ELECTRIC POWER RESEARCH INSTITUTE

Acceptance of Commercial Grade Design and Analysis Computer Programs

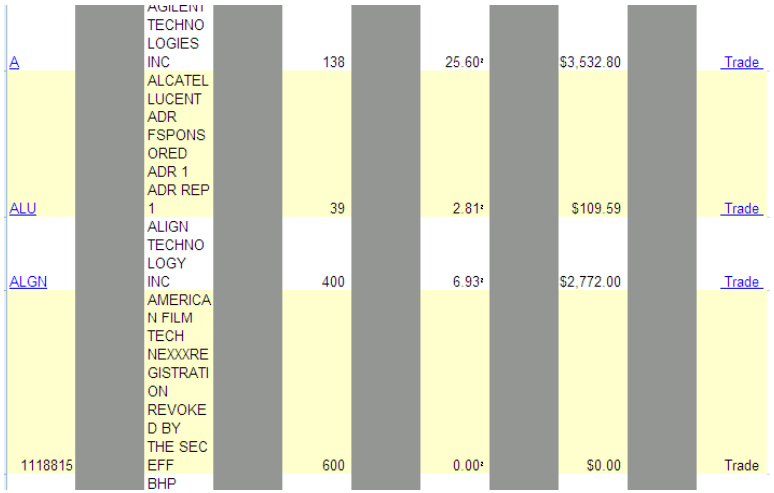
Marc H. Tannenbaum
Project Manager

3rd NRC Workshop on Vendor Oversight for New Reactor Construction
June 28, 2012

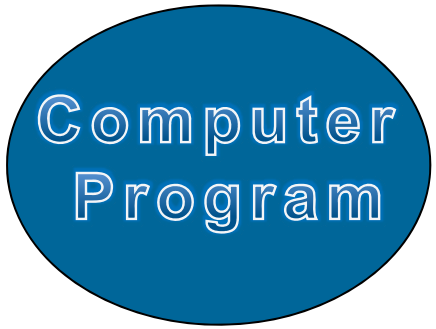
Baseline Terminology

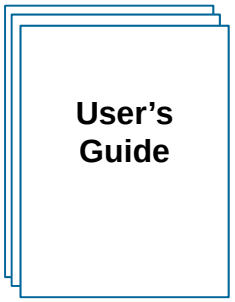
Adapted from presentation by Norm Moreau of Theseus Professional Services

Computer Code



Data





Documentation

Computer Program + Documentation = Software

Background

- Dedication methodology may not have always been applied to non-process computer programs in the past
  - Definitions of “commercial grade item” in 10CFR21 were interpreted as disqualifying computer programs
  - Effective Software Quality Assurance (SQA) programs were implemented to address special requirements and methodologies
  - Design and analysis computer programs were viewed as an important tool – much like a calculator

Background

- Use of computer programs has substantially increased
- Our reliance on computer programs has substantially increased
- The principles used to accept non-process computer programs in our industry are and have been sound
  - Verification and Validation

Background - Verification of design & analysis computer programs should not be a new idea

- Independent verification of results versus pre-verification of computer program methodology
  - NQA-1b-2011, Requirement 3, Design Control*
    - . . . computer program acceptability shall be *pre-verified*
      - (a) the computer program shall be verified to show that it produces correct solutions for the encoded mathematical model within defined limits . . .
      - (b) the encoded mathematical model shall be shown to produce a valid solution to the physical problem associated with the particular application
    - **or** *the results verified* with the design analysis *for each application* . . .

*Same language is contained in as NQA-1-1994, Requirement 3, Section 3.12

Starting Line for Current Guidance

- NUPIC and NRC findings impacting supply chain
- NQA-1 requirements for dedication of software
- No industry guidance specific to safety classification of non-process computer programs
- NRC precedent may exist to consider non-process software as:
  - A “basic component” as defined in 10CFR21
  - A “commercial grade item” as defined in 10CFR21

Starting Line for Current Guidance

- Safety Evaluation Report (SER) of Topical Report TR-106439, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications* (ADAMS accession number 9810150223)

  "The second sentence of the new Part 21 definition of CGI excludes "items where the design and manufacturing process requires many in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more, critical characteristics of the item cannot be verified)."

  "The staff considers verification and validation activities common to software development in digital systems to be a critical characteristic that can be verified as being performed correctly following the completion of the software development by conducting certain dedication activities such as audits, examinations, and tests."

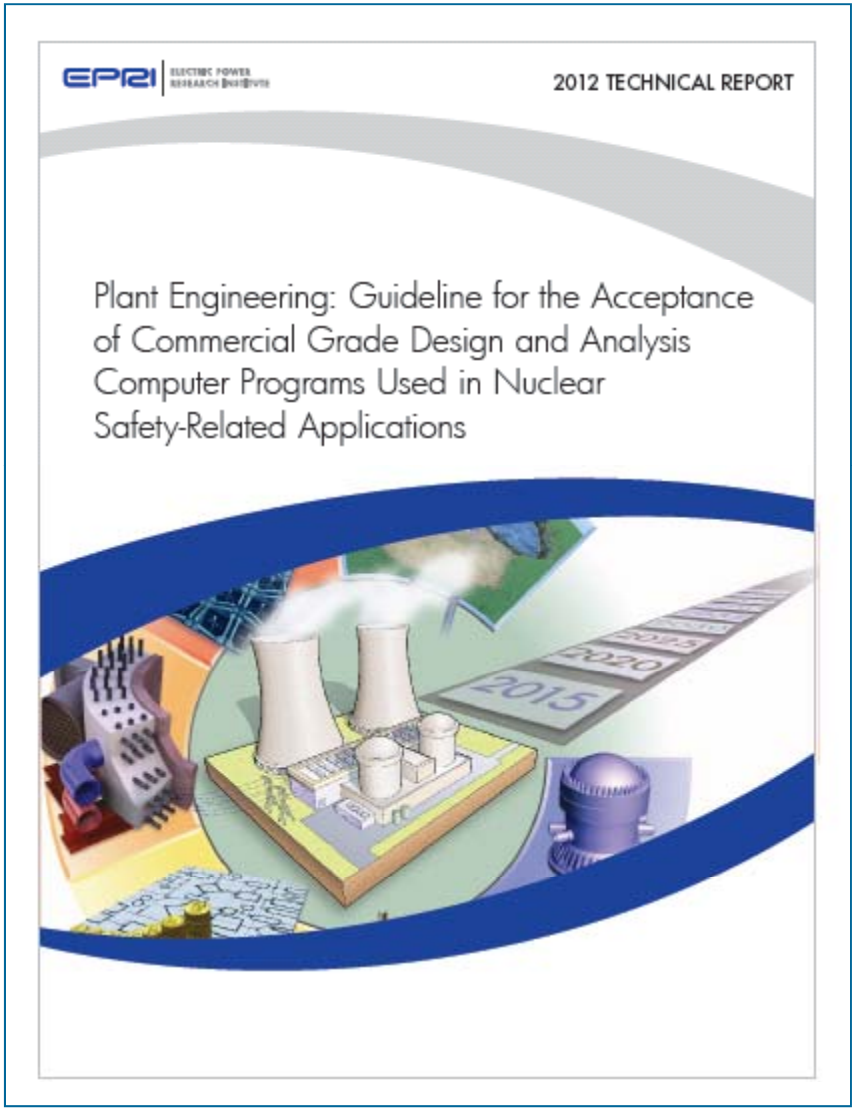
Starting Line for Current Guidance

- In the definition of “Basic Component” in 10CFR21 (1995)

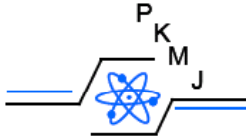
  “In all cases, basic component includes safety-related *design, analysis*, inspection, testing, fabrication, replacement of parts, or consulting services that are *associated with the component hardware, design certification, design approval*, or information in support of an early site permit application under part 52 of this chapter, whether these services are performed by the component supplier or others.”

EPRI 1025243

- Generic technical evaluation process overview
- Functional safety classification of computer programs
- Acceptance of commercial-grade computer programs using the dedication process



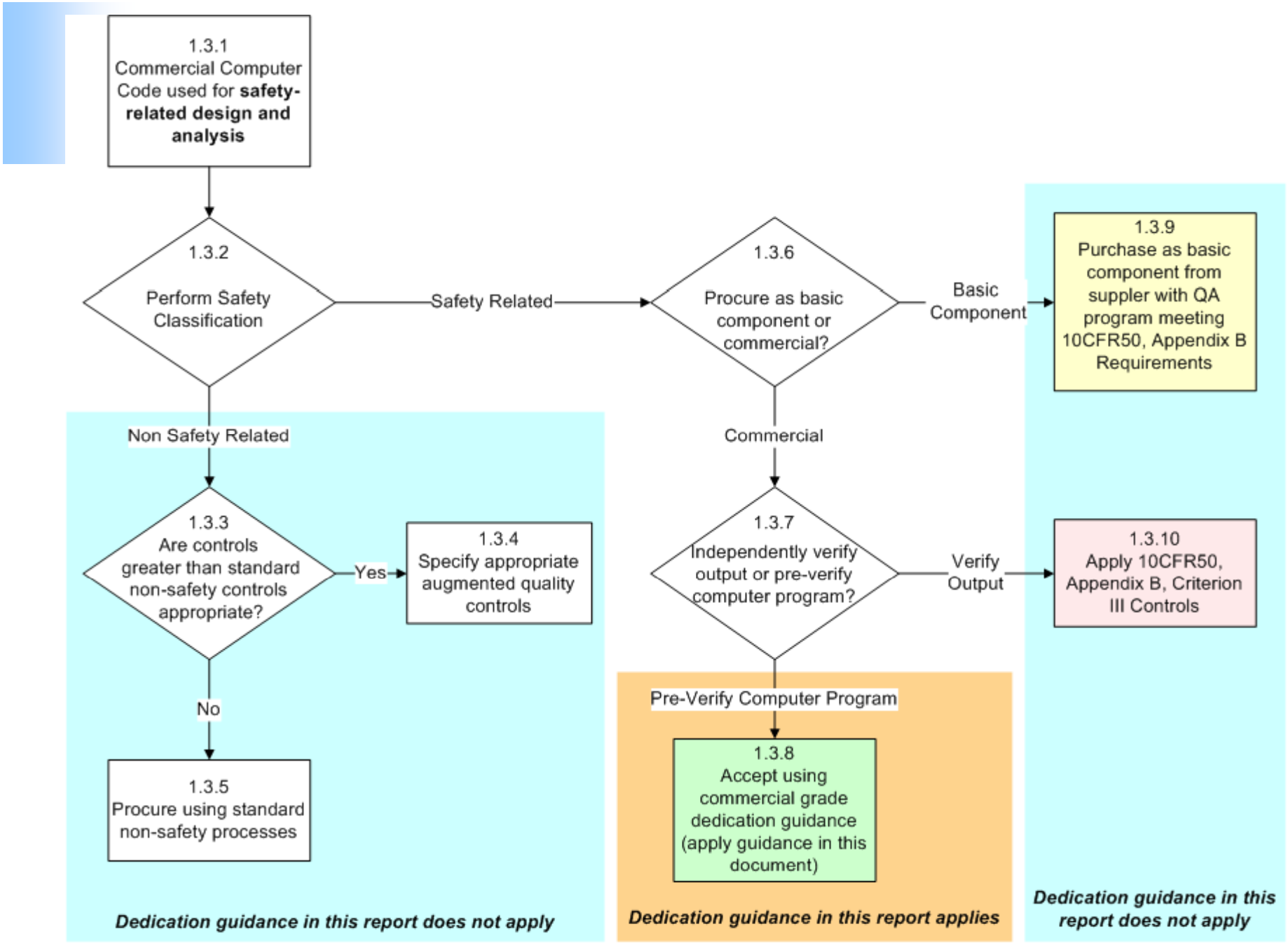
Represented on the team -



Does my computer program require dedication?

- Is it considered basic component / safety-related based upon its end use?
  - Yes
  - No

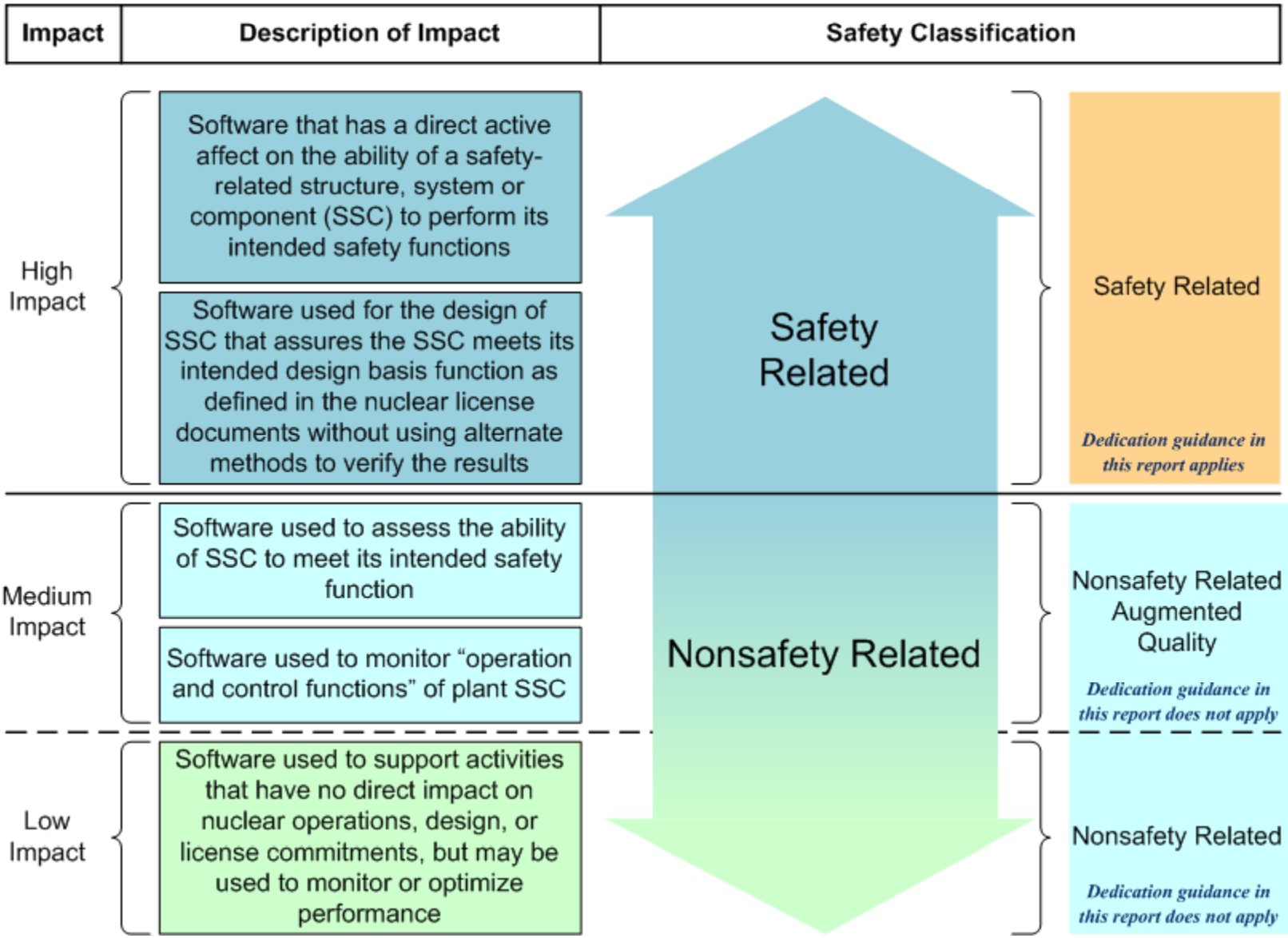
- What is the procurement scenario
  - Buy from “nuclear” supplier (10CFR50, App. B & 10CFR21 apply)
  - Buy from commercial supplier (10CFR50, App. B & 10CFR21 do not apply)

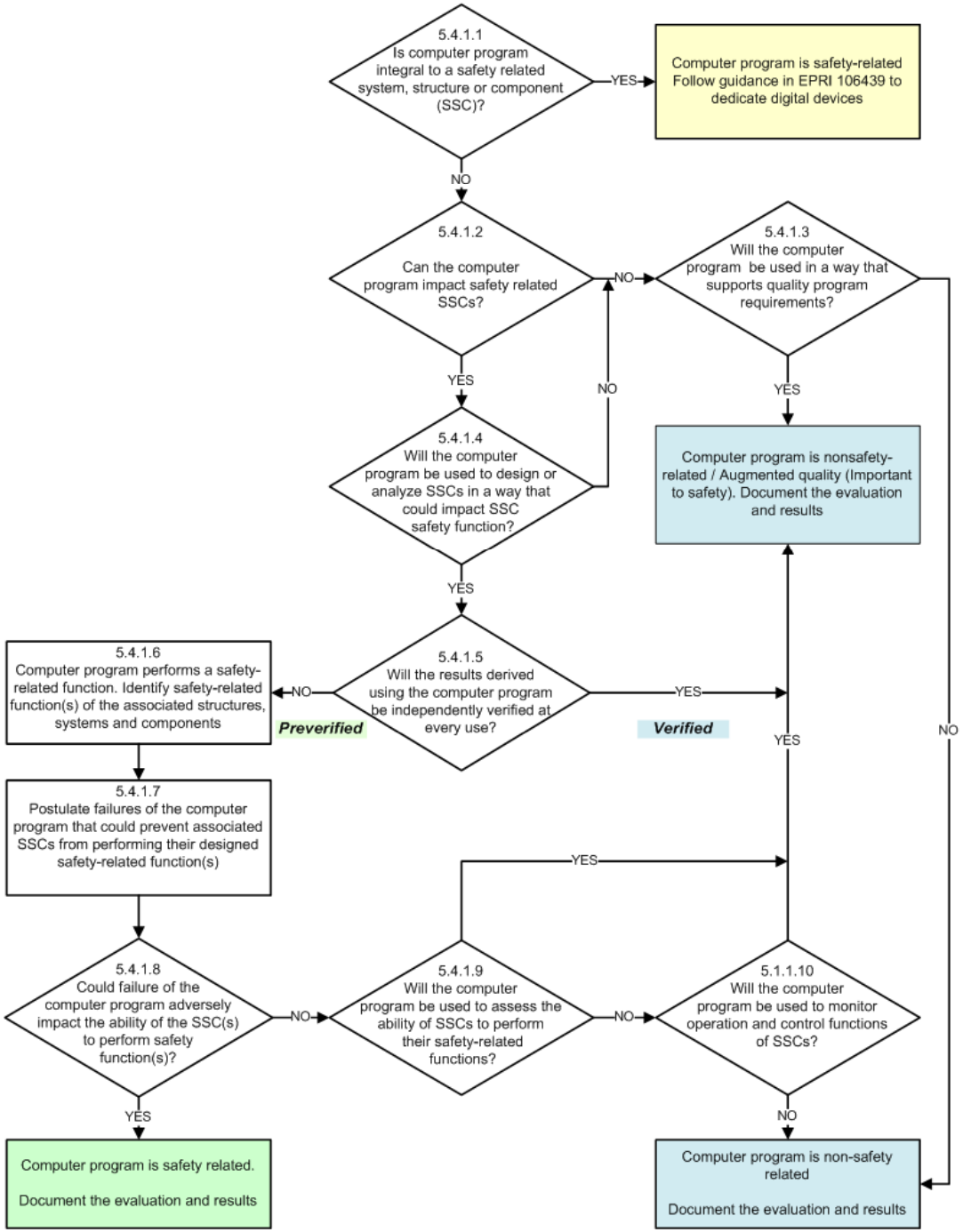


How do we know what replacement items are safety-related?

- Safety classification is performed
  - Where is the item used?
  - What is the item's function
- Final Safety Analysis Report (FSAR) or Updated FSAR
  - System classification based on system function (Safety or non-safety)
  - Component classification based upon component function and its effect on safety related function(s) of the system(s)
  - Part / Item classification based upon part/item function and its effect on safety related function(s) of the component

NITSL Impact Classification Methodology





Safety Classification of Computer Programs

- Based upon end use application
  - Plant SSC's impacted
  - Extent to which the program is relied upon

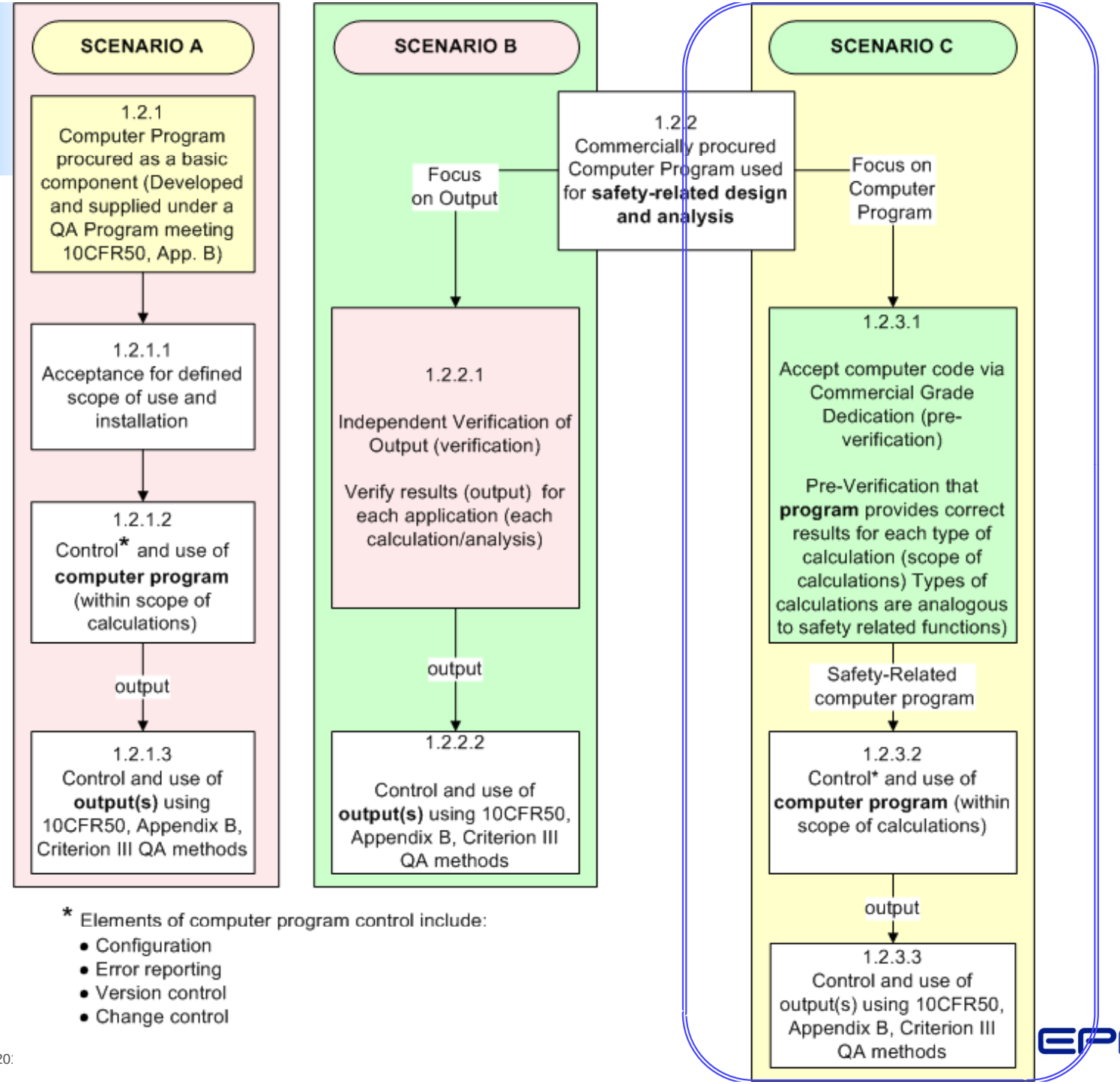
Back to the Calculator Question

- What happened when we used calculators in design and analysis applications?

Independent Verification

Independent Verification

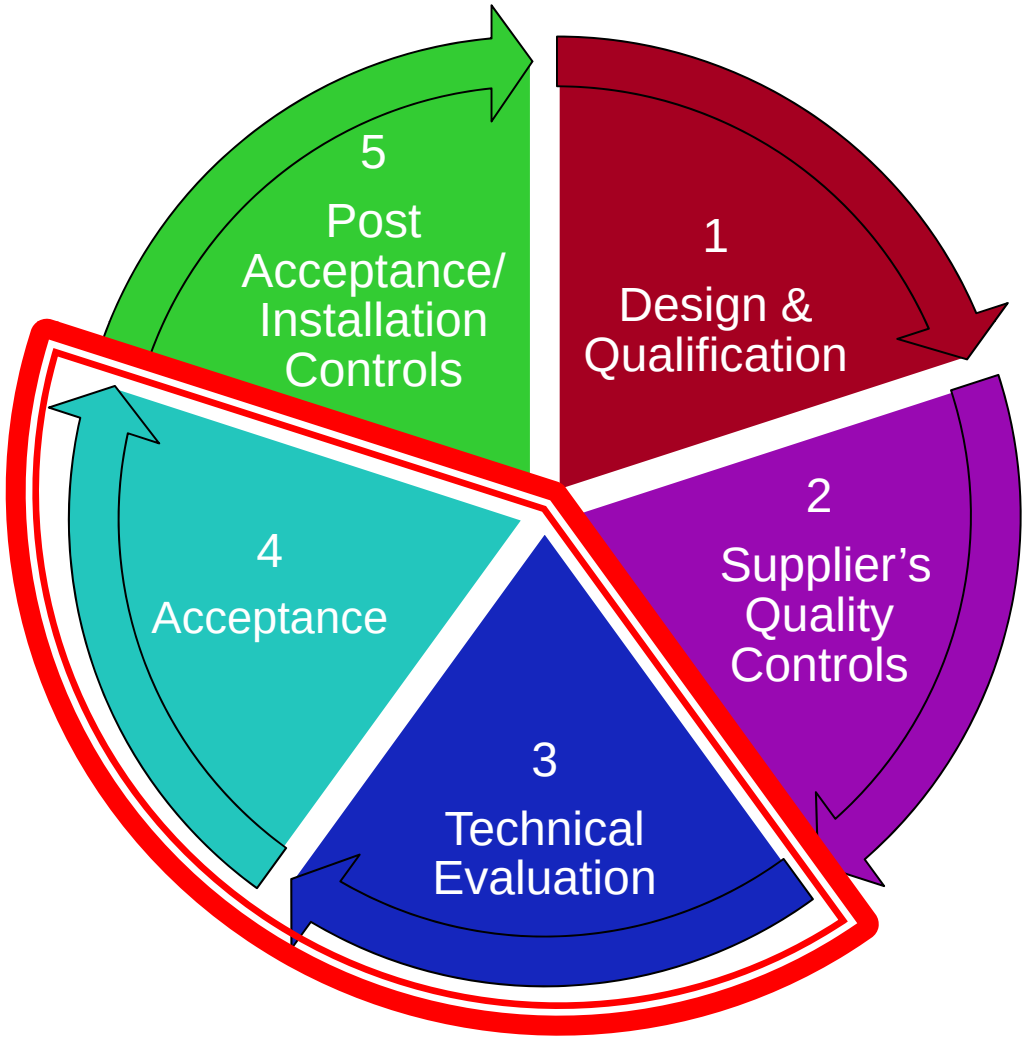
- What could we do if we couldn't perform independent verification?
  - Design reviews?
  - Qualification testing?
  - Alternate calculations?



* Elements of computer program control include:

- Configuration
- Error reporting
- Version control
- Change control

Elements assuring overall quality of plant equipment – Where does dedication start?



- 10CFR21 (1995)
  - "Dedication is an *acceptance* process"
- A technical evaluation is prerequisite to performing dedication
- Other processes are used when design is impacted
  - Equivalency Evaluation
  - Modification / Design Change

Relationship of Design and Acceptance for Software

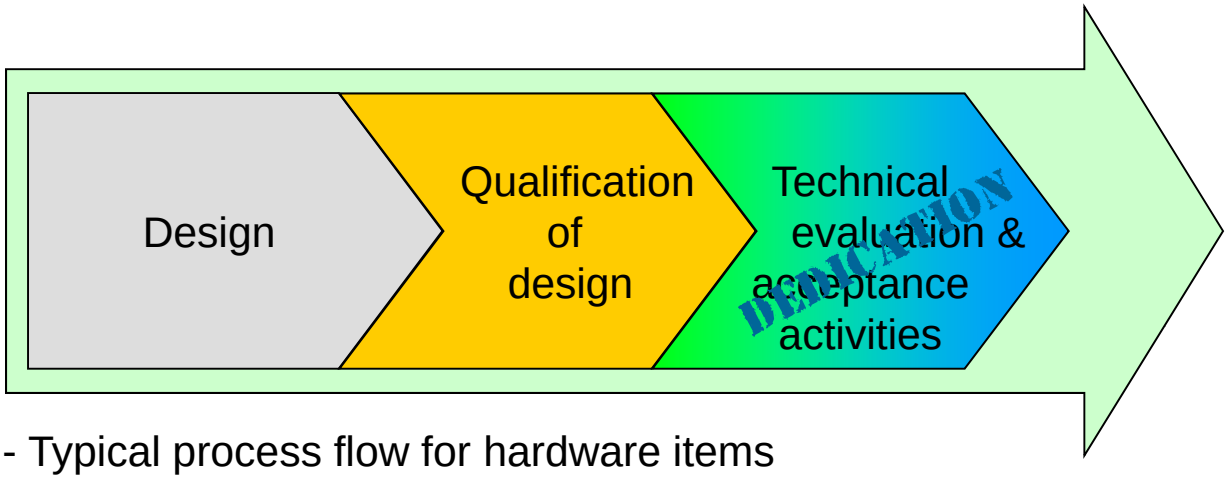


Figure 1 - Typical process flow for hardware items

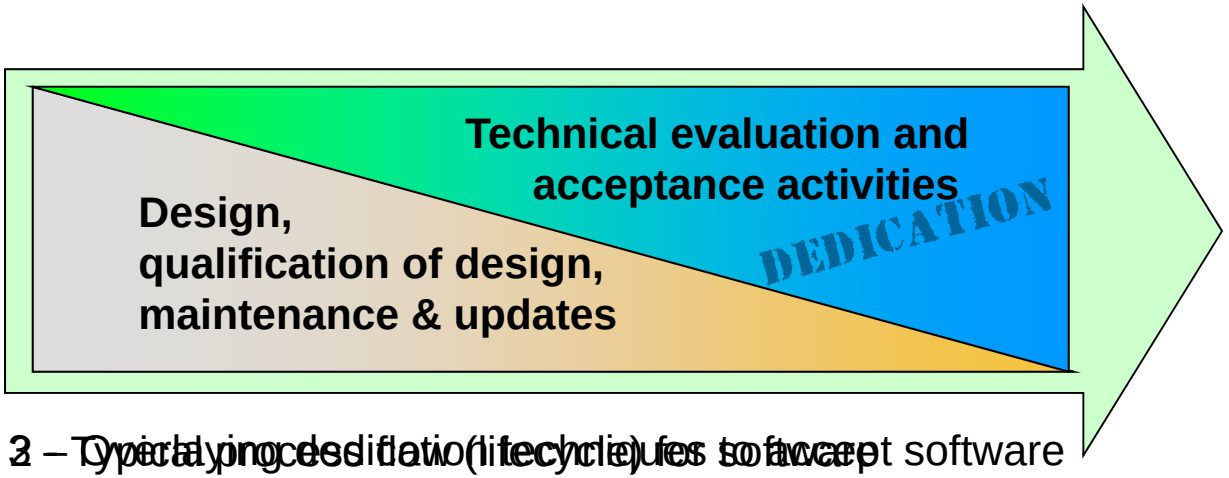
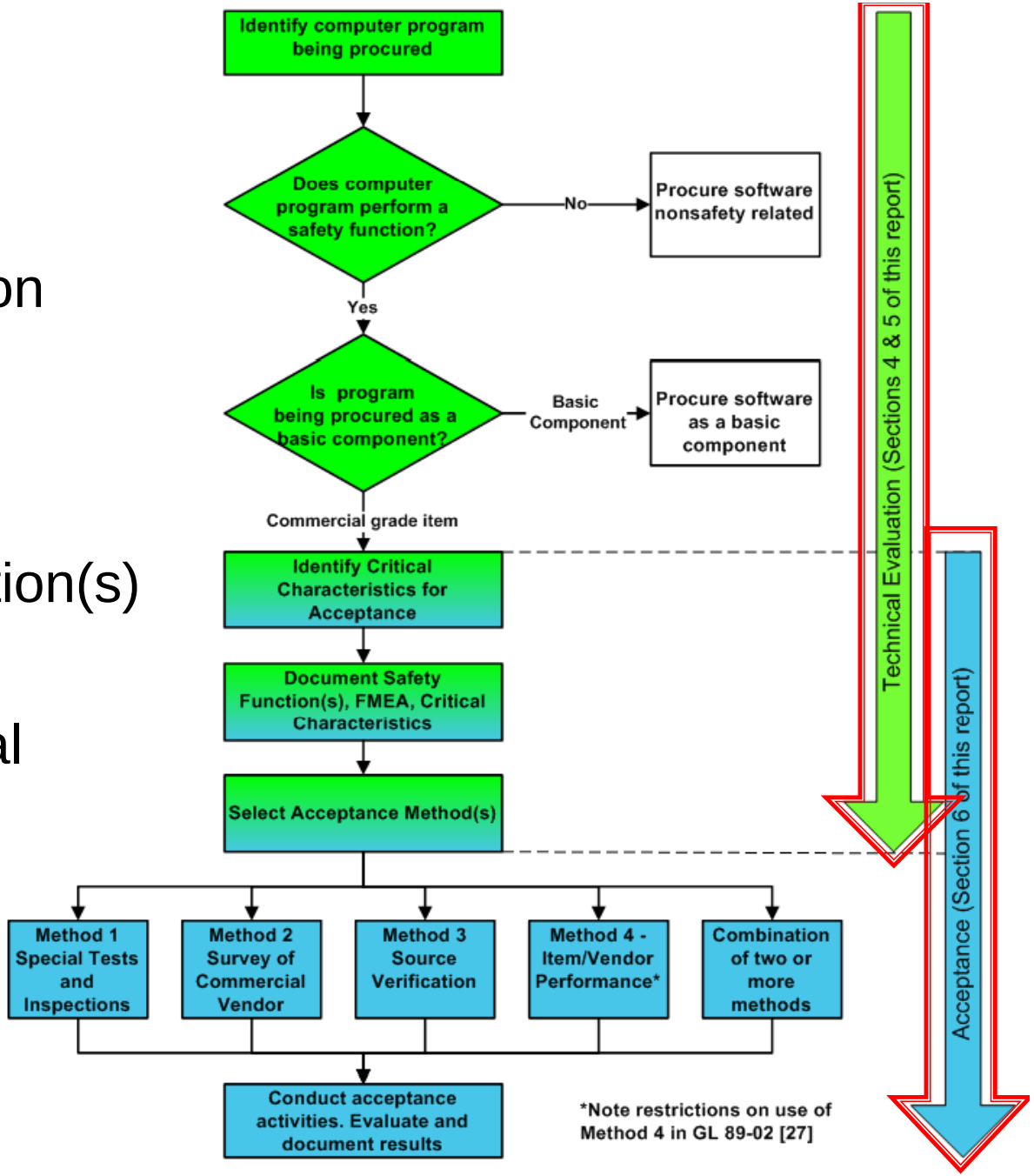


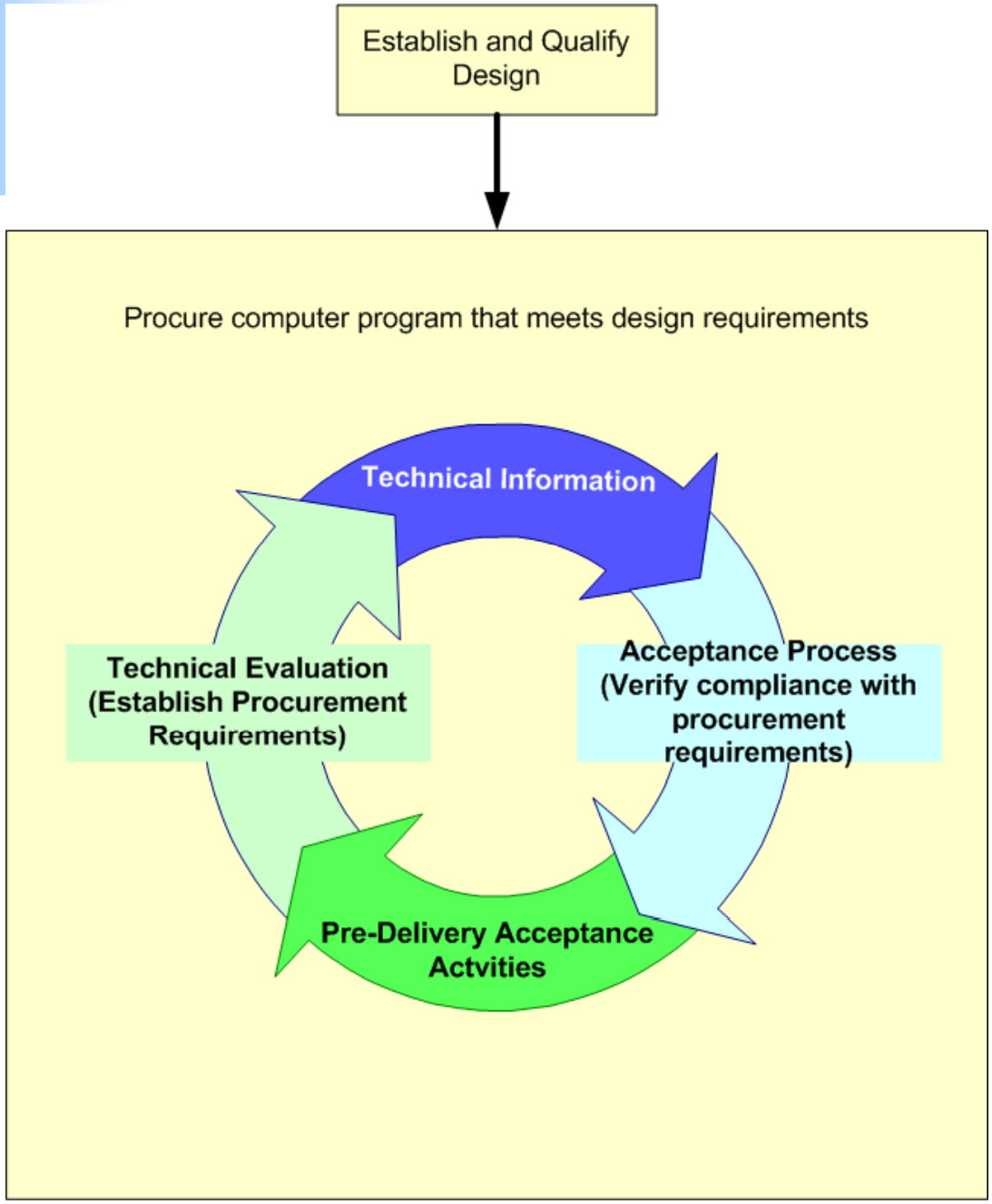
Figure 2 – Typical process flow (lifecycle) for commercial software

Basic Process

- Dedication based upon computer program's
  - Safety function(s)
  - Failures that could impact safety function(s)
- Identification of critical characteristics
- Identification of acceptance methods
- Acceptance activities



EPRI ELECTRIC POWER RESEARCH INSTITUTE



Dedication of Computer programs is specialized

- The right people must be involved
  - Selection of the right program
  - Understanding how the program works
  - Technical evaluation
  - Acceptance activities

Computer Program Failure Modes

- Failure Modes for safety classification are postulated based on failure of plant SSCs impacted by the program
  - Could failure of the program prevent a safety-related SSC from performing a safety function?
- Failure Modes for determining critical characteristics are based upon failure computer program
  - What kinds of failures could cause the program to fail (thus resulting in failure of plant SSCs)?
  - What characteristics are necessary to prevent those failures
- (for hardware, the same failure modes can be used for safety classification and determining critical characteristics

Typical Computer Program Failure Modes and Associated Critical Characteristics

Type of Failure	Critical Characteristics
Conceptual Error	Accurate/correct results are obtained for calculations performed within the specified range of use.
Arithmetic Error	Accurate/correct results are obtained for calculations performed within the specified range of use, engineering parameters.
Interface Errors	Accurate/correct results are obtained when computer program is installed and interfacing with other programs, hardware, or operating systems.

Product Selection Attributes

- Product Selection Attributes are not critical characteristics
- Selection takes place before technical evaluation and acceptance (dedication)

Product Selection Attribute	Description	Acceptance Criteria	Possible Methods of Evaluation During Product Selection/ Qualification for Use
Functionality required for intended end use(s) The computer program is capable of performing the desired calculations, analyses, and so forth.	When correctly installed in the designated environment, the computer program is capable of performing the types of calculations required over the identified range of inputs.	The computer program includes the capabilities specified/ necessary to support design and analysis. Note: Verification of the capabilities for acceptance takes place after product design, selection, and qualification are complete.	Review of published product literature.

Typical Product Selection Attributes

Product Selection Attributes
Functionality Required for intended use(s)
Validity of scientific basis for computer program functionality
Effective problem reporting
Supportability/maintainability
Environmental compatibility: portability
Host computer/operating environment identification
Computer program identification

Product Identification Attributes

- Product Identification attributes are not critical characteristics
  - Considered by the SMEs during selection of the program
  - May be verified at receipt to confirm the right program is received (similar to part number verification when hardware is received)

Product Selection Attributes
Host computer/operating environment identification
Computer program identification

Critical Characteristic

- As defined in 10CFR21 (1995)

  "Critical characteristics. When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, critical characteristics are those important *design, material, and performance characteristics* of a commercial grade item that, *once verified, will provide reasonable assurance that the item will perform its intended safety function*."

Performance Critical Characteristic	Description	Acceptance Criteria	Possible Methods of Verification
Tolerance of output	The allowable possible error in measurement.	Objective evidence through testing or similar means (such as verification or validation) that the computer program results meet the user's specified requirements. Criteria may be expressed similar to the following: Tolerance - ± 0.0000X	Inspection and testing. (Method 1) Commercial-grade survey of testing activities and documentation Observation and review of design. (Method 3) Review of the installed base to determine performance history. (Method 4)

Typical Performance Critical Characteristics

Performance Critical characteristics
Accuracy of Output
Precision of output
Tolerance of output
Functionality: Specific safety functions and algorithms
Functionality: Completeness and correctness
Interfaces: Critical input parameters and valid ranges
Interfaces: Output parameters

Typical Dependability Critical Characteristics

Dependability Critical Characteristics
Built-in quality - Effective quality and oversight of development process
Built-in quality - Structured development process - documentation
Built-in quality - Structured development process - adherence to coding practices
Built-in quality - Structured development process - configuration control and traceability
Built-in quality - Code structure (complexity, conciseness)
Built-in quality - Conformance to national codes, standards, and industry-accepted certifications
Built-in quality:- Internal reviews and verifications
Built-in quality - Testability and thoroughness of testing
Built-in quality - Training, knowledge, and proficiency of the personnel performing the work

Document the relationship between critical characteristics, acceptance criteria and methods

Inspection Attribute/ Critical Characteristics	Acceptance Criteria	Possible Method(s) of Acceptance
Software revision number	Software revision conforms to the number identified in the procurement document.	Standard receipt inspection
Update (configuration) control	Current configuration remains suitable for the application.	Method 2 (CG survey)
Platform compatibility (operating system, etc.)	Computer program is compatible with the current operating system.	Method 1 (Testing)
Hardware compatibility	Computer program is compatible with the current hardware.	Method 1 (Testing)
Built-in quality	Appropriate in-process tests and inspections are performed.	Method 2 (CG survey)
Quality of design and implementation	Design controls are performed in accordance with SQA.	Method 2 (CG survey)
Functions/applications	Outputs are consistent and accurate for various applications.	Method 1 (Testing), Method 2 (CG survey)
Range (input variables, limits of application, etc.)	Outputs are consistent and accurate over a range of inputs and applications.	Method 1 (Testing), Method 2 (CG survey)
Accuracy	Outputs are mathematically accurate.	Method 1 (Testing), Method 2 (CG survey)
Consistency repeatability	Outputs are consistent and accurate over numerous times the computer program is used.	Method 1 (Testing), Method 2 (CG survey)

Relationship of Design and Acceptance for Software

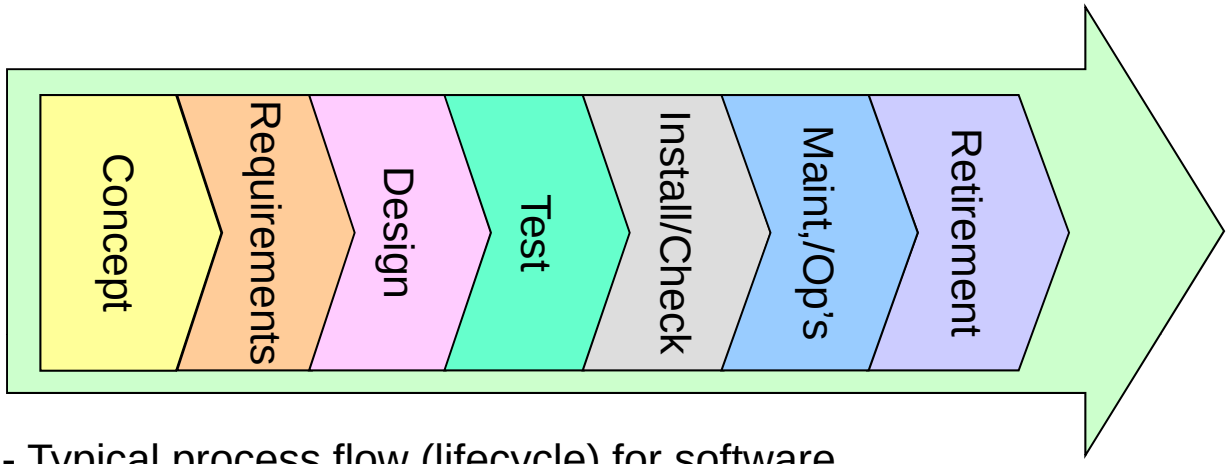


Figure 2 - Typical process flow (lifecycle) for software

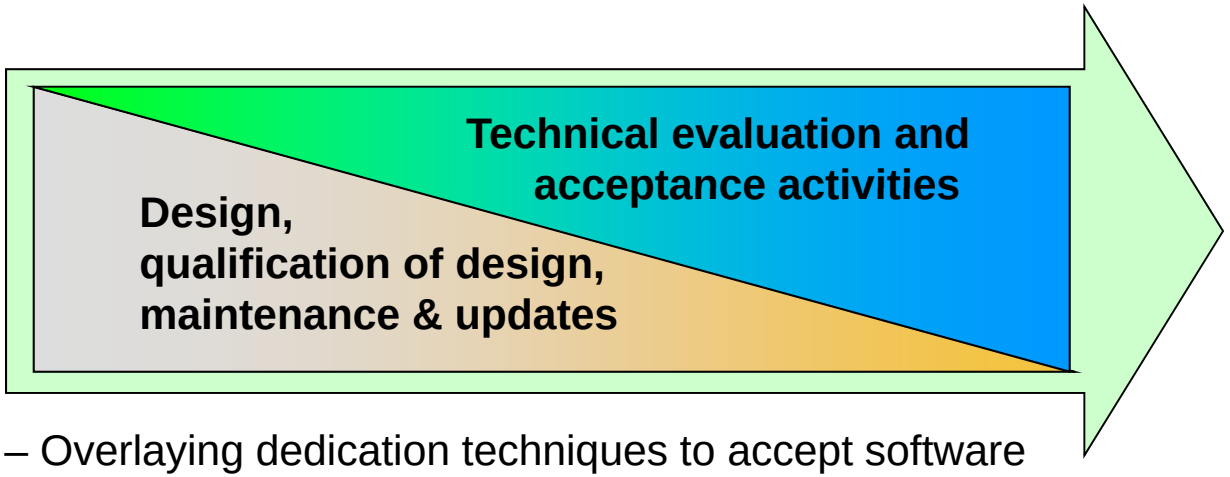
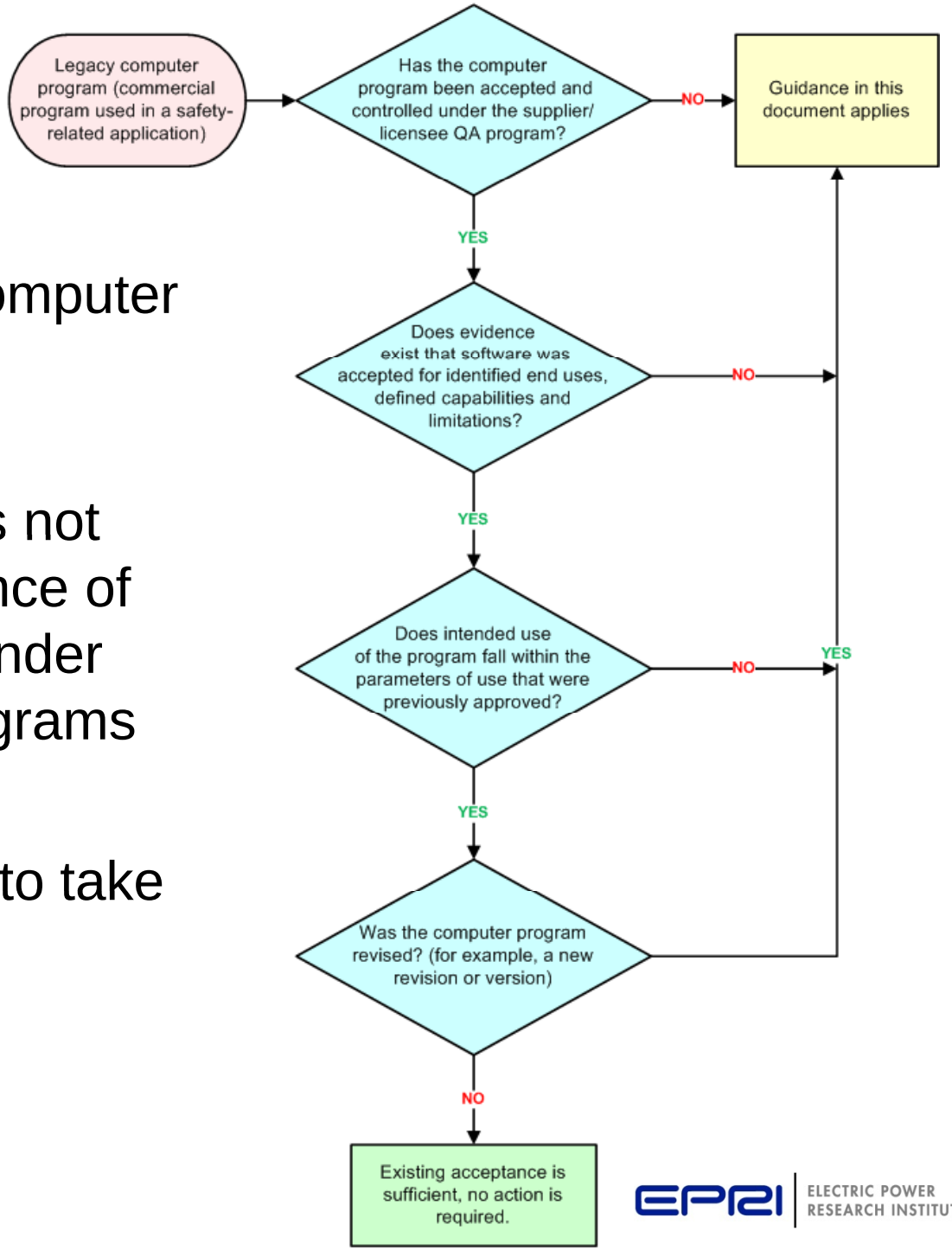


Figure 3 – Overlaying dedication techniques to accept software

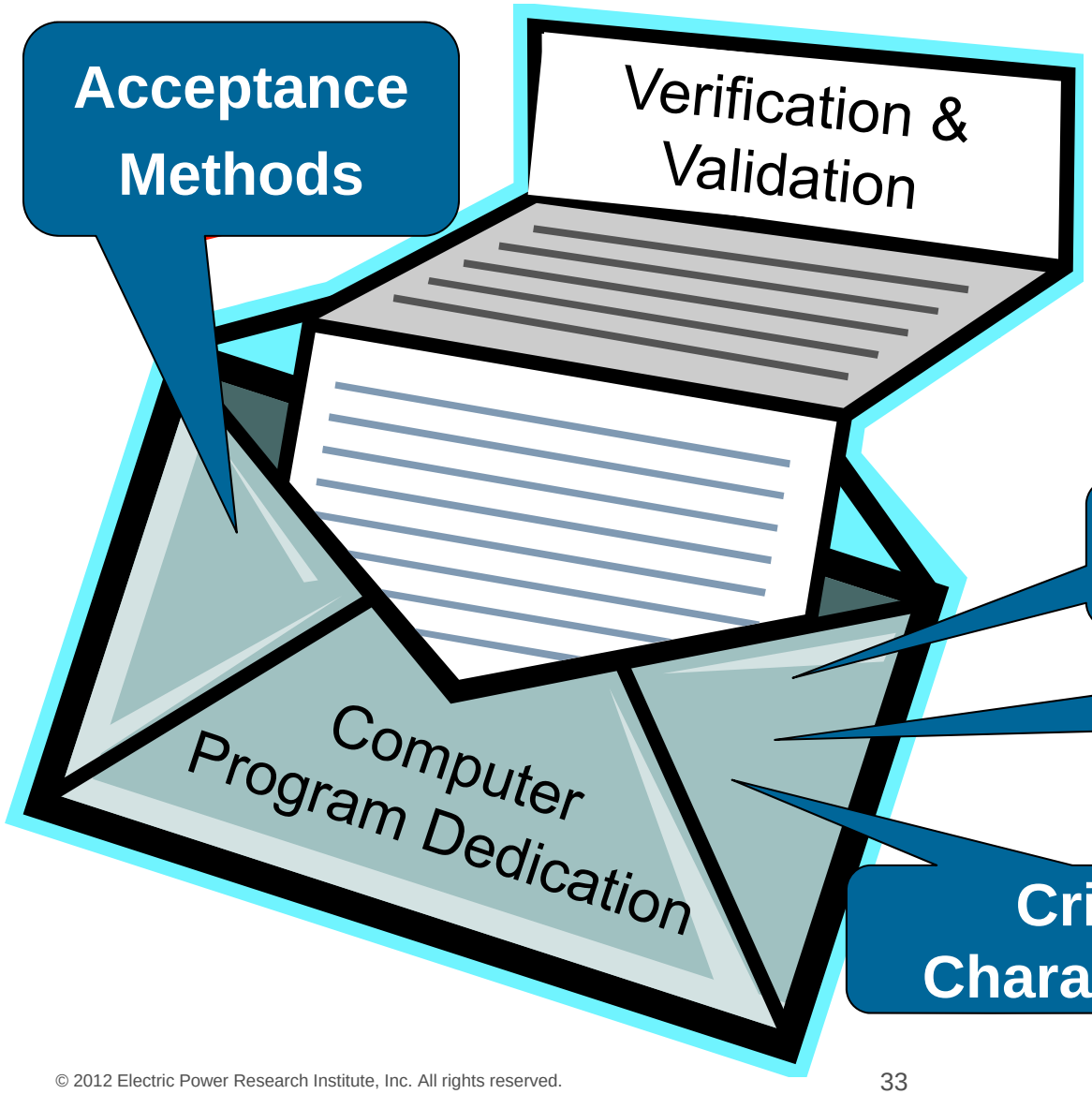
Legacy Programs

- What about legacy computer programs?
  - The guidance does not invalidate acceptance of legacy programs under “nuclear” SQA programs
  - When do we need to take another look?



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Acceptance of Commercial Computer Programs



- Dedication can be built around existing verification and validation

Safety Class and Function(s)

Failure Modes and Effects

Critical Characteristics

Together…Shaping the Future of Electricity