Simplification of Digital Safety Systems through the use of Distributed Logic FPGA-based Systems

2015 International Workshop On the Application of FPGA in NPPs

Shanghai China

LOCKHEED MARTIN

NextGenLM
TRANSFORMING FOR TOMORROW

Agenda

- Introduction to Lockheed Martin
- FPGA-based Safety System Platform
- NuPAC Logic Development Testing

NextGenLM
TRANSFORMING FOR TOMORROW

Introduction - Lockheed Martin

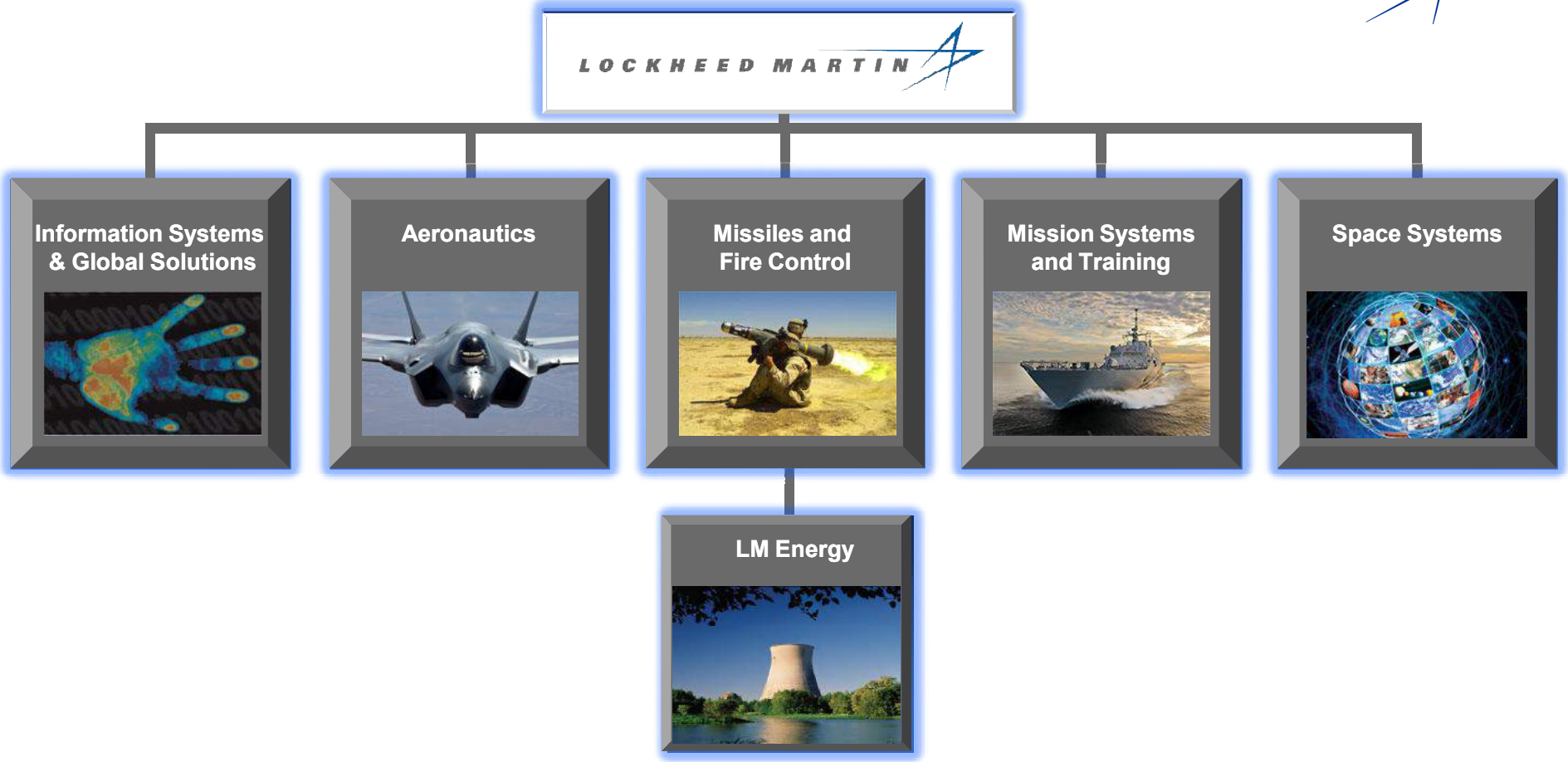
NextGenLM
TRANSFORMING FOR TOMORROW

100+ Years

60+ Years

NextGenLM
TRANSFORMING FOR TOMORROW

Lockheed Martin Corporation



LOCKHEED MARTIN ENERGY

Generation **Management** **Distribution**

OTEC

NUCLEAR CONTROLSYSTEMS

ENERGY STORAGE

TIDAL

ENGINEERING, PROCUREMENT & CONSTRUCTION

BIO

EFFICIENCY, DEMAND MANAGEMENT & SMART GRIDS

THE MEN AND WOMEN OF LOCKHEED MARTIN

- 112,000 Employees Worldwide
- 60,000+ Scientists, Engineers and IT Professionals
- Lockheed Martin is led by Chairman, President and CEO Marillyn A. Hewson
- Operations in 1,000 Facilities, 500 Cities, 50 States and 75 Countries

Partners to Help Customers Meet Their Defining Moments

NextGenLM
TRANSFORMING FOR TOMORROW

FPGA-based
Safety System Platform

NextGenLM
TRANSFORMING FOR TOMORROW

Safety System Platform

- **Problem Statement**
  - **The application of digital technology challenges the licensing of NPP I&C safety systems**
    - Potential software common-cause failures
    - Inter-channel communication
    - Secure operational & development environment
    - Communication between non-safety and safety systems
    - Dedication of commercial off-the-shelf equipment
- **Objective**
  - **Offer a *LICENSABLE* digital control system platform for safety-related NPP applications**
    - Non-microprocessor based
    - FPGA-based
    - No operating systems or executable software
    - Designed specifically for the nuclear industry
  - **Provide *CERTIFIED BUILDING BLOCK(s)***
    - Generically-qualified (with U.S. NRC approval) modules ready to be configured for customers' application-specific requirements
- **Current Situation**
  - **Developing a product, *NuPAC***
  - **Qualification Specimen undergoing qualification, Topical Report under US NRC review**

A Premier FPGA-based Platform Designed Specifically for Use in NPP I&C Safety Systems

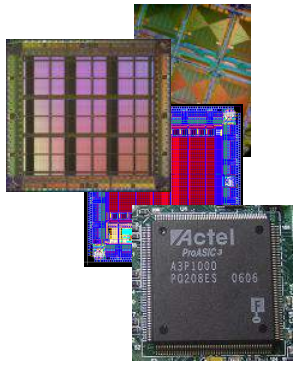
NextGenLM
TRANSFORMING FOR TOMORROW

Unique Features

- **Generic Functional Module**
  - **Each GLM (module) may be configured for various I/O types via installation of up to eight mezzanine cards**
  - **I/O types may be mixed and matched onboard the same GLM**
  - **Each GLM provides onboard logic solving capability**
    - Application Specific FPGA provided for user defined logic
    - Permits functional and physical partitioning/distribution of logic within a system of GLMs
    - Traditional platforms provide one centralized logic solving element, typically a microprocessor with software

Generic Logic Module

- **Core & Application Specific FPGAs**
  - **Standard Core FPGA accommodates common functions**
  - **Application Specific FPGA provided for user defined logic**
  - **Partition between Core and Application Specific FPGA facilitates reuse and limits recurring verification**
    - The Core FPGA is verified once and the configuration is frozen
    - Only modest instantiations of Application Specific logic are verified for each new application, using a standard, frozen interface to the Core FPGA

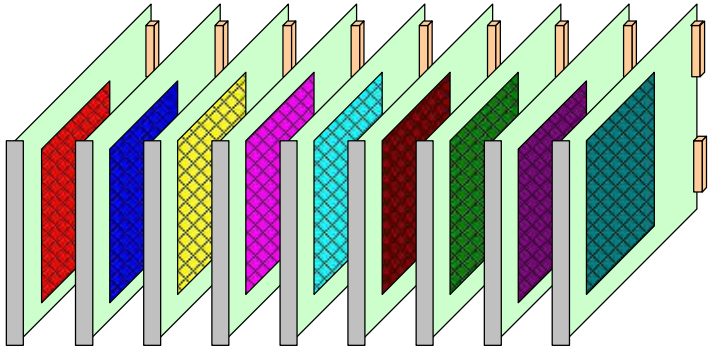


FPGA-Based

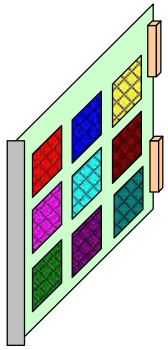
NextGenLM
TRANSFORMING FOR TOMORROW

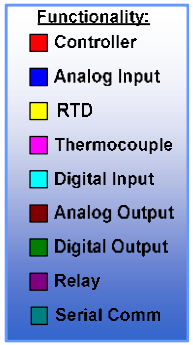
Paradigm

***Traditional Platforms** (Programmable Logic Controller)*



NuPAC Platform



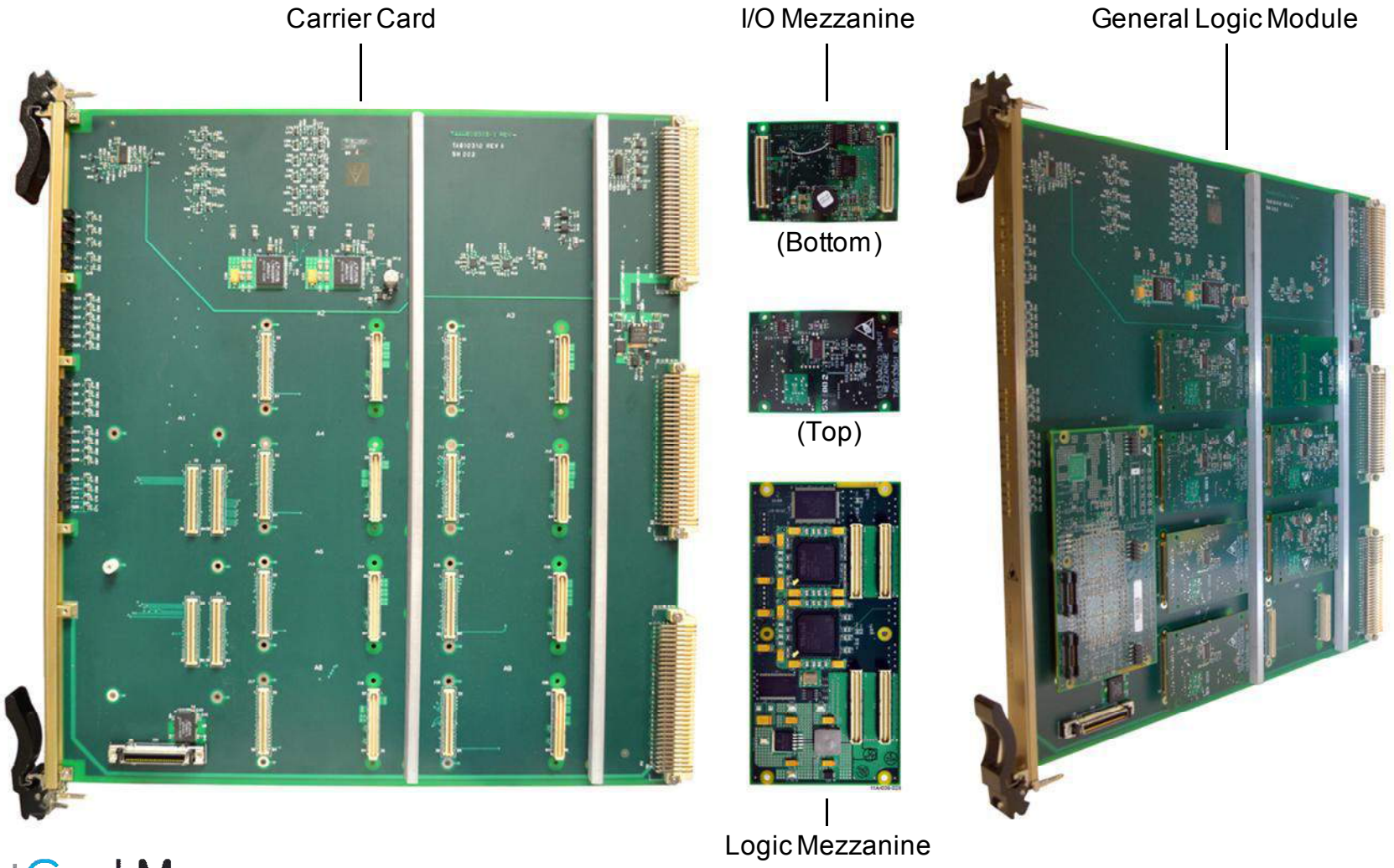


- **Integrates all functionality of a PLC on a single *GENERIC FUNCTIONAL MODULE*, the GLM**
  - User-configurable I/O supports all standard types
  - Provides an onboard FPGA-based logic solving capability
  - Scalability provided by paralleling and cascading GLMs
    - Efficiently supports partial system upgrades/retrofits up to complete safety system replacements or new plant safety system architectures
- **Supports *FUNCTIONAL & PHYSICAL PARTITIONING***
  - Avoids the highly-integrated and highly-complex (Decentralized vs. Centralized Architecture)
  - Facilitates diversity, verifiability, and thus licensability
- ***SIMPLIFIES* system-level *FMEA* for retrofits**
- **Permits *PROPER VERIFICATION***
  - Keeps the design as simple as possible - architecture reduces system infrastructure and associated complexity
  - Simple hardware-based state machine versus a complex microprocessor with an operating system and software

Akin to Hardware-based Systems & Trip Modules

NextGenLM
TRANSFORMING FOR TOMORROW

Generic Logic Module (GLM)



NextGenLM
TRANSFORMING FOR TOMORROW

Programmable Logic

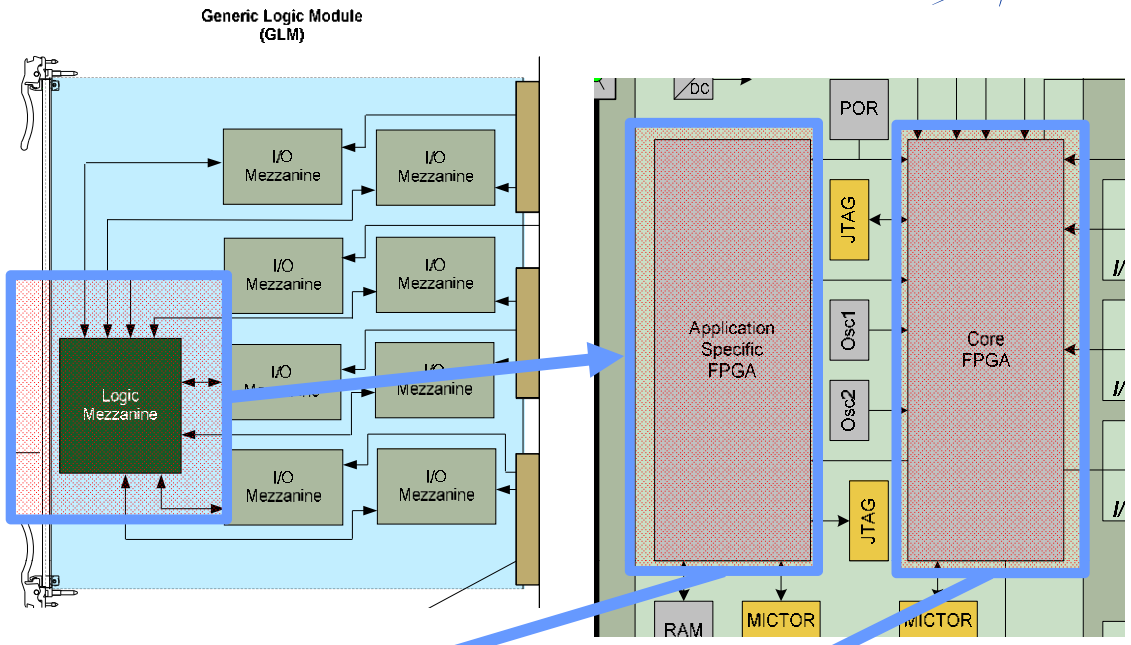
- **FPGA-based Logic Solving Element**

  Logic Mezzanine Card

  General Functionality

  - Core FPGA acts as a calibrated voltmeter
  - Application Specific (AS) FPGA receives accurate filtered measurements and makes all decisions
  - Core FPGA provides output generation and test
  - AS FPGA provides output commands
  - Core FPGA provides serial data routing
  - Application Specific FPGA processes serial data

- **System uses Two FPGAs**
  - Actel/Microsemi FPGAs
  - 3 Million Gate Part
  - 341 Single-Ended I/O Device
  - Operating Frequency 1.5 to 200 MHz



Application Specific FPGA

User Defined Functions

- Verifies hardware configuration
- Computes output commands
- Manages user defined interfaces
- Performs user defined BIT

Core FPGA

Common Functions (fixed configuration)

- Samples/measures inputs
- Controls outputs
- Routes serial data
- Performs BIT
- Controls card top LEDs
- Manages parameter database

Intra-rack LVDS(8)

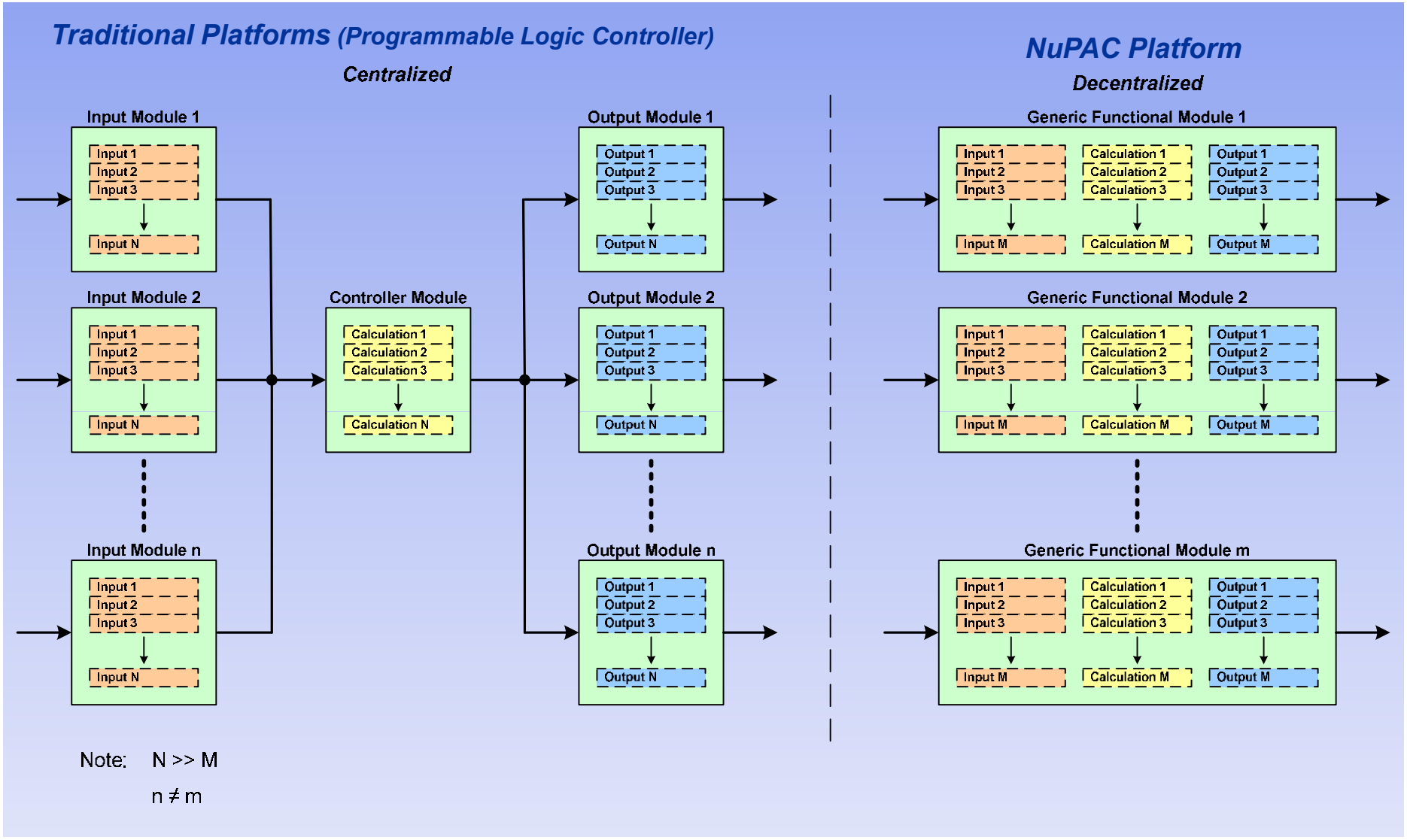
I/O Mezzanine Cards (8)

Parameter Memory

Card top LEDs

NextGenLM
TRANSFORMING FOR TOMORROW

Centralized vs. Decentralized



NextGenLM
TRANSFORMING FOR TOMORROW

Summary

- **Platform provides a flexible FPGA-based architecture**
- **Applicable to both safety & non-safety applications**
- **Seeking generic approval via NRC Safety Evaluation Report (SER)**
- **NuPAC Topical Report Currently Under US NRC Review**

NextGenLM
TRANSFORMING FOR TOMORROW

NuPAC Logic Development Testing

NextGenLM
TRANSFORMING FOR TOMORROW

FPGA and Programmable Logic Testing

- An Entire Mature Industry is dedicated to Logic Testing
  - Standardized Languages have been developed & qualified
    - (VHDL, Verilog, SystemVerilog)
  - Specific Language/Library/Methodology Support
    - Constrained Random Verification (CRV)
      - SystemVerilog Libraries (VMM, UVM, etc.)
    - Assertion Based Verification (ABV)
      - Dedicated Languages (PSL, SVA)
    - Formal (Static) Analysis Methods
      - Unreachable Code
      - Terminal States
      - Clock Domain Crossing (CDC)
      - Data Security/Sanctity
- Mature and Competing SW Tool Vendors

Traditional Dynamic Testing - Issues

- Functions and interfaces often tested in isolation
- FPGA internal interactions exposed late in design cycle
  - Unused code
  - Latent code deficiencies
- Defects not always repeatable in system integration test
- Post development and design failures experienced during and after qualification testing, fielding, and unusual operating conditions etc.

NextGenLM
TRANSFORMING FOR TOMORROW

Constrained Random Verification (CRV)

- Relevant FPGA features and interfaces tested simultaneously
  - Closely emulates practical system operation
  - Limited only by Requirements Scope (Definition)
    - As in any system, quality of requirements directly impact quality of product / verification
  - Expose “unknown unknowns” of requirements and implementation
- Standardized and effective approach
- Supported by all major logic design/test tool vendors
- Randomized Signals; Each test performed multiple times with unique signals for each run

NextGenLM
TRANSFORMING FOR TOMORROW

Thank You!

NextGenLM
TRANSFORMING FOR TOMORROW