U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

EVALUATING DIVERSITY IN NPP SAFETY SYSTEM DESIGNS

Michael E. Waterman, RES/DE
Richard T. Wood, ORNL

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

REGULATORY REQUIREMENTS FOR DIVERSITY

- 10CFR50 Appendix A, GDC 22, "Protection System Independence," requires
  - ". . . . Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

REGULATORY POSITIONS

- SRM for SECY 93-087
  - Verify adequate diversity has been provided to meet the criteria established by NRC requirements
- BTP 7-19
  - Identify potential CCFs
  - Analyze Chapter 15 events using realistic assumptions in conjunction with each CCF
  - If the calculation exceeds a safety threshold, add diversity to mitigate the effects of the CCF
- NUREG/CR-6303 describes a method for assessing D3

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

OBJECTIVE OF RESEARCH

- Issue
  - D3 analysis is used to determine whether diversity should be added or incorporated into a proposed safety system design
  - If diversity is required, how much diversity is enough?
- Objective
  - Develop a process for determining the adequacy of proposed diversity added or incorporated into safety system designs on the basis of experience from other industries, countries and agencies, and NUREG/CR-6303 diversity attributes and criteria

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ASSUMPTIONS

- Diversity strategies developed by other industries, agencies, and countries are based on experience and logical rationale
- This experience and rationale can be combined with NUREG/CR-6303 diversity attribute criteria to develop a process for evaluating diversity in proposed I&C designs
- The process can be used to evaluate diversity in I&C system designs independent of the technology used in the diverse designs
- The acceptance threshold can be derived on the basis of experience and best practices, with industry and public feedback

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SOURCES OF INFORMATION

- NASA
- Aviation
- Industrial Applications
- International Positions on Diversity
- Nuclear Power Plants using Diversity in Safety Systems
- Typical ATWS systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

REVISED NUREG/CR-6303 DIVERSITY ATTRIBUTES AND CRITERIA

Design
- Different technologies
- Different approaches within a technology
- Different architectures

Function
- Different underlying mechanisms
- Different purpose, function, control logic, or actuation means
- Different response time scale

Life Cycle
- Different design organizations/companies
- Different management teams within the same company
- Different designers, engineers, and/or programmers
- Different testers, installers, or certification personnel

Equipment Manufacturer
- Different manufacturers of fundamentally different designs
- Same manufacturer of fundamentally different designs
- Different manufacturers of same design
- Same manufacturer of different versions of same design

Logic Processing Equipment
- Different logic processing architectures
- Different logic processing versions in same architecture
- Different component integration architectures
- Different communication architectures

Logic
- Different algorithms, logic, and logic architectures
- Different timing or order of execution
- Different operating systems
- Different logic languages

Signal
- Different reactor or process parameters sensed by different physical effects
- Different reactor or process parameters sensed by the same physical effect
- The same process parameter sensed by a different set of similar sensors

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

USES OF DIVERSITY ATTRIBUTE CRITERIA

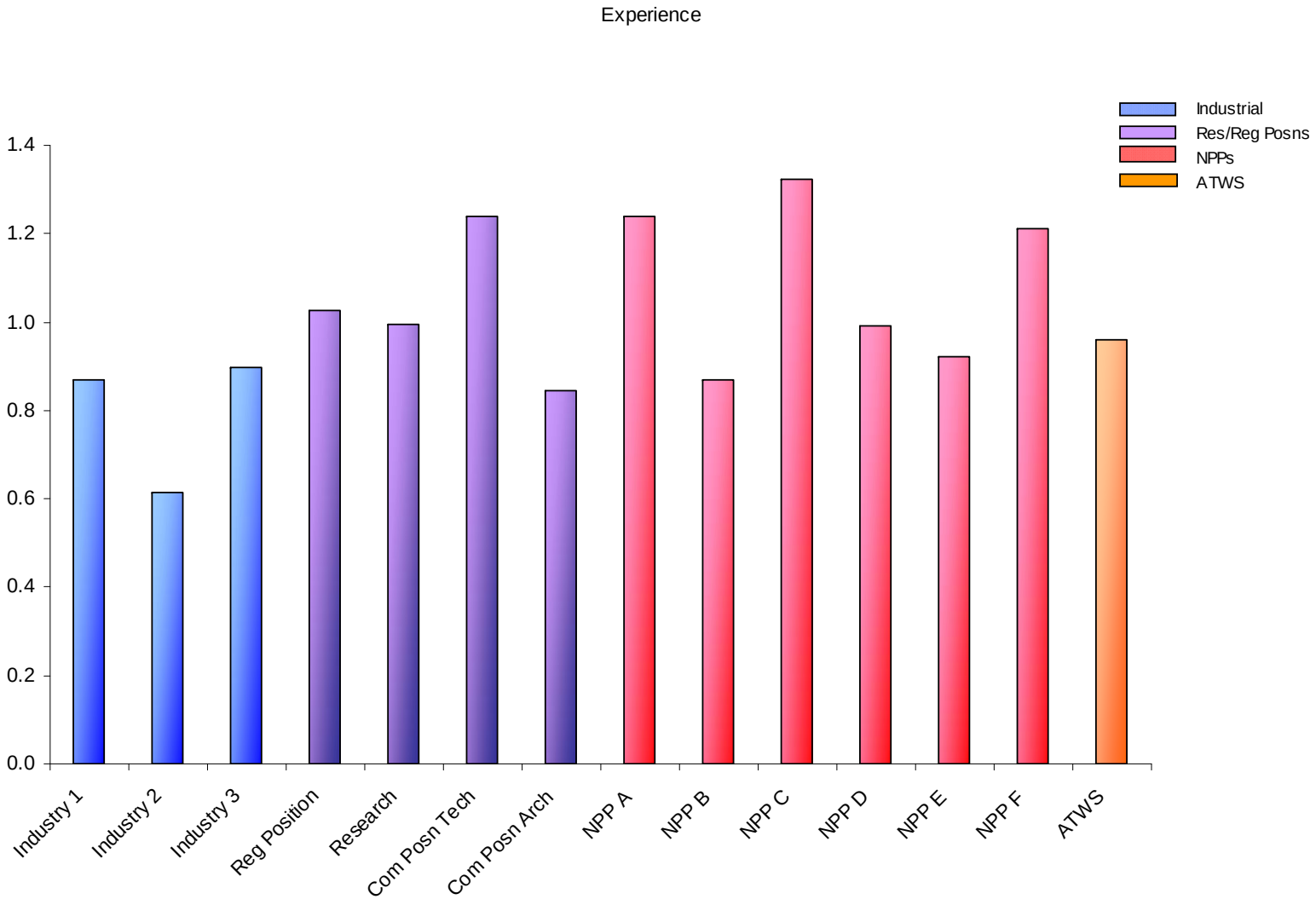
- Explicit use
  - Criteria used by a system developer to incorporate diversity into a system design
- Inherent use
  - Criteria invoked thru the explicit use of other criteria
- Example
  - A system developer chooses **Different Technologies** for the diversity approach, and implements the diverse system using analog components - **Different Technologies** has been selected explicitly
  - As a result, applicable **Equipment Manufacturer**, **Logic Processing**, **Software**, and **Life Cycle** diversity attribute criteria are inherently included in the diverse system implementation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

EVALUATING DIVERSITY IN SAFETY SYSTEM DESIGNS

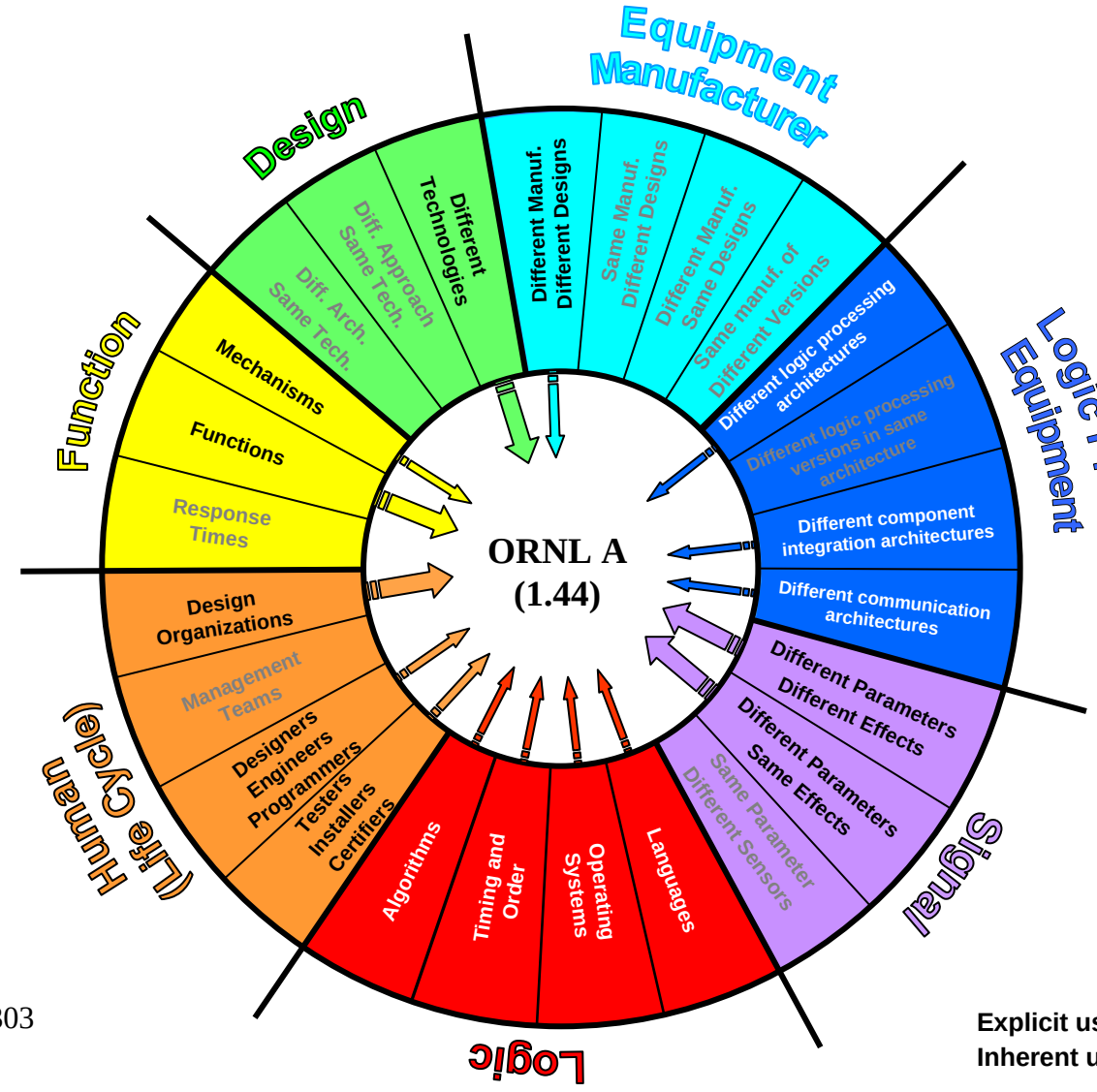
- Development of scoring method
  - Size, weight, and application complexity screened out NASA and aircraft system applications
  - Criteria usage by other countries, industries, and agencies were correlated with revised NUREG/CR-6303 diversity attributes and criteria to calculate weighted scores for each diverse I&C system design
  - The scores were used to develop an initial example threshold value
  - The scores and threshold value were then normalized by the threshold value
- Final acceptance threshold to be determined

DIVERSE SYSTEM DESIGN SCORING



ORNL DEVELOPED THREE DESIGN-BASED DIVERSE SAFETY SYSTEM APPROACHES

DIFFERENT TECHNOLOGIES

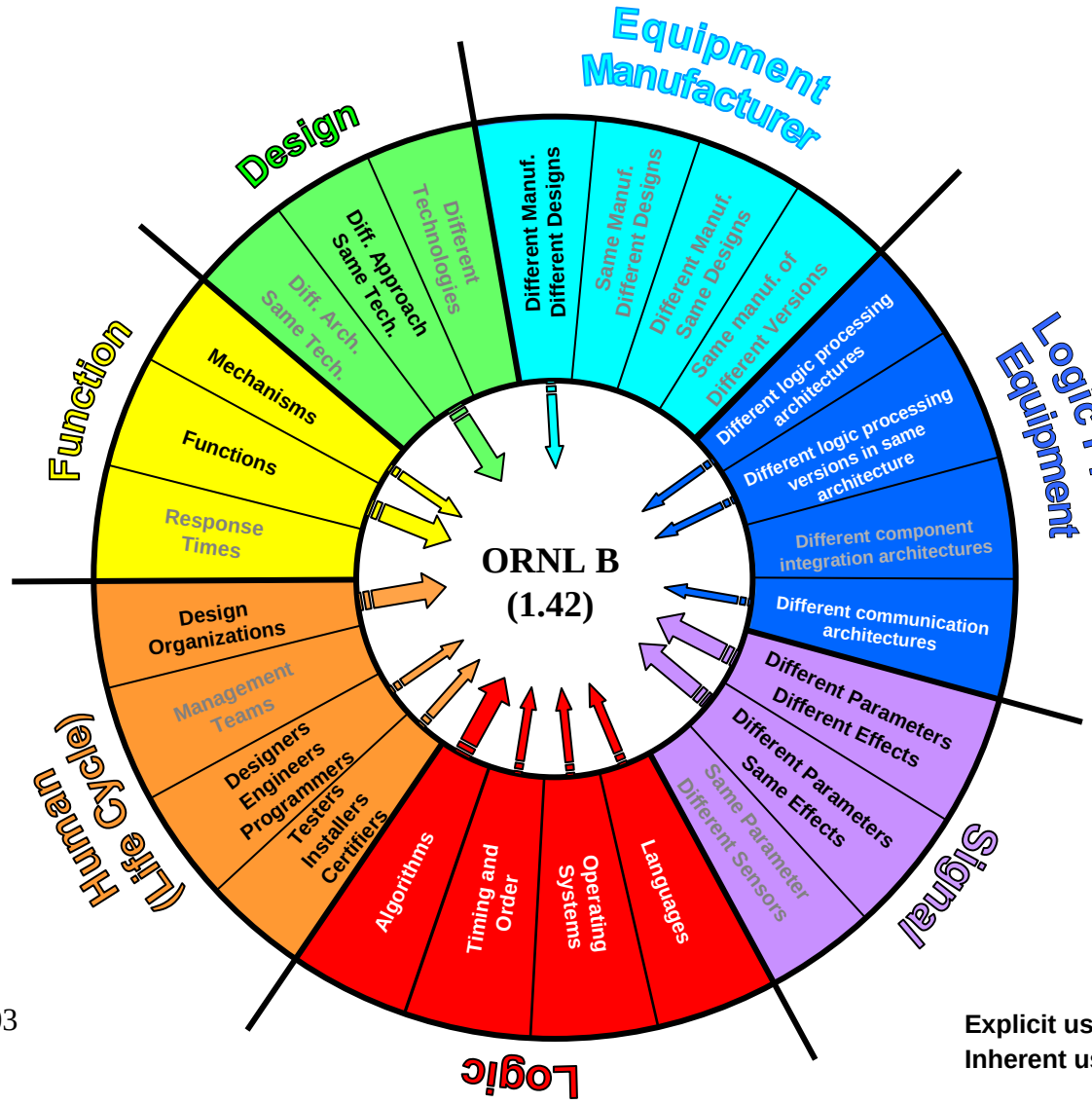


NUREG/CR-6303
Norm = 1.0

Explicit use of Criterion
Inherent use of Criterion

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIFFERENT APPROACHES IN SAME TECHNOLOGY

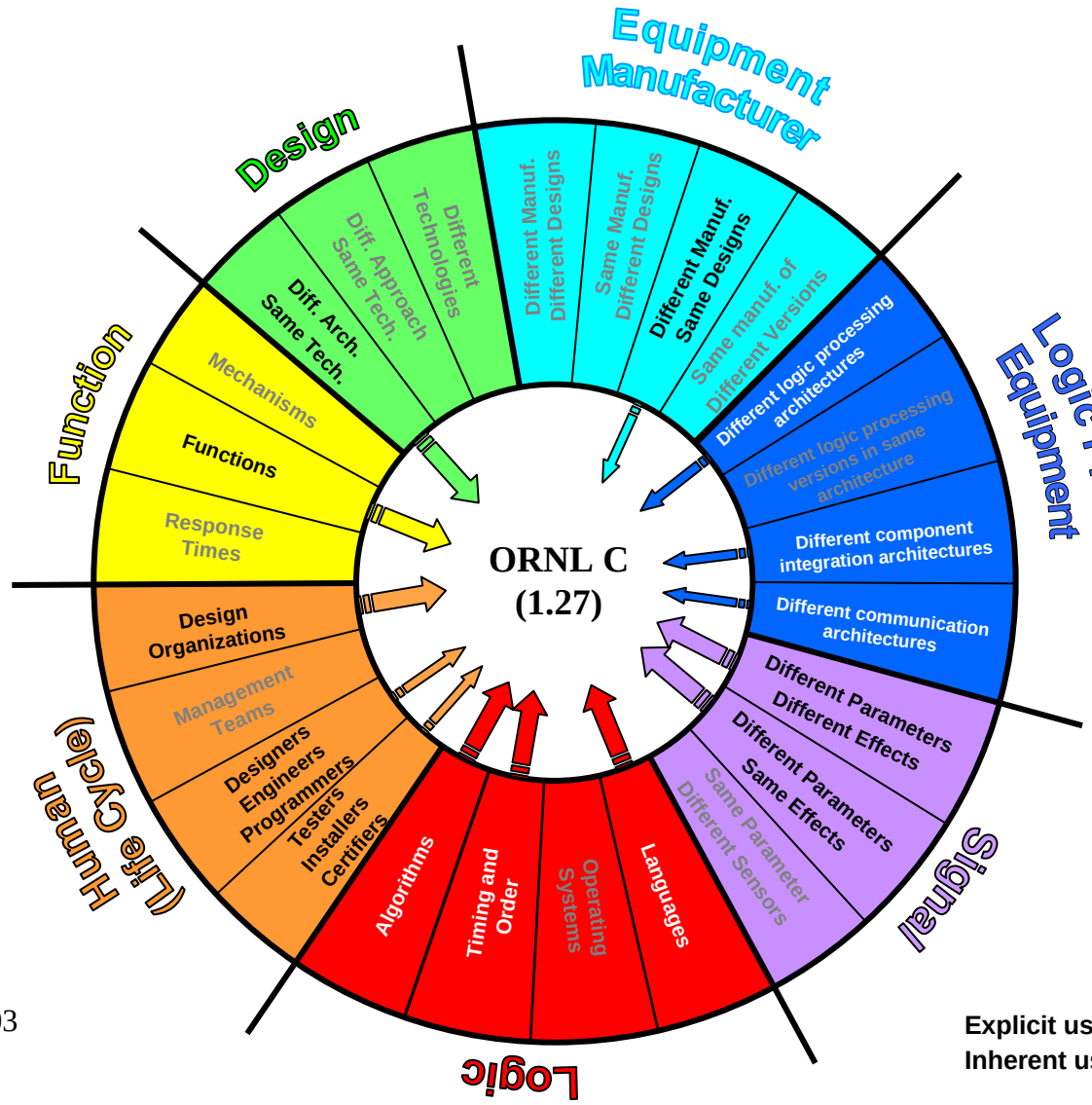


NUREG/CR-6303
Norm = 1.0

Explicit use of Criterion
Inherent use of Criterion

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIFFERENT ARCHITECTURES IN SAME TECHNOLOGY

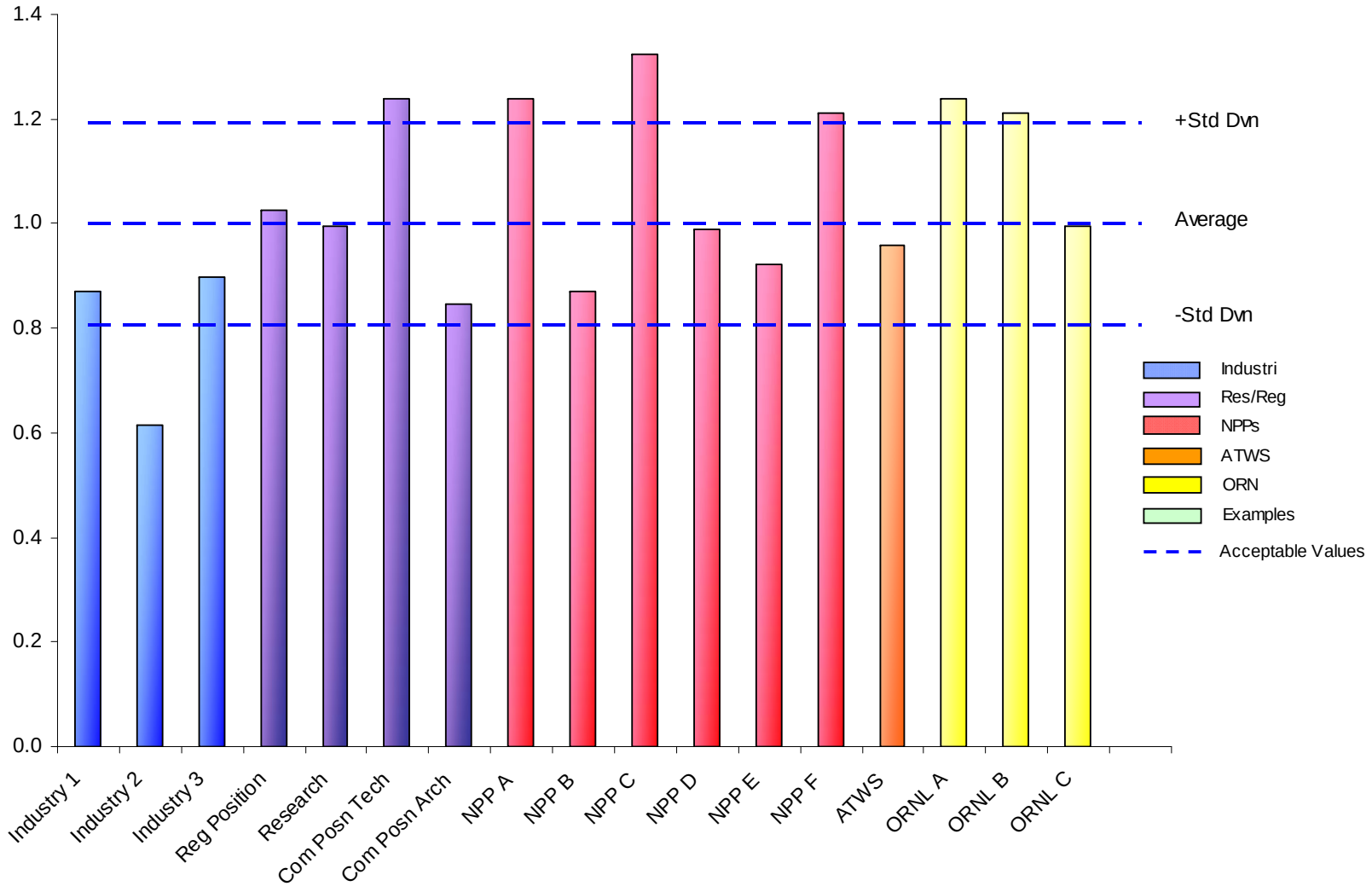


NUREG/CR-6303
Norm = 1.0

Explicit use of Criterion
Inherent use of Criterion

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACCEPTABLE DIVERSE SYSTEM DESIGN APPROACHES

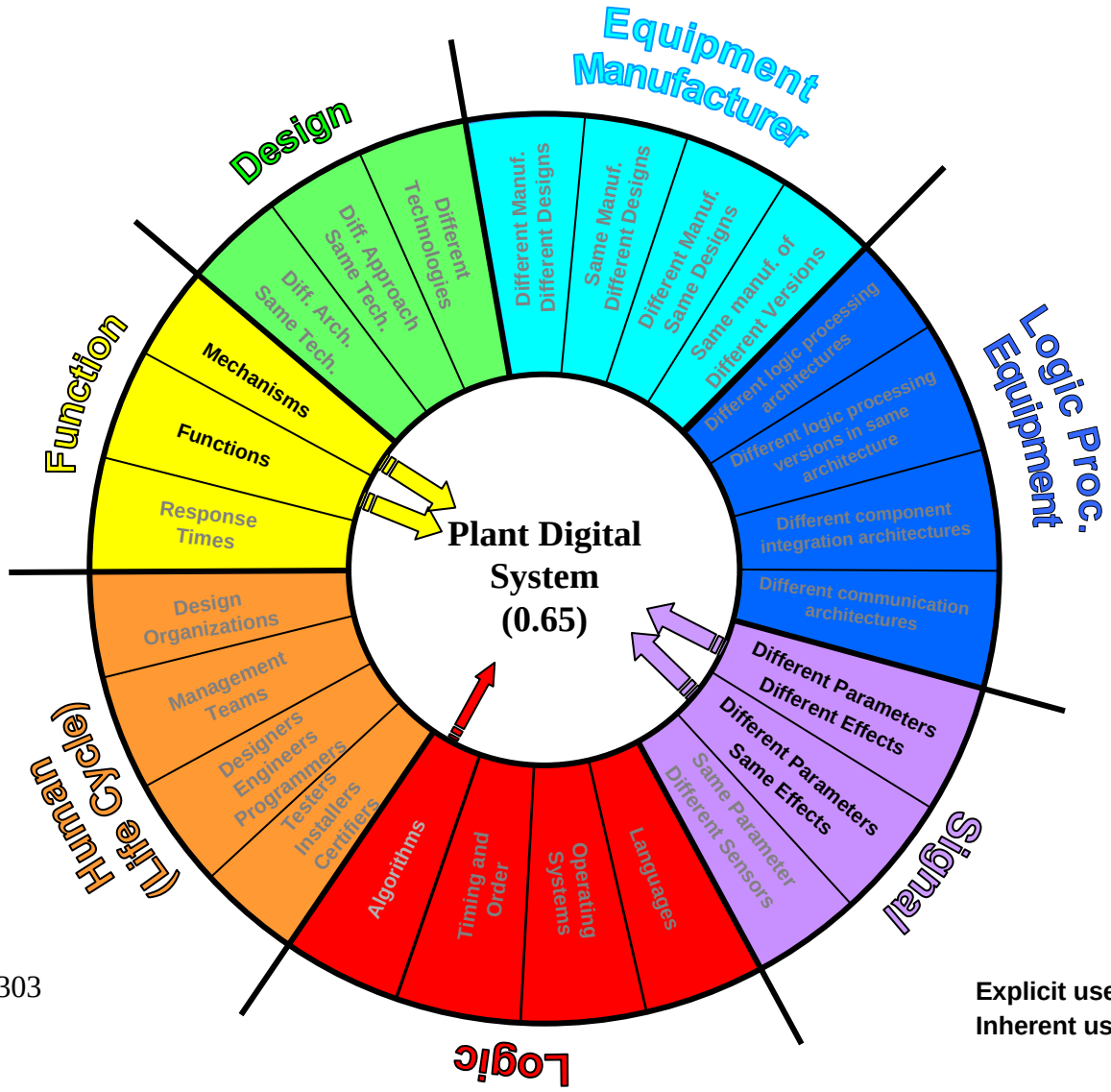


U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DEVELOPING A DIVERSE FUNCTION OR SYSTEM USING THE SCORING METHOD

EXAMPLE

INITIAL PLANT DIGITAL SYSTEM DESIGN

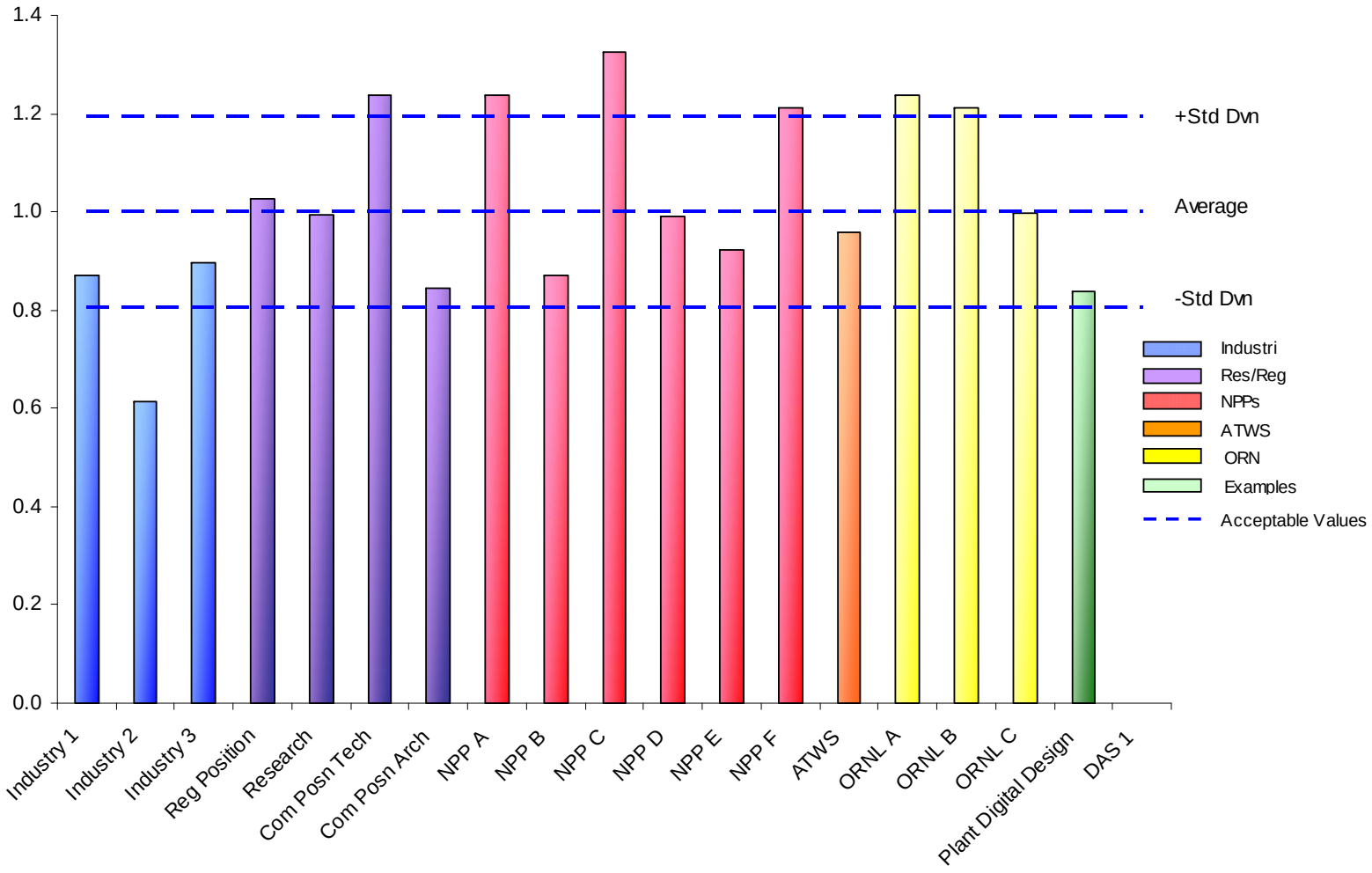


NUREG/CR-6303
Norm = 1.0

Explicit use of Criterion
Inherent use of Criterion

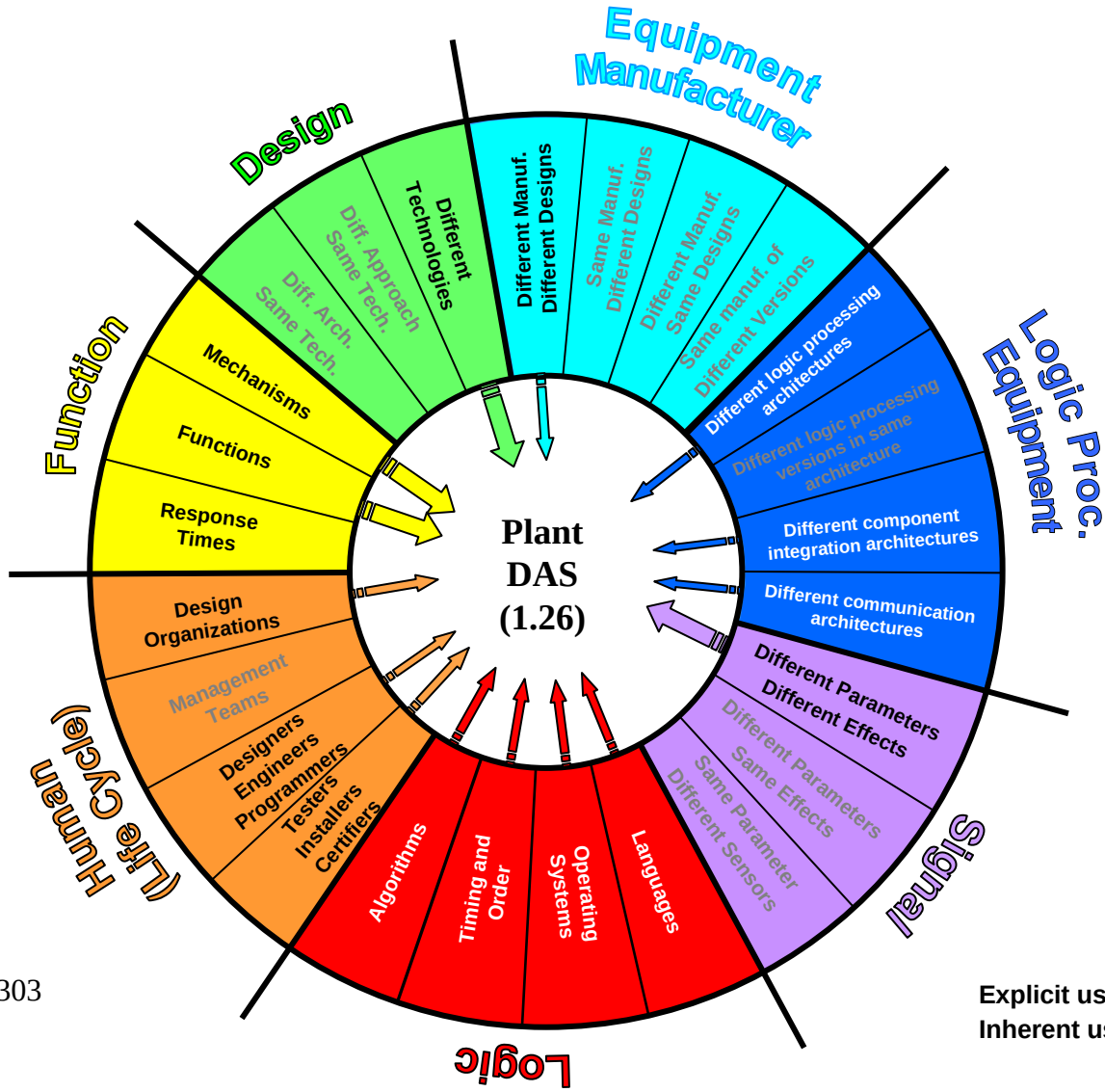
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

INITIAL PLANT DESIGN



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DAS DESIGN

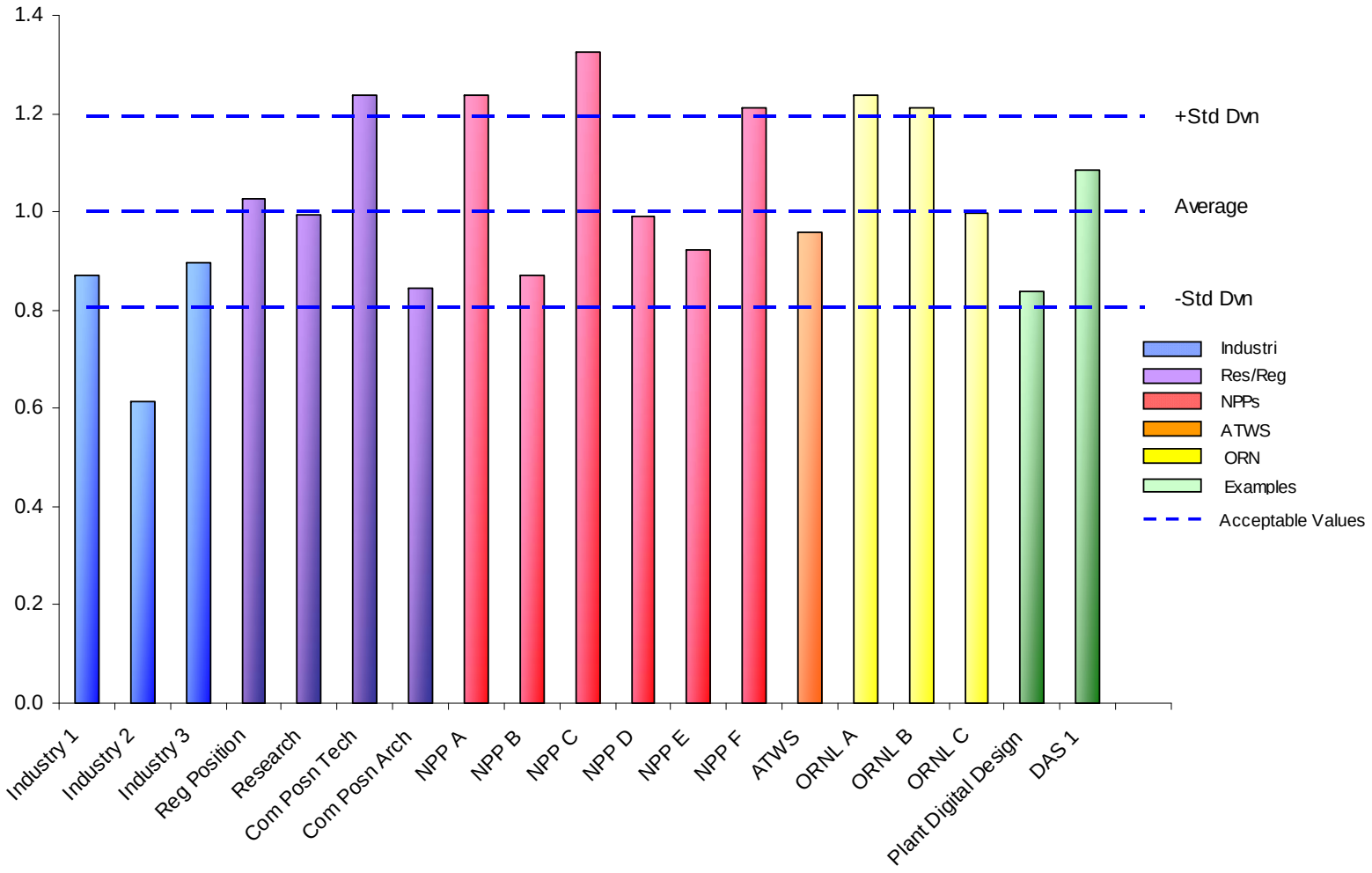


NUREG/CR-6303
Norm = 1.0

Explicit use of Criterion
Inherent use of Criterion

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

PLANT DESIGN DAS



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIVERSE SYSTEM DEVELOPMENT CONSTRAINTS

- The set of diversity attributes in the diverse system design should address the postulated CCF mechanisms
  - Example: If a Software CCF, a Function CCF, and a Logic Processing CCF are postulated, criteria from these attributes should be included in the diverse system design
- The diverse system should include design diversity attribute criteria; however, adequate diversity strategies can be developed without the Design attribute
- The threshold value (1.0) must be achieved

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

SUMMARY

- World-wide experience has been correlated with NUREG/CR-6303 diversity attribute criteria
- The correlation process is flexible enough to accommodate future data
- The correlated data can be used to evaluate proposed diverse system designs quantitatively
- An initial acceptance threshold has been determined on the basis of the relative effectiveness of NUREG/CR-6303 diversity attribute criteria and experience
- An acceptance threshold can be derived on the basis of data

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NEXT STEPS

- Stakeholder feedback
  - Determine appropriate acceptance threshold value
- Review and incorporate comments into NUREG and process
- Develop systematic process for evaluating proposed diverse safety system designs
- Incorporate acceptance criteria and evaluation process into licensing process
  - Revise NRC guidance to reference process
  - Evaluation procedures supporting SRP

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

BACKGROUND INFORMATION

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

DIVERSITY CRITERIA SCORING

- Criterion Effectiveness Ranking in Attribute
  - NUREG/6303 inverse rank/sum of the ranks in attribute
- Frequency of Usage
  - Number of diverse safety system designs using criterion/total number of diverse safety system designs
- Relationship Between Ranking and Frequency
  - Score = Weight * Ranking + (1-Weight) * Frequency
- Scores normalized by average score minus one std deviation
- Average score minus one std deviation used as threshold value for acceptable diversity

RANKING WEIGHT W_{Rij}

- **Ranking weighting factor for Criterion *i* in Attribute *j***

$$W_{Rij} = \frac{(N_{cj} - M_{cij} + 1)}{\sum_{i=1}^{M_{cj}} M_{cij}}$$

$$N_{cj} = \text{Number of Criteria in Attribute } j$$

$$M_{cij} = \text{Rank of Criterion } i \text{ in Attribute } j \ ^{*}$$

* Criterion rank specified in NUREG/CR-6303

FREQUENCY WEIGHT W_{Fij}

- **Frequency of usage weighting factor for Criterion *i* in Attribute *j***

$$W_{Fij} = \frac{N_{Sij}}{N_s}$$

N_{Sij} = Number of system designs using Criterion i of Attribute j

N_s = Number of system designs used to determine average score

CRITERION IMPORTANCE WEIGHT W_{ij}

- **Weight applied to Criterion *i* used in Attribute *j* for a diverse safety system design**

$$W_{ij} = W_I * W_{Rij} + (1 - W_I) * W_{Fij}$$

$W_I =$ Importance of Ranking weight relative to Frequency weight

$W_{Rij} =$ Ranking weight for Criterion i in Attribute j

$W_{Fij} =$ Frequency weight for Criterion i in Attribute j

ATTRIBUTE IMPORTANCE WEIGHT w_{ij}

- **Weight applied to Criterion *i* used in Attribute *j* for a diverse safety system design**

$$W_k = \frac{N_{ik}}{N_{ij}}$$

W_k = Importance of Attribute k relative to other diversity attributes

N_{ik} = Number of Criteria i used Attribute k

N_{ij} = Total number of criteria used in all Strategies

SCORING

- **Scoring a diversity strategy**

$$S_l = \left(\sum_{j=1}^{7} \sum_{i=1}^{Nij} (W_j * W_{ij} \times k) \right) \times 1000^*$$

$k = 1$ if Criterion i is used

$k = 0$ if Criterion i is not used

N_{ij} = Total number of Criteria i in Attribute j

W_{ij} = Weight applied to Criteria i in Attribute j

W_k = Weight of Attribute j

S_l = Non-normalized Diversity score for Strategy l

*Scaled by 1000 for readability

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example Normalizing Value

- **Normalizing value, S_n**

$$S_n = \bar{S} - \sqrt{\frac{\sum_{l=1}^{N_s} \left(S_l - \bar{S}\right)^2}{\left(N_s - 1\right)}}$$

$$\bar{S} = \frac{1}{N_s} \sum_{l=1}^{N_s} S_l$$

$S_l =$ Non – normalized score for Strategy l

$N_s =$ Number of Diversity Strategies used to calculate average score

SCORING

- **Normalized Diversity Strategy score, S_m**

$$S_m = \frac{S_l}{S_n}$$

$$S_l = \text{Non} - \text{normalized score for Strategy } l$$

$$S_n = \text{Normalizing constant}$$

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ASSESSMENT TOOL

	ATTRIBUTE CRITERIA	NUREG/CR-6303	Rank Wt 0.8		Diverse RPS		
	DESIGN	**CRIT. #**	**WT**				
DESIGN	Different technologies	1	1.771		x		1.771
DESIGN	Different approaches within a technology	2	1.181				0.000
DESIGN	Different architectures	3	0.990				0.000
DESIGN	SUBTOTAL			0.101	1		0.179
	EQUIPMENT MANUFACTURER	**CRIT. #**	**WT**				
EQUIPMENT MANUF.	Different manufacturers of fundamentally different equipment designs	1	1.131			i	1.131
EQUIPMENT MANUF.	Same manufacturer of fundamentally different equipment designs	2	0.763				0.000
EQUIPMENT MANUF.	Different manufacturers of same equipment design	3	0.737				0.000
EQUIPMENT MANUF.	Same manufacturer of different versions of the same equipment design	4	0.326				0.000
EQUIPMENT MANUF.	SUBTOTAL			0.101	0		0.114
	LOGIC PROCESSING EQUIPMENT	**CRIT. #**	**WT**				
LOGIC PROCESSING	Different logic processing equipment architectures	1	1.303			i	1.303
LOGIC PROCESSING	Different logic processing versions in same equipment architecture	2	0.806				0.000
LOGIC PROCESSING	Different logic processing equipment integration architectures	3	0.694			i	0.694
LOGIC PROCESSING	Different communication architectures	4	0.326			i	0.326
LOGIC PROCESSING	SUBTOTAL			0.132	0		0.306
	FUNCTION	**CRIT. #**	**WT**