Process based approach for Integrated Digital I&C for New Plants and Current Operating US NPPs

Presented by: Jay Amin
TXU Power
March 28, 2006
EPRI Digital I&C Issues Meeting
Washington, DC

1

Topics

- Industry Digital Upgrades Issues
- What are we learning?
- Regulatory Concerns & Issues
- What are the Root Causes?
- Basis for the Root Causes
- Digital guidance
- **Recommendations**
  - New Plants
  - Suggestions for One Step Licensing Approach
    - Define generic rules for the specific platform
    - One Step Licensing Submittal
  - Existing Plants
- Advantages of Process Based Approach
- Regulatory Issues needing clarifications
  - Recommendations for Regulators
- Recommendations for EPRI
- Overall Conclusion
- Visual Illustrations
- Questions & Comments

2

Industry Digital Upgrades Issues

- INPO/WANO SER 4-5, & INPO OEs
- US Operating NPP Industry Issues
  - Equipment Trips/Plant Trips
  - Human Performance Errors
  - New system functionality not fully understood
  - Design Rigor less than adequate
  - New system failure mechanisms not fully understood
  - New system change control and CC not fully understood
  - Incorrect/missing System level Functional Requirements
  - Less than adequate Impact Assessment

3

Industry Digital Upgrades Issues (conti.)

- US Operating NPP Industry Issues (conti.):
  - Inadequate task based training for station RWOs
  - Failure modes not fully understood, analyzed and tested
  - *EMI/RFI requirements not understood nor specified*
  - DC & CC requirements not specified or understood
  - Less than adequate Owner reviews
  - Missing critical digital requirements in the requirements specifications
  - Missed opportunities during Testing
    - FAT
    - SAT
    - OAT
  - Design basis and licensing basis not fully understood

4

What are we learning?

- Simulator
- Engineering Simulator
- Human Factors/Human Performance
- End Point Vision
- ***Processes, Procedures and Competencies***

5

Simulator

- Digital upgrades with Control Room modernization pose new challenges
- Plant Simulator modifications are expensive
- Class Room Simulators adding value
- Simulators proving to be very useful in transition to Digital
  - Dynamic modeling and response of control systems
- ***Simulator upgrade/modification needs to be part of the modification conceptual design***
  - Operations crews need to be trained on new systems
    - At own pace
      - Class Room Simulator
    - Visual Training tools needs to be explored to increase comfort zone
    - Validating operations procedures

6

Engineering Simulator

- Runs the same Plant Simulator Software
- Allows design team to test out design (preliminary, concepts, procedures, etc)
  - Upgrades/Modifications
  - Control Systems modeling
    - System Behavior and response
    - Dynamic Loop behaviors and predictability
    - Validation of design
  - Operator confidence Builder
- Aid in validating conceptual software designs
  - Fosters better understanding the upgrade
- Display/control system/Procedure/HFE/HP Validation

7

Human Performance/Human Factors

- Current method of "Backend HFE/HP" assessment is flawed
  - Back end verification and validation findings too costly to resolve
- HFE needs to be integrated ***UP-FRONT*** into the design process
- Up-front design must include
  - HFE requirements
  - HP requirements
  - Verification to ensure requirements have been adequately implemented for operations, maintenance in the area of HFE and HP especially during
    - CR Design
    - D3 Analysis
    - Display and Soft Control Design
    - Alarm System Design.....
- FAT/SAT must validate the HFE and HP requirements that have been verified in previous phases
- Operator and maintenance training must validate the HFE/HP requirements that have been verified and validated in previous phases

8

End Point Vision

- Begin with the End in Mind
- ***"Must Do" for Large scale platform based multi-outage implementations w/ Integrated CR operations***
- Buy-in from station is a "MUST"
- Change Mgmt must be understood, addressed and funded
- Up-front clear understanding of generic Platform requirements for
  - Architecture
  - Hardware
  - Software
  - Control Room Operations Philosophy
    - Alarm Response Philosophy
    - Display and Soft Controls
  - D3 Philosophy
  - Communications and IE/NIE Isolation
  - System Limitations and Precautions
  - Cyber Security Strategy
  - DC and CC

9

Regulatory Concerns & Issues

- **BTP 19 (D3)**
  - Need clear definitions and interpretations
  - Current regulation lacks specificity and open to interpretation based on recent experiences
  - Not well defined for integrated digital upgrades
    - Common Processors for ESFAS/RPS (Beyond Design basis requirements)
      - Inter-channel Communications is a good technique for D3
        - Applying analog mentality to integrated Platforms is a flawed strategy
- **Upcoming changes to NUREG 0800**
  - New Regulations?
  - More Interpretations
  - May want to update the standards forming the basis for update to NUREG 0800
    - A new NUREG clarifying the changes to NUREG 0800
- **D3 methodology for Control Room Integrated Work Station Strategies**
  - Integrated safety and non safety controls
  - CR Operations during normal and abnormal conditions
- Issues related to SERs' on Generic platforms
- **Lack of Risk informed PRA to address risk**

10

What are the Root Causes ?

1. Weakness in Programs, Processes, Procedures & Competencies
   - Vendor
   - AE
   - Integrator

   Quality should be built into the process to ensure sustained product quality
2. Weakness in Utility Programs, Processes, Procedures & Competencies
3. Regulations & Interpretations
   - Clarity and interpretation of certain requirements
   - Risk informed techniques not reflected in regulations
   - Analog mentality in assessing digital process/products

11

Basis for the Root Causes?

- Lack of value based focus
  - Requirements Specification
  - Failure modes
    - Equipment level (HW & SW)
    - Plant System level
    - Integrated Systems Architecture (Equipment + System) Level
  - Digital DC & CC Process
  - ***Logic reviews (RSA & applications)***
    - ***Rules, Rigor and consistency in application***
  - Testing Rigor
  - System baseline documentation

12

Basis for the Root Causes (conti.)

- Too much focus on vendor product ***software*** and non value added enhanced functionality
  - Simplicity Principles ignored
  - Complexity from non value added functionality on the rise
- Industry experience points to issues that have very little to do with pure product software
  - Weakness in Utility Requirements Specifications
  - Weakness in vendor processes
  - FMEA
  - Testing
  - Utility understanding of the Product
    - Training
    - Competencies

13

Basis for the Root Causes (conti.)

- Vendor/Integrator/AE Issues
  - Understanding of
    - Application Systems
    - own product functionality, limitations
    - Failure modes
    - Communications requirements/protocols
    - US NRC Regulations
    - Systems interaction requirements (third party, end devices, temporary tie ins, test points)
  - Understanding of Nuclear Culture
  - Lack of effective review process during various phases of LCD
  - Understanding and use of US NPP endorsed standards for Nuclear Design vs. ISO Certification
  - Understanding of plant systems, design basis, and licensing basis for consideration in platform/equipment architecture and application design

14

Basis for the Root Causes (conti.)

- Station Level Utility Change Management Plan
  - Weakness in utility process and procedures/guidance for digital tasks
    - Consistency issue
    - Knowledge issue

    Resulting in less than adequate owner reviews and vendor oversight
  - Less than adequate commitment to training in-house utility personnel
    - Based on R&R

15

Basis for the for Root Causes (conti.)

- ***Digital Design Control & Configuration Control***
  - Limited understanding within
    - Utilities/Vendor/AE/Integrator
  - Less than adequate
    - rigor and discipline
    - technical guidance and technical standards
  - Most misunderstood digital attributes
    - Software hierarchy & design controls
      - Operating System Software
      - Application Software
      - Communication Software
      - Third Party Software
    - Firmware/Hardware/ design Control
    - Database Design Control
    - Display/Screen Based Soft Controls Design Control
    - Software settings (set-point) Control
  - Not adequately addressed and enforced during design phase, Testing Phase and Post Implementation Phase

Critical Industry Issue

16

Digital Guidance

Is Guidance Adequate?

Nuclear Industry appetite for Guidelines is like a BEAR hunting and eating FISH

- Volumes of already produced EPRI guidance exists and addresses all aspects
  - ***Exception is risk informed PRA driven D3 analysis***
  - **Cyber Security Strategy for PLANT SYSTEMS (new)**
- Industry issues point to
  - Utilities/vendors/integrators complacent in using the guidance
    - NUREG 0800 (Questions/Answers)
  - Inadequate digital processes and procedures
  - Lack of task based competencies
- Current EPRI/NEI guidance coupled with NRC endorsed IEEE standards are sufficient
- Vendors and Integrators for New Plants need clarifications on regulatory issues
  - NOT GUIDANCE

17

Digital Guidance (conti.)

Core Guidance for Digital

- IEEE standards as endorsed by Reg Guides
- IEEE 7.4.3-2
- NUREG 0800
- NUREG 0711
- NEI 1-01
- NEI 4-04
- EPRI Guide on EMI/RFI and NRC Reg Guide
- IEEE 603
- **EPRI Hybrid Control Room Guidelines**
- **IEEE guide on ACEs (FMEA)**

Industry Issue is Digital Competencies

- **Basic Knowledge (Computer Engineering Degree)**
- **Experience in digital design**
- **Understanding of standards and regulations**

18

Recommendations

19

New Plants

- Advance Plants Integrated I&C design and implementation should
  - Be process driven
  - Be RULE based standardized Architecture
  - Considers field equipment CMF
- Consider Lessons learned from current operating Plant digital upgrades/implementation
- Leverage methodologies developed across both, new plants and current operating plants
- Prepare and submit a Life Cycle Development process for one step licensing of Integrated Digital Upgrades

20

New Plants:

Establish Rules for the Chosen Platform Architecture and establish the processes to be followed thru out the LCD & LCM

US NRC:

Inspect and audit rule driven pre approved processes around a pre established platform

21

Suggestions for: One Step Licensing Approach

- For each AP proposed Integrated I & C platform, identify the Integrated "Bounded" Architecture
  - End point Vision Definition
  - Engineering & Maintenance Tools
  - Simulator/Engineering Simulator
- Architecture should meet the current US Standards and consider strategies for coping with CMFs and system failures
  - Be based on simplicity principles

22

Define Generic Rules for the Specific Platform

- Develop Standard Templates for Methodologies & Specifications based on US Standards & NUREG 0800
- Identify & Develop generic methodologies for the AP Platform
- Identify & Develop platform specific generic specifications for specific AP Platform
- Identify and Develop the process to be followed for LCD & LCM
- Identify and Develop System Design Control & Configuration Control Requirements
- Develop Applications Specific Generic Functional Requirements Specifications

23

One Step Licensing Submittal

For a pre-defined "bounded" AP Platform Architecture, submit the following to the US NRC for a step license

- Platform Architecture
  - Rules, basis and assumptions
  - Methodologies
- Generic Requirements Specifications
- Processes for LCD & LCM
- This process shall be used during the design, construction, commissioning and post implementation LCM of the Platform

Note: The above should address and meet current US standards and NUREG 0800

24

Existing Plants

- Processes and methodologies can be leveraged for existing operating plant I&C modernization
- New Integrated Platform design and applications can be leveraged and applied to current operating plant Integrated I&C modernization

25

Advantages of Process Based Approach

- Will ensure consistency over period of time within the lead entity and its' subcontractor organizations
  - Lead Vendor/Integrator/Utility
  - Third party vendors/contractors
  - A/E
- Lessons learned can be pinpointed to specific process for improvement
- Quality built into the process vs. reliance on knowledge of few
- Bounded platform will ensure ease of analysis and in coping with
  - EMI/RFI; CMF; Change Mgmt; Failure modes; .....
- Pre defined methodologies, generic requirements, and clearly defined Roles, responsibilities, and accountabilities will result in clear technical and process related directives
- Provides continuity and ease of Regulatory Interface and reviews by regulators
- Critical to success considering the current world wide evolving business model of "OUT SOURCING"
  - Expect more out sourcing of work

26

Regulatory Issues needing Clarifications

<u>New Plants and US NRC work together to define common understanding of potential issues:</u>

- RPS/ESFAS Digital Upgrades Issues
  - Pre approval of LCM approach including
    - D3 methodology
    - Control Room Operations Philosophy, including HFE/HP
    - Diverse Trip System requirements.....
- Generic pre approval of US Regulatory Standards based LCM process via SER
- Revisit 10CFR 50, Appendix B requirements for emphasis on in-house vendor process for digital
  - Cyber Security Program
  - Software Testing Program
  - Design Review Standards,.....
- Shift in Regulatory focus from pure software to real issues based on industry experience
  - Shift focus to functional requirements, risk informed techniques, requirements specifications, failure modes, testing, isolation, CC, etc

27

Regulatory Issues needing Clarifications

<u>New Plants and US NRC work together to define common understanding of potential issues:</u>

- Integrated upgrades coupled with integrated Compact Work Station based CR operations puts more emphasis on D3 for
  - Control Room
  - Safety & Non Safety Systems/platform interaction
  - Communication, isolation and Cyber Security
  - Field Equipment diversity (MCCs, ...)
- Overall Architecture Level Requirements **(Rules for the bounded Platform)**
  - Limitations and precautions
  - Control Room Philosophy
  - Alarms
  - Cyber Security
  - Normal & Abnormal System Behavior
  - D3.....

28

Recommendations: For Regulators

Clarify:

- BTP 19, D3 for
  - ESFAS/RPS
  - Integrated Control Room Strategy
- Allow Risk informed PRA techniques to address common mode failures for Integrated Digital Platforms
- ***<u>Issue SER for the "bounded " process based AP Integrated I&C Platform Architecture as part of ONE step license</u>***

29

Recommendations for EPRI

- Explore with US Utilities need for the following:
  - Graded Approach based STAND ALONE Technical & Administrative Guidance Procedures for SR/NSR Digital Design
    - FMEA/Testing (FAT/SAT/OAT)/EMI-RFI/V&V/Cyber Security.....
  - Procedures for Digital Systems Design Guidance in
    - Design Control/Change Control/Configuration Control/Functional Specifications
  - Generic methodologies and templates (as discussed in this presentation)

<u>Note: Products developed need to be generic and of direct use to the utility staff for new as well as advanced plants</u>

- Products should be developed for improving utility programs, processes, procedures and competencies for digital

30

Overall Conclusion

Suggest forming under NEI, a Focused Team of New Plant vendors/US NRC/EPRI/Select Utility Members to address regulatory positions for Integrated I&C Platforms

1. Develop a list of all perceived regulatory issues from both sides and develop an action plan.
2. Address each issue and clarify the regulatory interpretations
3. Identify regulations needing urgent attention
4. Document the regulatory clarifications and reach mutual consensus

Note: Effort should be a time restrained focus effort

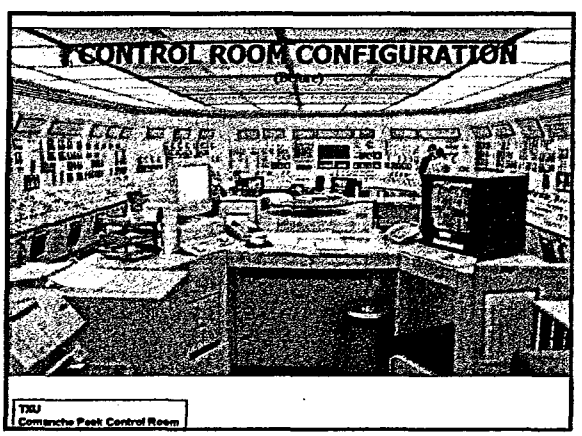
31

Overall Conclusion

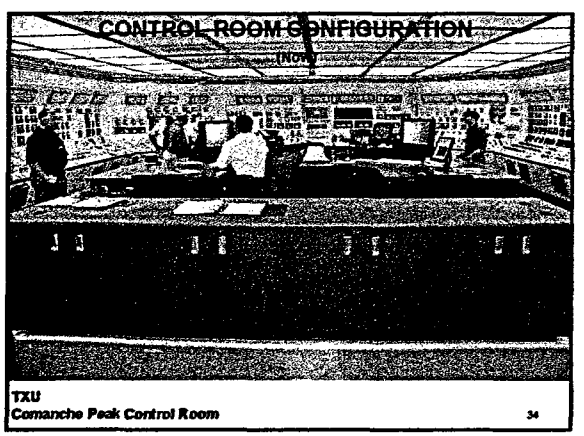
- Define a standard Process based framework for Integrated Digital I&C modernization that leverages on
  - Standardized Integrated bounded Platforms
  - Methodologies
  - Generic Requirements
  - Technical Standards
  - *Programs, processes and procedures*
- Recommend NEI Led joint effort w/ EPRI/New Plant Vendors/Select Utility members support development of a uniform methodology for One Step ***Process based*** License for Integrated Digital I&C
- Recommend NRC involvement in the process to accelerate the effort

Note: Effort should be a time restrained focus effort

32

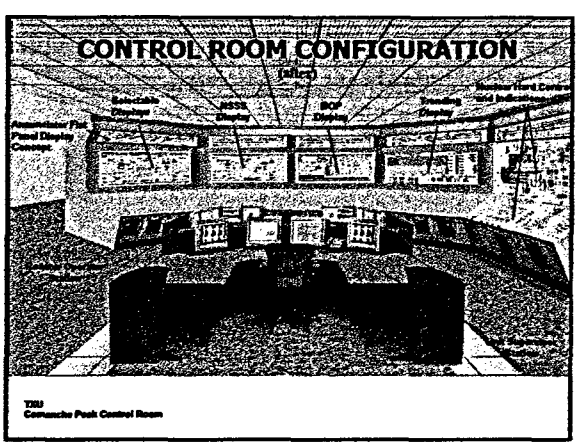


TXU
Comanche Peak Control Room



TXU
Comanche Peak Control Room

34



TXU
Comanche Peak Control Room

Questions & Comments

36