Regulatory Requirements for Safety Classified FPGA-based VDU Systems

Gerard Lekhema

National Nuclear Regulator - South Africa

For the protection of persons,property and the environment against nuclear damage.

12th International Workshop on Application of FPGAs in Nuclear Power Plants

14 – 16 October 2019, Budapest, Hungary

Executive Summary

Human-System Interfaces play a vital role in ensuring safe and reliable operation of NPP: Information display, controls and alarms.

Rapid developments in technology and behavioral science

First Generation

HFE Based on Intuitive Common sense

Second Generation

HFE based on Ergonomic and Anthropometric Norms

Third Generation

HFE addressing cognitive aspects of human performance

- Regulatory requirements for Safety Classified VDU Systems
- Standards and guidelines for application of VDUs in Control Rooms
- The role FPGA-based controller play in VDU

Contents

1. Overview of NPP in South Africa

2. NNR Regulatory Framework

3. Design Basis for VDU Systems

4. FPGA-based Drivers for VDU Systems

5. Conclusion

NPP in South Africa

The NPP Regulated by NNR - Koeberg

- 2 Units each rated at: 921 MW_e (net)
- Commercial operation since 1984 & 1985
- Analogue I&C Safety Systems (i.e. RPS)
- Digital I&C safety related systems (i.e. Reactivity control)

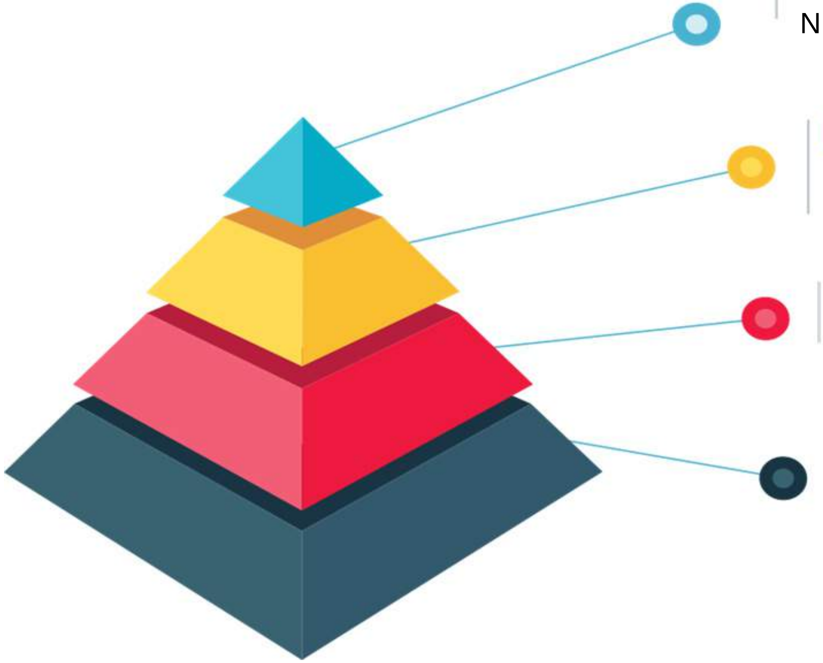
Source: J. Lagerwall

Control Room Systems:

- Second generation/hybrid
- Safety Systems: Analogue displays
- Safety related and support system: Computer driven VDU
- Modernisations: Fire detection

Regulatory Framework

Process-based regulatory approach



Level 0

NNR Act, Regulations

Level 1

Regulatory Requirements, Regulatory Directives and Policies *

Level 2

Regulatory Guides, Position Papers **

Level 3

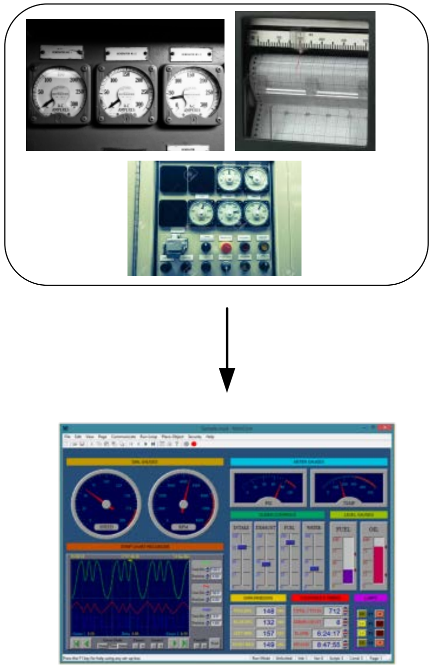
Technical Reports (review and research reports)
Compliance Assurance Reports (Inspections, audit and Surveillance reports), Safety Evaluation Reports, Letters

* RD-0034: Quality and Safety Management Requirements for Nuclear Installations

** PP-0017: Design and Implementation of Digital I&C for Nuclear Installations - 2014

** RG-0014: Guidance on Implementation of Cyber Security for Nuclear Facilities – 2015

VDU Systems in NPP



Display aspects: Transitioning from single-sensor single-display to Consolidated display - WHAT & HOW)

- Display types: cathode-ray tube (CRT) and flat-panels displays (Plasma display, LCD, LED Display, Organic LED, etc.)
- Display locations
- Display content
- Methods of navigation through displays

Control aspects: Transition from hardwired to soft controls

- Soft controls: touch screens, light pen, mouse and keyboard
- Control action uniformity
- Spatially dedicated and continuously available controls

Design Basis for Displays and Controls

- Safety classification of SSCs important to safety
- Specification of requirements for different safety classes
  - Architectural requirements for I&C systems
  - Human-systems interface requirements

• Safety classification

- Reference standards: IEC 61226, IAEA SSG-30, IEEE 603-2009
- Identification of safety functions: reactivity control, heat removal, confinement of radioactive materials.
- Categorisation of safety functions: Consequences of failure, frequency of PIE.
- Allocation of categorised functions to safety classes.
- Requirements specification for different safety classes.
- Inconsistencies in I&C functions classification - CORDEL Digital I&C Task Force
- Safety categories: IEC/IAEA - (A, B, C); IEEE – essential to safety
- Safety classification: IEC/IAEA – (1, 2, 3); IEEE (Class 1E)

Safety Classification…cont.

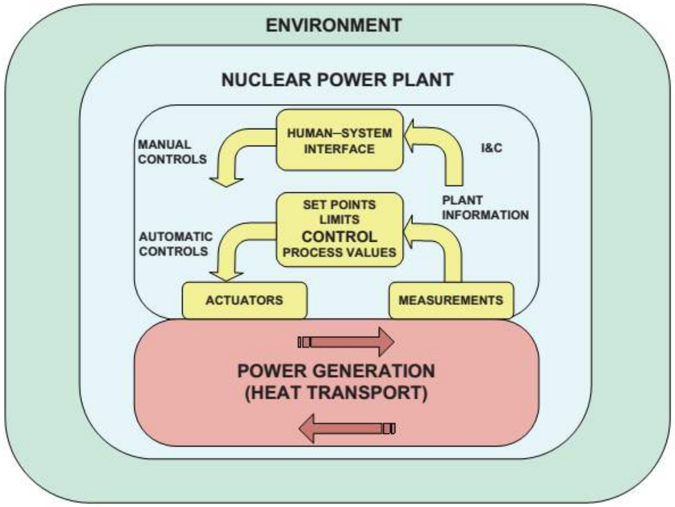
Allocation of VDU Based on Classification			
IEC 61226:2009		IEEE 603-2009 & IEEE 7-4.3.2-2016	
Cat A	Essential info. for Operator Actions	Class 1E	- Display and controls should be dedicated to specific safety divisions. - Conditions for use of non-safety displays and controls
Cat B	Automatic control, protection & post accident monitoring		
Cat C	Alarms, data processing systems		

- Typical application of VDUs
  - Screens on dedicated safety panels
  - Screens and LSD for safety related functions
  - Screens and LSD for with no safety relevance
  - Screens with integrated soft controls

Design Criteria for Safety VDU Systems

VDUs should maintain the safety I&C architectural requirements:

- Diversity at different levels of defense
- Redundancy and independence
- Quality
- Reliability requirements i.e. soft vs hardwired failure rates
- Environmental and seismic qualification
- Simplicity in design
- Testability



Conditions for Multidivisional VDU

Additional restrictions/conditions for safety & non-safety multidivisional VDU & Controls (IEEE 7-4.3.2, DI&C-ISG-04**, IEC 61500):

- Primary objective should be to enhance safety
- Independence and Isolation: Safety systems should maintain independence (communication of information, prioritization of control signals, etc.)
- Malfunctions and spurious actuations: should be bounded by the plant safety analysis

HFE Considerations

The design of VDU should take into consideration the interaction of the user with the display and control systems.

- Display requirements: task analysis, information required, actions to be undertaken, workload reduction.
- Information presentation: Simple, clear, standardized formats (colors,& symbols), screen update frequency, view angle, room lighting.
- Control/display considerations: administrative and security features, interactive logic displays.
- The level of expertise and training of user.

Advantages and Limitation of VDU

Advantages	Limitations
Information condensation and abstraction – most relevant information is displayed.	Navigating between pages may result in operator action delay
Compact size allows for reduction in size of main control room – improvement in ergonomics.	Rich graphics require microprocessors & runtime software – increased V&V efforts
Enhanced operator support: alarms, computerized procedures, logic based diagnosis, etc.	The software CCF vulnerability of computer driven VDU should be addressed
	Rapid obsolescence of microprocessor technology

FPGA-Driven Safety VDUs

Developments in FPGA driven display graphics i.e. NuScale Power:

- Diverse technology for display units drivers
- Lower complexity (no run-time software): simpler V&V, faster response time, deterministic performance
- Less prone to obsolescence due to greater application portability

Conclusion

- Safety VDUs should maintain the architectural design requirements of safety I&C functions.
- The design of safety VDUs should take into consideration the human factors engineering aspects.
- The FPGA-based graphics drivers for safety VDUs can addresses some of the microprocessor based graphics drivers.

THANK YOU

Gerard Ratoka Lekhema
Senior Analyst - NPP Assessments Department

National Nuclear Regulator – South Africa
Phone: +27 (12) 674 7157
Mobile: +27 (83) 667 2138
Email: glekhema@nnr.co.za

Eco Glade Office Park I Eco Glades Office 2 Block GI 420 Witch Hazel Avenue I Centurion
P. O. Box 7106 I Centurion I 0046 I South Africa