Digital Instrumentation & Control Training

Module 4.0

Qualification

TABLE OF CONTENTS

LIST OF FIGURES

4.0 QUALIFICATION

Module Introduction:

Welcome to Module 4.0 of the Digital and Microprocessor Control Systems Course! This is the fourth of five modules available in the Digital Instrumentation & Control Training Course. The purpose of this module is to assist the trainee in understanding the major methods and requirements in qualifying digital equipment for nuclear safety related applications and the associated terminology. This module is designed to assist you in accomplishing the learning objectives listed at the beginning of the module.

Learning Objectives

After studying this chapter, you should be able to:

1. Explain what the bases of "equipment qualification" requirements are.
2. Explain in general terms what takes place in each of the major elements of equipment qualification as addressed in the following major areas:
   a. Environmental, including aging
   b. Seismic
   c. Electromagnetic Interference (EMI)/Radio Frequency Interference (RFI)
   d. External world interface
   e. Power supply requirements
   f. Grounding
3. Explain in general terms the limits that are imposed in each of the above requirements and the source document for each.
4. Understand the documentation requirements that are applicable to both the vendor and the utility in implementing upgrades to safety related equipment using this equipment.
5. Describe in general terms the testing activities that occur during the major qualification phases described above.
6. Understand how these requirements apply to "commercial off the shelf" or COTS equipment that is qualified for use in safety related applications.
7. Understand the application of these requirements to at least two cases where new digital equipment was qualified for installation in nuclear safety related applications.
8. Understand the considerations and guidelines now in process to allow wireless communication to be used between safety related equipment in nuclear power stations.

4.1 Qualification Background

Digital equipment has been successfully and widely used in industrial facilities for over 20 years. A digital upgrade at a nuclear plant involves a collection of hardware and software specifically designed to perform a set of functions that were traditionally performed using electro-mechanical (e.g., relays) and single function electronic devices (e.g., single-loop controllers). The controls for most of the safety systems in nuclear power plants fall into this category.

Since its inception, digital equipment has been designed to operate in industrial environments. Therefore, most commercially available digital equipment hardware is capable of withstanding the stresses applied to it during nuclear safety-related Class 1E qualification testing. However, the digital equipment contains both application and operating software that requires a broader qualification effort.

A generic qualification encompasses a selection of digital equipment and the operating software. The generic qualification does not absolve the licensee from demonstrating that the specific application is

enveloped by the generic qualification. This is really no different from current qualification of devices. A qualified device can only be applied within the qualification range.

4.2 Overview and Requirements

The goal of this module is to review the generic requirements for qualifying digital equipment for use in safety-related applications in nuclear power plants. This does not relieve the utility or its designee from all the tasks needed to actually apply that digital equipment in a specific plant application.

Implicit in this qualification process is recognition of the importance of the general specification to define the essential technical characteristics of the entire equipment to address the range of plant safety applications for which it is intended. Process-oriented considerations, including system and software development and quality processes, are addressed in separate modules of this training.

The generic qualification process must address as an overview the following major focus areas as shown on Figure 4-1:

- Quality Assurance
- Environmental Qualification
- Seismic Qualification
- Power and Grounding
- Electromagnetic Interference
- Validation and Verification
- Common Mode Failure
- Diversity
- Defense in Depth

This module focuses only on the qualification related tasks listed above and their performance in the context of the applicable Quality Assurance program. The tasks for Verification (V&V), Common Mode Failure, Diversity and Defense in Depth are all addressed in separate sections of the training.

The following major steps are involved in completing a generic qualification effort:

- Selecting the digital equipment that supports the utility and application specific requirements
- Evaluating the manufacturer's (including third party and or sub-tier supplier) hardware and software QA programs applied to the products of interest
- Procure a set of modules and any associated supporting devices
- Define and produce the test system application program (TSAP) – a synthetic application designed to aid in the qualification and operability tests
- Combine the modules and the TSAP into a suitable test configuration and perform the set of acceptance testing
- Specify the set of qualification testing required
- Perform the qualification testing; review and approve the results

There are different roles and responsibilities in the development of a qualification program. These roles may be performed by a variety of organizations, but must include characteristics that meet the responsibilities included in the following:

- Manufacturer – produces the digital equipment
- Qualifier – responsible for confirming that the product line meets the requirements of the specification
- Applier – responsible for designing, implementing and testing the specific application in a specific plant

- Utility – has ultimate responsibility for the safety application and its impact on plant safety, regardless of whether the utility itself has performed any of the above roles

A number of definitions are implicit in the qualification process. A selected set from Electric Power Research Institute (EPRI) TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Plants," are included in the following, as shown in Figure 4-2:

- Baseline – a specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for application or further development, and that can be changed only through formal change control procedures
- Configuration ID – An element of configuration management, consisting of selecting the configuration items for a system or device and recording their functional and physical characteristics in technical documentation
- Test Specimen – The set of digital equipment, hardware and software configuration and test system application program used as the basis for generic Qualification Testing

In review for qualification, the following key points summarize this section:

- Qualification of digital equipment requires completion of a set of qualification tests and documentation necessary to cover all requirements as listed in NRC regulations and industry standards
- Roles for each specific set of activities have been defined
- Many safety related and Commercial-Off-the-Shelf (COTS) components have been successfully qualified to these standards as we will discuss in this module

There is a strong need for nuclear Class 1E digital equipment for upgrade of U.S. nuclear facilities.

The industry has established a process through EPRI for generic guidance on qualification of new equipment and Commercial-Off-the-Shelf (COTS) equipment.

As shown on Figure 4-3, the major requirements for qualification of digital equipment, as defined in EPRI TR-107330 are included in the following list of tasks:

- Quality Assurance
- Detailed Testing Requirements
- Engineering Analyses
- Documentation

The major emphasis on project planning needs to include development of the:

- Quality Assurance Plan
- Master Test Plan
- Software Quality Assurance Plan

The Software Quality Assurance Plan is addressed in the training section on software.

EPRI TR-107330 addresses the following major qualification requirements that must be met for Class 1E Qualification:

- Operability
- Prudency
- Environmental
- EMI/RFI

- Seismic
- Surge Withstand Cap.
- 1E/non-1E Isolation
- Electrostatic Discharge
- Availability/Reliability
- Failure Modes and Effects (FMAE)
- System Operating
- Software (generic)
- Test Application Specific
- Software Programming
- Quality Procedures

This module addresses the primary qualification areas of environmental, EMI/RFI and electrical isolation. The areas of software qualification and FMEA are addressed as part of the software module.

The major steps in conducting qualification of the new equipment are as follows:

- Define/Configure Test Specimen
  - Platform, Specific Modules
- Develop Test Specimen Application Program (TSAP)
  - Typical Set of Nuclear Power Plant Applications
  - Verify and Validate as Safety Related Software (V&V)
- Conduct Qualification Tests
  - Prequalification Tests (Baseline)
  - Qualification Tests (Stress: Environmental, Seismic, etc.)
  - Performance Proof (Check for degradation, trends)
- Quality System Software
- Provide Engineering Evaluations
- Final Report Submittal

Separately, the software is required to be qualified. This is addressed in another section of the training.

The qualification testing is conducted in a required set of phases that includes the following major sections:

- Pre-Qualification
- Setup & Checkout
- Operability
- Prudency
- Qualification Tests
- Environmental
- Seismic
- EMI/RFI
- Surge
- 1E/Non 1E Isolation
- Performance Proof Tests
- Operability
- Prudency

The first phase is the developing and performing the Operability Testing, which includes the following requirements:

- Accuracy
- Response Time
- Input/Output (I/O) Operability
- Communication Operability
- Timer Test
- Power Quality Tolerance
- Fault Operability
- Failure to Complete Scan
- Failover Operability
- Loss of Power Test
- Power Interruption Test

Next, the Prudency Testing is performed which includes the following major tests:

- Burst Of Events Test
- Failure of Serial Port Receiver Test
- Serial Port Noise Test
- Fault Simulation

Now we will focus on the major requirements in qualification. First, the environmental qualification is addressed in IEEE 323, "Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," and includes meeting the following overall requirements as shown on Figure 4-4:

- Temperature
  - 35° to 140° F
- Relative Humidity
  - 5% to 95% (non-condensing)
- Minimum Voltage and Frequency
  - 97 VAC , 57 Hz
- Temperature Profile
  - 24 Hrs @ 140° Operability, Prudency
  - 8 Hrs @ 35° Operability
  - Ambient Operability

Next, the seismic qualification requirements addressed in IEEE 344, "Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations," include the list of testing shown on Figure 4-5:

- Resonance Search
- Six Simulated Seismic Events
  - 5 Operating Basis Earthquake (OBE), 1 Safe Shutdown Basis Earthquake (SSE)
- Test Response Spectrum
  - 10g @ 5% Damping
- Test Frequencies
  - 1 To 100 Hz
- Tri-Axial Vibration
- Monitor Specimen, Relay Contacts
- Post-Seismic Testing

The last major phase of qualification is included in the EMI/RFI and electrical isolation requirements and testing as shown on Figure 4-6:

- EMI/RFI
  - Conducted Emissions
  - Radiated Emissions
  - Conducted Susceptibility
  - Radiated Susceptibility
  - High Frequency Transients
- Surge Withstand (Destructive)
- 1E/Non 1E Isolation (Destructive)

In summary, qualification for nuclear Class 1E application involves basic requirements in:

- Quality Assurance (QA) measures applied to the qualification activities
- Documentation to support the qualification
- Documentation needed to for applying the digital equipment to the specific application

Qualification Requirements

The start of all qualification activities involves the establishment of the set of requirements applicable to the digital equipment of set of components intended to be qualified. The basis for all qualification is included in the following list of references:

1. 10CFR21 - Title 10, CFR, Part 21 – Reporting of Defects and Non-Compliances
2. 10CFR50 - Title 10, CFR, Part 50, App. B, Quality Assurance Criteria

3. EPRI TR-102323 Rev. 1 - Guideline for Electromagnetic Interference Testing in Power Plants
4. EPRI TR-107330 - Generic Requirement Specification for Qualifying a Commercially Available PLC for Safety-Related Applications in Nuclear Power Stations
5. IEEE Std 279-1971 – Criteria for Protection Systems in Nuclear Power Generating Stations
6. IEEE Std 323-1983 – Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations
7. IEEE Std 344-1975 – Recommended Practice for Seismic Qualification of Class 1E Equipment and Circuits
8. IEEE Std 498-1981 – Standard Criteria for Independence of Class 1E Equipment and Circuits
9. IEEE Std C62.41 – 1991 – Recommended Practice on Surge Voltages in Low-Voltage AC Power Circuits
10. ISA S67.04 Part 1 and 2, 1994, Methodologies for the Determination of Instrument Setpoints for Nuclear Safety Related Applications
11. ISO 9000-3: 1991(E) – Guideline for the Application of ISO 9000 to the Development, Supply and Maintenance of Software
12. ISO 9001: 1987 (E) – Quality Systems – Model for Quality Assurance in Design/Development, Prediction, Installation and Servicing
13. MIL-Std 217F – Reliability Prediction of Electronic Equipment
14. Reg Guide 1.180 Rev. 1, Guidelines for Evaluating Electromabnetic and Radio Frequency Interference in Safety-Related Instrument and Control Systems
15. Reg. Guide 1.100, June, 1988 – Seismic Qualification of Electrical Equipment for Nuclear Power Plants
16. Reg. Guide 1.175 Rev. 2 – Physical Independence of Electrical Systems
17. Reg. Guide 1.180, Rev. 1, October, 2003, Guideline for Evaluating Electromagnetic Interference and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems
18. Reg. Guide 1.89, June 1984 – Qualification of Class 1E Equipment for Nuclear Power Plants
19. SQTS-01-GSQTP – Rev. 4 – Generic Seismic Qualification Technical Procedure
20. SQTS-01-Rev. 3 – Generic Seismic Test Specimen

The above listing provides the basis for all qualification requirements. It is the list, used as the basis for NRC staff review of generic qualification and has been documented many times in the Safety Evaluation Reports issued by the NRC for generic or specific qualification.

Environmental Qualification

There are a series of definitions that are very important to the overall qualification process and are included in IEEE 323:

- Aging – The effect of operational, environmental, and system conditions on equipment during a period of time up to, but not including design basis events, or the process of simulating these events
- Design Life – The time during which satisfactory performance can be expected for a specific set of service conditions

- Harsh Environment – An environment expected as the result of the postulated service conditions appropriate for the design basis and post-design basis accidents of the station. Harsh environments are the result of a loss of cooling accident (LOCA) /high energy line break (HELB) inside containment and post-LOCA or HELB outside containment.
- Mild Environment – An environment expected as a result of normal service conditions and extremes (abnormal) in service conditions where seismic is the only design basis event (DBE) of consequence
- Installed Life – The interval from installation to removal, during which the equipment or component may be subject to design service conditions and system demands
- Margin - The difference between service conditions and the conditions used for equipment qualification
- Qualification – The generation and maintenance of evidence to ensure that the equipment will operate on demand to meet the performance requirements
- Qualified Life – The period of time, prior to the start of a design basis event, for which equipment was demonstrated to meet the design requirements for the specified service conditions
- Service Conditions – Environmental, loading, power and signal conditions expected as a result of extremes (abnormal) in operating requirements, and postulated conditions appropriate for the design basis events of the station

Next to be considered are the environmental qualification requirements for normal environmental – basic requirements, as shown on Figure 4-7.

The operating environment where the digital equipment must meet the performance requirement given in EPRI TR-107330 Sections 4.3, as follows:

1. Temperature Range – -60° to 104° F
2. Humidity – 40 to 95% (non-condensing) relative humidity range
3. Power Sources – Must operate within the ranges as follows:
   - AC – 90 to 150 VAC and frequency range of 57 to 63 HZ
   - DC - +/- 15% of stated voltage
- Radiation – Up to 10^3 RADS

Next, the abnormal requirements for qualification of digital equipment are as shown in Figure 4-8 and Figure 4-9:

- The abnormal operating environment where the digital equipment must meet the performance requirement given in EPRI TR-107330 Sections 4.3, as follows:
- Temperature Range – -40° to 120° F
- Humidity – 10 to 95% (non-condensing) relative humidity range
- Power Sources – Must operate within the ranges as follows:
  - AC – 90 to 150 VAC and frequency range of 57 to 63 HZ
  - DC - +/- 15% of stated voltage
- Radiation – Up to 10^3 RADS

Seismic Qualification

The set of definitions application to seismic qualification, as defined in IEEE 344 include:

- Floor Acceleration – The acceleration of a particular building floor (or equipment mounting)
- Ground Acceleration – The acceleration of the ground resulting from a given earthquake's motion
- Natural Frequency – The frequency of frequencies at which a body vibrates due to its own physical characteristics
- Operating Basis Earthquake (OBE) – That earthquake which could reasonably be expected to affect the plant site during the operating life of the plant
- Safe Shutdown Earthquake (SSE) – That earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional

The overall requirements for seismic qualification are given on Figure 4-10 and Figure 4-11 (Figure 2):

The digital equipment shall be suitable for qualification as a Category 1 Seismic device. The digital equipment shall meet its performance requirements during and following the application of a Safe Shutdown Earthquake (SSE) simultaneously applied in three orthogonal directions. The SSE level shall be as shown in Figure 4-11 (Figure 2). The digital equipment shall withstand the SSE vibration following the application of five OBE's as shown in Figure 4-11 (Figure 2).

The digital equipment shall be operated as intended for the specified level of vibration and remain intact and fully functional.

If relay outputs are included, then the relay contacts shall be capable of changing state and maintaining state. Any spurious change shall not exceed 2 milliseconds, as documented in EPRI TR-107330.

Electromagnetic Interference

The set of definitions applicable to EMI/RFI qualification are documented in EPRI TR-102323, Rev 1 and include the following:

- EMI/RFI Sensitive Equipment – Equipment characterized by its susceptibility to electromagnetic emissions. For the purposes of the EPRI guide, it typically refers to digital safety-related equipment
- EMI/RFI Emitter – Equipment characterized by its high levels of electromagnetic emissions. In the TR-102323, these emitters are further classified as Power Generation EMI/RFI Emitters and/or High Frequency EMI/RFI Emitters
- Power Generation EMI/RFI Emitters – High voltage equipment including switchgear, motors, generators, transformers, etc, common to traditional power plant design
- High Frequency EMI/RFI Emitters – Plant digital instrumentation and control and other equipment capable of generating continuous signals or pulse trains at a frequency above 50kHz
- EMI/RFI Sensitive Cables/Conductors – Typically power and signal cables and conductors connected to low voltage Instrumentation and Control (I&C) EMI/RFI sensitive equipment

The overall requirements for EMI/RFI qualification include passing the following tests, included in EPRI TR-102323, or suitable alternative testing endorsed by Regulatory Guide 1.180:

- Radiated susceptibility per Appendix B Section 3.1.2
- Conducted susceptibility per Appendix B Section 3.2.2

- Radiated emissions per Section 7
- Conducted emissions testing per Section 7

Acceptance requirements for the EMI/RFI qualification, as provided in TR-107330 are:

- The main and any coprocessors shall continue to function
- The transfer of I/O data shall not be disrupted
- The emissions shall not cause the discrete I/O to change state
- The analog I/O shall not vary more than 3%

Electrostatic Discharge (ESD)

The overall requirements for ESD withstand are:

- When installed in the chassis, the digital equipment and associated devices shall have ESD withstand that conforms to EPRI TR-102323 Appendix B – Section 3.5. Subjecting the digital equipment to this level of ESD shall not disrupt operation or cause any damage.
- For digital equipment that includes redundancy, the performance is satisfactory if the digital equipment still performs its intended function after being subjected to the specified level of ESD. A failure of one of more of the redundant devices that does not result in the inability of the digital device to operate as intended is acceptable.

Electrical Isolation

IEEE 384, "Standard Criteria for Independence of Class 1E Equipment and Circuits," and TR-107330 provide the overall requirements for electrical isolation qualification.

First, the major definitions applying to this electrical separation and isolation include:

- Associated Circuit – Non-Class 1E circuits that are not physically separated or are not electrically isolated from class 1E circuits by acceptable distance, safety class structures, barriers or isolation devices
- Division – The designation applied to a given system or set of components that maintains isolation from other sets of components
- Isolation Device – A device in a circuit which prevents malfunctions in one section of a circuit from causing unacceptable influences in other sections of the circuit or circuits
- Separation distance – Space which has no interposing structures, equipment or materials that could aid in the propagation of fire or that could otherwise disable Class 1E equipment

Next, the basic requirements documented in IEEE 384 and TR-107339 are as follows:

- Per EPRI TR-107330, the electrical separation barriers shall be part of the overall system design requirements
- The class 1E/Non-1E isolation requirements shall be provided to at least 600 VAC and 250 VDC applied for a period of 30 seconds. Isolation features shall conform to the instrumentation and control requirements for class 1E to non-class 1E connections given in IEEE 384. Isolation capability testing shall be performed to the digital equipment and any auxiliary isolation devices to be covered by the qualification. It previously qualified external isolators are used, then this testing is not required

The acceptance criteria are shown on Figure 4-12.

For discrete I/O, relay outputs, and analog inputs, applying this level of isolation for the specified time shall not disrupt the operation of any other modules or disrupt the operation of the main processor. For analog outputs, applying a signal within the specified range for the specified time, shall not cause more than a 0.05% change to any other channel on the module, or disrupt the operation of the chassis backplane. External devices, previously qualified, may be used to meet these requirements.

Power Supply Requirements

Per EPRI TR-107330, all qualified equipment must have the capabilities of continuous operation under the following conditions:

- Power supplies for connection to AC sources with operation varying from 90 to 150VAC and a minimum frequency range of 57 to 63 Hz
- Power supplies for connection to a DC source shall be operable over a range of 15% variation from the nominal value
- The supplies shall be capable of supplying 1.2 times the bus loading when the digital equipment contains a main processor plus a module in each of the slots (for example). The power capability shall be based on the load for a presumed I/O configuration included in the qualification process

Grounding Requirements

Grounding and shielding is critical to both meeting and maintaining the qualification of digital equipment as Class 1E. IEEE 1050, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," and EPRI TR-102323 provide the overall and specific requirements for shielding connections for chassis and I/O modules. If this grounding process is not followed, exposure to many kinds of electrical and electrostatic transients, not included in the qualification process, can have major adverse effects on equipment performance.

Summary of Qualification Requirements

The major areas of qualification have been addressed in this section including:

- Environmental Qualification (EQ)
- Seismic
- EMI/RFI
- Electrostatic Discharge
- Electrical Isolation
- Power
- Grounding Requirements

Many cases of successful qualification of new or COTS digital equipment have been completed and accepted by NRS staff in issued Safety Evaluation Reports (SERs).

In review for qualification, the following key points summarize this section:

- The basis for qualification is clearly defined but still evolving in areas such as EMI/RFI
- Many digital I&C components have been qualified through this set of requirements and are being installed in nuclear plants.
- The key to a successful upgrade is meeting the requirements for the specific installation used and maintaining the qualification onsite.

4.3 Qualification Testing and Analysis

Pre-Qualification Acceptance Tests:

Prior to qualification testing, various acceptance and operability testing is conducted. These tests cover the following major areas and objectives:

- In general, the acceptance tests are those tests performed on a test specimen prior to any qualification tests to confirm that the test specimen operates correctly and to provide baseline data for the qualification testing
- The operability tests are tests performed at various points in the qualification process to confirm that the digital device operation is satisfactory following the stresses applied during qualification
- Prudency testing exercises the digital equipment in ways that tests its ability to perform under highly dynamic conditions

Prior to Qualification Testing, the following tests are performed to demonstrate that the hardware and software test specimen operate as expected and to provide a basis for the qualification tests:

- Initial calibration – check on calibration to requirements
- System integration – based on requirements specification
- Operability testing – establishes baseline performance
- Prudency tests – establishes baseline performance
- Burn-in test – operates equipment for a minimum of 352 hours – used to detect any early life failures

The following critical characteristics are verified by this initial acceptance testing as shown on Figure 4-13:

- Accuracy
- Response time
- Discrete input operability
- Discrete output operability
- Communications operability
- Coprocessor operability
- Timer tests
- Test of failure to complete scan detection
- Failover operability tests
- Loss of power test
- Power interruption test

Prudency testing is conducted next.

These tests shall be applied to specific equipment configuration – at the minimum power supply source values as specified and shall include (as an example):

- Burst of events testing
- Failure of serial port receiver testing
- Serial port noise testing
- Fault simulation

Qualification Testing and Analysis

The following major steps are conducted in sequence to complete qualification testing of a specific component:

- Benchmark the digital product line against the requirements that can be demonstrated by test or analysis. Select the item from the product line to be qualified.
- Evaluate any exceptions or enhancements to the requirements document applicable to the specific configuration
- Prepare qualification and test plans based on the requirements specified
- Assemble the test specimen with the appropriate configuration
- Perform the testing following the test plans
- Evaluate the recorded data against the acceptance criteria.

- Document the qualified configuration and limits of qualification.

The hardware configuration to be used shall be developed and documented consistent with the requirements and shall consist of at least the following:

- At least one of each type of module needed to encompass the requirements
- Any additional modules needed to support operability testing
- At least one of each type of ancillary device
- At least one of each type of chassis
- Power supplies to meet the requirements
- If necessary, dummy modules to assure all slots are filled to provide power supply and weight loading
- At least one type of termination device used to provide field connections
- Any modules needed to demonstrate redundancy per spec.

Test equipment to support the acceptance testing and operability testing shall also be provided, including:

- Panel or other devices for connection to the inputs and outputs
- Test and measurement equipment with accuracy needed to support the acceptance criteria
- Any special tools and devices needed to support testing
- All test equipment shall be controlled per IEEE 498

The qualification testing shall be performed in the following sequence:

- Environmental testing for abnormal temperature and humidity
- ESD testing
- Seismic testing
- EMI/RFI testing
- Surge withstand testing
- Class 1E to Non-1E Isolation testing

NOTE: Per EPRI TR-107330, the order of the last five items may be interchanged to account for testing stresses on the samples and for convenience.

Environmental qualification is the first of the major testing phases and encompasses the following major requirements, following IEEE 323:

- Temperature
  - 35° to 140° F
- Relative Humidity
  - 5% to 95% (non-condensing)
- Minimum Voltage and Frequency
  - 97 VAC , 57 Hz
- Temperature Profile
  - 24 Hrs @ 140° Operability, Prudency
  - 8 Hrs @ 35° Operability
  - Ambient Operability

Seismic qualification is the next major phase and is conducted following IEEE 344 and includes the following:

- Resonance Search
- Six Simulated Seismic Events
  - 5 OBE, 1 SSE
- Test Response Spectrum
  - 10g @ 5% Damping
- Test Frequencies
  - 1 To 100 Hz

- Tri-Axial Vibration
- Monitor Specimen, Relay Contacts
- Post-Seismic Testing

Next, EMI/RFI and electrical isolation qualification testing is performed, with the following major tests:

- EMI/RFI
  - Conducted Emissions
  - Radiated Emissions
  - Conducted Susceptibility
  - Radiated Susceptibility
  - High Frequency Transients
- Surge Withstand (Destructive)
- 1E/Non 1E Isolation (Destructive)

All of the following activities during the testing phase must be conducted in accordance with 10 CFR 50 Appendix B, for the testing to be valid:

- Development of the test acceptance criteria and test plans
- Procurement of all items included in testing
- All tests and analysis that are performed as part of testing including data recording.

After qualification, the manufacturer will provide qualification documentation of the generically (or specifically) qualified equipment. This should include:

- Description of the generic qualified equipment
- Description of the types of tested interconnections
- Overview and selection guide of the tested modules
- Overall capacity in terms of the qualified I/O and processing speeds
- Installation information to conform with qualification

In summary, the qualification testing for nuclear applications involves requirements for:

- QA measures applied to the qualification activities
- Documentation to support the qualification
- Documentation needed to for applying the digital equipment to the specific application

4.4 Commercial-Off-the-Shelf (COTS) Equipment

The purpose of this section is to describe the process, technical issues, and tradeoffs associated with evaluating and accepting commercial grade (COTS) digital equipment.

The objectives of this section are as follows:

- Describe how the commercial grade item dedication process can be applied to digital equipment
- Understand how to obtain reasonable assurance a commercial digital item is equivalent to one developed under Appendix B
- Identify critical characteristics and verification methods for digital equipment

There is a set of terminology that applies to COTS equipment, as follows:

- Commercial equipment
- Commercial grade equipment
- Commercial off-the-shelf (COTS) equipment

This equipment has NOT been developed under a nuclear QA (Appendix B) program. In almost every case, it has been developed by a vendor for commercial business purposes and can be used for a wide range of non-nuclear applications – many of which may be of highly critical nature, based on environmental and process needs (examples: pharmaceutical industry manufacturing, space shuttle instrumentation).

It is developed by a commercial vendor, that in many cases is a:

- Vendor who does not have a qualified Appendix B QA program, or
- Vendor who is not supplying the equipment under his Appendix B program (e.g., equipment is coming from commercial part of the organization)

There are many reasons for utilizing COTS equipment including:

- Availability
- Lower initial cost (purchase price)
- Greater flexibility
- Mature, proven in other industries
- More open, compliant with standards
- Supportable for the long term

There is good news and bad news as shown on Figure 4-14 and Figure 4-15 in addressing the use of COTS in nuclear applications.

There are a set of important references that have been used in a number of pilot applications for COTS qualification of all equipment and then of digital equipment, and have been approved by the NRC.

These references are:

Commercial Grade Item Dedication

Industry Guidance

- EPRI NP-5652, "Guidelines for the Utilization of Commercial-Grade Items in Nuclear-Safety-Related Applications"
- EPRI TR-102260, "Supplemental Guidance for the Application of EPRI Report NP-5652"

NRC guidance

- GL 89-02, "Actions To Improve The Detection Of Counterfeit And Fraudulently Marketed Products"
- GL 91-05, "Licensee Commercial-Grade Procurement and Dedication Programs"
- NRC Inspection Procedure 38703, "Commercial Grade Dedication"

Key Regulation

- 10 CFR 21 (1995)

Commercial Grade Digital Equipment

Industry Guidance

- EPRI TR-106439 (dedication of digital equipment)
- EPRI TR-107339 (supplement to TR-106439)
- IEEE 7-4.3.2-1993

NRC guidance

- NUREG 0800 (Standard Review Plan – SRP) Chapter 7 (1997 update)

NUREG 0800 Appendix 7.0-A provides the following guidance in Section C.3.8 on COTS:

"An acceptable set of fundamental requirements for this process [dedication of PDS items] is described

in IEEE 7-4.3.2[1], Section 5.3.2…. ***This standard allows the use of engineering judgment for the acceptance of existing software, and the use of compensating factors to substitute for missing elements of the software development process.***"

"***These provisions should not be interpreted to permit unsupported subjectivity in the acceptance of existing software.*** The guidance provided herein for the review of newly developed software provides technical background pertinent to evaluating the use of the engineering judgment and compensating factors provisions."

This same section provides an overview of the acceptance of COTS for Class 1E applications, as follows:

"In order to demonstrate reasonable assurance, the acceptance process for most PDS [previously developed software] can be expected to comprise a variety of technical activities conducted in significant detail. Guidance on these activities is provided in EPRI TR-106439."

CGI dedication has been conducted successfully a number of times over the past few years. EPRI NP-5652 describes the process in detail, as shown on Figure 4-16.

Also, Figure 4-17 provides a visual of the overall process to complete COTS application in a nuclear plant with the following major phases:

- Project Definition
- Establishment of requirements
- Design
- Testing, installation and verification

Figure 4-18 provides an overview of the comparison between the major elements to ensure an adequate level of assurance – for both nuclear grade digital equipment and COTS. You can easily see the higher degree of responsibility applied to the utility for use of COTS and the associated analysis required.

Determination of the critical characteristics for digital includes the following types of characteristics:

- Physical characteristics
  - Dimensions, part identification, etc., checked by inspection
- Performance characteristics
  - Functionality, response time, etc., typically checked by testing
- Dependability characteristics
  - Reliability and maintainability
  - Built-in quality, including quality of design, software development and QA, failure management
  - Configuration control
  - Problem reporting

To qualify COTS, a variety of methods are included as follows:

- Inspection and testing
  - Includes failure mode testing
- Commercial grade vendor survey
  - Checks software development and QA practices
  - Can check HW/SW design, architecture, failure management
  - Checks configuration control and problem reporting
- Source inspection

[1] IEEE Std 7-4.3.2, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations"

  - May be used to ensure specific characteristics for individual procurements
- Performance record
  - Checks relevance, extent, and success of operating history

Figure 4-19 provides a detailed schematic for inclusion of the critical characteristics into the equipment and procurement specifications for the new equipment utilizing COTS.

Figure 4-20 provides an example matrix that utility and or verifying personnel can use to document the verification of critical characteristics for a COTS qualification.

In conclusion, COTS equipment may be suitable for use in the system upgrade for Class 1E applications. Some COTS has already been generically qualified (Example: Invensys TRICON). The utility needs to be careful in addressing the cost of COTS qualification versus utilizing previously qualified equipment that has NRC approval for qualification. Also, the roles and responsibilities, as addressed in this section of the module, are important for the utility personnel to understand if they are signing up to qualify the equipment themselves.

4.5 Case History – Qualification of the Tricon by Invensys

The slides included in Section 4.5 provide an overview of the experience and documentation associated with the qualification of the Tricon by Invensys. The NRC approved this qualification with the SER referenced in the slides.

4.6 Case History – Qualification of the ABB Common Q PLC Platform

The slides included in Section 4.6 provide an overview of the qualification of the Asea Brown-Boveri (ABB) Common Q platform with NRC approval by SER.

4.7 Case History – Qualification of the Siemens Teleperm XS Platform

The Slides included in Section 4.7 provide an overview of the Siemens Teleperm XS (Safety-Related) platform with NRC approval by SER.

4.8 Cyber Security Guidelines

NOTE: This module contains security-related information – withhold under 10 CFR 2.390

The purpose of this section is to provide a short review of the lessons learned and requirements for addressing cyber security at nuclear power plants. The outline of covered issues is as follows:

- Background
- NRC Guidance
- Industry Guidance
- Current TWG Activities and Output
- Wireless communications in nuclear plants
- Summary

Overall, the background issues and status of the recent application of cyber security at nuclear plants:

- Current security regulations do not contain requirements related to cyber security (“Power Reactor Security Requirements,” Federal Register/Vol. 71, No. 207, 62669).

- However, the following 4 documents contain guidance or proposed regulatory requirements for cyber security:
  - EA-02-026, "Interim Compensatory Measures (ICM) Order," dated February, 2002
  - NEI 04-04, "Standard Cyber Security Program for Operating Reactors," Rev 1, Nov. 2005, and Rev 2(Draft)
  - Reg. Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev 2, Jan. 2006
  - Power Reactor Security Requirements," Federal Register/Vol. 1, No. 207, 62669/Thursday, October 26, 2006

The following points provide a description of this subject:

- High-integrity, real-time computer systems, such as the safety-related digital instrumentation and control systems in nuclear plants, must be secure against physical and electronic threats.
- Computer systems are secure if the consequences of unauthorized and inappropriate access to and use are limited to assure that safety is not significantly impaired.

Additionally:

- The security of computer systems is established by:
  - Designing in security features to meet the licensee's security requirements
  - Developing the systems without undocumented codes (e.g., back doors), including viruses, worms, Trojan horses and bomb codes
  - Installing and maintaining those systems IAW station admin procedures and licensee's security program.

The overall objective is :

- …the design of the plant data communications systems that interface to the safety-related systems at nuclear power plants should ensure that the communications pathways do not present an electronic path by which a person can make unauthorized changes to plant safety systems or display erroneous plant status information to the operators.

Figure 4-21 provides an overview for both illustrative and analysis purposes, of a generic DCIS system that must be protected by application of cyber security guidelines in accordance with the referenced standards. We will use this to apply the guidance in this lecture and review options for defensive models.

The NRC guidance put forth for cyber security is:

- In January, 2006, NRC Revised Reg. Guide 1.152 (Rev 2) to endorse the updated IEEE Std. 7-4.3.2-2003. Because IEEE Std. 7-4.3.2-2003 does not provide adequate guidance regarding security of computer-based safety system equipment, NRC included Reg. Positions 2.1 thru 2.9 to provide specific guidance concerning computer safety system cyber security.
- More recently, NRC issue a proposed rule change to 10 CFR 73.55 that includes provisions for cyber security of critical digital systems at power reactors, such as safety systems, security systems, and emergency preparedness systems. Rule anticipated to be final in 2007.

Additional requirements are included in:

- EA-02-026, "Interim Compensatory Measures (ICM) Order," dated February 25, 2002 (March 4, 2002: 67 FR 9792)

- Imposed cyber security requirements on operating reactors – Safeguards Information. These are reflected in the proposed regulations October 26, 2006

Additional proposed regulations are:

- "Power Reactor Security Requirements," Federal Register/Vol. 71, No. 207/Thursday, October 26, 2006.
- This proposed rule would contain detailed programmatic requirements for addressing cyber security at power reactors, which build on the requirements of the Feb. 2002 Order.
- Proposed cyber security requirements are design to be consistent with ongoing industry cyber security efforts.

Regulatory Guide 1.152 Rev 2:

- Provides methods that the NRC staff deem acceptable for complying with NRC regulations for promoting high functional reliability, design quality, and cyber security for the use of digital computers in safety systems.
- Definition of "computer" – a system that includes computer hardware, software, firmware and interfaces.
- References IEEE Std. 7-4.3.2-2003

The implementation of Reg. Guide 1.152 guidance covers the entire hardware-software lifecycle including [Reference Figure 4-22]:

- Concepts
- Requirements
- Design
- Implementation
- Test
- Installation, Checkout and Acceptance Testing
- Operation
- Maintenance
- Retirement

Following the lecture slides, we review the guidance provided for each phase of the hardware-software lifecyle and options for meeting the intent of the guidelines.

Additional guidance on cyber security assessments is included in NUREG/CR-6847:

- "Cyber Security Self-Assessment Method for U.S. Nuclear Power Plants"
- October, 2004
- Follows similar process to NEI 04-04

NEI met with NRC October 19, 2006 and requested endorsement of NEI 04-04, Rev. 1. Industry took the action to complete a comparison of NEI-04-04 Rev. 1 and Reg. Guide 1.152 to identify gaps and take appropriate corrective actions

Figure 4-23 through Figure 4-25 provide a review of the gap analysis conducted by the Cyber Security Technical Working Group (TWG) in 2007. These were used in development of the Interim Staff Guidance (ISG) which was issued in August, 2007 and will be covered in this section.

Industry has been moving forward with guidance in parallel with the NRC with issue of NEI 04-04 Rev 1, in November, 2005 which addressed the following eight major elements needed for an effective continuing program:

- Roles and responsibilities
- Policies and procedures
- Training and awareness
- Cyber security defensive strategy

- Configuration management
- Risk mitigation
- Incident response and recovery, and
- Assessment

The primary goals of NEO 04-04 Rev 2 are as follows:

- –Provide comprehensive approach to cyber security
- –Provide methods to assess
- –Aid in determining cyber security risk
- –Provide tools to develop defensive strategy
- –Provide methods and techniques
- –Support awareness of cyber security issues

A good program description following NEI 04-04 includes:

- A graded approach with multiple levels of protection
- Previously identified critical systems
- Inside-out assessment process vs. outside-in
- Configuration validation
- Development of a detailed defensive strategy

Figure 4-26 provides an overview of the program management outline of a good cyber security program.

The definition of a Critical Digital Asset (CDA) is:

- A digital device or system that plays a role in the operation or maintenance of a critical system and can impact the proper functioning of that critical system. A CDA may be a component or a subsystem of a critical system; the CDA may by itself be a critical system; or the CDA may have a direct or indirect connection to a critical system. Direct connections include both wired and wireless communication pathways. Indirect connections include pathways by which data or software are manually carried from one digital device to another and transferred using disks or other modes of data transfer.

Figure 4-27 provides an overview of the defensive model following NEI 04-04.

Figure 4-28 provides an example of the risk significance index developed following NEI 04-04.

Following NEI 04-04, training and awareness should focus on:

- **Awareness training** – user training to improve awareness of the need and techniques
- **Technical training** – for system administrators, design engineers and network administrators
- **Specialized cyber security training-** for subject matter experts and incident response personnel

Figure 4-29 provides an overview of the program assessment process – following both NEI 04-04 and NUREG/CR 6847.

Figure 4-30 provides an overview of the analysis modeling of the design characteristics of the boundary considerations for a system or plant wide network under evaluation.

Figure 4-31 provides a visual representation of the relationship of the cyber security plan to the overall physical security plan.

The current NRC-NEI TWG activities address the following problem statement and provide the following deliverables:

- Problem Statement:
  - –Cyber security requirements for safety systems: Regulatory positions 2.1-2.9 of RG 1.152 and NEI 04-04 provide conflicting guidance for implementing cyber security re-

quirements for safety systems at nuclear power plants.

- Deliverables:
  - –Develop Interim Staff Guidance to document the regulatory and design guidance developed by the Cyber Security TWG #1
  - Due Date: Sept 28, 2007

The ISG on cyber security, released in August, 2007 has the following status:

- •ISG issued draft – review in progress
- Reg. Guide 1.152 now complimentary to NEI 04-04 R2
- Long term – NRC regulatory guide to be issued
- NEI 04-04 Rev 2 endorsed with following exceptions:
  - NEI-04-04 Rev 2 provides framework but not all of the implementing details – does not establish minimum standards of acceptable risk and lacks specific measures needed to mitigate such risks. Also, does not provide quantifiable metrics for assessment.
  - Licensee to develop own criteria and standards
  - Next, we will review an example of a cyber security intrusion included in NRC Information Notice 2003-14, for an event that occurred at Davis Besse in 2003.

4.9 Wireless Local Area Networks (LAN)

There are two major references by EPRI that address the introduction of wireless LANs (WLANs) in power plants, including nuclear:

- EPRI Report 1003584, "Guidelines For Wireless Technology in Power Plants – Vol. 1 – Benefits and Considerations:
- EPRI Report 1007448, "Guidelines for Wireless Technology in Power Plants – Vol. 2 – Implementation and Regulatory Issues"

There are excellent capabilities and also concerns with the introduction of wireless communications in nuclear facilities. First, wireless communication can and does provide data, voice and video services without wires. The voice over WLAN is growing the fastest in the U.S. for commercial applications.

WLANs are a dynamic environment – and can be subject to interference in the 2 – 4 GHz range, as well as interference caused by closed doors and people standing in front of access points.

In summary, there are many benefits to the use of wireless technology for the following departments of technical applications at nuclear facilities:

- Work management and scheduling
- Electronic procedures
- Plant operations
- Chemistry
- Radiation protection
- Training and evaluation
- Enterprise data applications

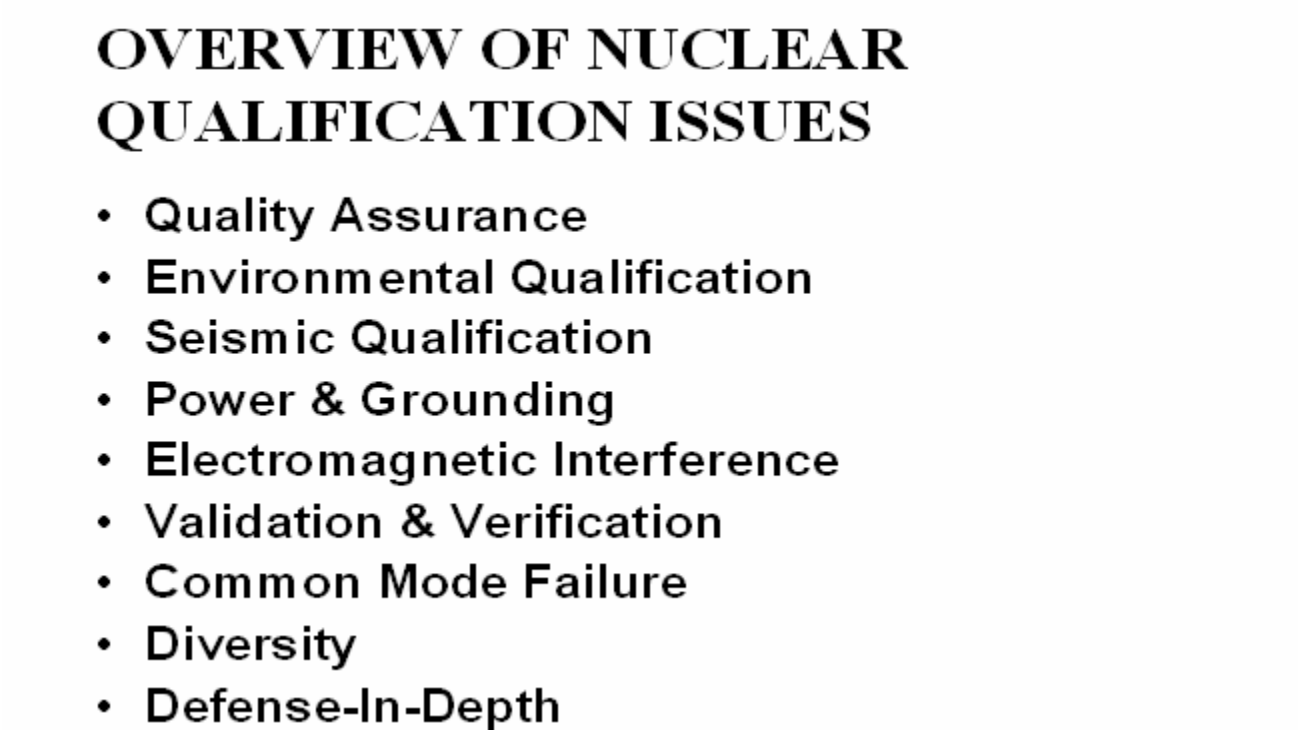


Figure 4-1: Overview of Nuclear Qualification Issues

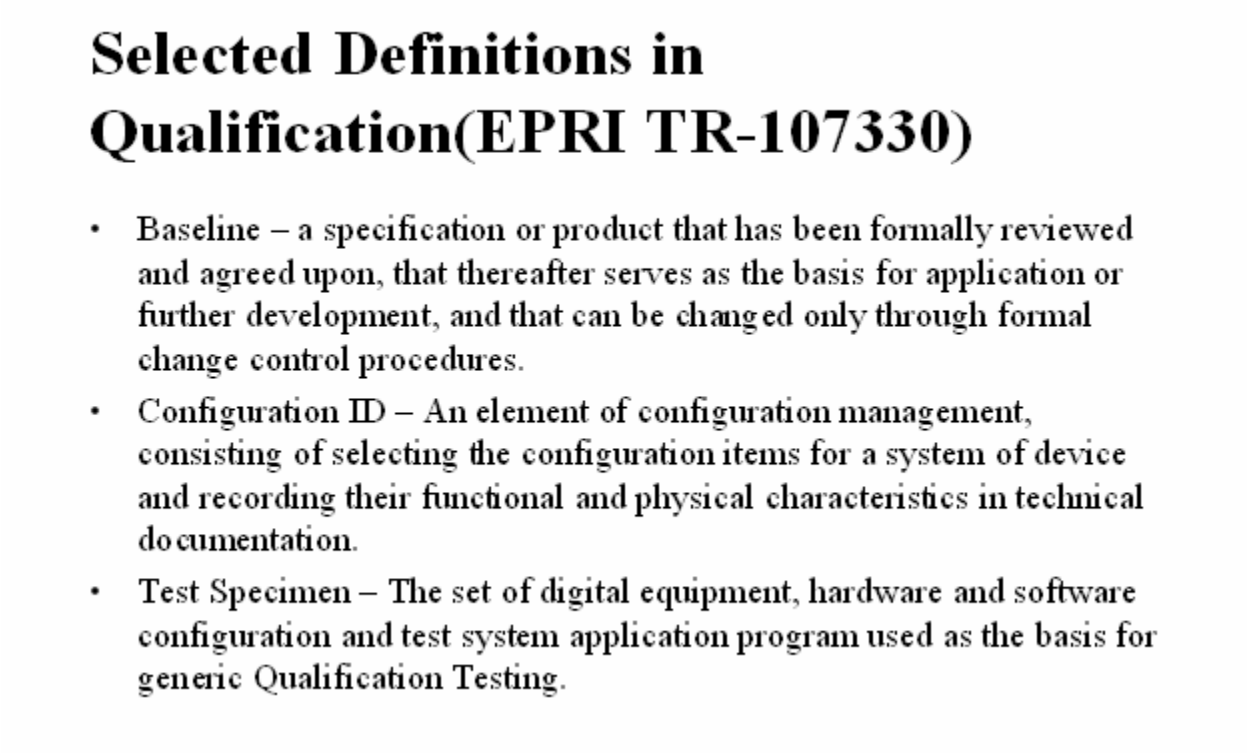


Figure 4-2: Selected Definitions in Qualification (EPRI TR-107330)

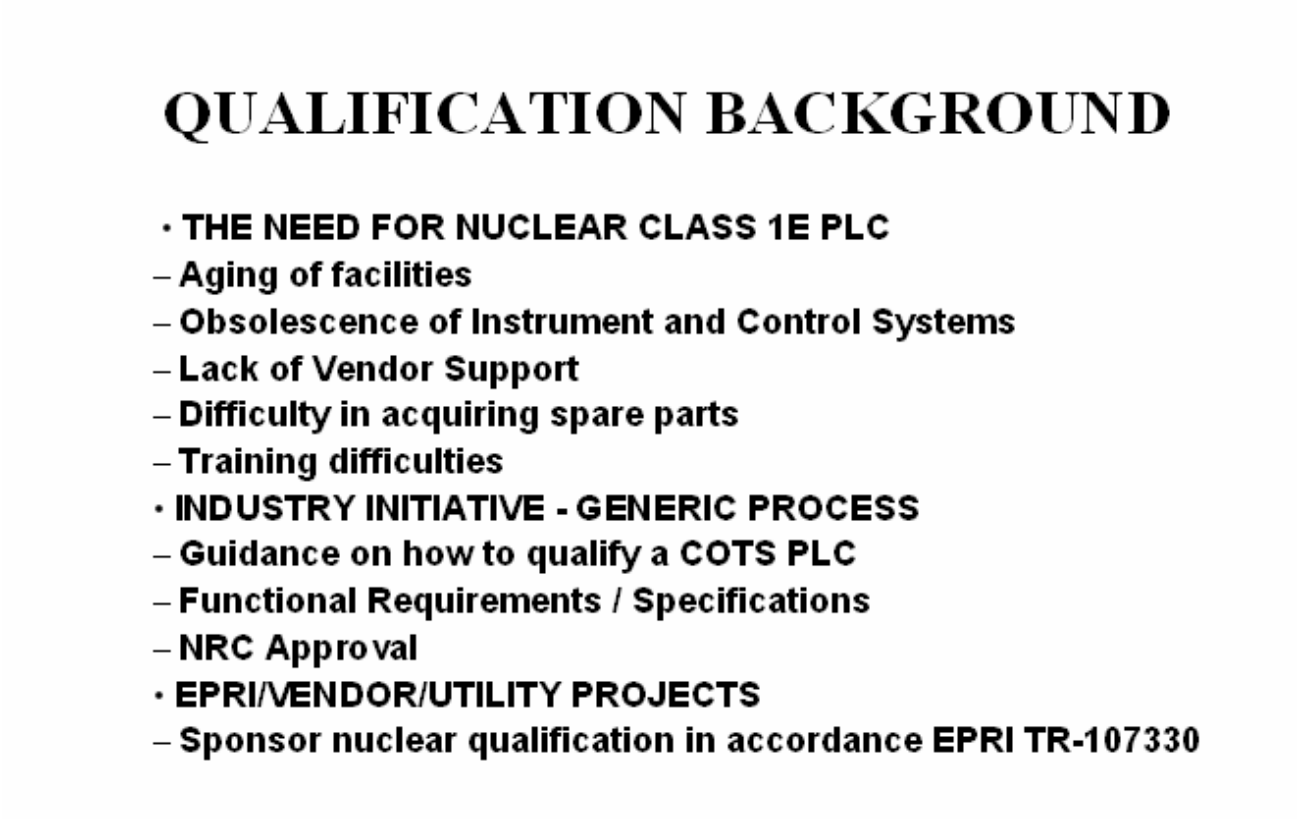


Figure 4-3: Qualification Background

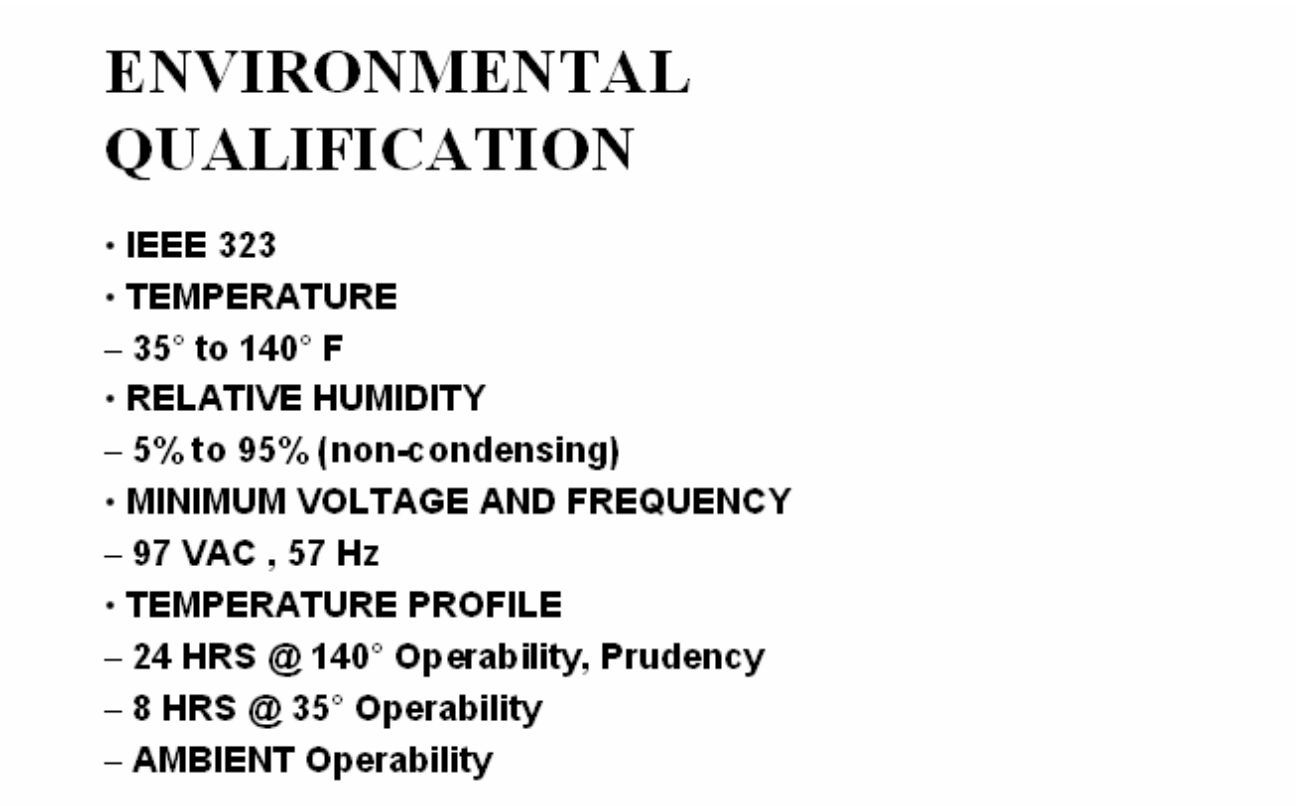


Figure 4-4: Environmental Qualification

Figure 4-5: Seismic Qualification

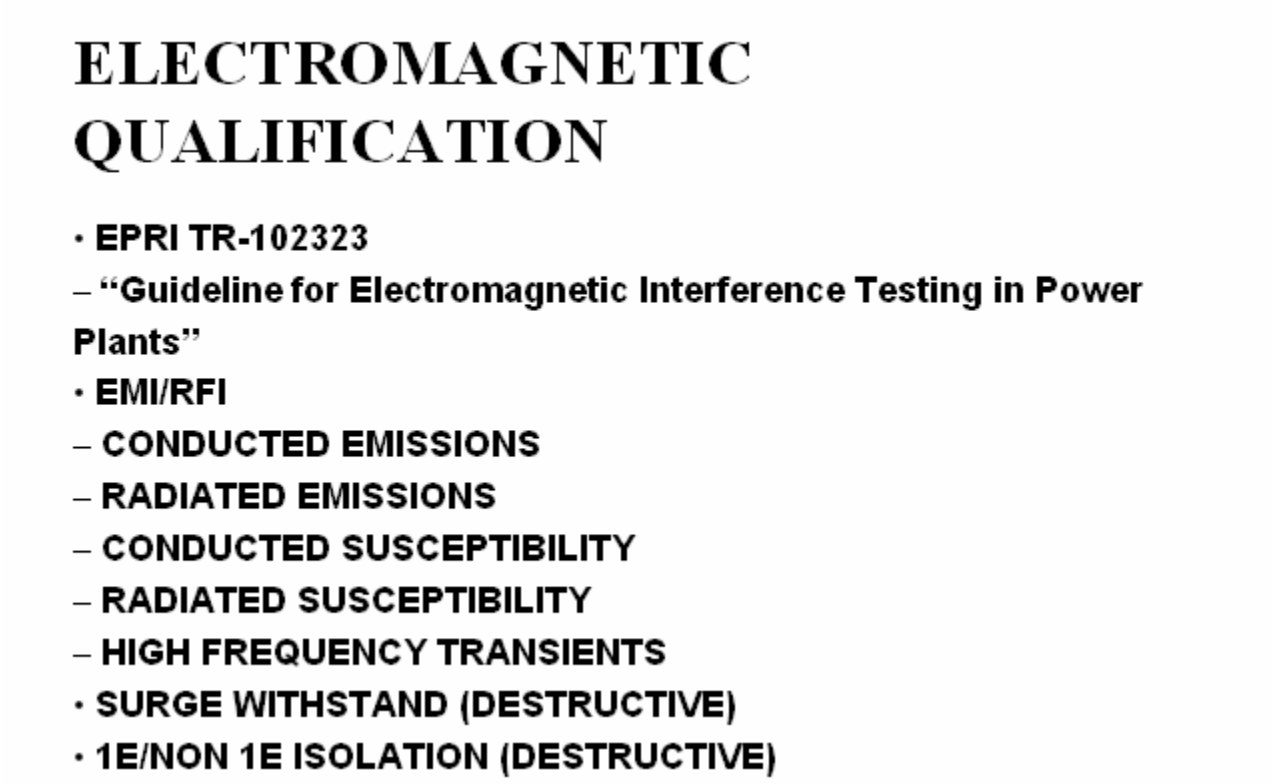


Figure 4-6: Electromagnetic Qualification

ENVIRONMENTAL QUALIFICATION REQUIREMENTS (EPRI TR-107330)

- Normal Environmental Basic Requirements
  - The operating environment where the digital equipment must meet the performance requirement given in EPRI TR-107330 Sections 4.3, as follows:

  - A. Temperature Range – – 60° to 104° F
  - B. Humidity – 40 to 95% (non-condensing) relative humidity range
  - C. Power Sources – Must operate within the ranges as follows:
    - AC – 90 to 150 VAC and frequency range of 57 to 63 HZ
    - DC - +/- 15% of stated voltage
  - D. Radiation – Up to 10^3 RADS

Figure 4-7: Normal - Environmental Qualification Requirements (EPRI TR-107330)

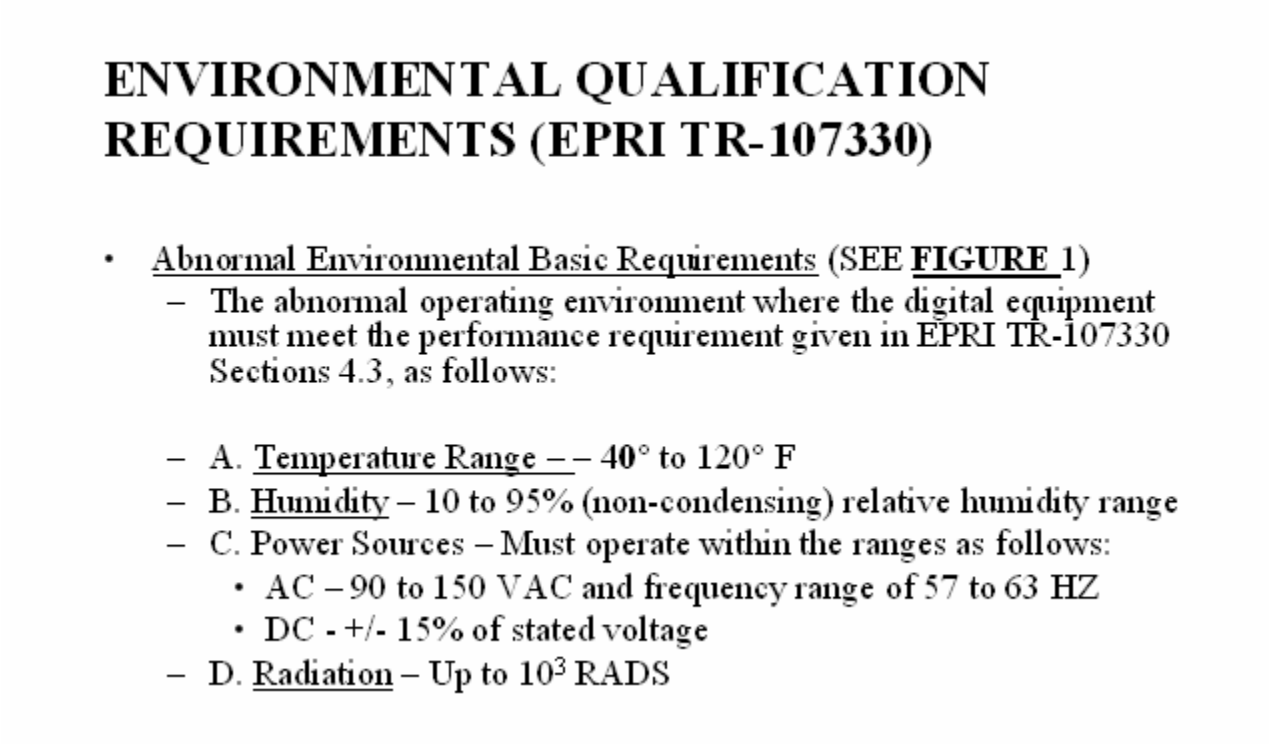


Figure 4-8: Abnormal - Environmental Qualification Requirements (EPRI TR-107330)

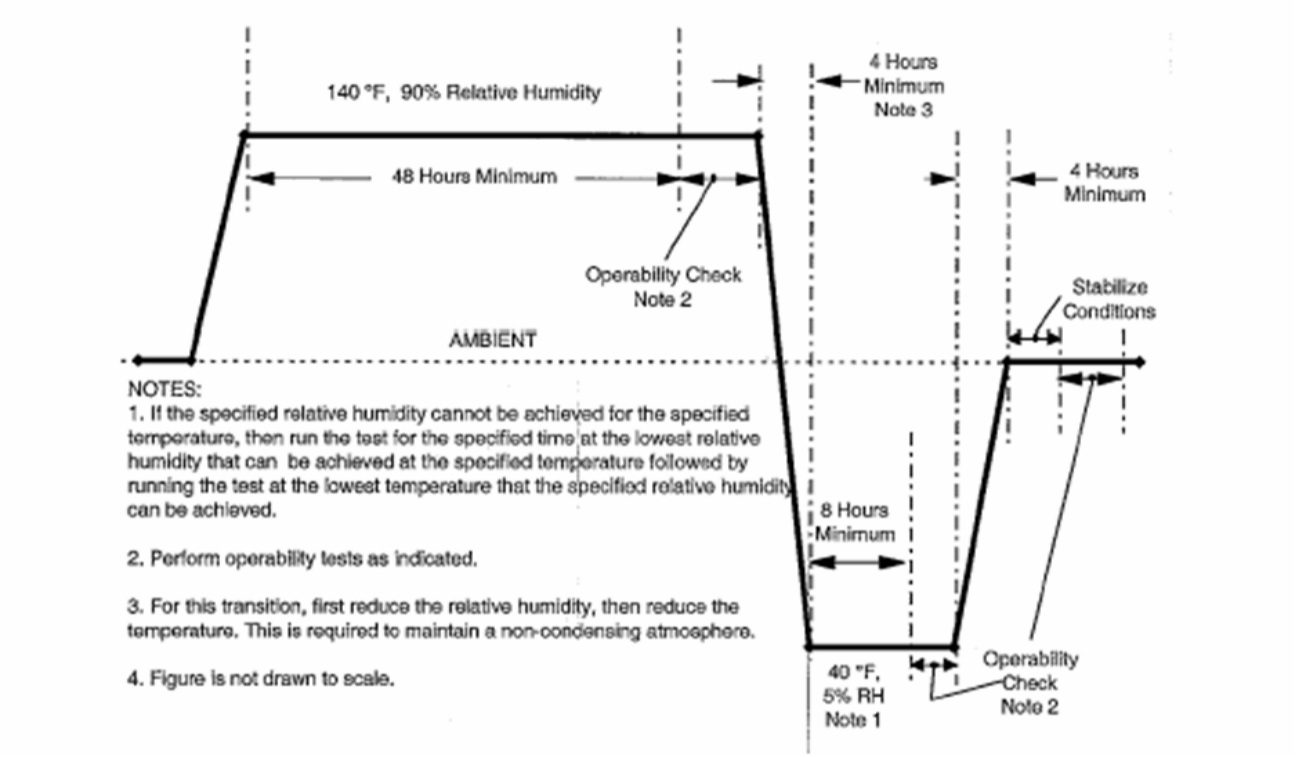


Figure 4-9: Figure 1

SEISMIC REQUIREMENTS (EPRI TR-107330)

- The digital equipment shall be suitable for qualification as a Category 1 Seismic device. The digital equipment shall met its performance requirements during and following the application of a Safe Shutdown Earthquake (SSE) simultaneously applied in three orthogonal directions. The SSE level shall be as shown in Figure 2. The digital equipment shall withstand the SSE vibration following the application of five OBE's as shown in Figure 2.

Figure 4-10: Seismic Requirements (EPRI TR-107330)

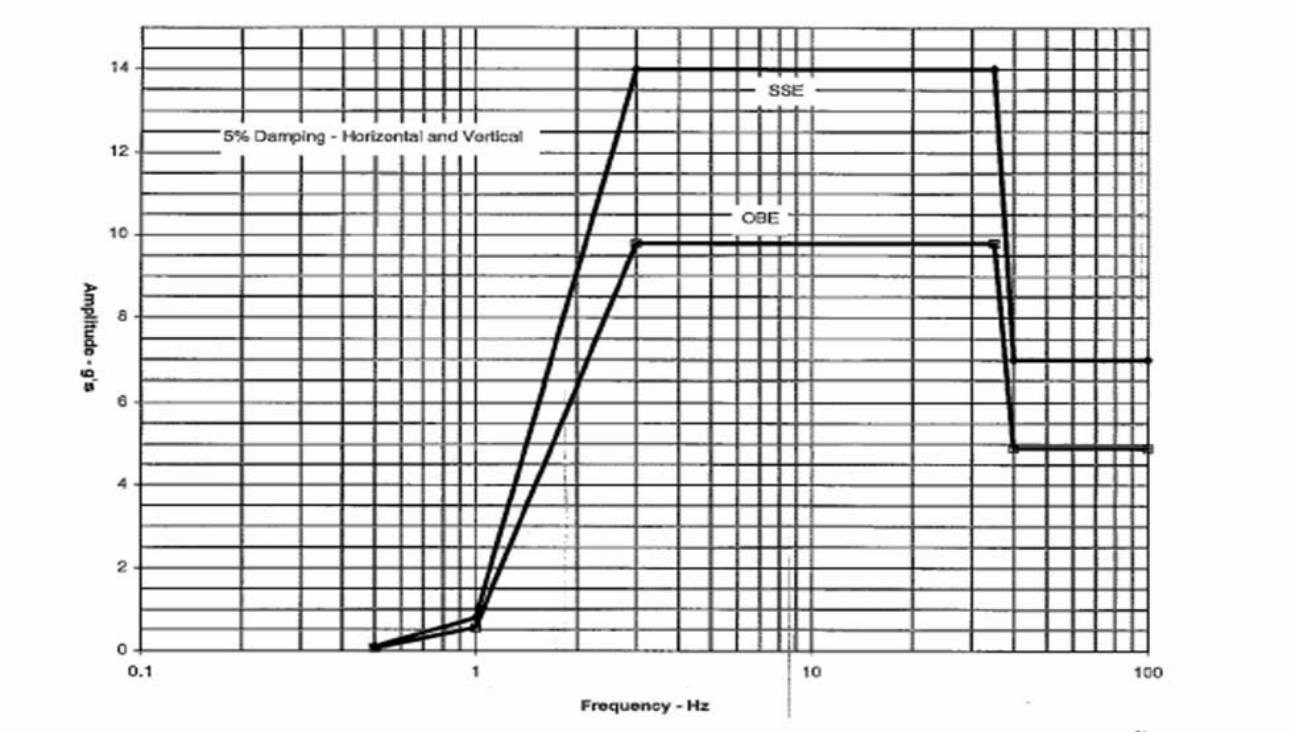


Figure 4-11: Figure 2

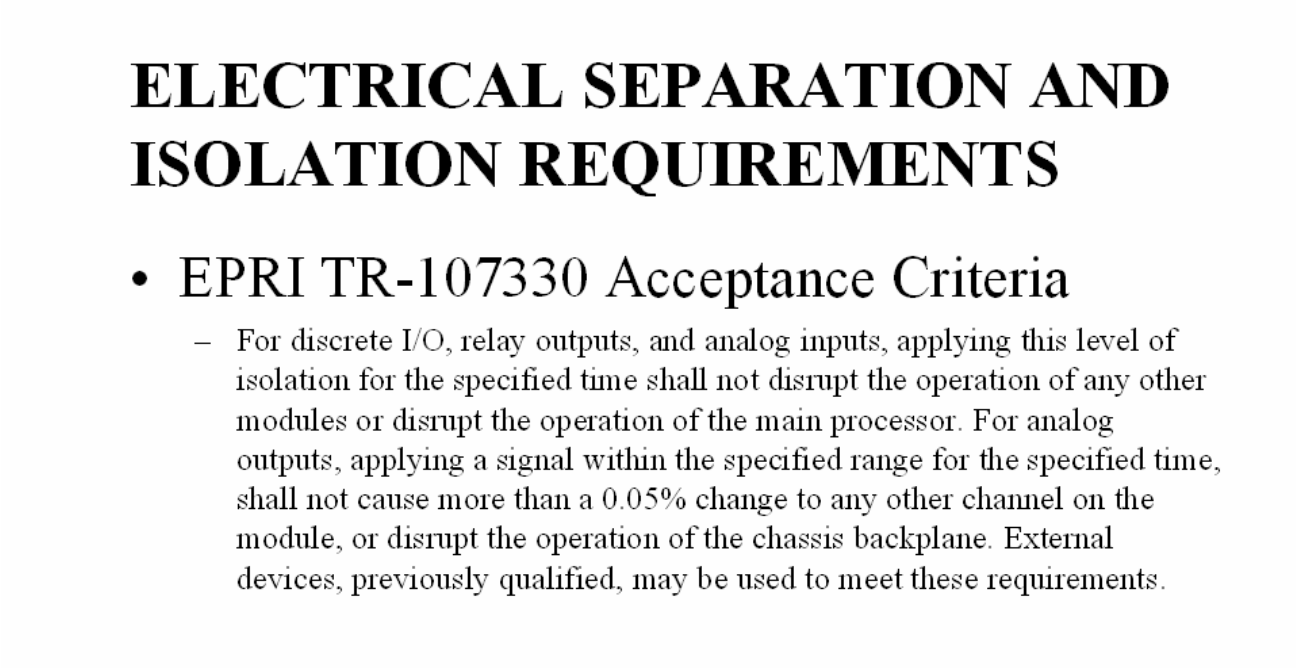


Figure 4-12: Electrical Separation and Isolation Requirements

OPERABILITY TEST REQUIREMENTS

- The following critical characteristics are verified by this initial acceptance testing:
  - Accuracy
  - Response time
  - Discrete input operability
  - Discrete output operability
  - Communications operability
  - Coprocessor operability
  - Timer tests
  - Test of failure to complete scan detection
  - Failover operability tests
  - Loss of power test
  - Power interruption test

Figure 4-13: Operability Test Requirements

The Bad News

- Regulations require a rigorous design, development and verification process for digital equipment -- process very important
  - Commercial vendors don't follow nuclear regulations, standards or processes
- Risk management and recognition of hazards is needed to get safe digital systems
  - Most commercial equipment not designed for safety-critical applications

Figure 4-14: The Bad News

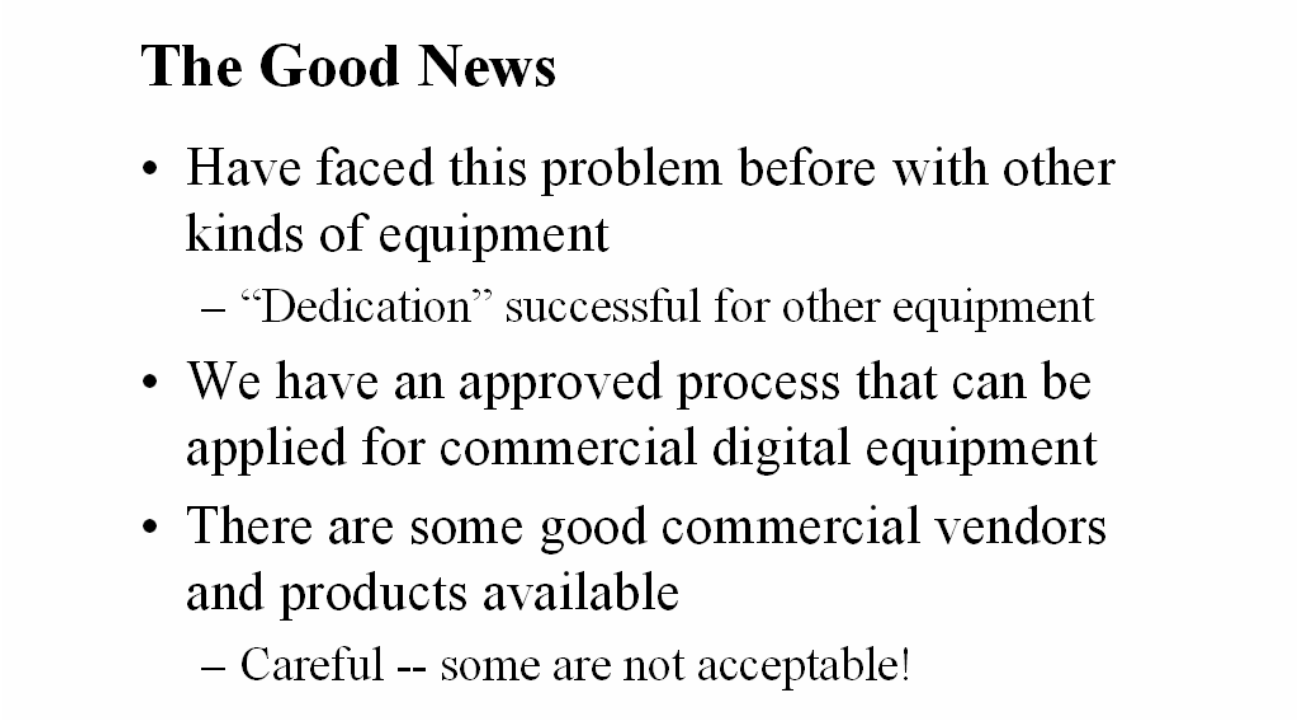


Figure 4-15: The Good News

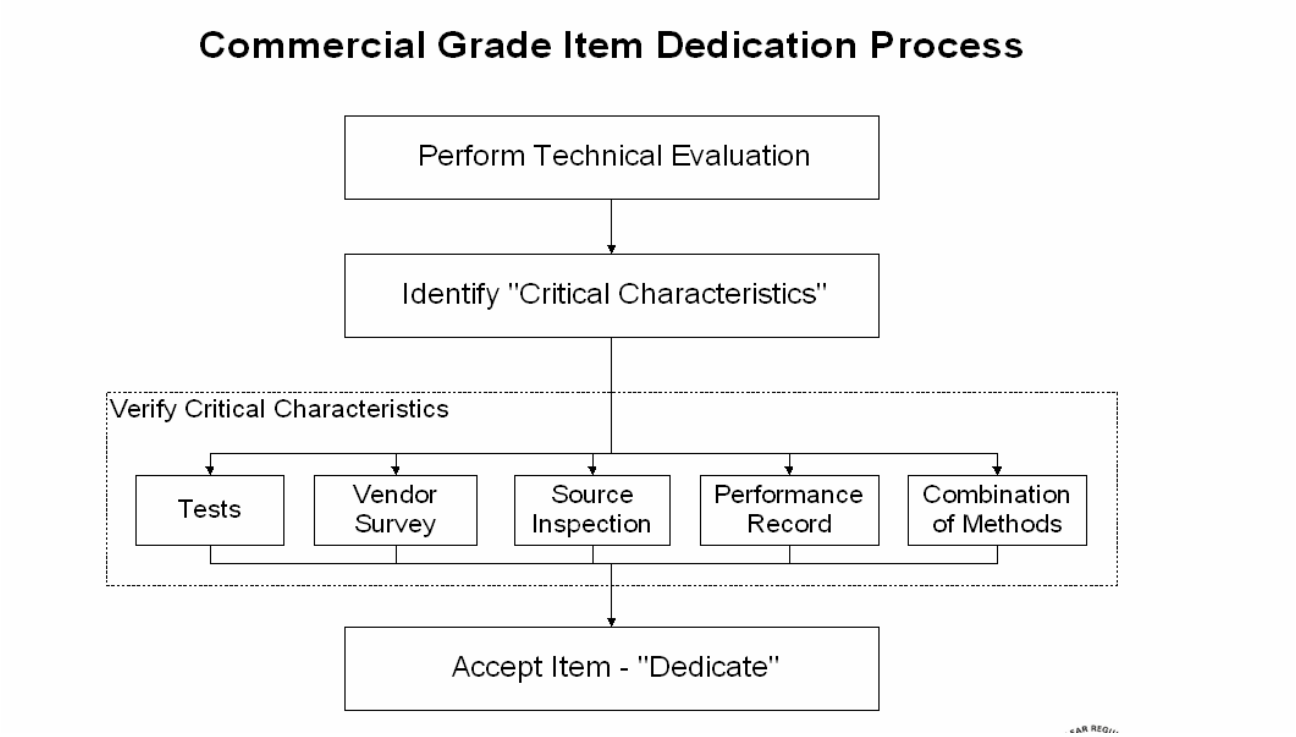


Figure 4-16: Commercial Grade Item Dedication Process

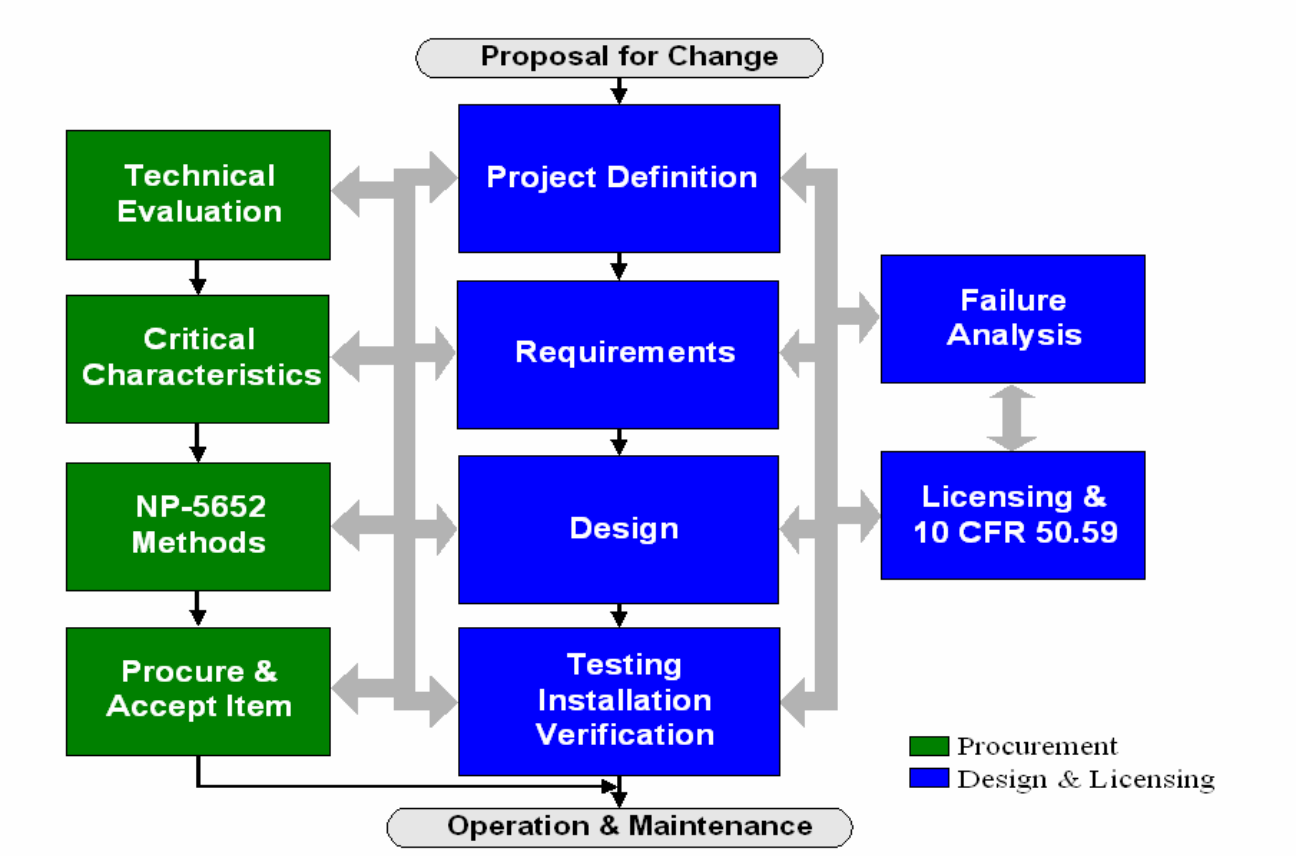


Figure 4-17: COTS Development Phases

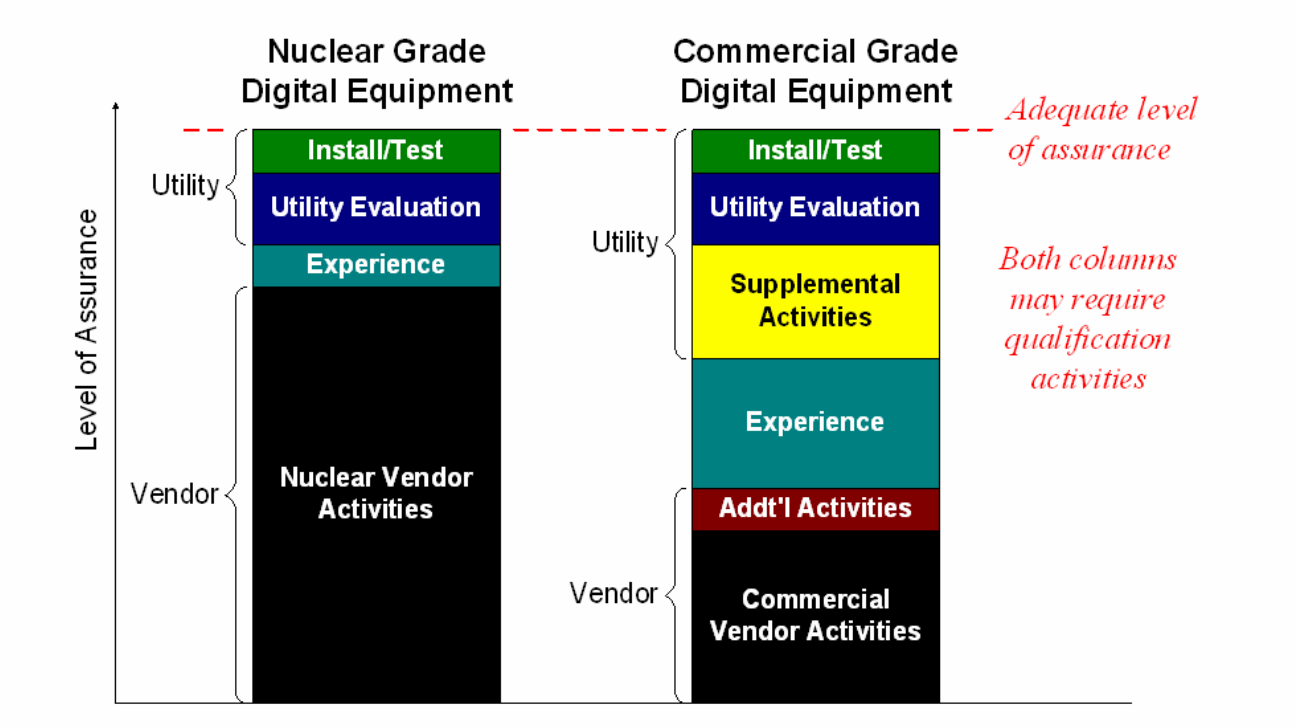


Figure 4-18: Nuclear Grade vs Digital Comparison

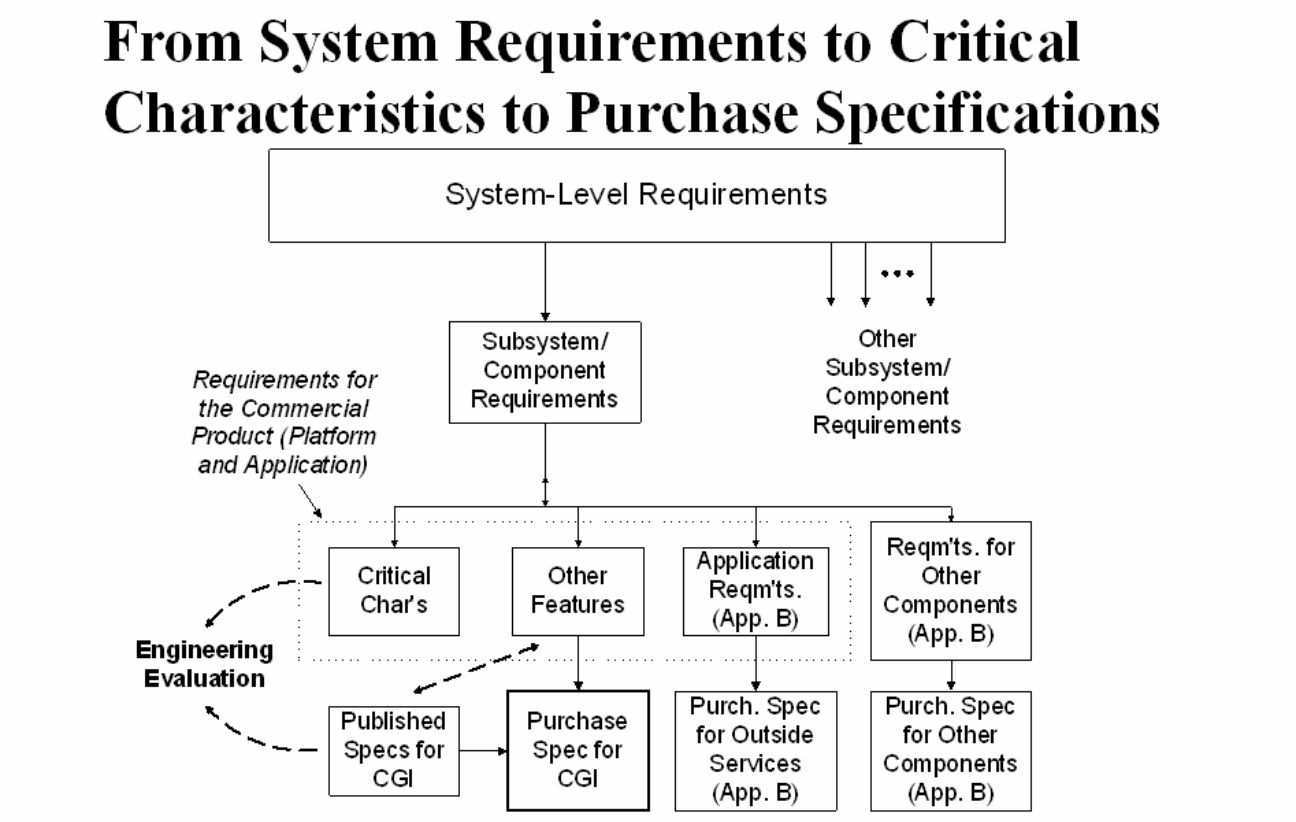


Figure 4-19: COTS Critical Characteristics

Critical Characteristics Matrix Used in the Examples

Critical Characteristics	Criteria	Methods of Verification
Physical		
Performance		
Dependability		

Figure 4-20: Example Critical Characteristics Matrix

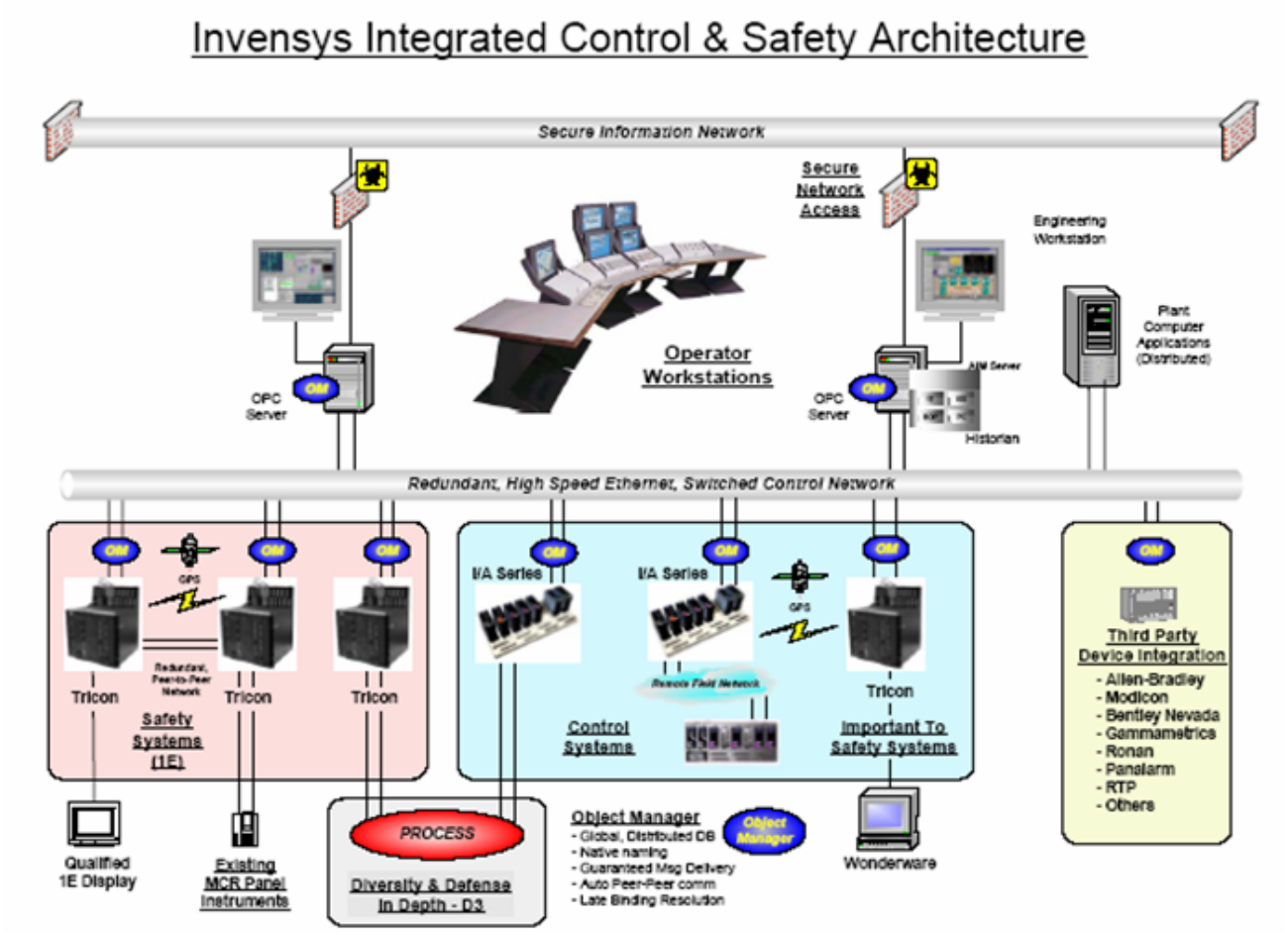


Figure 4-21: DCIS Overview

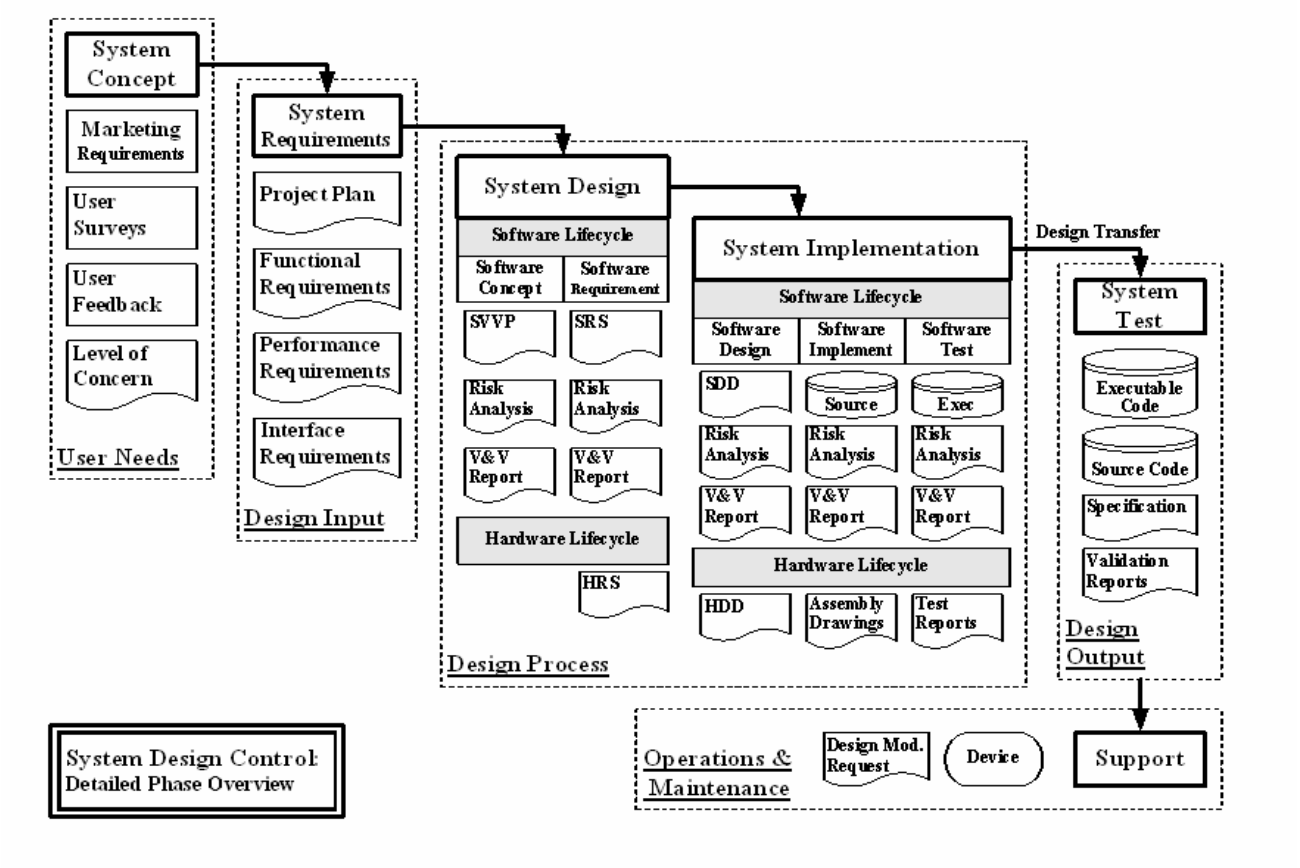


Figure 4-22: System Design Control Detailed Phase Overview

Regulatory Guide 1.152 and NEI 04-04 Cyber Security Requirements Analysis

Example of what is included in TWG Activities

Regulatory Guide 1.152	NEI 04-04	Gaps Between 1.152 and 04-04	Recommendations	NEI-NRC 5-8-07 Meeting agreement
Section C. Regulatory Position	**Section 4.2, Cyber Security Defensive Strategy: 4.3 Risk Mitigation Section 4.4 Policies and Procedures Section 7.2, Evaluations to Support New or Modified Digital Assets**	RG 1.152 is focused solely on lifecycle issues of safety systems. Therefore, more detail is provided for each phase of the example lifecycle process (i.e., Waterfall model) with respect to computer safety systems. NEI 04-04 is a risk-management document that provides guidance on implementing cyber security programs at NPPs, and is NOT a requirements document (please refer to **Section 1 Introduction**).	Retain positions 2.1-2.9 in RG 1.152. These positions are not contradictory in nature when compared to NEI-04-04, but rather are complimentary and provide additional and specific guidance with respect to safety systems.	See overall summary above.

Figure 4-23: Cyber Security Requirements (1 of 3)

Regulatory Guide 1.152 and NEI 04-04 Cyber Security Requirements Analysis

Regulatory Guide 1.152	NEI 04-04	Gaps Between 1.152 and 04-04	Recommendations	NEI-NRC 5-8-07 Meeting agreement
2.1 Concepts Phase	**4.2 Cyber Security Defensive Strategy** **4.3 Risk Mitigation** **5.2 Examine Plant-Wide Cyber Security Practices** **5.3 Identify CDAs** **Appendix B Cyber Security Defensive Model** **Appendix C Defensive Techniques**	Control systems and safety systems are in the defense level (level 4) in NEI 04-04, while safety systems are isolated from control systems in RG 1.152.	Provide additional regulatory guidance on the issue. Safety Systems are more accurately represented as "island systems" existing within Layer 4 with one-way communications allowed to non-safety systems. Refer to existing guidance on separation of safety and non-safety systems.	This item to be part of Communications TWG. (SR-NSR communications)
		RG 1.152 stipulates that remote access to the safety system should not be implemented, while NEI 04-04 strongly discourages remote access to CDAs; however, if necessary, remote access can be allowed provided mitigation strategies are in place as described in Appendix C (C-2).	Prohibit remote access to Safety-Related systems. Provide regulatory guidance and requirements regarding remote access to control assets or systems designed to protect control assets. Additionally, provide definitions as to what is meant by remote access (i.e. between defensive levels vs. offsite)	Defer to the COM-TWG and IEEE-603 for all bi-directional communications questions between Safety and Non-Safety. NEI Action (1) Definition of remote access needs to be provided and discussed in NEI-04-04. Specifically restrict remote access to safety related systems based on that definition and to Level 4 non-safety control system in general.

Module 4. Section 4.8 Slide 27

Figure 4-24: Cyber Security Requirements (2 of 3)

Regulatory Guide 1.152 and NEI 04-04 Cyber Security Requirements Analysis

Regulatory Guide 1.152	NEI 04-04	Gaps Between 1.152 and 04-04	Recommendations	NEI-NRC 5-8-07 Meeting agreement
2.1 Concepts Phase(Cont.)		NEI 04-04 allows connectivity within the safety/controls level (level 4), therefore two-way communication from safety critical assets to control related assets is allowed by the process; whereas RG 1.152 uses one communication from safety systems to non-safety systems. NOTE: Clarification on the issue provided by the author of this section of NEI 04-04 revealed that the communication referred to in Appendix B, page B-2 paragraph was never intended to include Safety-Related to Non-Safety-Related communications. Rather, the statement was intended to address communication between Non-Safety-Related systems or networks existing within the same defensive level. This concept was never intended to circumvent existing requirements for Safety-Related to Non-Safety-Related communications.	Stipulate one way communication between safety and control systems and suggest methods for implementing this one way communication. Additionally, provide regulatory guidance regarding the monitoring of Safety Systems / networks for anomalous activity and how to implement such monitoring.	NEI Action (2) NEI 04-04 will refer to RG BTP-14 for further information on this subject.

Figure 4-25: Cyber Security Requirements (3 of 3)

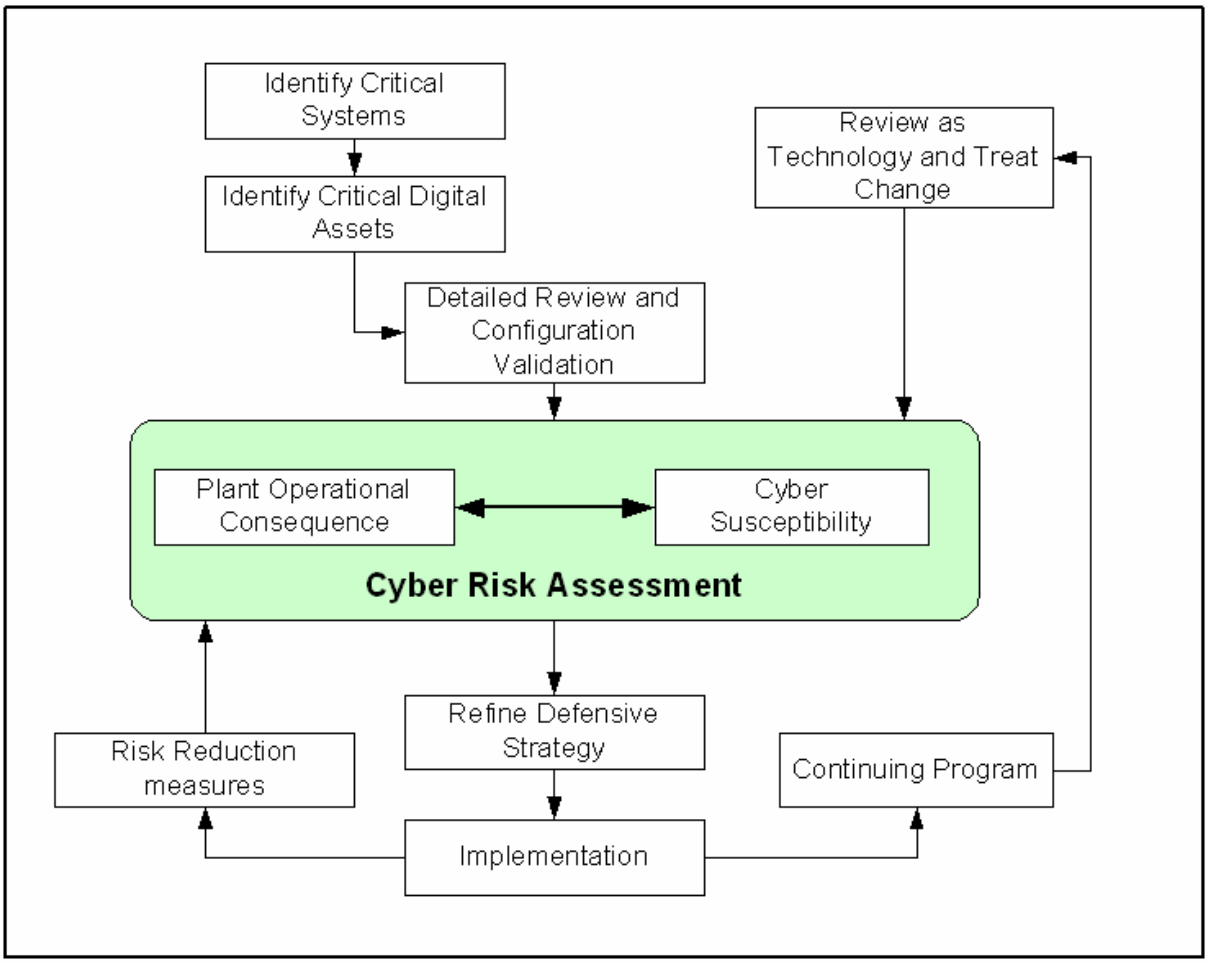


Figure 4-26: NEI 04-04 Figure 3.1: Program Management Outline

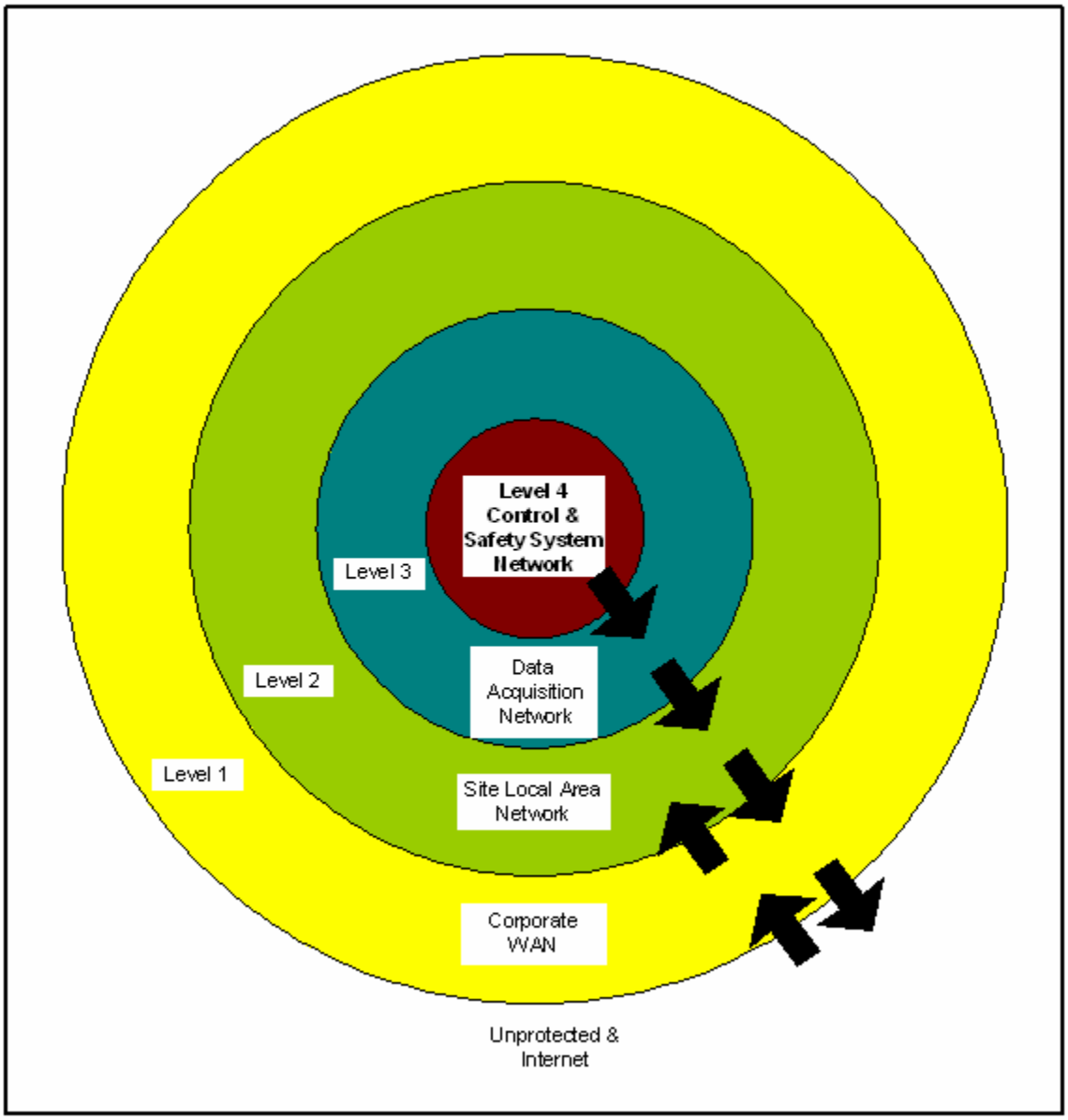


Figure 4-27: NEI 04-04 Figure B-1: Defensive Model

Risk Categories									
Consequence Category	Susceptibility Levels: Low								High
	1	2	3	4	5	6	7	8	9
Low Impact	G-1	G-2	B-3	B-4	Y-5	Y-6	O-7	O-8	R-9
Moderate Impact	G-2	B-3	B-4	Y-5	Y-6	O-7	O-8	R-9	V-10
High Impact	B-3	B-4	Y-5	Y-6	O-7	O-8	R-9	V-10	V-11

Figure 4-28: NEI 04-04 Rev. 1 and Rev. 2

PROGRAM ASSESSMENT

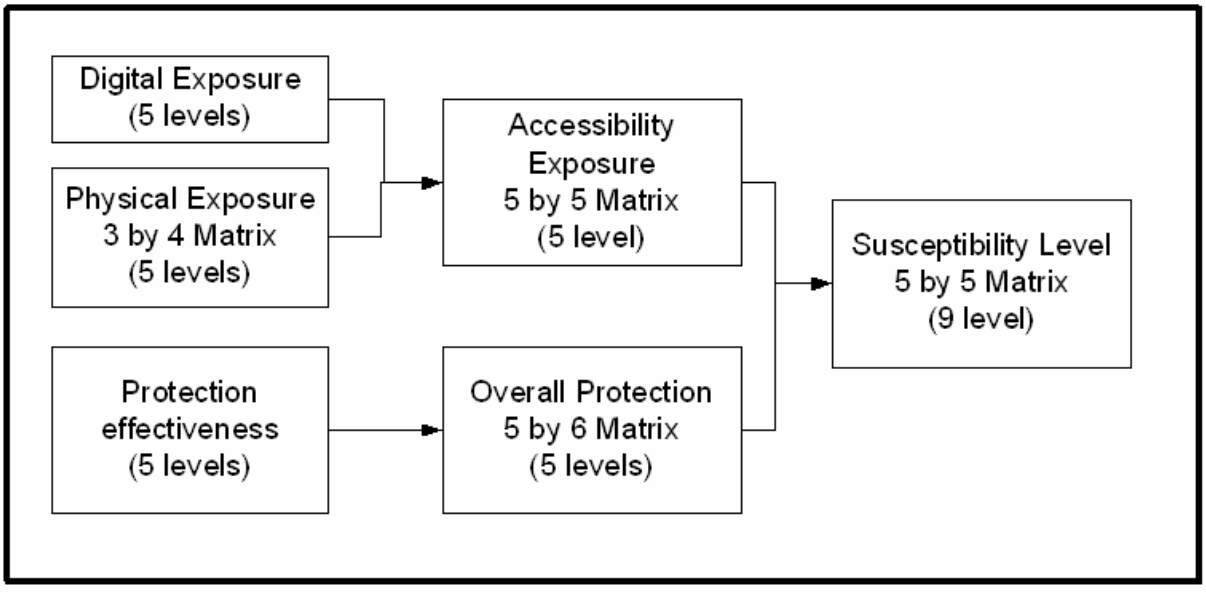


Figure 4-29: NEI 04-04 Figure 5.1: Assessment Matrix

NEI 04-04 Rev 1 and 2

Design Characteristics of a boundary interface

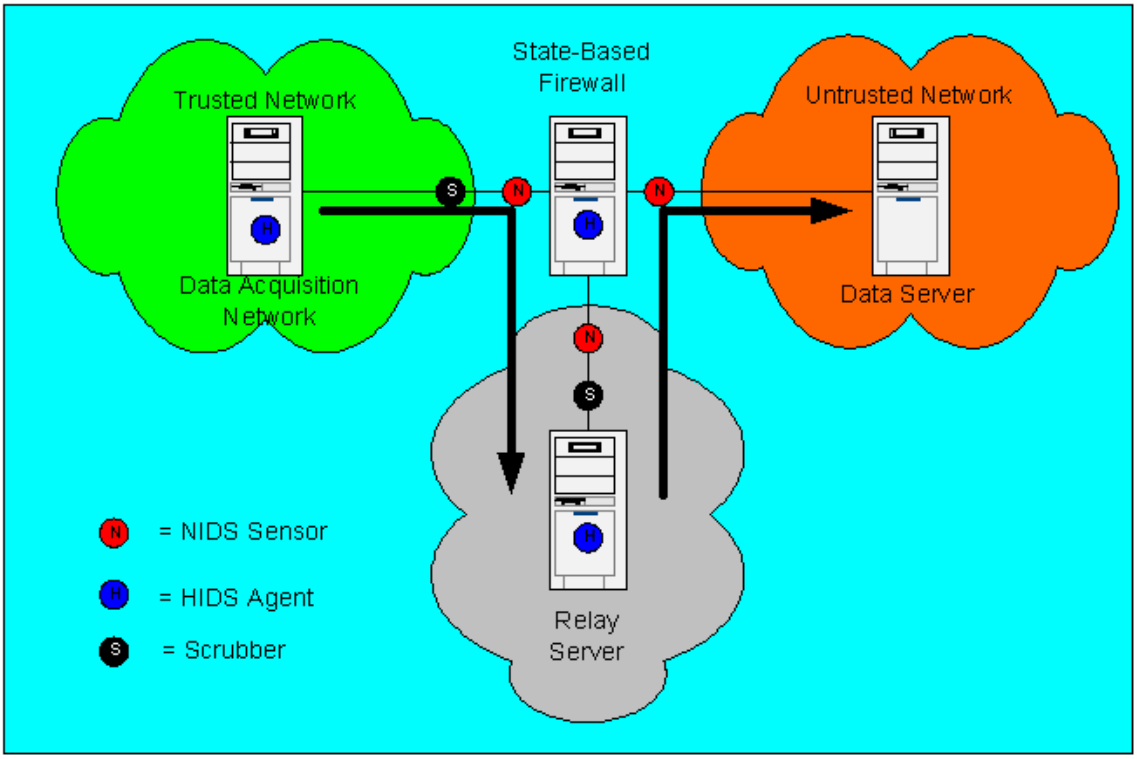
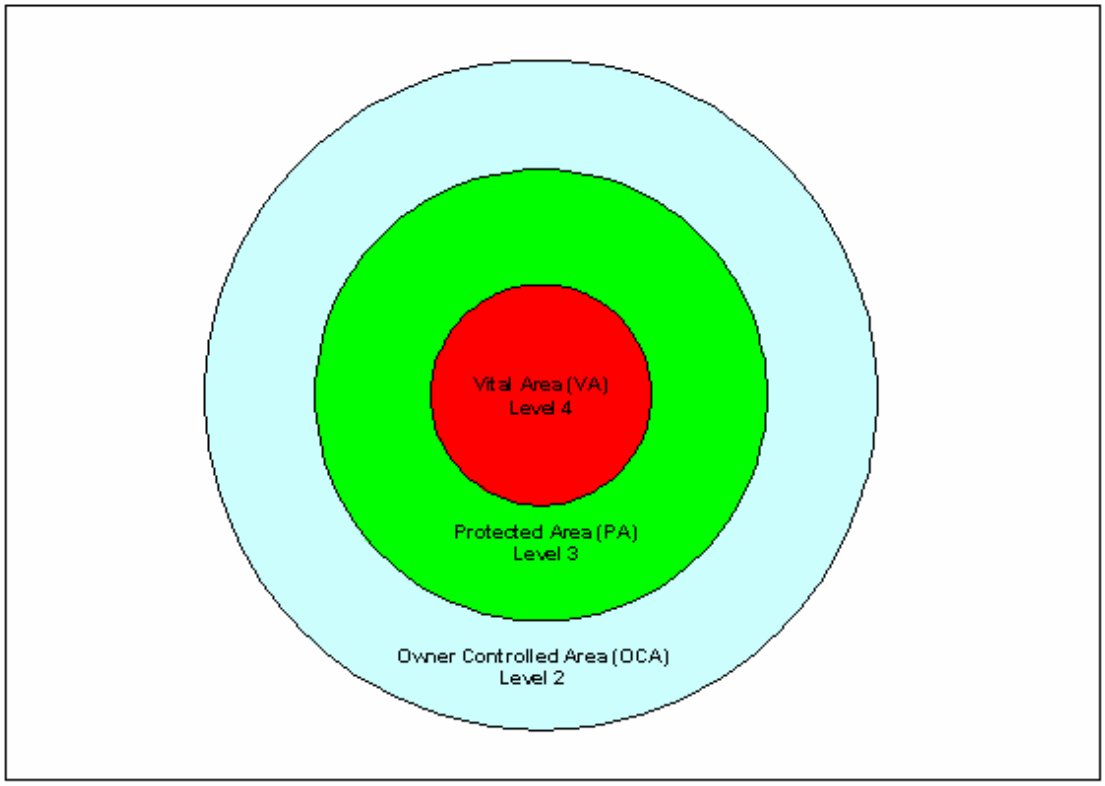


Figure 4-30: NEI 04-04 Figure B-2: Demilitarized Zone Example

NEI 04-04 Physical Security



NEI 04-04 Figure B-3: Physical Security Model

Figure 4-31: NEI 04-04 Physical Security