Acceptance of Commercial Grade Design and Analysis Computer Programs

Marc H. Tannenbaum
Technical Leader

NRC Workshop on Vendor Oversight
June 23, 2016

St. Louis, Missouri

"I do not fear computers, I fear the lack of them"

Isaac Asimov

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

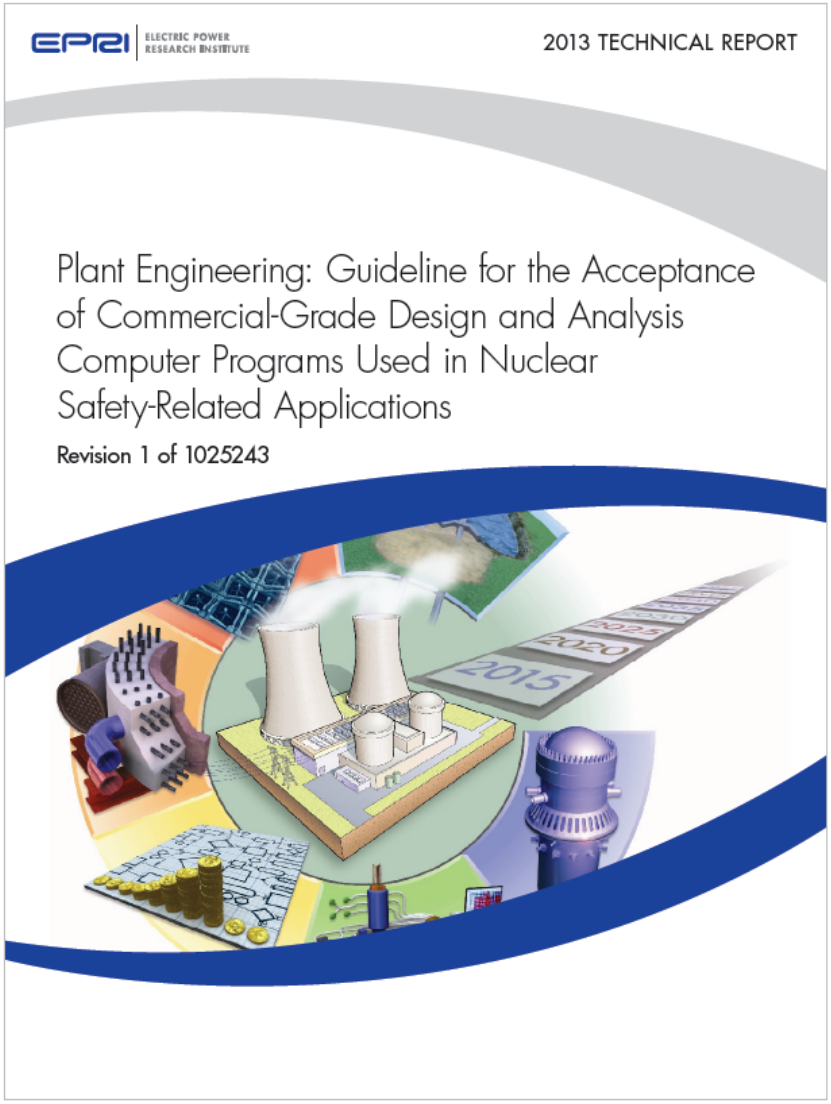
Starting Line for EPRI Guidance

- NUPIC and NRC findings
- Lack of 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

- NRC precedent exists to consider verification and validation activities common to software development in digital systems to be a critical characteristic
  - Safety Evaluation Report (SER) of Topical Report TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications (1997)

EPRI 3002002289 (Supersedes EPRI 10252443)

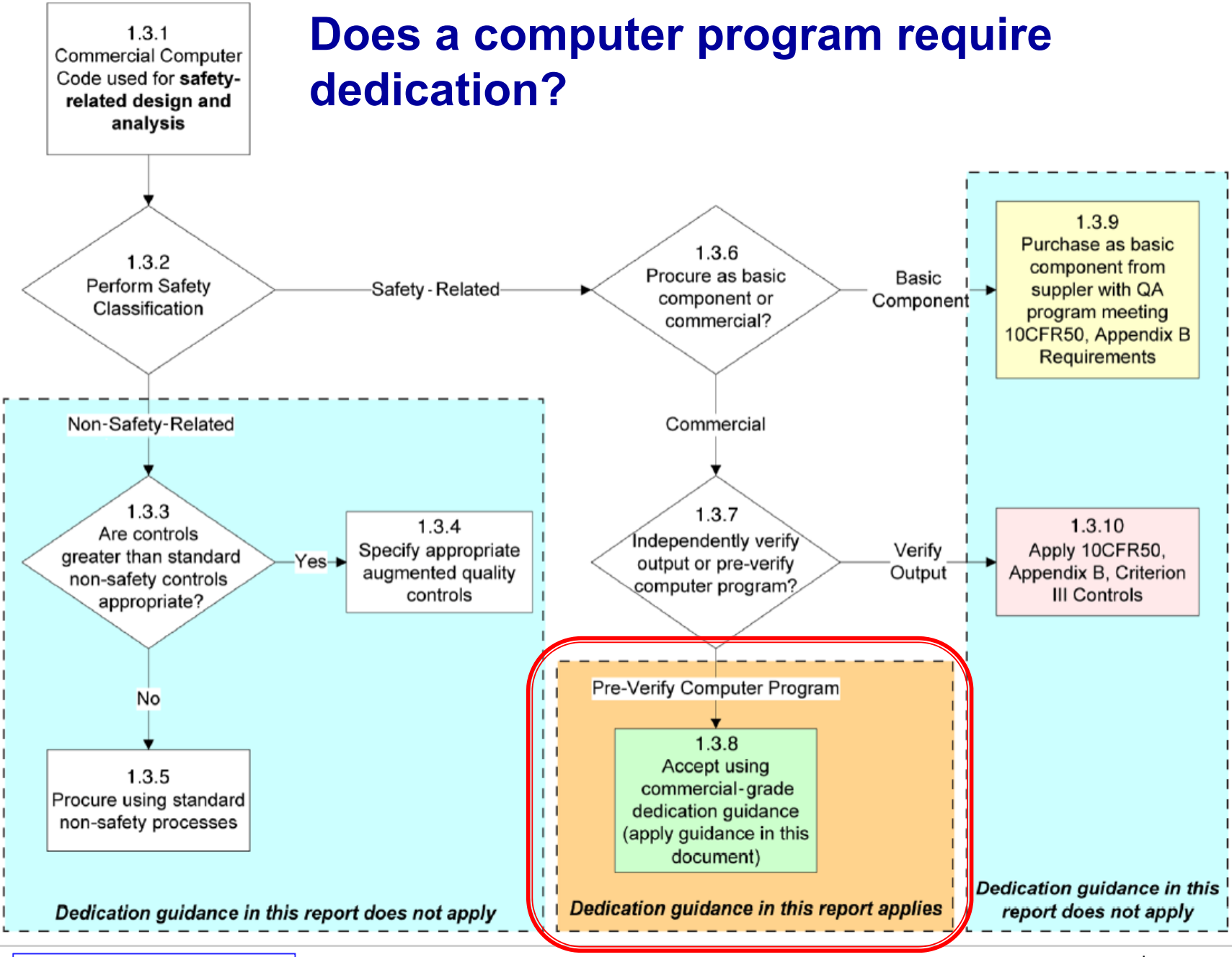
- Incorporates NRC RAI Comments
- Generic technical evaluation process overview
- Functional safety classification of computer programs
- Acceptance of commercial-grade computer programs using the dedication process



Represented on the original team – EPRI 1025243

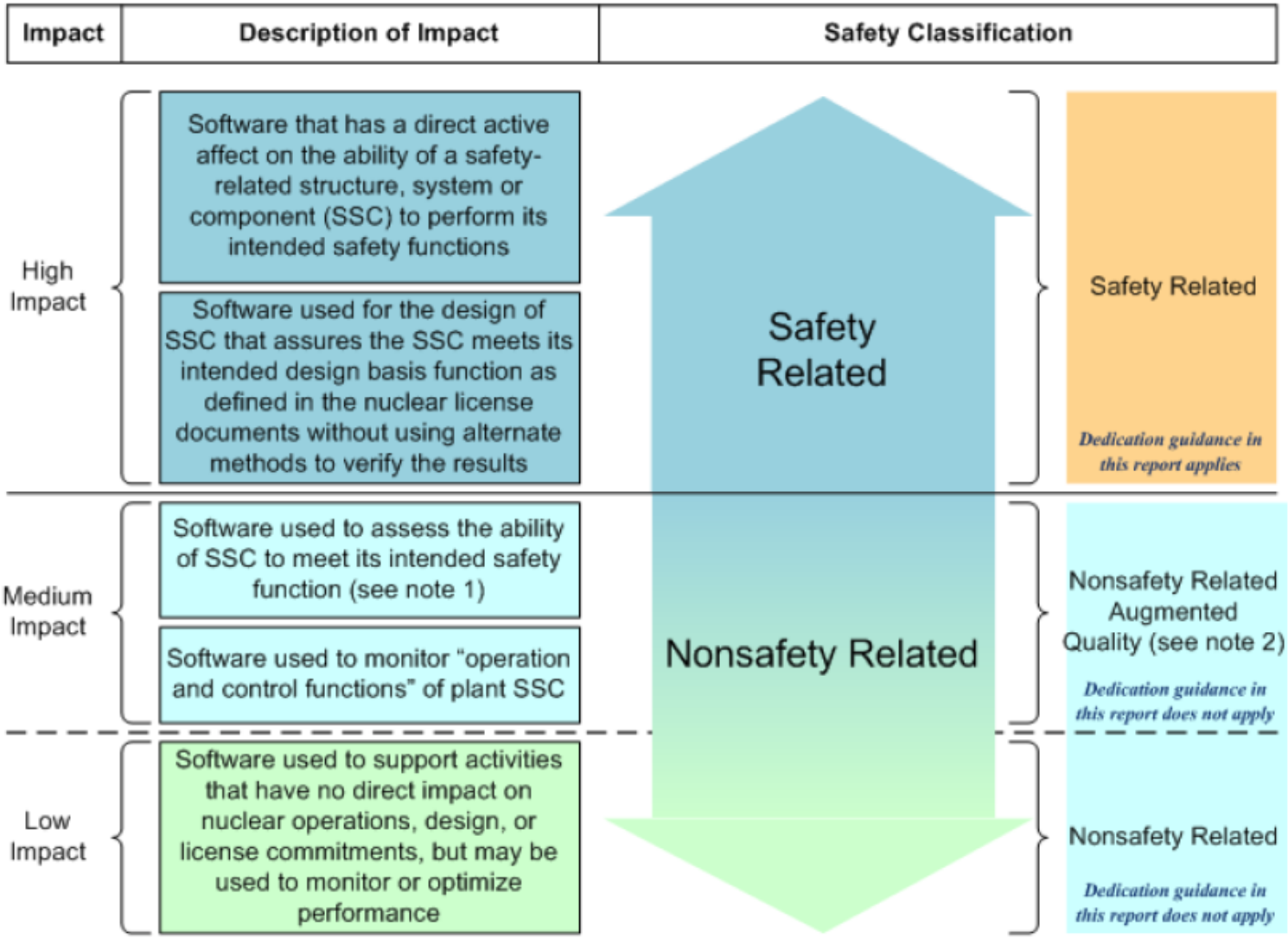
Represented on the RAI team – EPRI 3002002289

Does a computer program require dedication?



Report page 1-7

NITSL Impact Classification Methodology

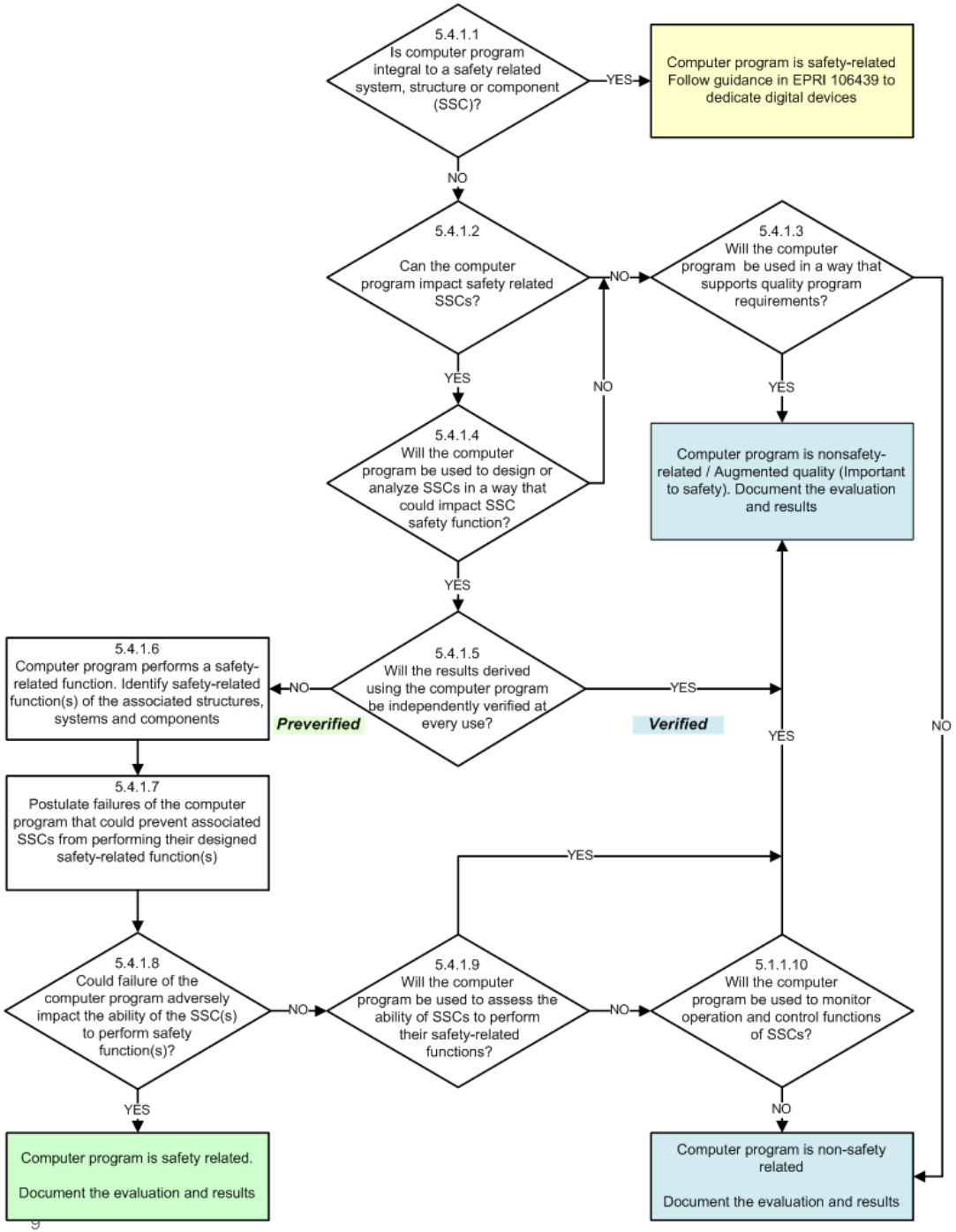


Note 1: It is important to recognize that software used to establish suitability of design of a safety related SSC may not be categorized as medium impact software unless alternative methods are used to verify the results.

Note 2: The term *augmented quality* is used as defined in this report and is not limited to only the non-safety-related SSCs credited for regulated events described in Section 17.5V. of NUREG-0800, *Standard Review Plan* [38].

Report page 5-12

Safety Classification of Computer Programs



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

Report page 5-5

Back to the Calculator Question

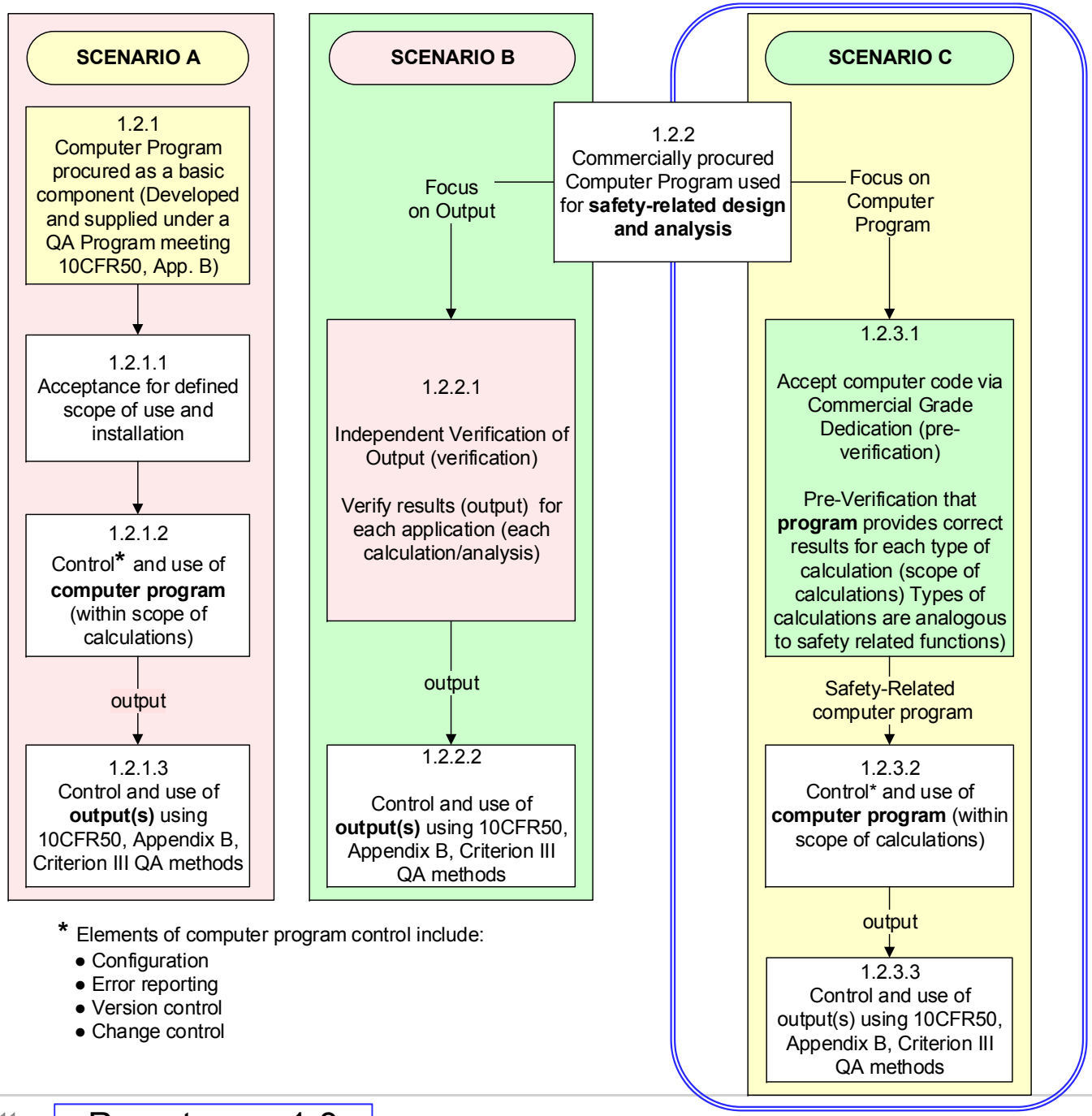
- What happened when we used calculators in design and analysis applications?

Preparation

Independent Verification

- What could we do if we couldn't perform independent verification?
  - Design reviews?
  - Qualification testing (*testing to establish suitability of design*)?
  - Alternate calculations?

Three procurement scenarios for computer programs

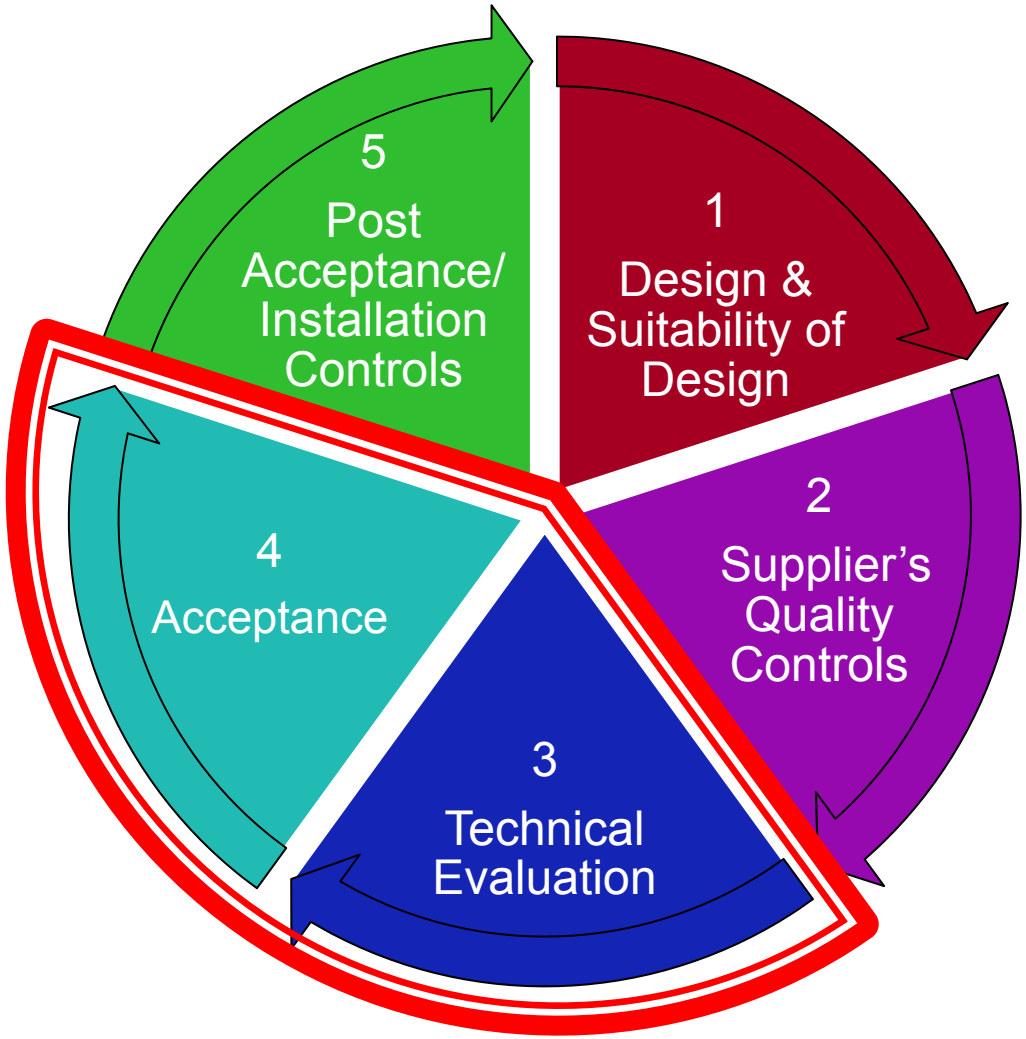


* Elements of computer program control include:

- Configuration
- Error reporting
- Version control
- Change control

Report page 1-3

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

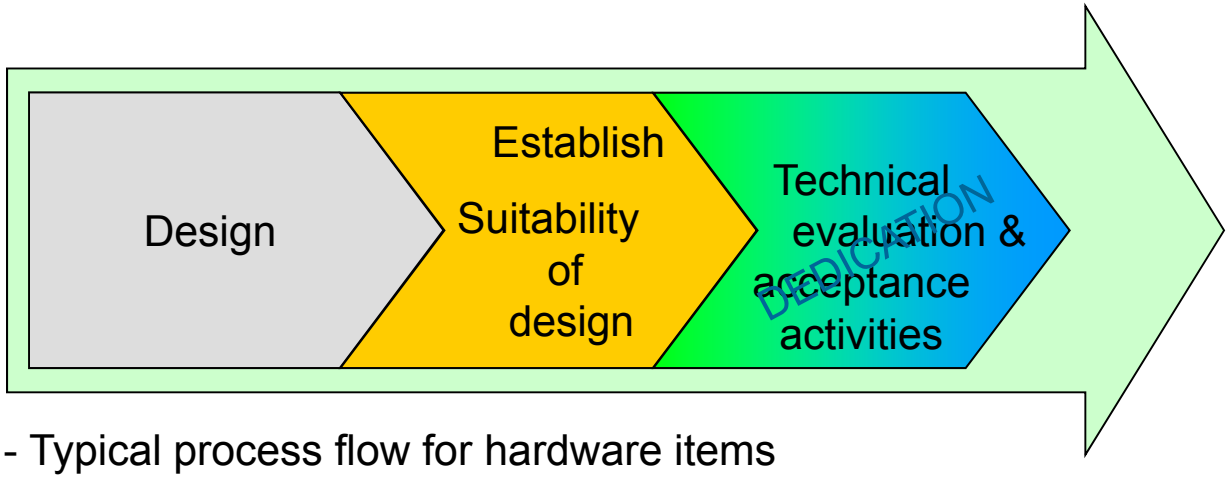


Figure 1 - Typical process flow for hardware items

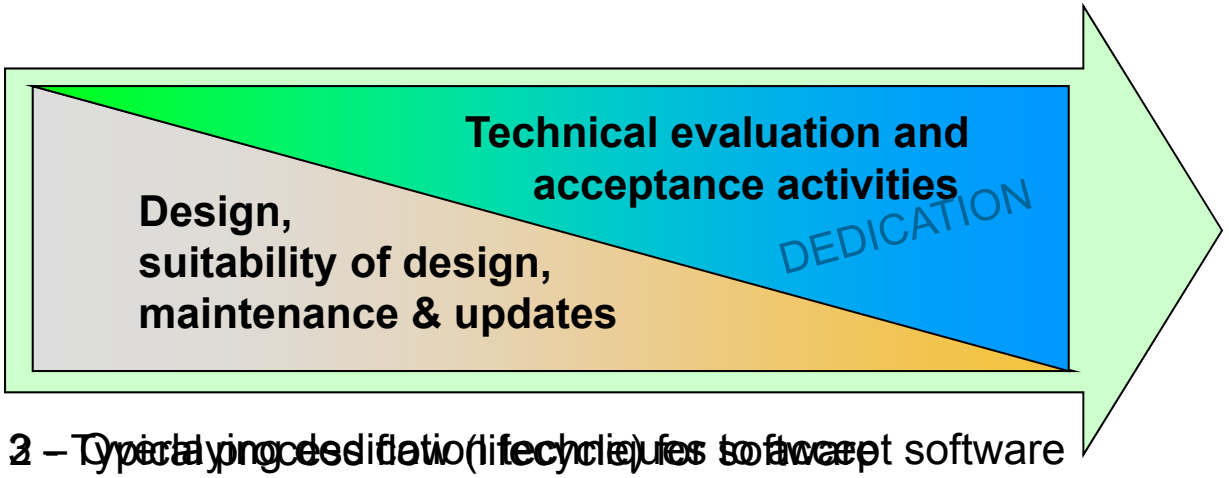
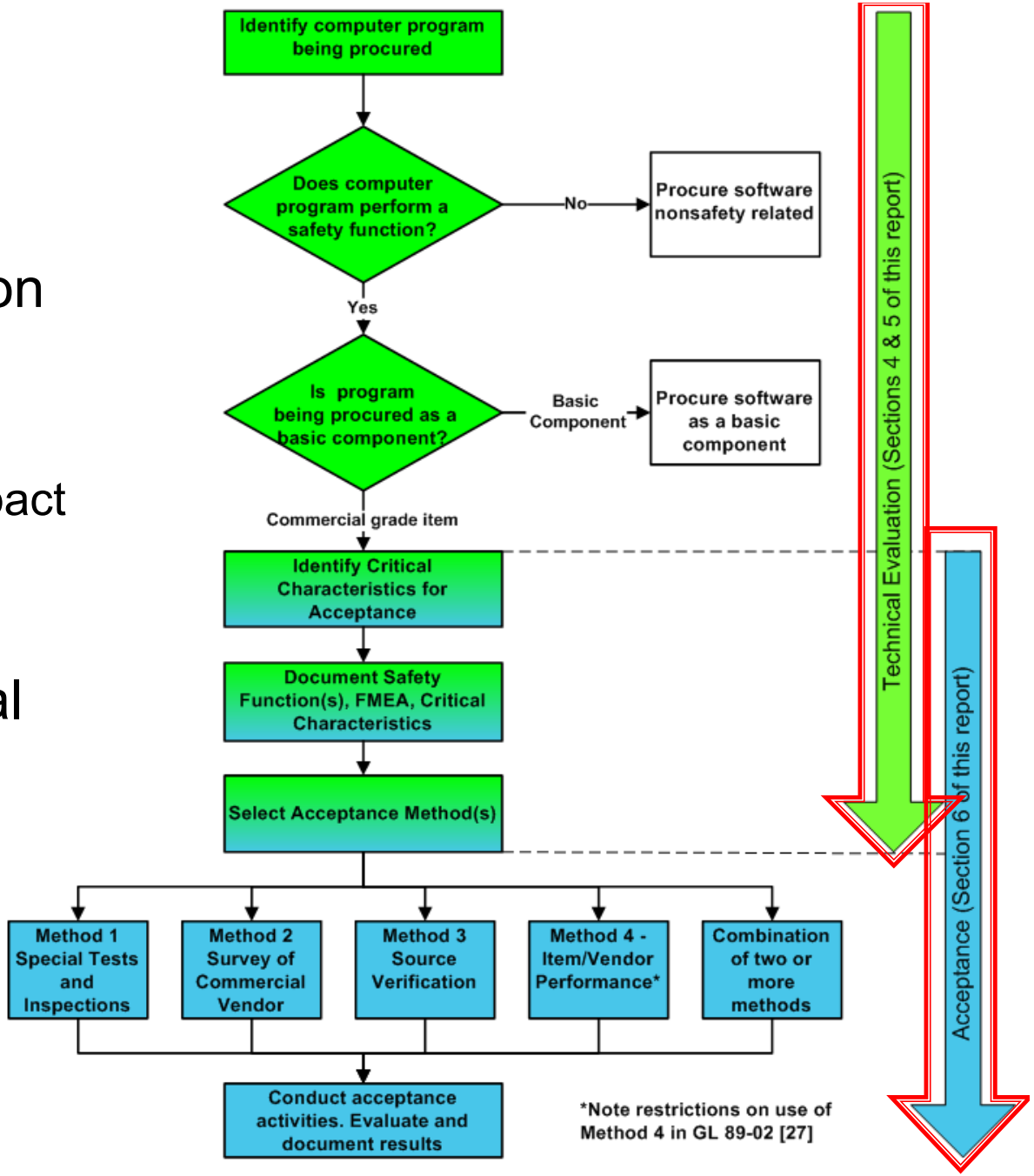


Figure 2 – Typical process flow (lifecycle) for to accept software

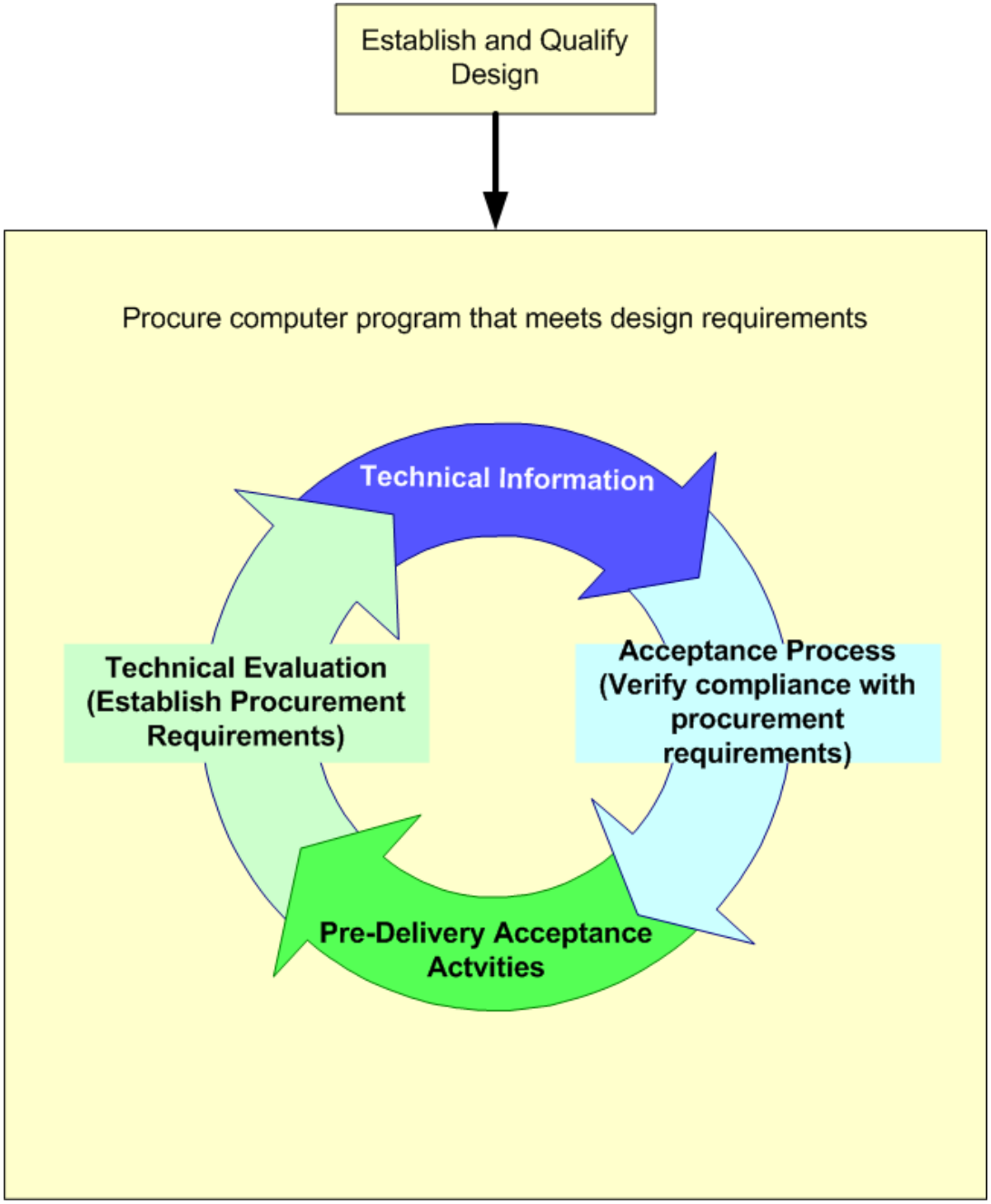
Report page 1-7

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



Report page 1-3



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

Report page 4-3

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 of the computer program itself
  - 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

- Unlike hardware, where 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.

Report page 6-5

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/ Establishing Suitability 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 establishing suitability of design are complete.	Review of published product literature.

Report pages 6-9 to 6-12

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

Report pages 6-9 to 6-12

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 Identification Attributes
Host computer/operating environment identification
Computer program identification

Report page 6-12

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)

Report pages 6-13 to 6-15

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

Report pages 6-13 to 6-15

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

Report pages 6-16 to 6-19

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)

Report page 1-7

Relationship of Design and Acceptance for Software

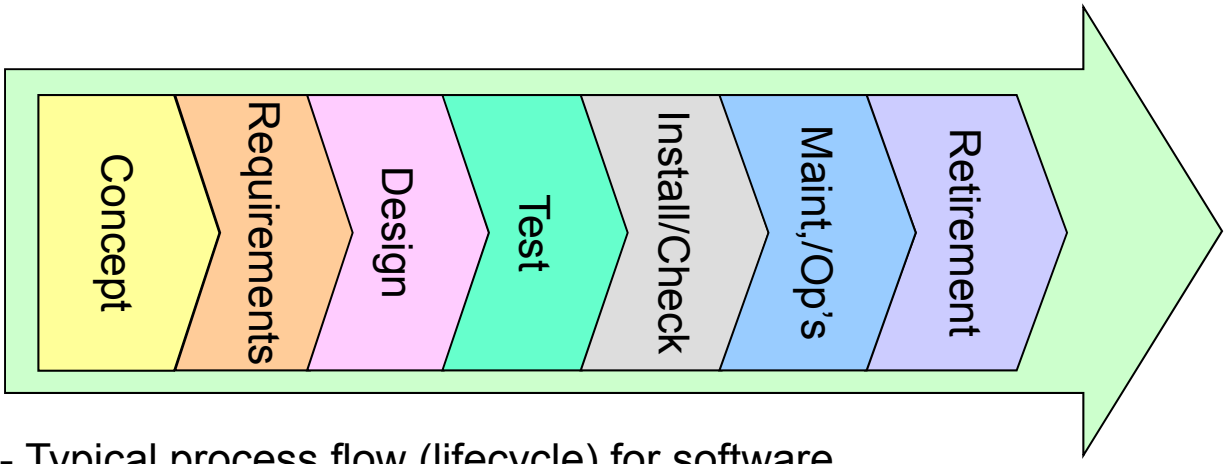


Figure 2 - Typical process flow (lifecycle) for software

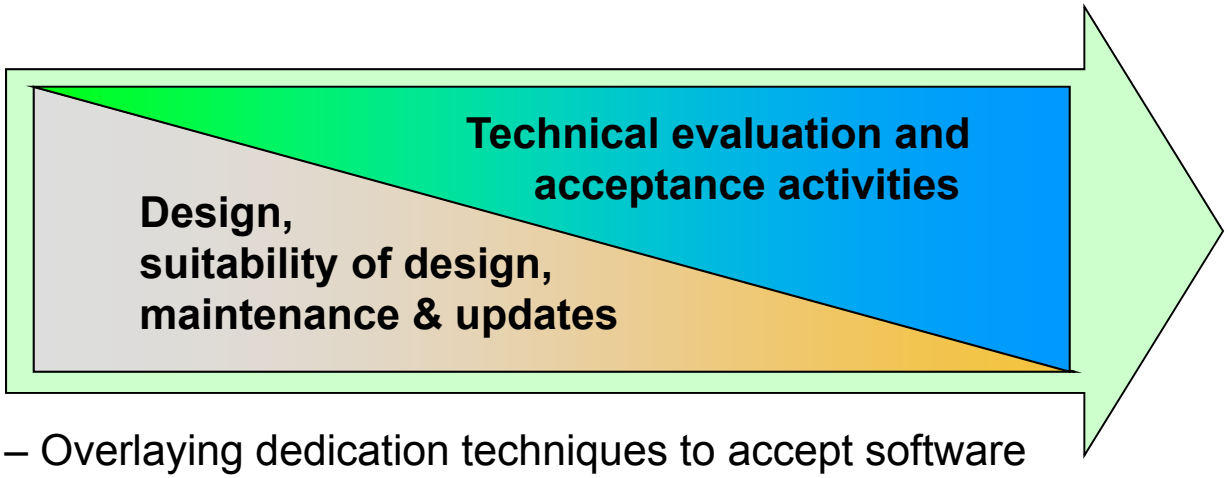
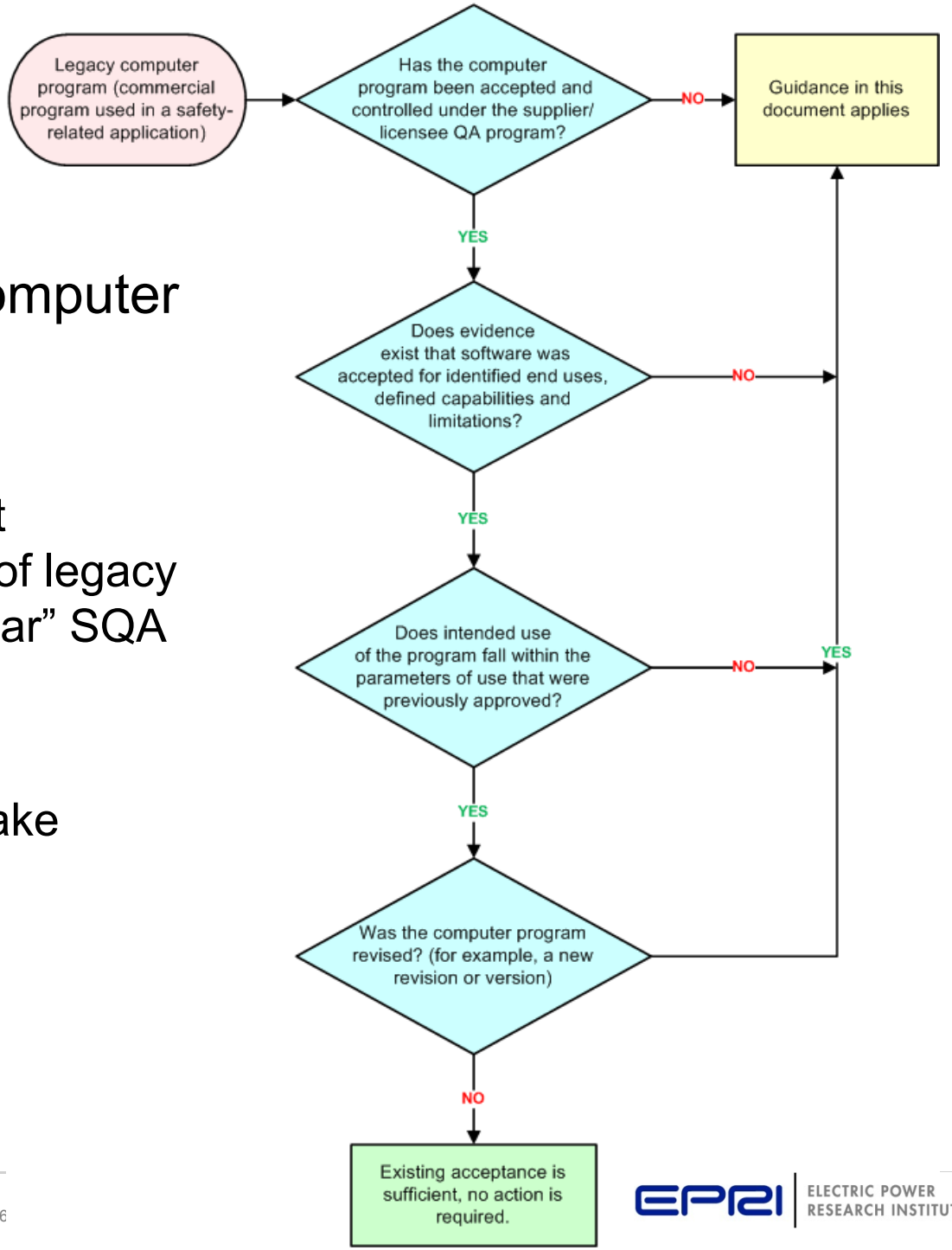


Figure 3 – Overlaying dedication techniques to accept software

Report page 6-27

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?

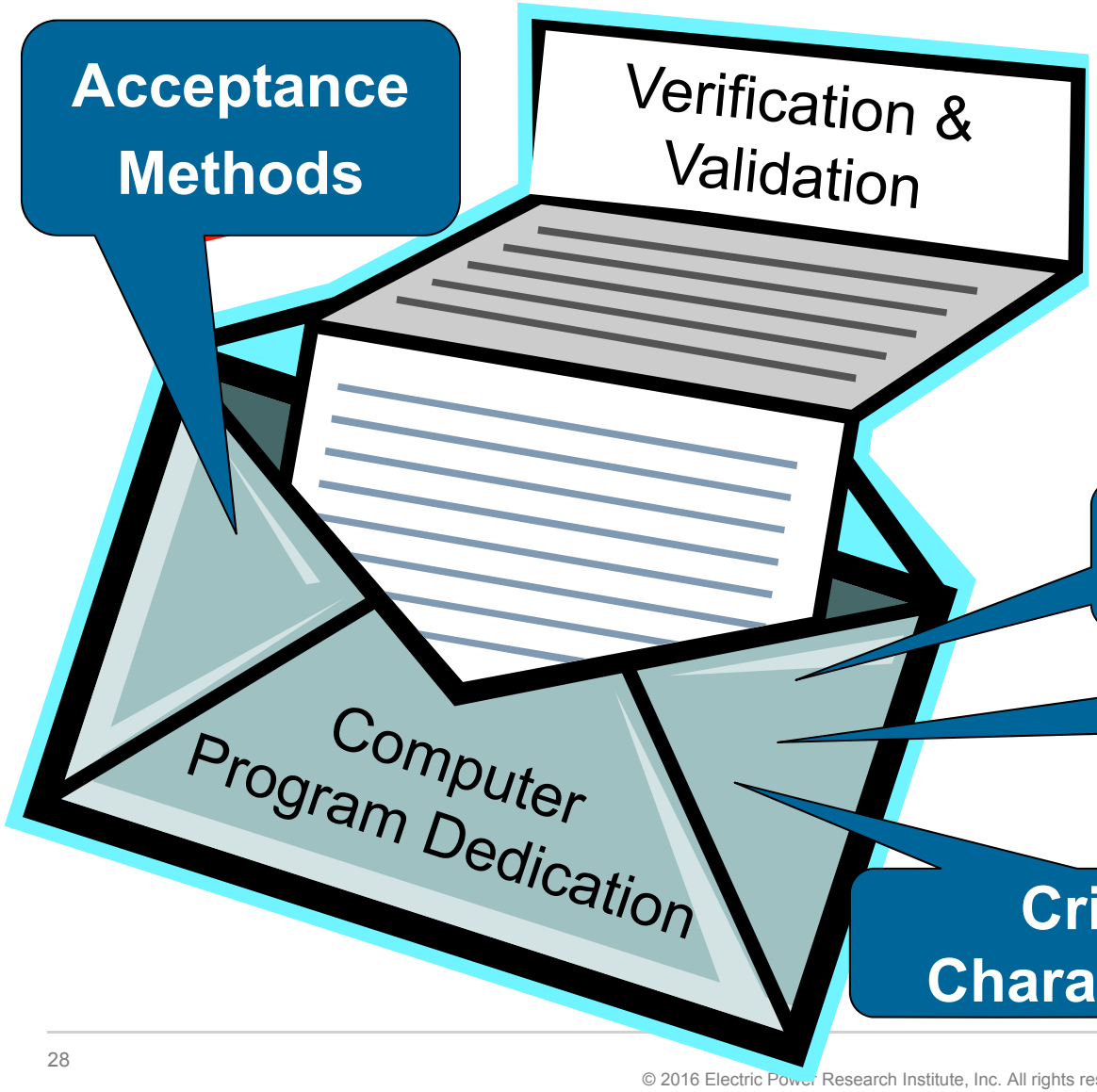


Report page 1-16

What's new in 3002002982?

Section	Summary of Changes
Title Page	Revised to reflect new product number and quality assurance program statement
Acknowledgements	Added acknowledgments applicable to Revision 1.
Executive Summary	Purpose updated to reflect the revision and add the precaution that the extent to which computer programs may or may not perform a safety-related function depends on the way in which the programs are implemented, configured, relied on, and used.
Throughout	Clarified use of the term "qualification" by replacing it with "establish suitability for use" where appropriate.
Figure 1-4	Figure 1-4 added to compare and contrast the differences between acquisition of plant SSCs and design/analysis computer programs.
Section 1.6.7	Clarified last sentence by adding, "for which guidance in this document applies per Figure 1-5" to the parenthetical phrase.
Definitions	Updated definition of basic component to definition from 10CFR50.2 [37] and updated definition of augmented quality to clarify that augmented quality as used in this report is not limited only to the non-safety-related SSCs credited for regulated events identified in Section 17.5 V. of NUREG-0800 [38].
Table 4-1	Clarified the intent of using an equivalency evaluation in situations, such as when the vendor proposes an alternative product, to determine the suitability of the proposed replacement computer program that is not identical to the original. Also clarified that an equivalency evaluation is not intended to address control of computer programs after they are accepted for use, as discussed in Section 1.2.1.2.
Section 5	Added a note to explain that it is important to discuss safety classification in this document because computer programs that are not classified as safety-related are not considered basic components and are not required to be either procured as basic components or procured as commercial grade items and dedicated.
Section 5.4.1.9	Added a sentence to clarify that non-safety-related computer programs are not considered to be basic components and therefore do not require commercial grade dedication.
Section 5.4.2	Added a sentence to clarify that when following the NITSL methodology, it is important to recognize that software used to establish suitability of design of a safety related SSC may not be categorized as medium impact software unless alternative methods are used to verify the results
Figure 5-3	Added precautionary notes 1 and 2 to the bottom of the figure.
Table 5-2	Added precaution to note 3.
Section 6.5	Removed reference to security problems.
Section 7	Clarified if examples pertained to design/analysis computer programs. Non-design/analysis examples are included to illustrate safety classification.
Section 8	Added references 37, 38, and 39.
Appendix B.5	Removed last sentence referring to management of cyber security issues.
Appendix C	Added introductory paragraph
Appendix D	Added this appendix.

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

"It is not necessary to change. Survival is not mandatory"

W. Edwards Deming


EPRI
ELECTRIC POWER
RESEARCH INSTITUTE
Questions?
Together...Shaping the Future of Electricity

Together…Shaping the Future of Electricity