Lockheed Martin
Architecture for FPGA and Digital Safety Systems

FPGA Workshop

14 October, 2019 – Budapest, Hungary

Larry Erin

Chief Engineer, Nuclear Systems

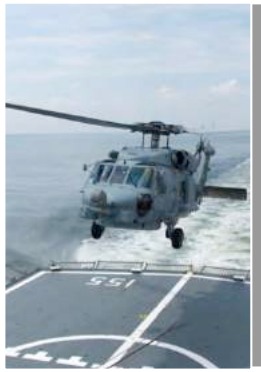
Lockheed Martin Business Areas

Aeronautics

- Tactical Fighters
- Tactical /Strategic Airlift
- Advanced Development
- Sustainment Operations

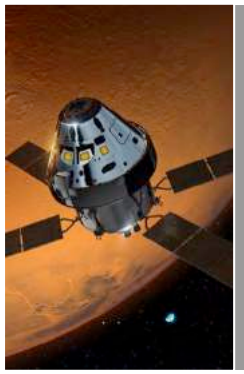
Missiles and Fire Control

- Air and Missile Defense
- Tactical Missiles
- Fire Control
- Combat Maneuver Systems
- Energy



Rotary and Mission Systems

- Maritime Solutions
- Radar and Surveillance Systems
- Aviation Systems and Rotorcraft Platforms
- Training and Logistics Solutions



Space Systems

- Surveillance and Navigation
- Global Communications
- Human and Deep Space Exploration
- Strategic and Defensive Systems

Lockheed Martin International

- Global Business Opportunities
- Wide Spectrum of Products
- Sustainability & Support

LM Energy Overview

Energy Management

Energy Storage

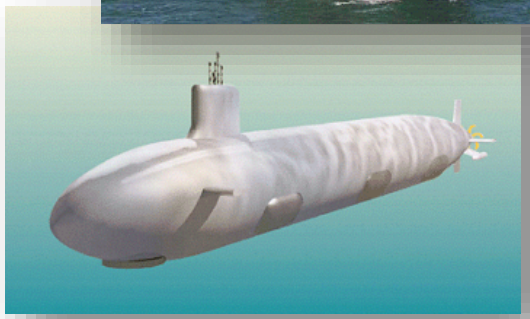
Nuclear Systems

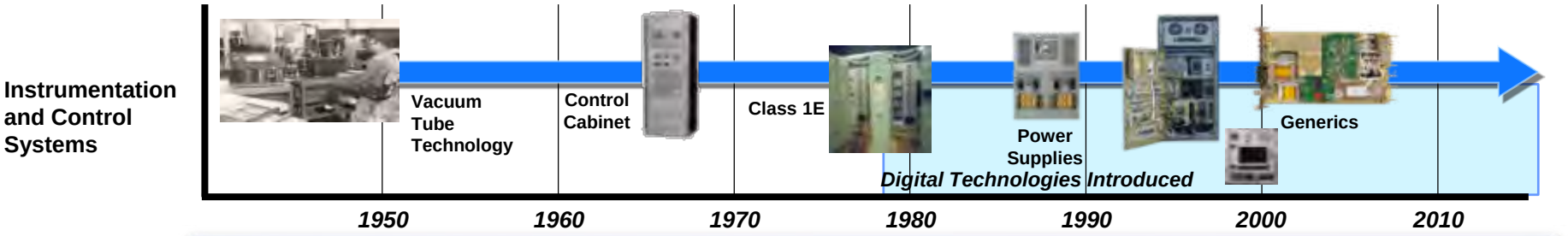
Bioenergy

Tidal Energy

Nuclear I&C and Complementary Products

- Largest I&C supplier to the U.S. Navy – systems on ALL nuclear vessels
- Integrated analog and digital designs
- Harsh environment/high reliability
  - Devices qualified to strict military standards (environmental)
- Design and manufacturing for GEN3+ reactor systems
  - Contracted and teamed with providers of safety-related equipment and designs
  - Safety (Class 1E) and important to safety equipment applications





Proven Track Record on Domain-Relevant Products

Commercial Nuclear I&C Platforms

NuPAC FPGA-based Platform

- Programmable FPGA-based Logic
- Expanded Input/Output Offering
- Building Blocks for I&C Systems
- Diverse Logic Solving Variants

FPGA-based
(Field-Programmable Gate Array)

NuPAC®

Discrete Logic Solving Platform

- Custom Hardware-based Logic
- No Software-like Elements
- Basic Input/Output Offering
- Building Blocks for I&C Systems

Discrete Logic
Integrated Circuits

DLSS®

- Common industry-standard form factors and interfaces
- Generic, modular, scalable, and distributed
- Input processing, logic solving, output processing
- Eliminate common-cause failure vulnerabilities
- Chassis mounted / cabinet installed
- Suitably rugged for design basis events

Modules

Chassis

Cabinet Enclosure

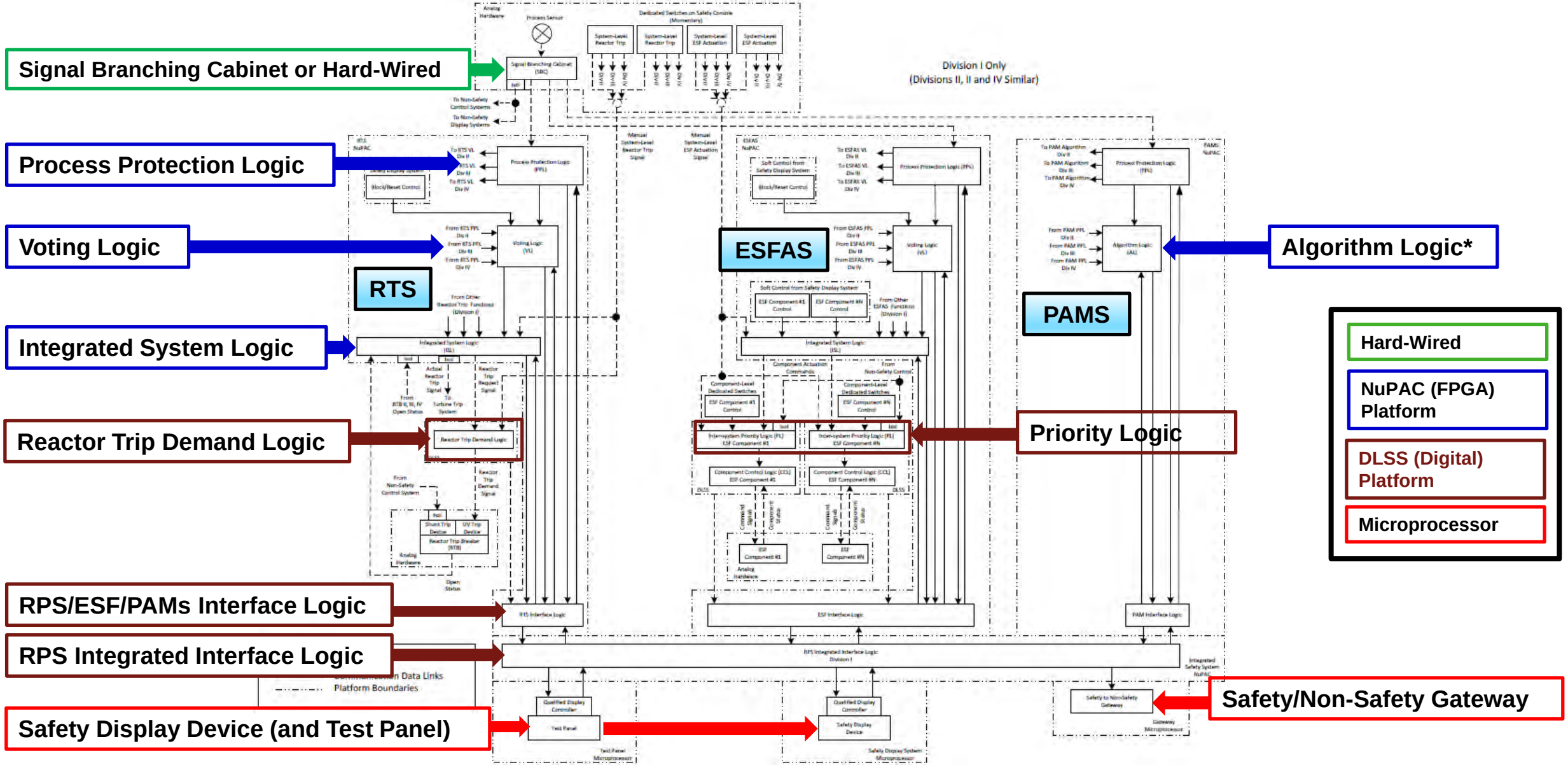
Platforms designed specifically for use in NPP Safety Systems

FPGA and Digital Safety System Architecture

- **Integrated FPGA and Digital Safety System Solution includes:**
  - Reactor Trip System (RTS)
  - Engineered Safety Features Actuation System (ESFAS)
  - Safety Display System (SDS)

- **Safety Display System**
  - Display of RG 1.97, Rev 4, PAMS variables & the state of ESFAS components
  - Man-Machine Interface to the Safety System
  - Capability to block and reset operating bypasses via soft controls
  - Display of applicable RTS and ESFAS operating bypass status
  - Capability to change state of ESF components via soft controls
  - Capability to change calibration constants via soft controls

FPGA and Digital RPS System Architecture



FPGA and Digital Safety System Design Compliance

Design-Specific Review Standard, Section 7.1; I&C Fundamental Principles

- Design Basis
- Redundancy
- Independence: Physical, Electrical, Communications, and Functional
- Diversity and Defense-in-Depth
- Predictability and Repeatability

DI&C-ISG-04, Section 1, Interdivisional Communications

- Channel Independence, Item 1
- Interdivisional Isolation, Item 2
- Simplicity, Item 3
- Cycle time, Item 5
- Point-to-Point Communications, Item 14

Design-Specific Review Standard, Section 7.1

Design-Specific Review Standard, Section 7.1; I&C Fundamental Principles

Design Basis:	Generic design basis documents; Plant specific upon contract
Redundancy:	4 independent/redundant divisions
	PPL signal (each div) subjected to 2-o-o-4 Voting Logic; failure does not preclude actuation
	Actuation capability maintained with one division in maintenance and failure of 2nd division
Independence Physical:	Safety Display in MCR and RSS; NuPACs distributed in I&C rooms
Independence Electrical:	Independent power sources, independent SDL lines
Independence Communication:	No interdivisional communication in Safety Display System

Design-Specific Review Standard, Section 7.1

Independence Functional:	Each SDS is independent; loss of one does not result in loss of PAMs
	For RTS and ESFAS, primary functions implemented on one FPGA, backup on another
	For RTS, one RTDL module per breaker; module failure results in loss of control of one breaker
	For ESFAS, ISPL and CCL for each ESF component implemented on a separate DLSS
	For PAMS, primary and backups variable are implemented on separate FPGAs
Diversity & Defense-in-Depth:	Two divisions of PPL, VL & ISL on one type of FPGA, other 2 divisions implemented on another
	RTDL, ISPL, and CCL implemented on DLSS platforms
	Each redundant division of SDS implemented on the same microprocessor-based platform, but the architecture allows for a select set of variables to be hardwired to a diverse non-safety display system
Predictability & Repeatability:	SDS designed with same execution path (time response) for normal ops & after design basis event

Design-Specific Review Standard, Section 7.1

Features designed into the FPGA and Digital Safety System to address postulated software CMFs:

Signal Branching Cabinet (SBC)

Specified process variable input signals are electrically isolated and hardwired to a diverse non-safety display system

- Addresses software CMF in the SDS to meet the guidance in NUREG-0800, Chapter 7, BTP 7-19, Sect 1.4

System-Level Manual Reactor Trip Controls

- Hardwired directly to the RTDL

Manual System-Level ESF Controls

System-level ESF manual command signals are hardwired directly to the inter-system priority logic

- Addresses diverse manual system-level actuation requirement in IEEE Std. 603-1991, Clause 6.2.1 and NUREG-0800, Chapter 7, BTP 7-19, Sect 1.5

Design-Specific Review Standard, Section 7.1

Inter-System Priority Logic (ISPL)

ISPL designed to provide the operator capability to change the state of ESF components using diverse manual dedicated controls (I&C rooms) if the soft control capability of the ESF components is degraded

- Addresses software CMF in the SDS to meet the guidelines in NUREG-0800, Chapter 7 and BTP 7-19, Section 1.4

Reactor Trip Breaker Attachments

Reactor trip breakers are tripped using undervoltage trip circuity and a shunt trip device

- Addresses diverse scram system requirements in 10 CFR Part 50.62, & guidance in NUREG-0800, Chapter 7.8

DI&C-ISG-04, Sect 1, Interdivisional Communications

DI&C-ISG-04, Section 1, Interdivisional Communications

Channel Independence, Item 1	For SDS, four independent divisions; no interdivisional communications
	For RTS & ESFAS, interdivisional communication only for performing 2-o-o-4 voting logic
	For PAMS, interdivisional communication only for calculating redundant signal group values
Interdivisional Isolation, Item 2	No interdivisional communication associated with SDS
	Interdivisional SDL associated with the Integrated Safety System are isolated
	A single failure of an interdivisional SDL (low %) results in 2-o-o-3 voting which results in actuation upon demand

DI&C-ISG-04, Sect 1, Interdivisional Communications

Simplicity, Item 3 Information on SDS is well defined communication path within a division

RTS/ESFAS protective functions & PAMS implemented on different FPGAs

RTS & ESFAS backup & primary protective functions mostly implemented on different FPGAs

RTDL is implemented on DLSS module, one per reactor trip breaker

ISPL & CCL associated with each ESF component are implemented on a separate DLSS module

PAMS primary and diverse variables are implemented on different FPGAs

DI&C-ISG-04, Sect 1, Interdivisional Communications

Cycle time, Item 5	Same execution path (time response) followed in normal operation & following a design basis event
	Cycle time, described as the time from a change in value of an input signal to the time it is displayed on the SDS, is the same regardless of the state of the plant
Point-to-Point Communications, Item 14	All comm paths associated with the NuPAC platform utilize RS-422 point-to-point serial data links
	SDS receives signals from the NuPAC platform via a RS-422 serial data link
	Safety display receives signals from the SDS via a VGA communication link in each division

FPGA and Digital Safety System Summary

Summary:

- **The integrated FPGA and digital safety system architecture complies with the design principles provided in:**
  - Design-Specific Review Standard, Section 7.1., and
  - Communication Design Guidance provided in DI&C-ISG-04, Section 1

- **The integrated FPGA and digital safety system architecture is applicable to digital upgrade modernization on an operating plant, as well as an integrated safety system on an advanced plant.**

- **The integrated FPGA and digital safety system architecture provides the owner with significant flexibility when considering a digital modernization project.**


LOCKHEED MARTIN