MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

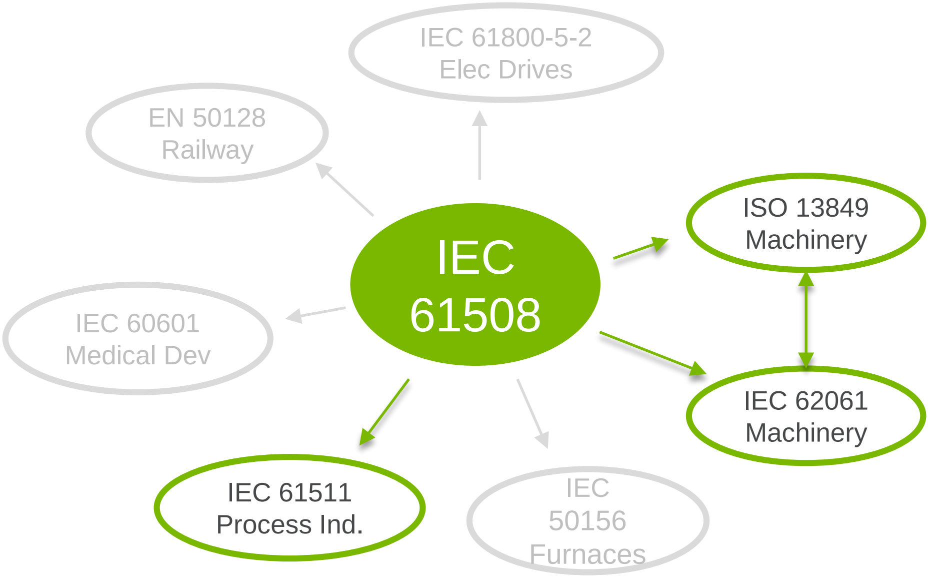
JOE LENNER
Argonne National Laboratory
Advanced Photon Source
Safety Interlocks Group

U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a
U.S. Department of Energy laboratory
managed by UChicago Argonne, LLC.

9/11/2019

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Applicable Standards



- IEC 61508 is the parent standard
  - Applicable in any situation
  - Used when no applicable child standard exists
  - Very general, many requirements are overly complex
- Child Standards
  - Specialize the requirements of 61508 for a specific application
  - If you meet the requirements of the child, you meet the relevant requirements of 61508
- Best fit for Accelerators
  - IEC 62061
  - ISO 13849
  - IEC 61511

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Certified hardware benefits

- Use of a single PLC
  - Eliminates redundant systems and associated wiring.
  - Ability to clearly separate safety from non-safety tasks
  - Built-in diagnostics
  - Safety I/O allows reduction of relays
- Programming
  - Use of certified and proven functions reduces programming effort
    - Easier to apply = Less errors
  - Reduces safety and standard programs/tasks
    - Reduced size of safety program
    - Reduces review & test time

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Vendor Software Management

- Programming tool updates
  - Only when necessary
    - The “Microsoft“ effect
    - Development platform support
- Firmware Updates
  - Quarterly reviews unless alert

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Software

- The latest generation of PLCs bring with them a lot of new features.
  - Tag based instead of memory based programing
  - User defined data types or structures (UDTs)
  - Add on instructions or functions (AOIs)
  - Arrays
- Proper use of these features can allow for
  - Improved code readability
  - Improved code reviewability
  - Enforcement of tag naming consistency
  - Simplification of functional changes
  - Reduction of errors cause by repetitive tag entry for similar devices
  - Reduce errors caused by repetitive programming of same function for similar devices

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Certified software function benefits

- Use certified functions where possible
  - Dual channel inputs
  - Dual channel outputs
- More diagnostics
  - More complete than at the I/O module level
  - Readily available in the program
    - Don’t have to query module for data
- Testing is done for you
  - Independently examined by third party
  - High confidence in execution
  - Lowers end user testing

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Software – Code Structure, UDTs, AOIs

- Modular Code Structure
  - Breakup code by functionality
  - Smaller routines
    - Easier to review
    - Easier to test
- User Defined Tags (data structures)
  - Organize data around function or structure
  - Enforces naming consistency
- Use of Add On Instructions (functions)
  - User Developed
  - Encapsulates common functions
  - Helps enforce common data naming
  - Can be tested independently
    - Lock the AOI with signature
    - Confidence that AOI is unchanged

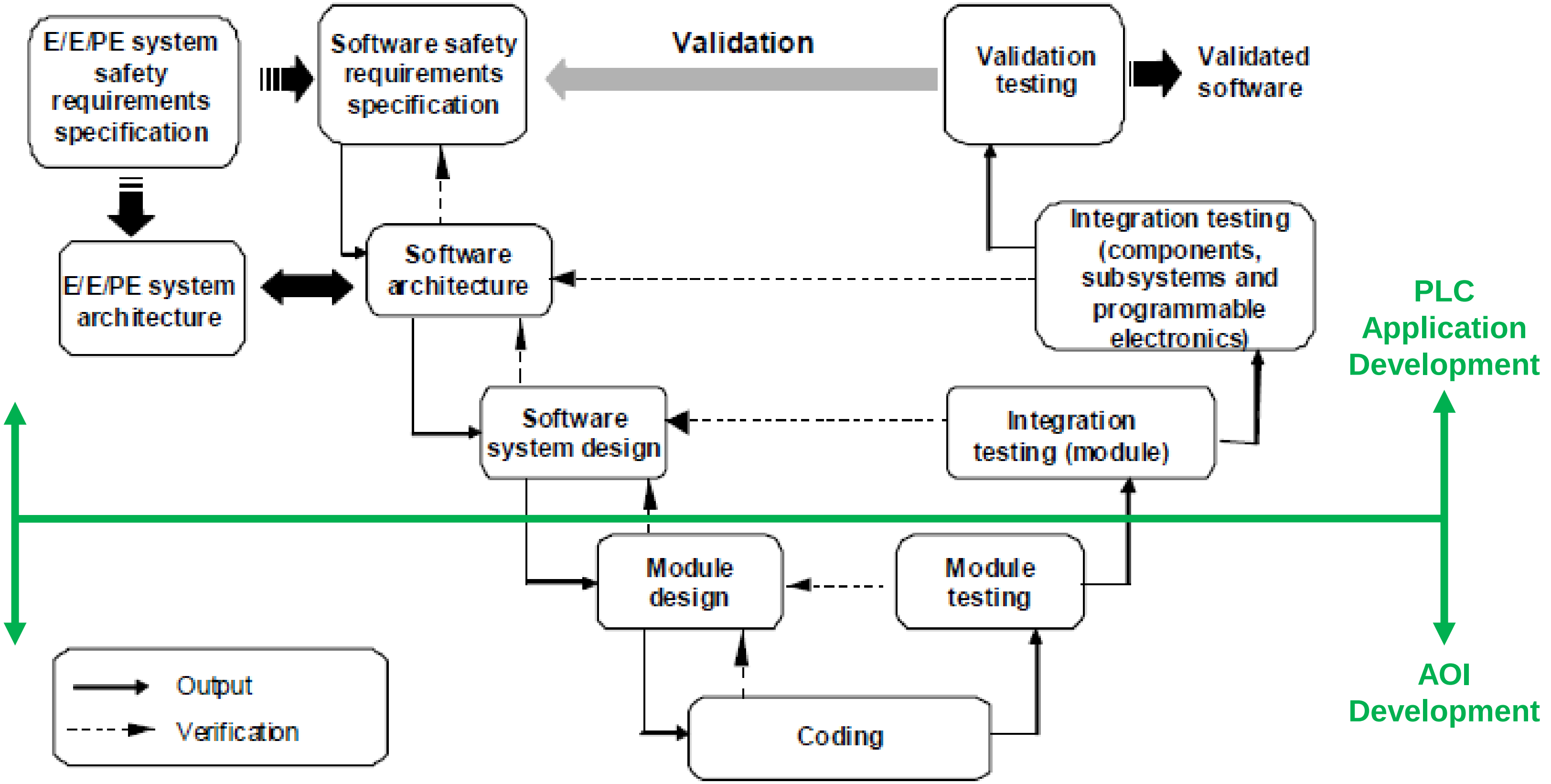
MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Limits impact of software changes

- Without AOIs
  - Code Changes typically requires testing of all functions
  - Time consuming
- With AOIs selective regression testing
  - Limit the scope of test
    - Analysis required
  - Reduces time and resources

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Relating the IEC 61508 V-model to PLC application development


E/E/PE system safety requirements specification
Software safety requirements specification
Validation
Validation testing
Validated software
E/E/PE system architecture
Software architecture
Integration testing (components, subsystems and programmable electronics)
PLC Application Development
Software system design
Integration testing (module)
Module design
Module testing
Coding
AOI Development
Output
Verification

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

V-Model Software Implementation at the APS

- Create Functional Specification
  - Define safety functions
  - Hardware defined and I/O identified
- Create Software Specification
  - Implement safety function logic, diagnostics, operations interfaces
  - Software architecture and design
- AOI Development (Module)
- Review/Test modules
  - Review code
  - Built prototype / simulator
  - Test
- Verification Testing
  - Complete testing of safety function logic, diagnostics, operations interfaces
  - Confirms design meets specification
  - Real hardware or simulator
- Validation Testing
  - Developed from Functional Specification

MANAGEMENT OF PROGRAMMABLE SAFETY SYSTEMS

Configuration Control

- Revision Control
  - Module (AOI)
    - Electronically signed module after test
    - Safety lock after verification
  - Safety Code
    - Locked after validation
    - Stored in ICMS by developer
    - Policy dictates formal release and change control
- Change Control
  - APS maintains a design review process
    - Graded approach