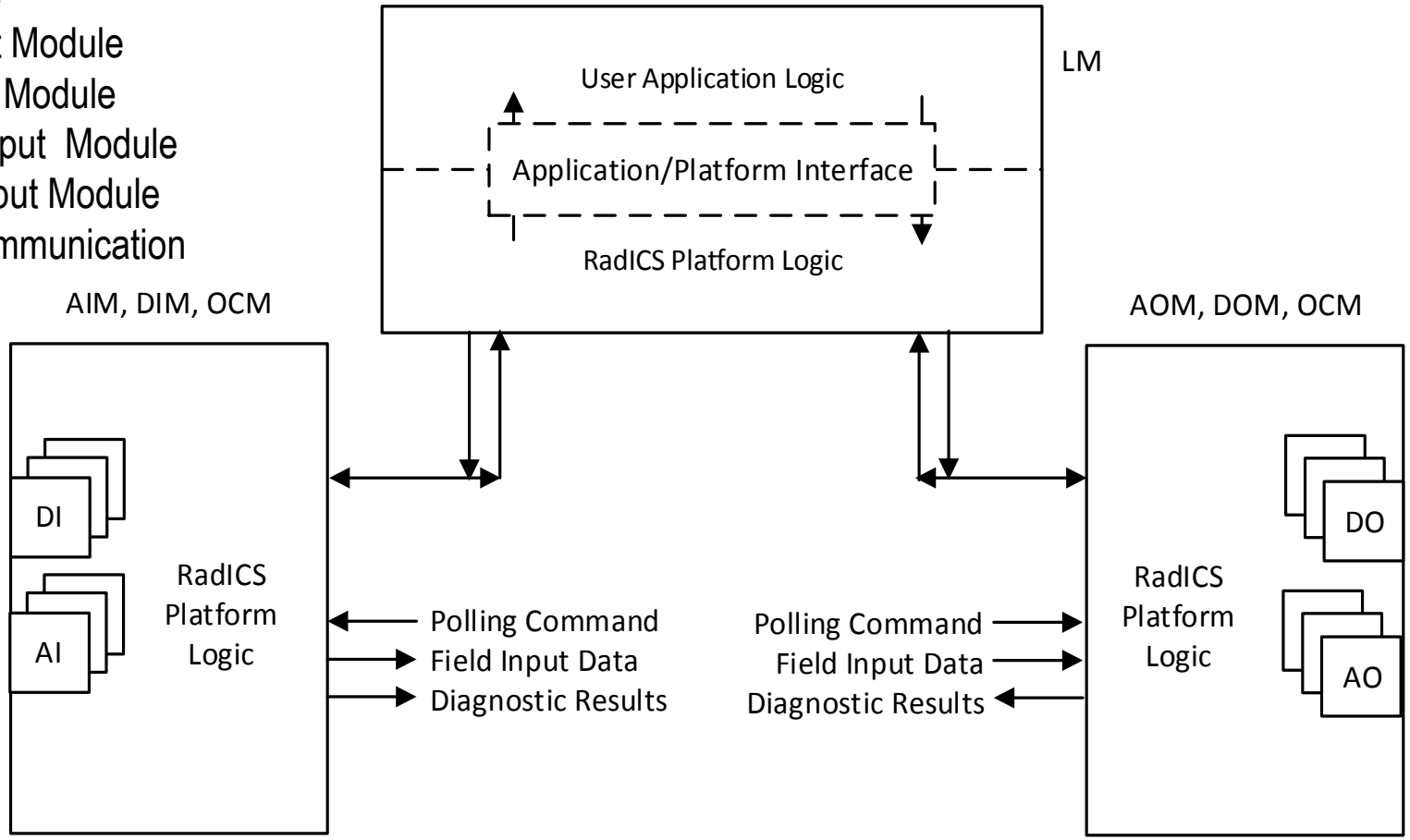
- Platform Electronic Design for all modules (i.e., standard programmable logic)
- Application Electronic Design for Logic Modules (i.e., project-specific programmable logic)

Radiy Product Configuration Toolset:

- Functional Block Library
- Separate libraries for platform and application

RadICS Platform Architecture

LM – Logic Module
AIM – Analog Input Module
DIM – Digital Input Module
AOM – Analog Output Module
DOM – Digital Output Module
OCM – Optical Communication Module



RadICS Platform General Attributes

- Fail-safe
- Fault-tolerance
- Diverse
- Functional Isolation
- Deterministic
- 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

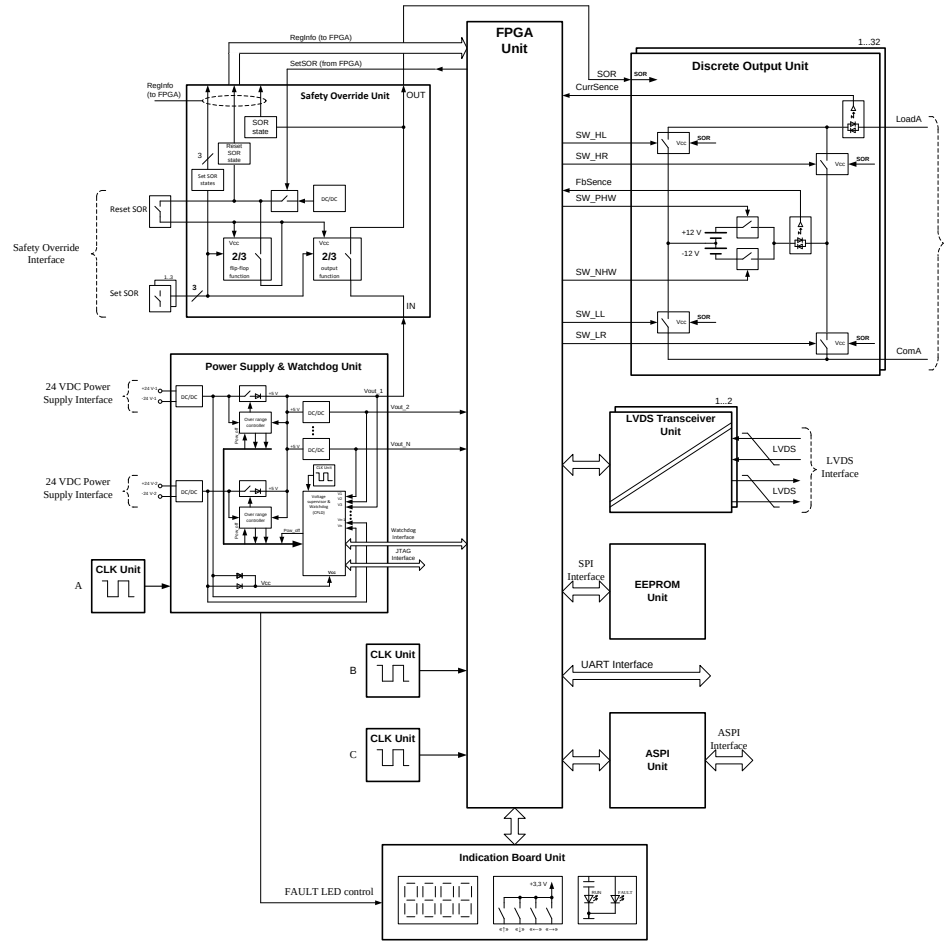
- De-energize to trip
- Automatic Transitions to the Safe State
- Human Action to Leave the Safe State
- Safety Modules Only
- IEC SIL 3 Capacity by Design
- Application Logic Functionality
- Controlled Scope and Interfaces

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 Overvoltage\Overcurent Protection
- Checking of User Configuration and Tuning Values
- User Safety Override
- Hot Swappable Modules
- Authentication of the RadICS Module Version

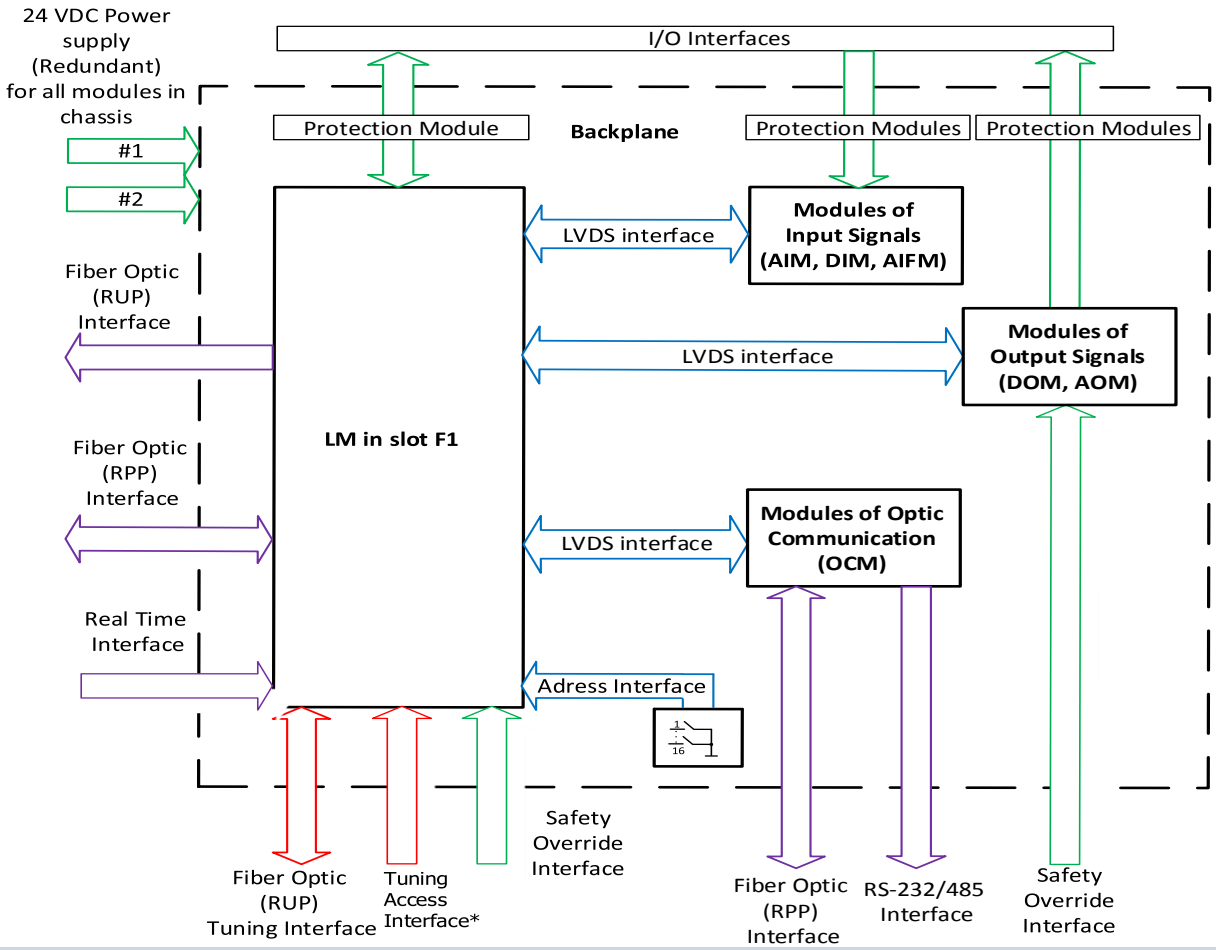
RadICS Module Architecture

DOM



- 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 Logic and Output Modules

RadICS Platform Interfaces

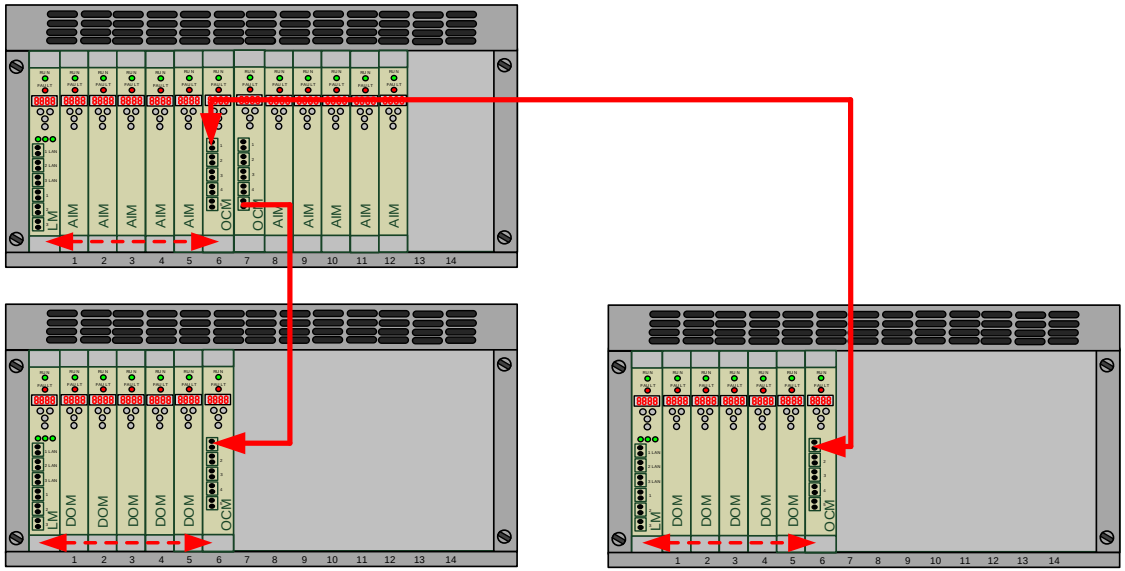


Interfaces:

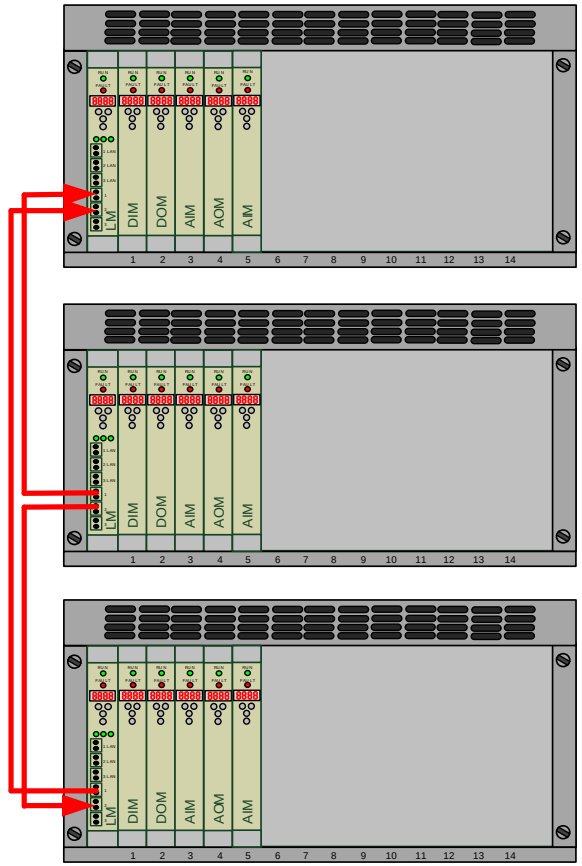
- External
- Internal
- Online
- Offline

RadICS Platform System Interfaces

- Typical System Interfaces



Data flow within the chassis
Data flow between chassis



Data flow between chassis

RadICS Platform Communication Features (1/2)

Communications

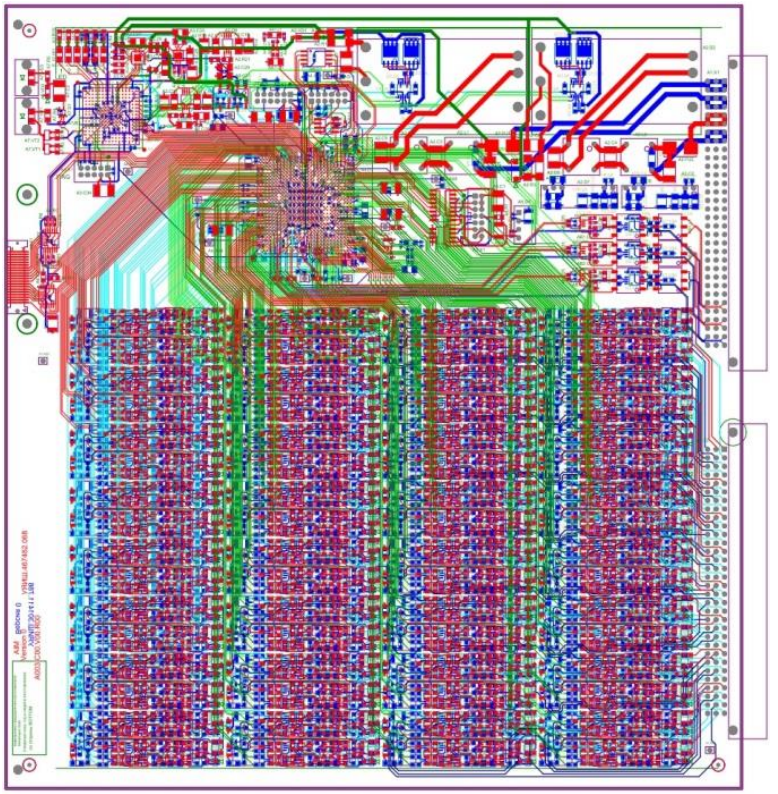
- Low-Voltage Differential Signaling (LVDS) Interface
  - Safety-related communications with other modules within same chassis based on dedicated slot-to-slot (point-to-point) connections between predefined specific slot locations
  - Logic Module (LM) has a dedicated slot so that it does not require any additional address information to communicate with any other modules within the same chassis
  - I/O Modules can communicate only with the LM within the same chassis
  - Four physical lines to provide fully independent full duplex differential communications in both directions for each link
  - Backplane communications is safety-related and designed as a SIL 3 black-channel

RadICS Platform Communication Features (2/2)

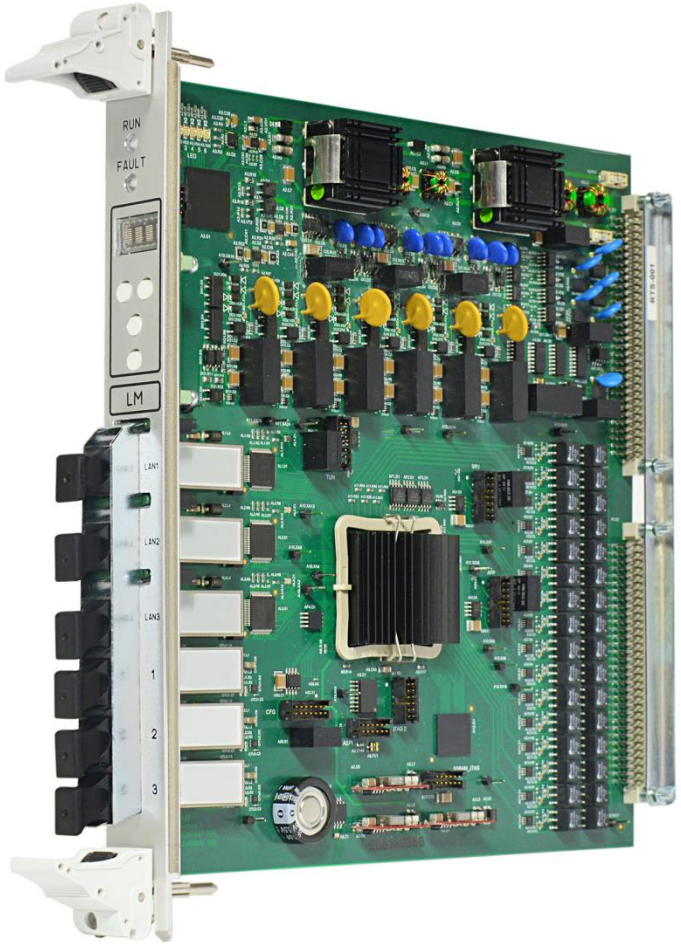
Communications

- LM-to-LM Fiber Optic (RPP) Interface
  - Safety-related communications with other LMs outside chassis (i.e., for voting) based on dedicated OCM to OCM
  - Uses Radiy Proprietary Protocol for communication
- LM-to-MATS Fiber Optic Interface
  - One-way non-safety broadcast to MATS using UDP-based interface (RUP) protocol
- Tuning Interface with Tuning PC
  - One bidirectional fiber optic link using the proprietary Radiy Tuning Interface (RTP)
  - Includes a safety-related special discrete input to de-energize RTP Fiber Optic Interface to LM based on state of Arming

RadICS Modules



RadICS Modules (1/6)



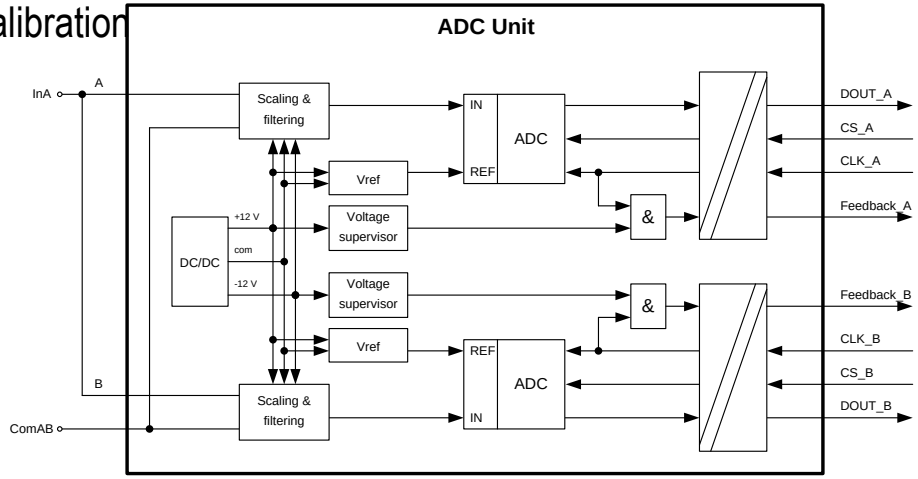
Logic Module (LM)

- 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

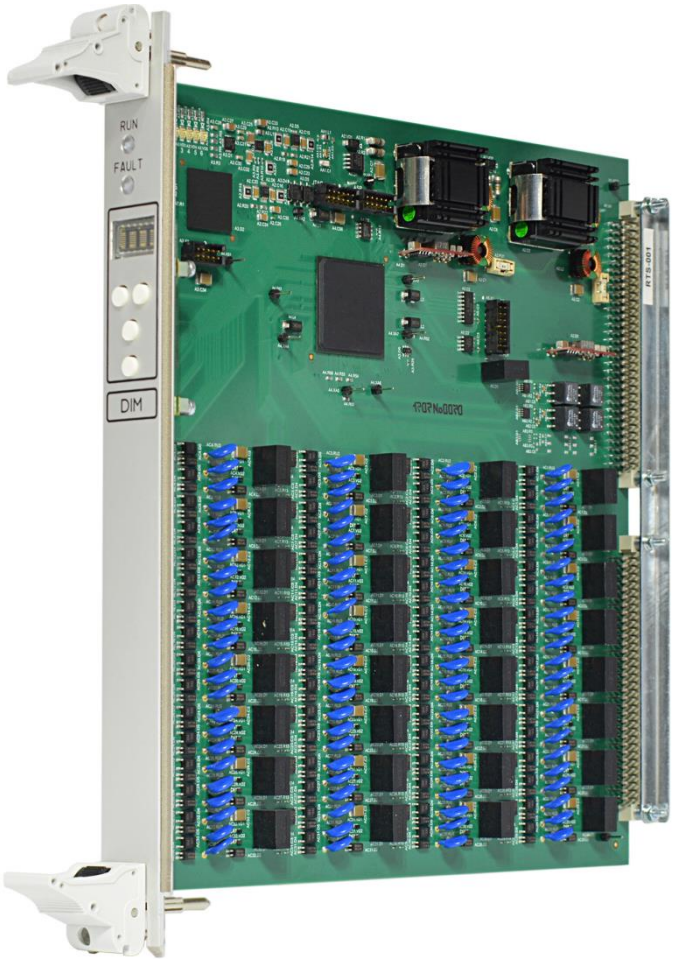
RadICS Modules (2/6)

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 – 0.04%
- Built-in calibration

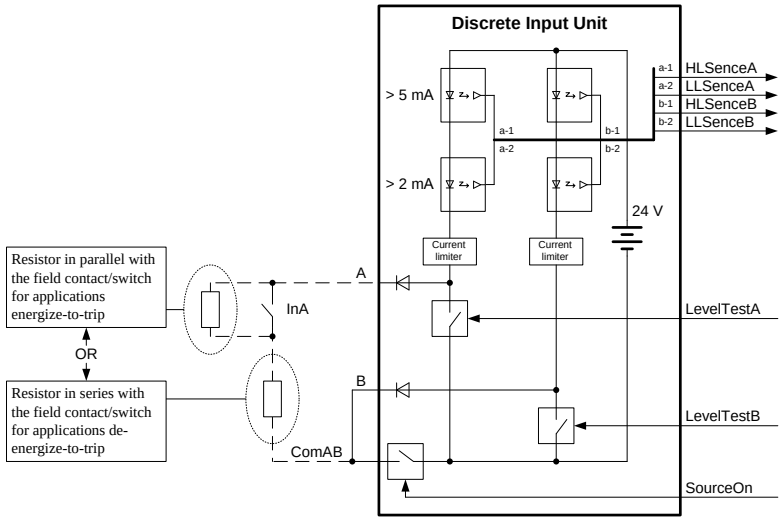


RadICS Modules (3/6)

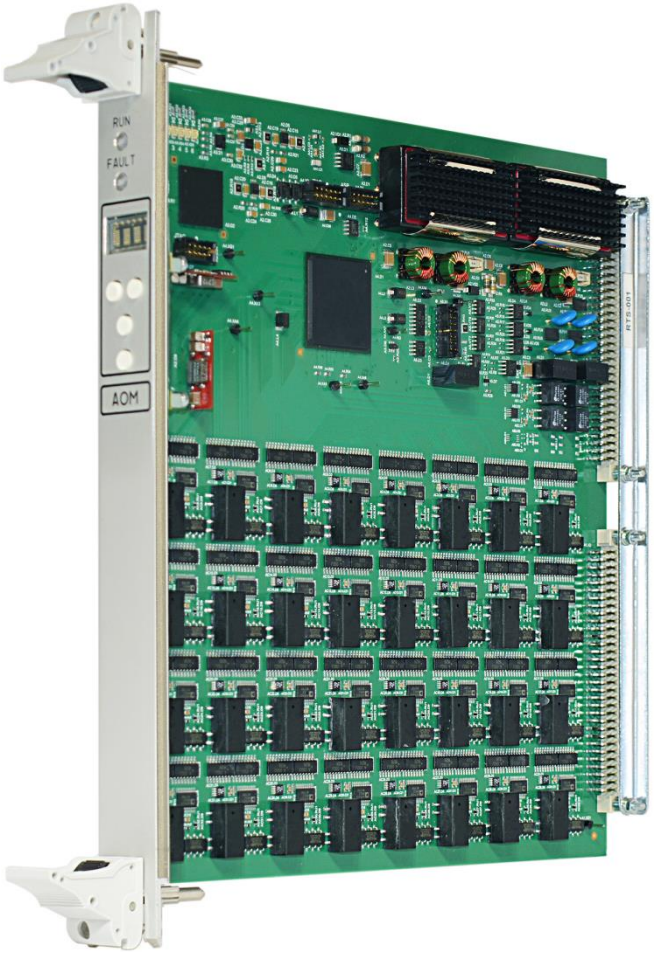


Digital Inputs Module (DIM)

- 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

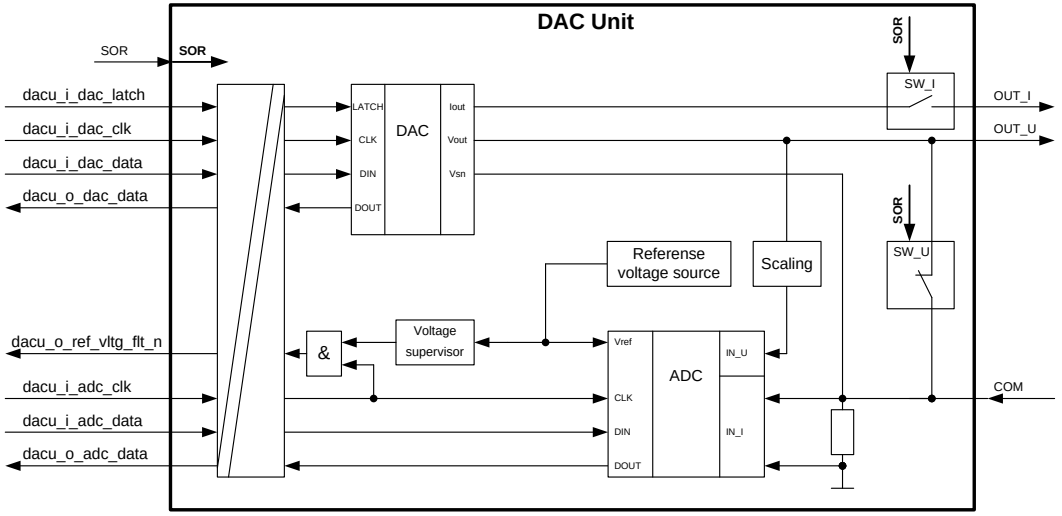


RadICS Modules (5/6)

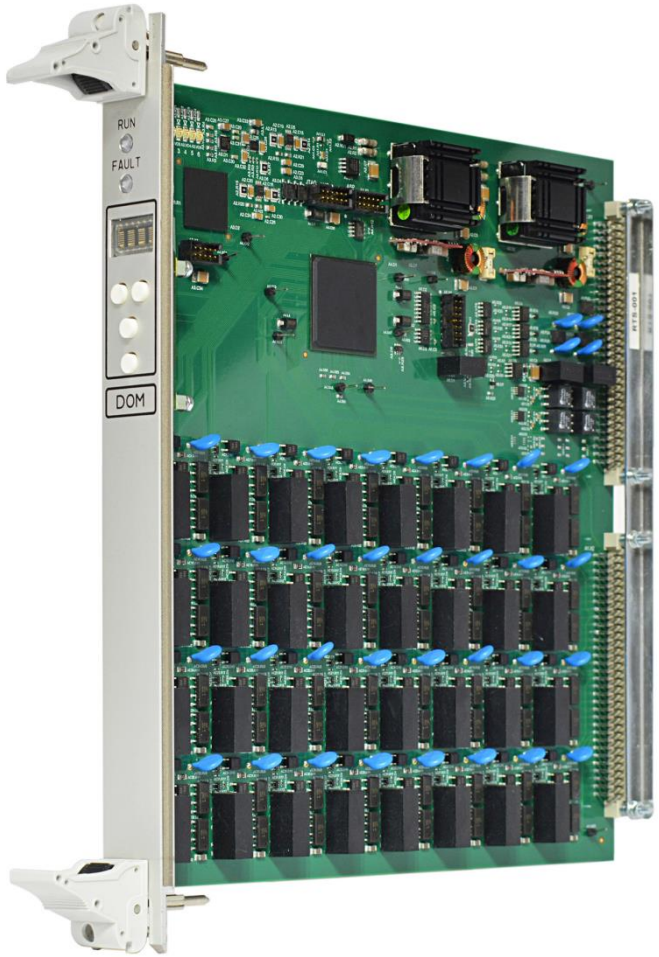


Analog Outputs Module (AOM)

- 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

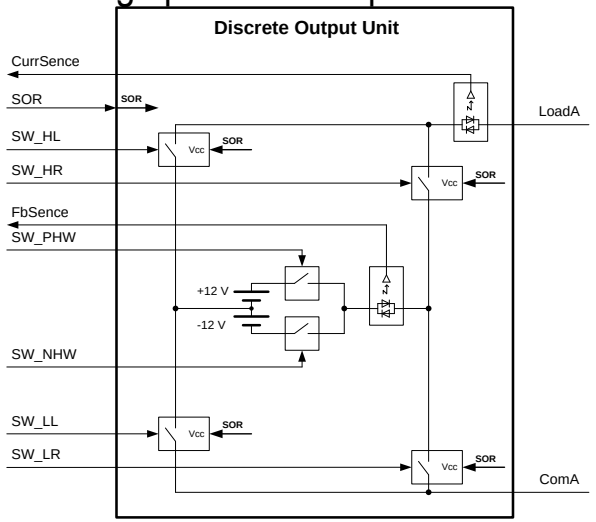


RadICS Modules (5/6)



Digital Outputs Module (DOM)

- Enhanced active output diagnostics
- 32 independent digital form-A optic-relay isolated output channels (switching up to 48 V DC / 0.2 amp)
- 2 LVDS (redundant diagnostic and control data exchange)
- Integrity checks on each communication line
- Fuse and Overvoltage protected outputs

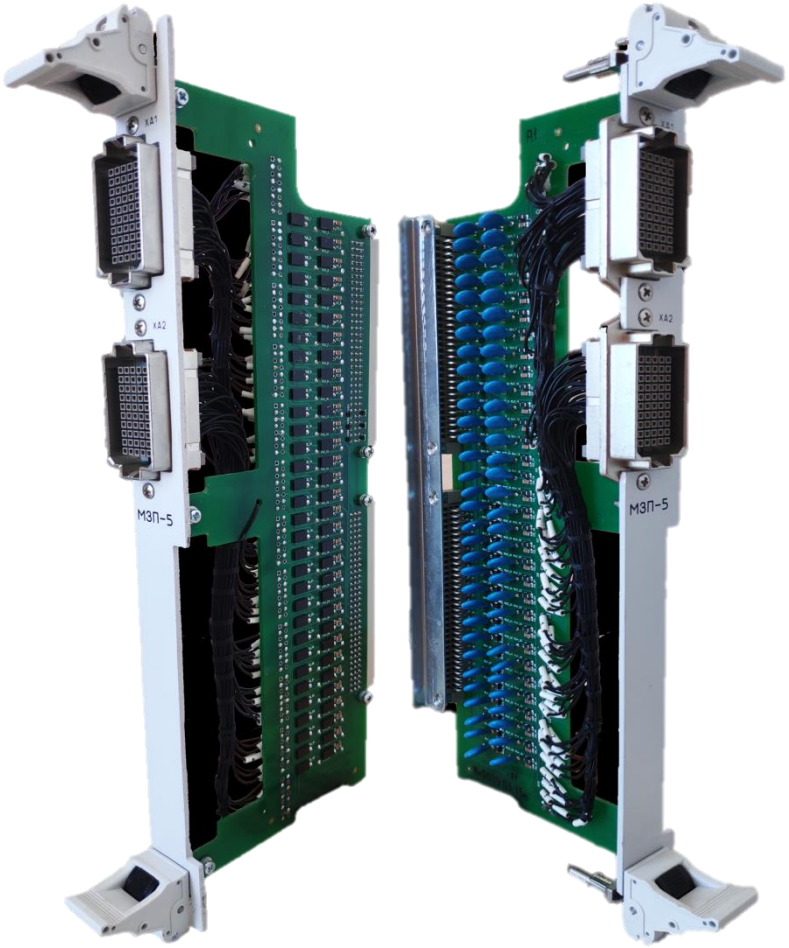


RadICS Modules (6/6)

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 (one way only)

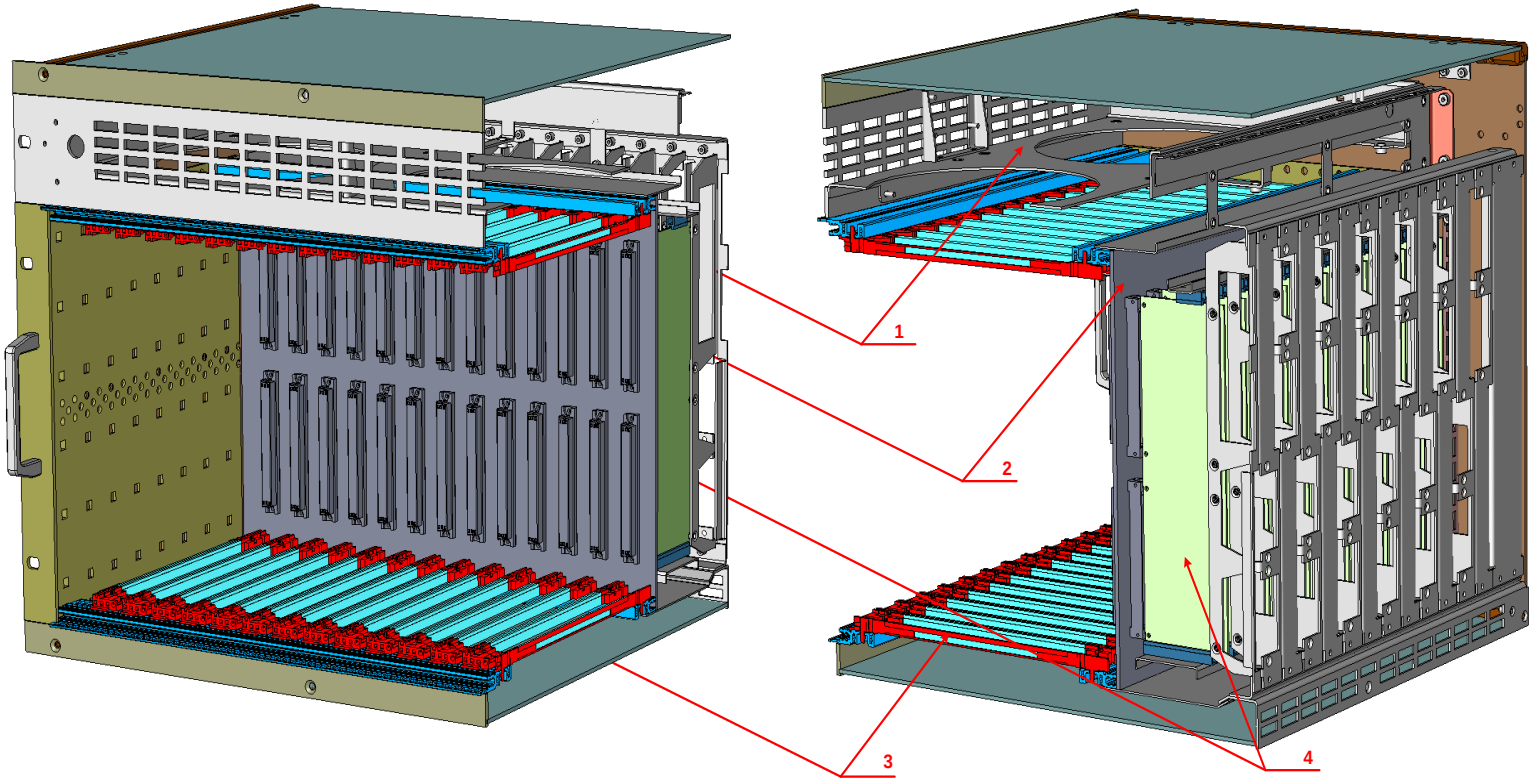
RadICS Input Output Connections Protection Module (IOPM)



Input Output Connections Protection Module (IOPM)

- Compatible with AIM, DIM, AOM, DOM
- Provides field I/O connection
- Overvoltage and overcurrent protection
- Only passive components are used

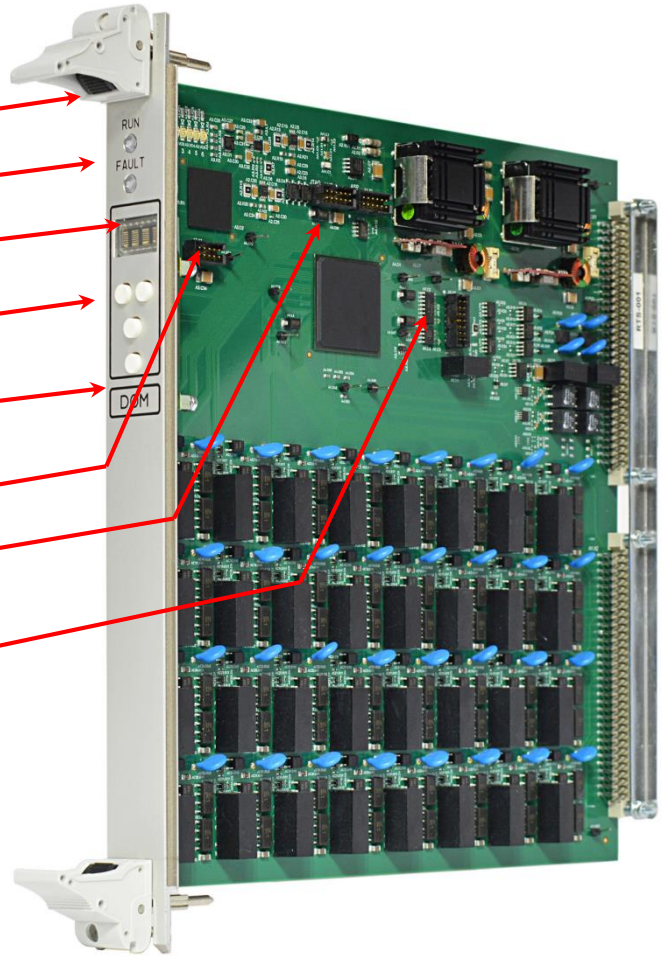
RadICS Platform Chassis



1 – Slots for fans
2 – Backplane
3 – Rails for modules
4 – Protection modules

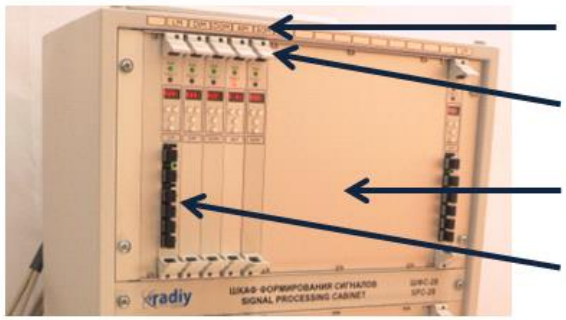
RadICS Modules Maintenance Features (1/2)

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



RadICS Modules Maintenance Features (2/2)

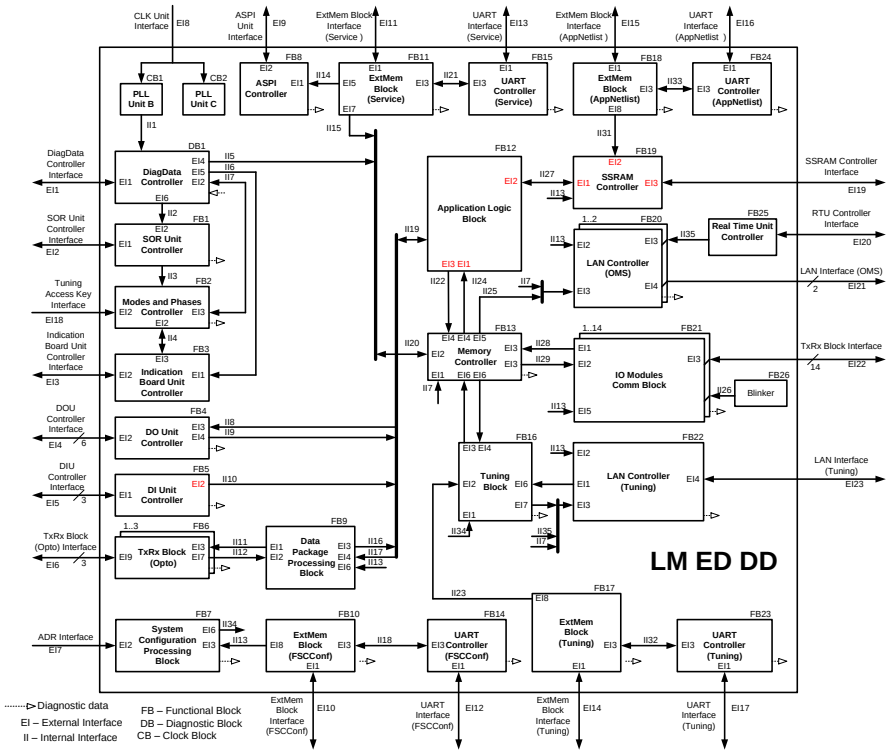
Maintenance Friendly Features



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

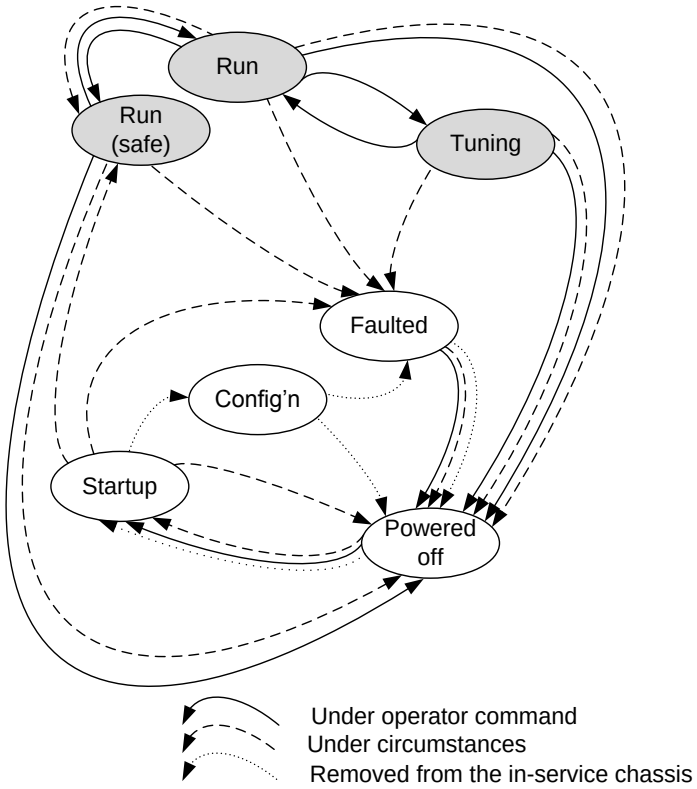
- Non-interfering local status display on every module
- Comprehensive diagnostics relayed to MATS
- Detection of some maintenance errors (e.g., wrong module in a slot)
- Hot-swap capability
- Validated maintenance documentation
- User Safety-Override

RadICS Platform Electronic Design Features



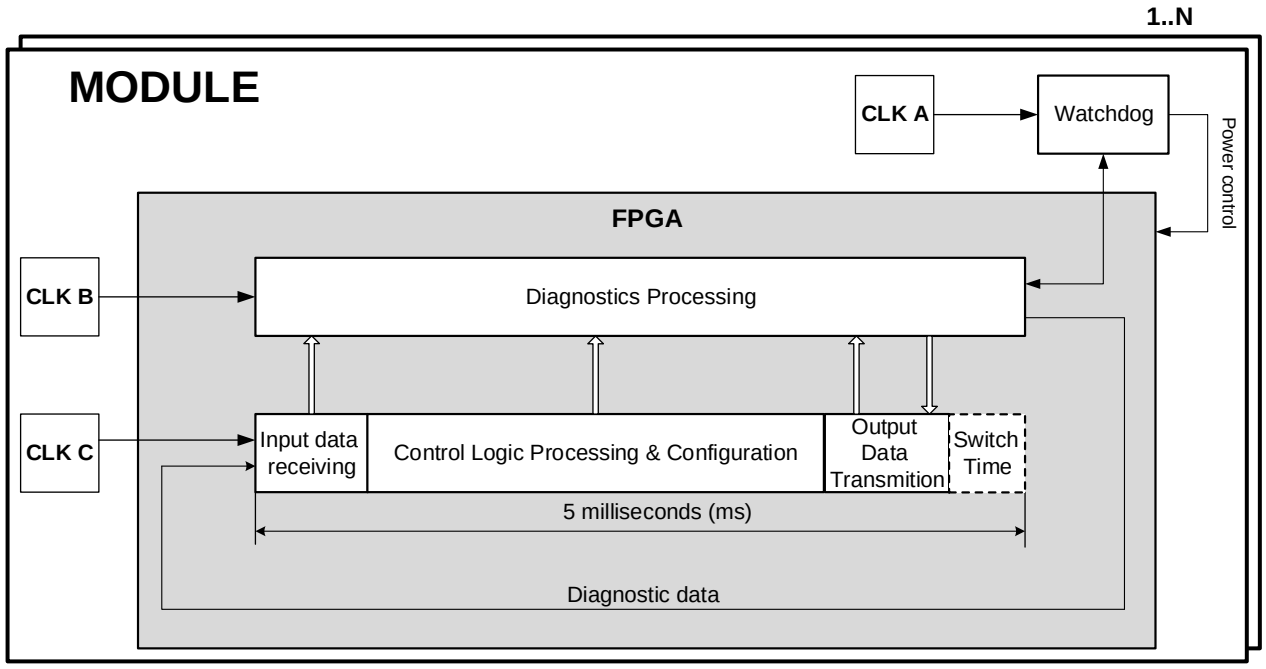
Standardized Module Modes of Operation

LM Modes of Operation



POWERED-OFF	Removal of power from Module by human action or by loss of the power sources .
START-UP	FPGA acquires configuration from EEPROM . Starts normal operation and performs all RUN mode self-diagnostic tests plus some extra tests. Failures result in exit to FAULTED mode. If no failures, modules exit to RUN (SAFE) or RUN mode (depending on the module). It is possible for operator to trigger exit to CONFIGURATION mode.
RUN(SAFE)	Application logic running, but outputs are overridden by Safety Override (SOR) and maintained in safe state. Operator intervention required to advance to RUN mode. This mode not used for input modules (since no field outputs).
RUN	Application logic running and controlling outputs. RUN mode self-diagnostic tests are executed.
TUNING	Parameters defined in application logic design can be adjusted by connecting a PC with special software. Tuning mode requires TUNING key and a contact that comes from end-user downstream safety logic that indicates it is locked into safe state (controlled by ARMING key). Permits the end user to fully test tuning changes under safe conditions.
FAULTED	All outputs are forced to safe state. Only exit from this mode is via powering off the RadICS Platform.
CONFIGURATION	Changes to Application Logic or configuration of RadICS Platform have to be made in a chassis equipped for this purpose, called Download Station (DLS). All modules also store authentication data in EEPROM which includes version information. Analog modules (AIM and AOM) use this mode to perform hardware calibration. Calibration can be done in in-service chassis, but application designer must design logic to ensure safety during calibration. Calibration can also be performed in the DLS.

Standardized Module Work Cycle



Work Cycle Phases

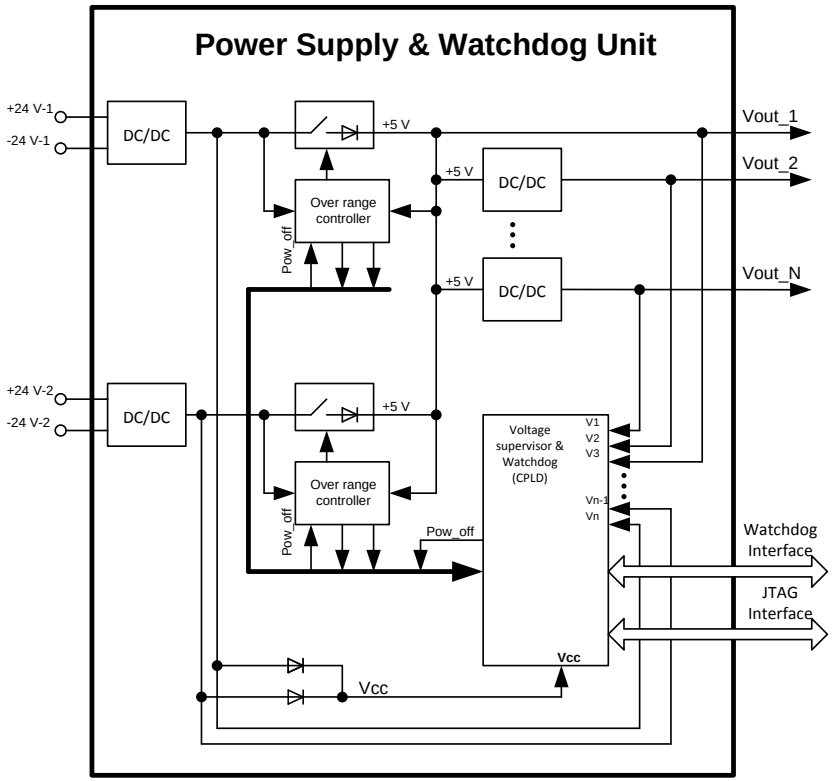
- Input Data Receiving (1 ms)
- Application Logic Processing (2.5 ms)
- Output Data Transmission (1 ms)
- Switch Time (0.5 ms)

Module Clocks

- 3 separate clocks (reference quartz oscillator)
- Clocks not controlled by Electronic Design
- Clocks are compared to verify health of clocks and Module
- Goes into FAULTED mode if clocks disagree

RadICS Platform Safety Features

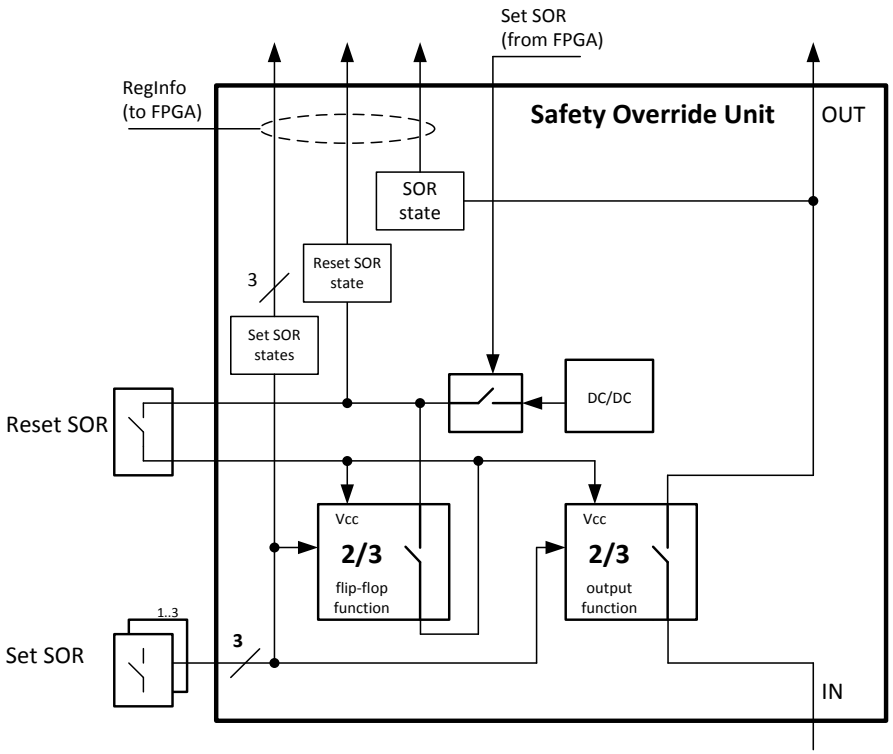
RadICS Module Safety Features (1/3)



Power Supply and Watchdog Unit (PSWD)

- Receive heartbeat of FPGA Unit and de-energize module if its heartbeat is absent
  - Sequence monitoring for FPGA based on a diverse (FLASH-based) CPLD and independent clock
- Receive configuration RAM error signal from FPGA and de-energize module if CRAM error detected
- Check the various voltages and shut off power, causing a safe state, if any are out of range high or low
- If self diagnostic Type I faults are detected, module power supply voltages shall cut-off
- Monitors temperature and provides a diagnostic signal (temperature value) to the FPGA Unit for alarm signal transmission to MATS

RadICS Module Safety Features (2/3)

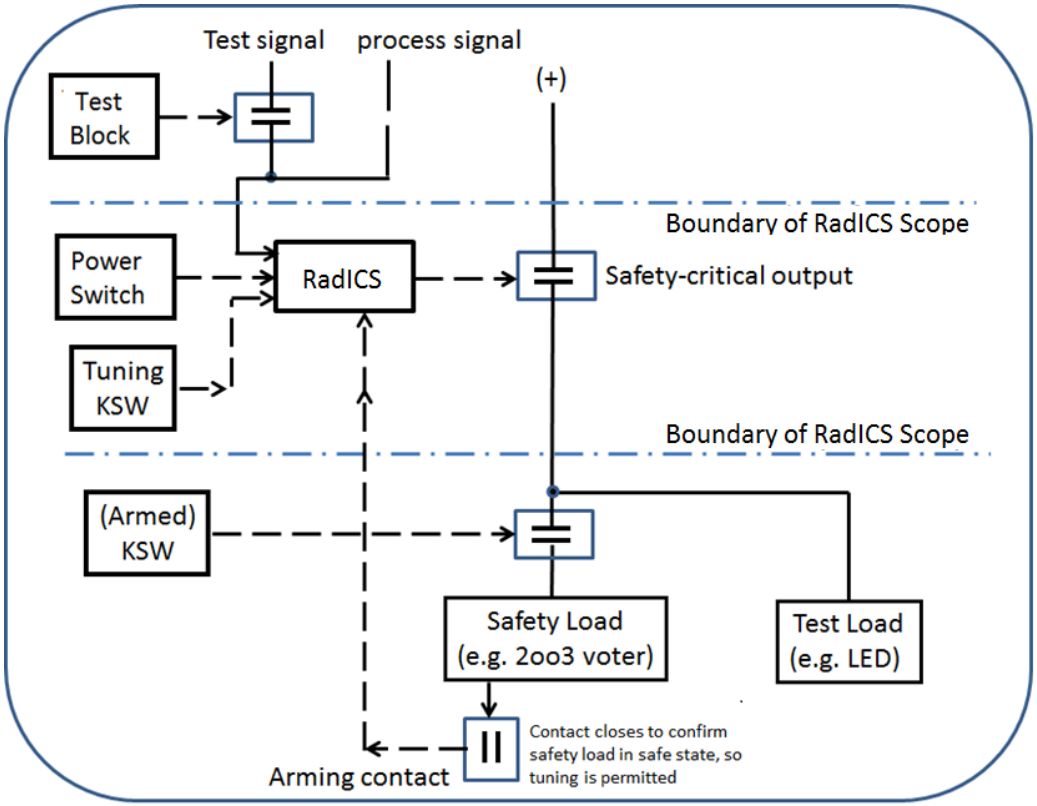


Safety Override Unit (SOR)

- Sets safety override signal from the user (via key switch)
- Sets safety override signal from FPGA
- Reset SOR signal from user after Set SOR signal cleared
- Interrupts power supply on Set SOR signal
- Safety Override Unit has solid-state relay based design

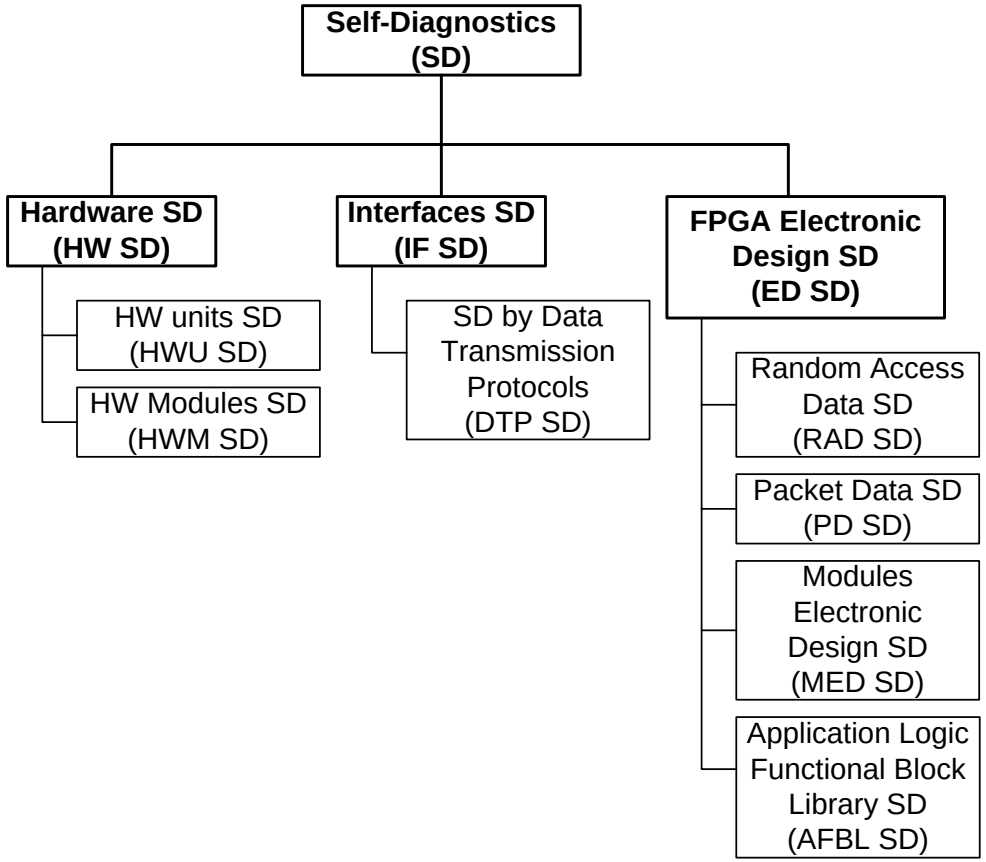
RadICS Module Safety Features (3/3)

Tuning Mode Access Control



- TUNING Key:
  - RadICS Platform chassis mounted
  - Connects directly to a dedicated contact input on the LM
- ARMED Key:
  - Dry contact supplied by end user is used by RadICS Platform and may be driven by any secure means (e.g., keyswitch)
  - Dry contact is used to indicate that end user's downstream safety logic is secured in safe state
  - ARMED key contact is connected to designated input on LM
- TUNING PC Password Control

RadICS Platform Self-Diagnostic Features (1/5)



- Self-diagnostics capabilities for each module
- Automated tests run continuously during system operation
- Data integrity checking performed on transmission, reading/writing, and processing
- Diagnostic module gathers data on cabinet environmental conditions and diagnostic data from modules and sends diagnostic information to MATS
- Diagnostic features designed to be independent from executing control functions
- Self-diagnostic are performed by both the application and platform levels and are aimed at different types of faults

RadICS Platform Self-Diagnostic Features (2/5)

- Module Fault Handling
  - Watchdog-detected Level Faults (Type I) – Watchdog cuts off power supply voltages
  - Critical Level Faults (Type II) – HW or part of ED cannot properly perform functions but another part of platform that drives safety outputs can guarantee driving outputs to the safe state and transitions to RUN (Safe) mode
  - User-defined Level Faults (Type III) – User defines criticality of detected errors and their processing algorithm (performed by application logic)

RadICS Platform Self-Diagnostic Features (3/5)

- System Fault Handling
  - Input Module Faults – Application logic decides how to manage it, as specified by end user
  - Logic Module Faults – If LM suffers a Type I or Type II fault, the error must be treated as a product level Type I fault and all outputs are driven to the safe state
  - Output Module Faults – If an output Module detects a Type I fault, it is de-energized and the LM will trip to the safe state when it detects the loss of communication with the de-energized output Module. If an output Module detects a Type II fault, it will drive its outputs to the safe state and report this to the LM. If an output Module detects a Type III fault, the Application Logic in the LM can decide (by Application Logic) how to manage it, as specified by the end user's functional requirements).

RadICS Platform Self-Diagnostic Features (4/5)

- Random Access Data Self Diagnostics (RAD SD) covers random access data integrity during transmission, storing, reading and writing
  - CRC-5-USB for each 16 bit word
  - Address is added to data during CRC calculation to ensure data were written/read with right address
  - Numerator is added to data during CRC calculation to increase static error detection capability and to ensure data are actual in this work cycle
  - Data are encoded (inverted or not) by numerator LSB to add dynamic change parameter even in case of static data
- Packet Data Self-Diagnostics (PD SD) covers packet data integrity self-diagnostics while transmission, storing, reading, and recording
  - CRC-64-ISO for each data packet
  - Numerator is added to data during CRC calculation to increase static errors detection capability and to ensure that data are actual in this work cycle

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