

EPRI

ELECTRIC POWER
RESEARCH INSTITUTE

Acceptance of Commercial Grade Computer Code for Use as a Basic Component in Safety Related Applications

Marc Tannenbaum
Project Manager

NUPIC Vendor Meeting
June 15, 2011

Background

- EPRI is currently developing guidance in response to NRC comments at NUPIC meetings and ASQ meetings
 - Verification and validation is no longer enough
 - Dedication methodology should be applied
- The Technical Advisory Group includes:
 - Auditors (NUPIC)
 - Utility procurement engineers (JUTG)
 - Utility software experts (NITSL)
 - ASME NQA-1 Software Subcommittee
- EPRI is working with NRC through NEI

Background

- Existing EPRI reports do not address dedication of computer code that is not integral to plant structures, systems, and components (SSCs)
 - EPRI NP-5652
 - EPRI TR-102260
 - No content specific to software

ASC	American Society for Quality
EPRI	Electric Power Research Institute
JUTG	EPRI Joint Utility Task Group
NEI	Nuclear Energy Institute
NRC	U.S. Nuclear Regulatory Commission
NUPIC	Nuclear Procurement Issues Committee
SSC	Systems, Structures, Components

Background

- Several existing EPRI reports do address *acceptance* of commercial grade digital devices *integral to plant SSCs*
 - EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications (October 1996)
 - EPRI TR-107339, Evaluating Commercial Digital Equipment for High-Integrity Applications: A Supplement to EPRI Report TR-106439 (December 1997)
- Methodology is helpful as digital devices include computer programs

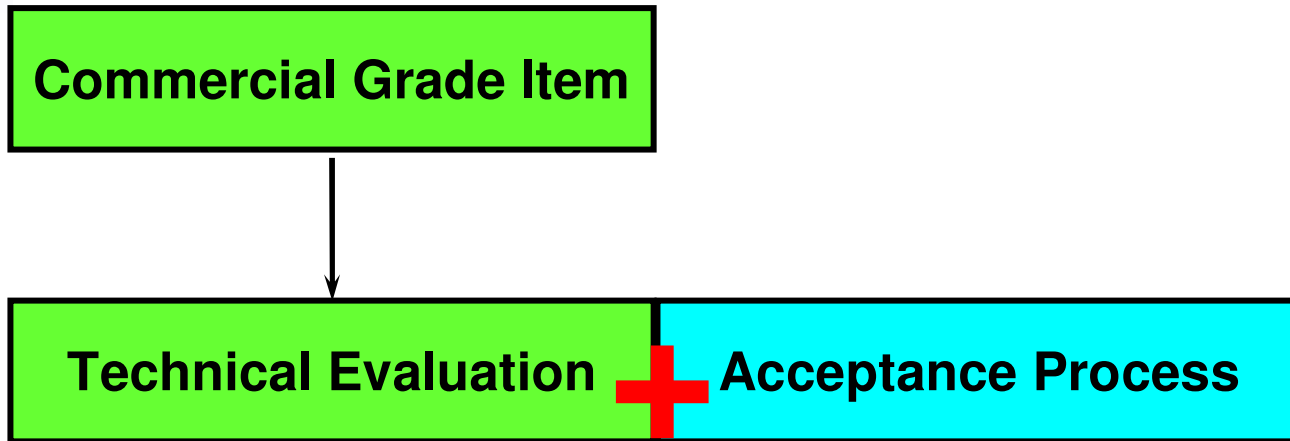
Background

- Focus of EPRI guidance currently in development
 - Acceptance of computer code (not integral to SSCs installed in the plant)
- Objectives
 - Provide guidance on how to perform safety classification of software
 - Provide guidance on how to accept computer code using methodology that finds basis in commercial grade item dedication methodology
 - Obtain regulatory acceptance

Target Audience for EPRI Guidance

- Utilities
 - Many accept software using a full-scale software quality assurance (SQA) program that may be more robust than the commercial grade dedication process
 - Change may be necessary in light of NRC's position
- Suppliers
- Auditors

Commercial Grade Dedication Fundamentals

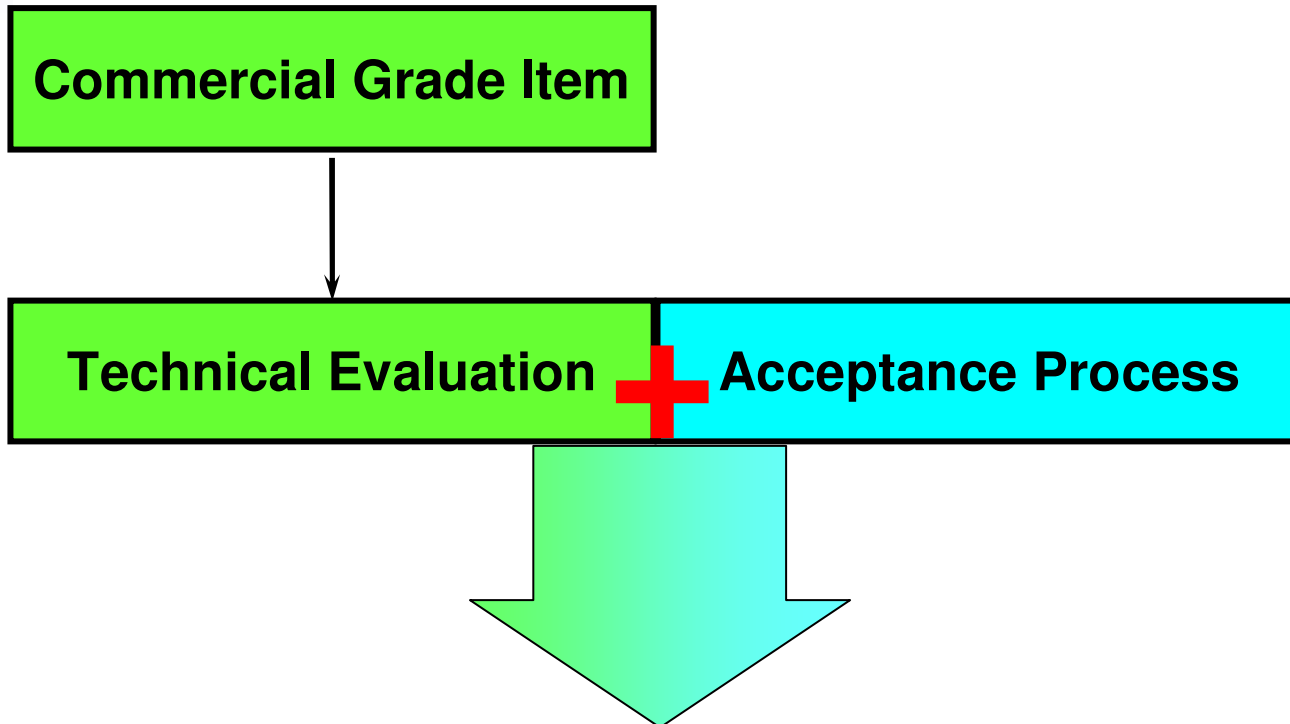


Process to ensure technical requirements for the item are *“specified”* correctly

(Design was already completed and qualified)

Process to produce objective evidence providing reasonable assurance the commercial grade item received is the item specified

Commercial Grade Dedication Fundamentals



Together, these two processes contribute to assuring the purchased item will *perform its safety-related function(s) as defined by the dedicating entity*

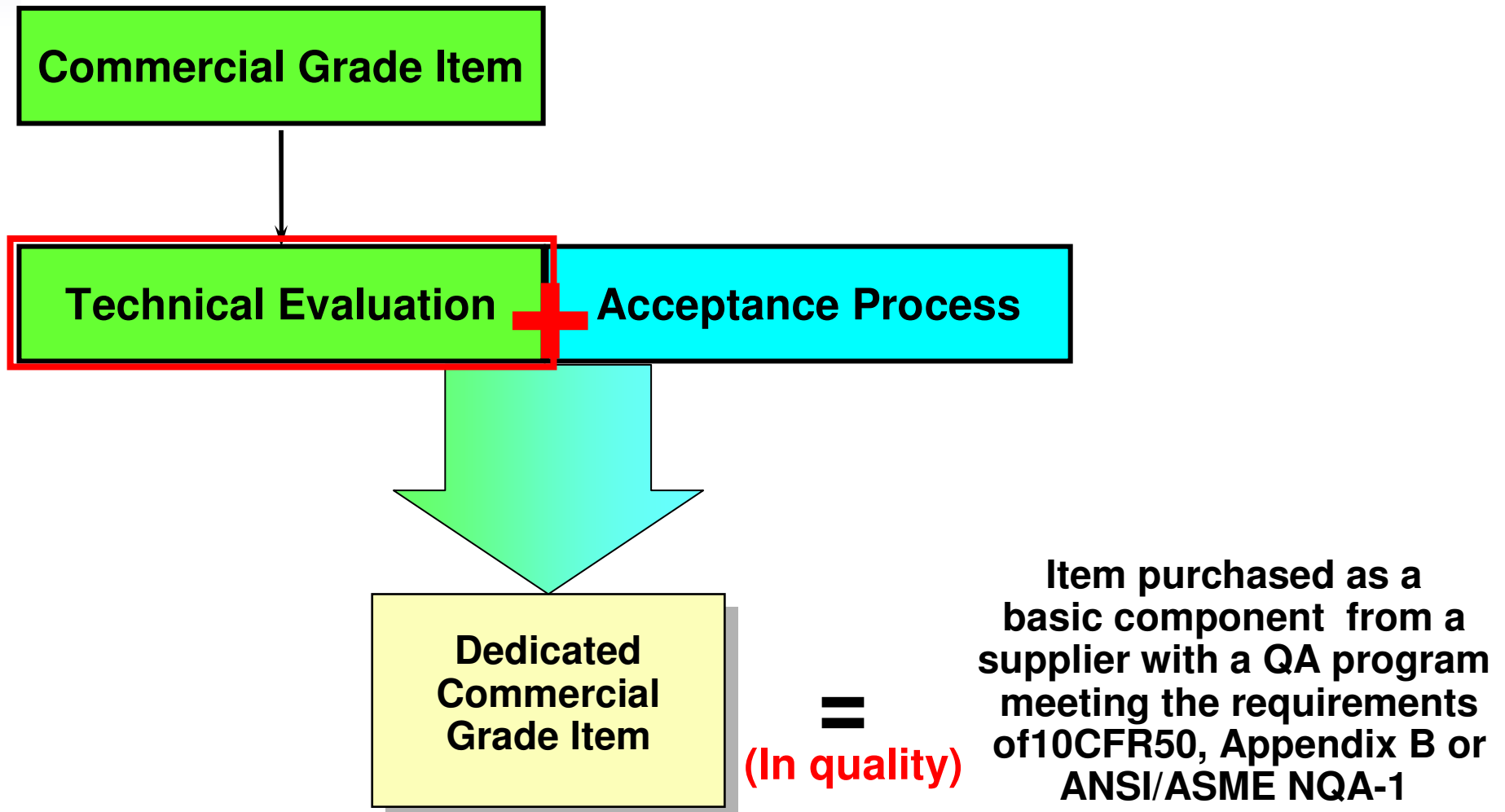
Technical Evaluation for Items

- Identify Application / End Uses
- Perform safety classifications
 - Identify Function(s)
 - Failure modes and effects analysis
- Identify Critical Characteristics
 - Physical (dimensions, materials, configuration, etc.)
 - Performance (resistance, closing time, input/output, etc.)
- Select Acceptance Methods and Criteria
 - Test & Inspect, Survey, Surveillance, Historical Performance

Pop Quiz!

- How many of you use software to design or analyze safety-related SSCs?
- How many of you have a formal process for accepting the computer code for use?
- How many of you employ “verification” and “validation” (V&V) in your acceptance process for computer code?
- What fundamental part of the commercial grade dedication process might need more attention in your process?

Commercial Grade Dedication Fundamentals



Technical Evaluation

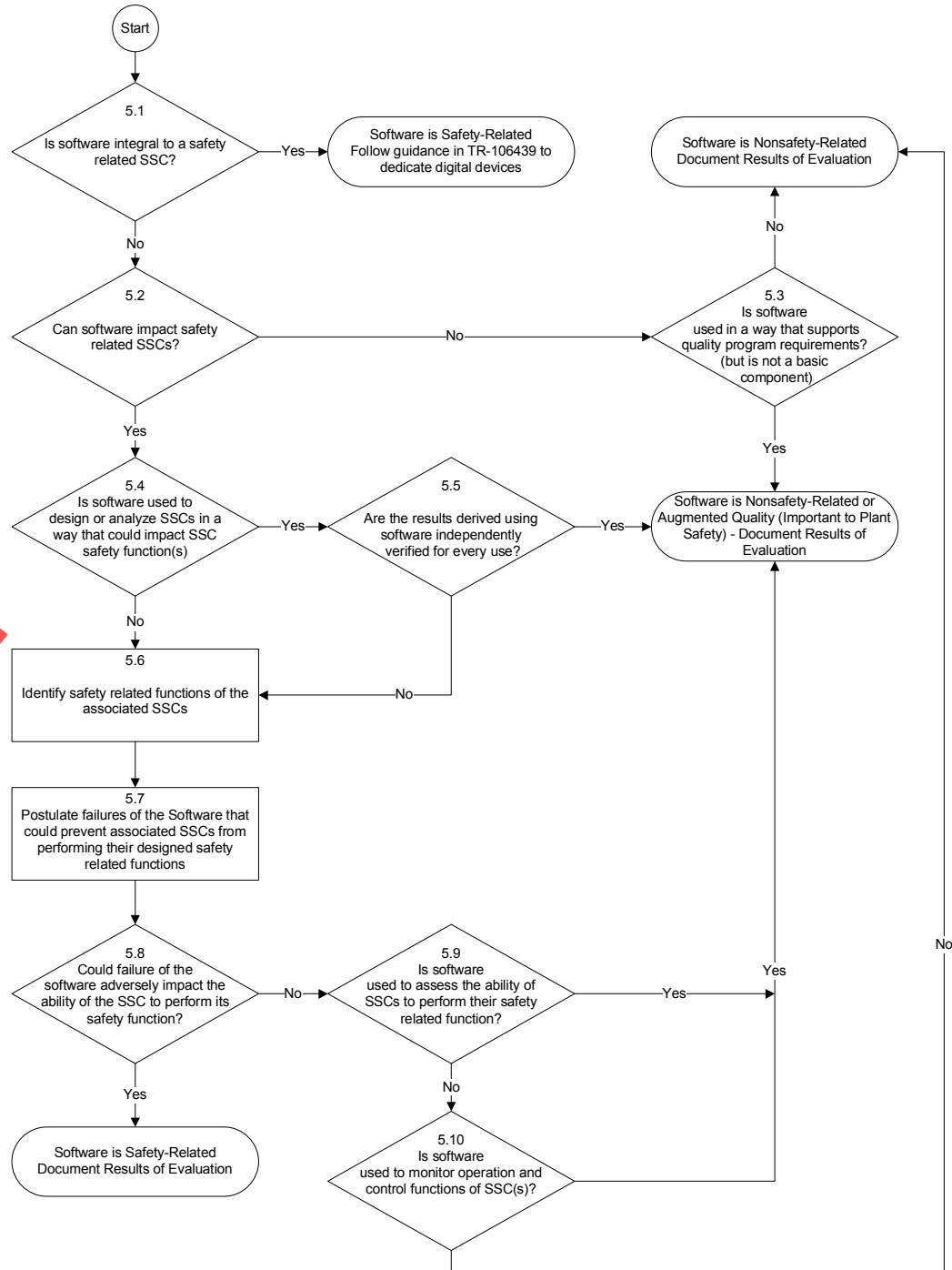
- Identify software being procured
 - What software am I acquiring?
- Identify end use application(s)
 - How will the software be used?
 - What types of calculations / modeling is being performed
 - Can it impact safety related SSCs?

Technical Evaluation

- Determine if the computer code performs a safety function
 - What happens if it fails? (Failure modes and effects)
 - Can failure impact the safety function(s) of the SSCs?
 - Can information obtained from the computer code result in failure of the SSC to perform its safety function(s)
 - Is it the sole basis for design/analysis decisions?
- Identify safety function(s) of the computer code
 - What does the computer code have to do to ensure associated SSCs will be capable of performing their safety related function(s)

Computer Code Safety Classification Process

DRAFT



Technical Evaluation

- Identify Critical Characteristics for Acceptance
 - Important characteristics of the software that once verified will provide reasonable assurance that the computer code will perform its intended safety function(s)
- Critical characteristics must be based upon the application(s) and safety function(s) documented in the technical evaluation
- Currently available references:
 - EPRI TR-107339
 - EPRI TR-106439 (www.epri.com)

Technical Evaluation

- Physical Characteristics (Examples)
 - Media type
- Performance Characteristics (Examples)
 - Consistency
 - Accuracy
 - Compatibility with operating environment
- Dependability Characteristics (Examples)
 - Built in Quality
 - Quality of Design

Technical Evaluation

- Identification
 - “Part” number
 - Version/build number

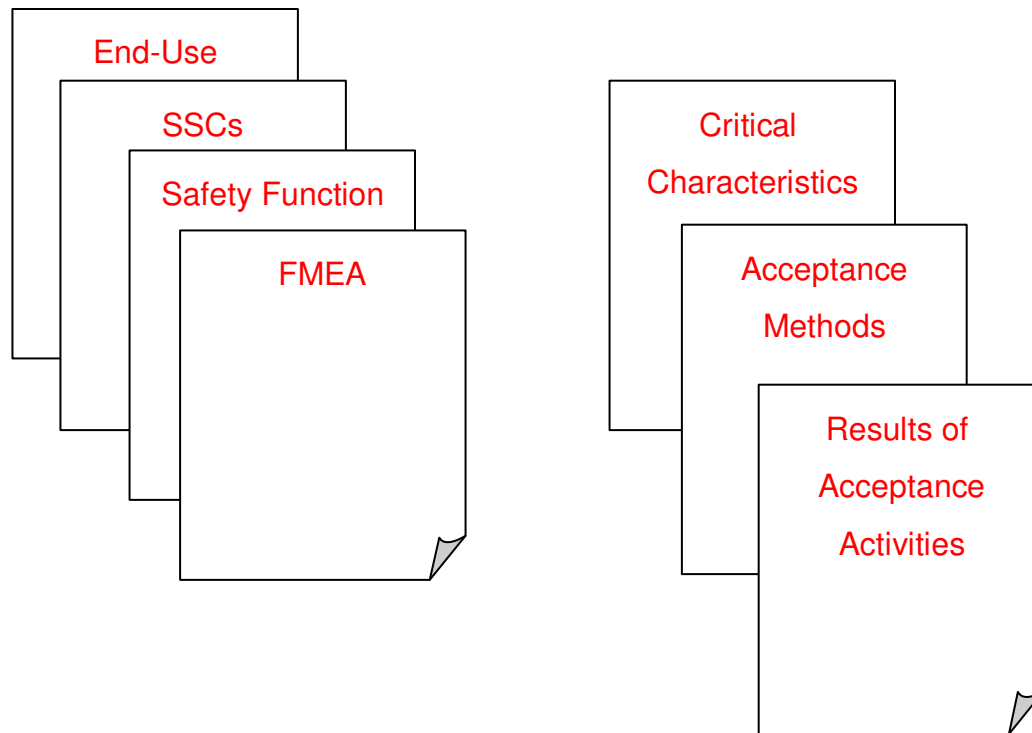
- Establish Boundaries
 - Acceptance must envelope scope of use
 - Applicable functions, environments, etc.

Technical Evaluation

- Select Acceptance Methods and Tolerances
 - Test and Inspection
 - Commercial Grade Survey
 - Source Surveillance
 - Historical Performance (restrictions in GL 89-02)
- Ensure acceptance bounds intended use
 - Acceptance must envelope scope of use
 - All applicable functions and range of input variables
 - Environments, etc.

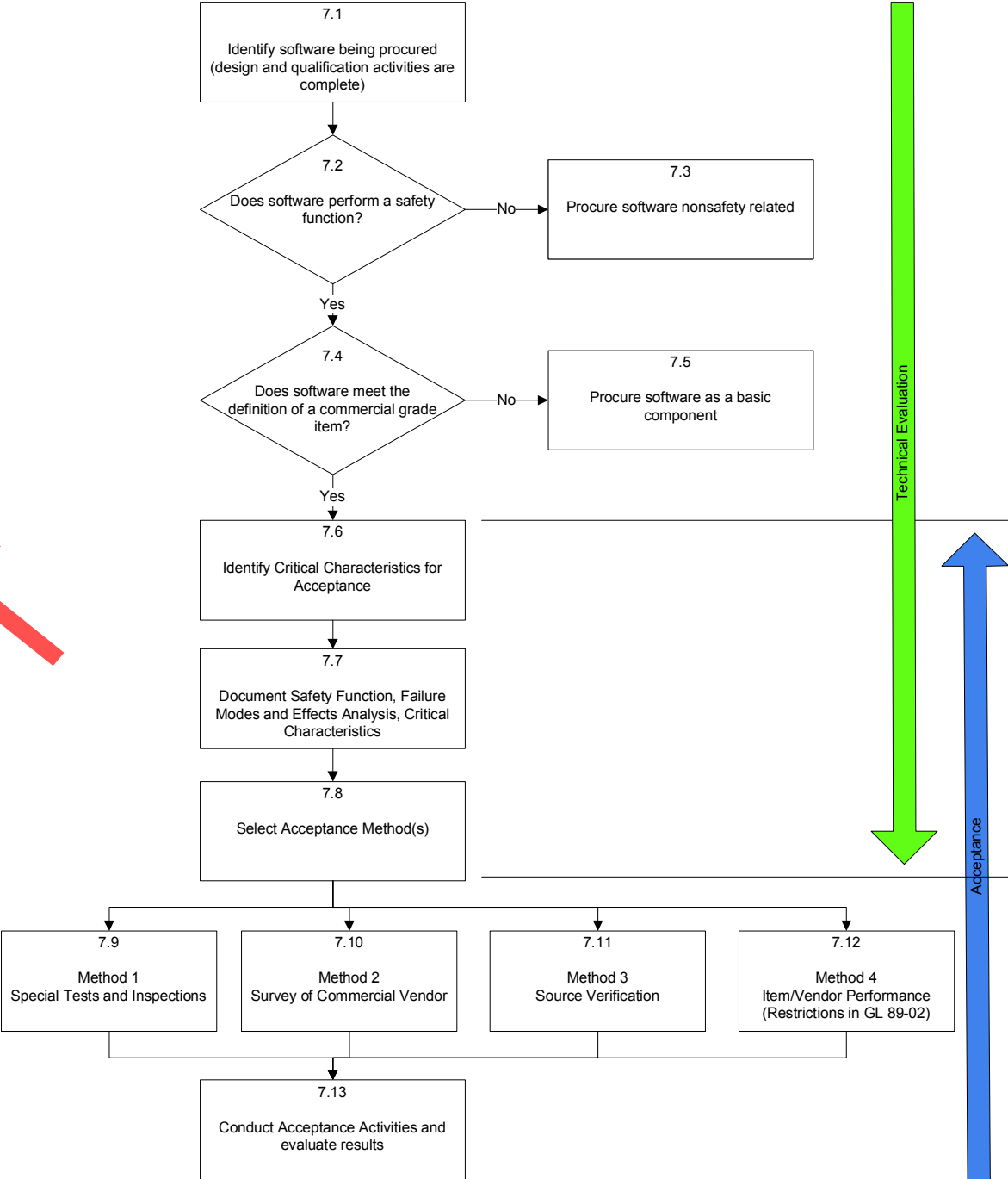
Technical Evaluation

- Document the technical evaluation



Computer Code Acceptance Process

DRAFT



Relationship of Design and Acceptance for Software

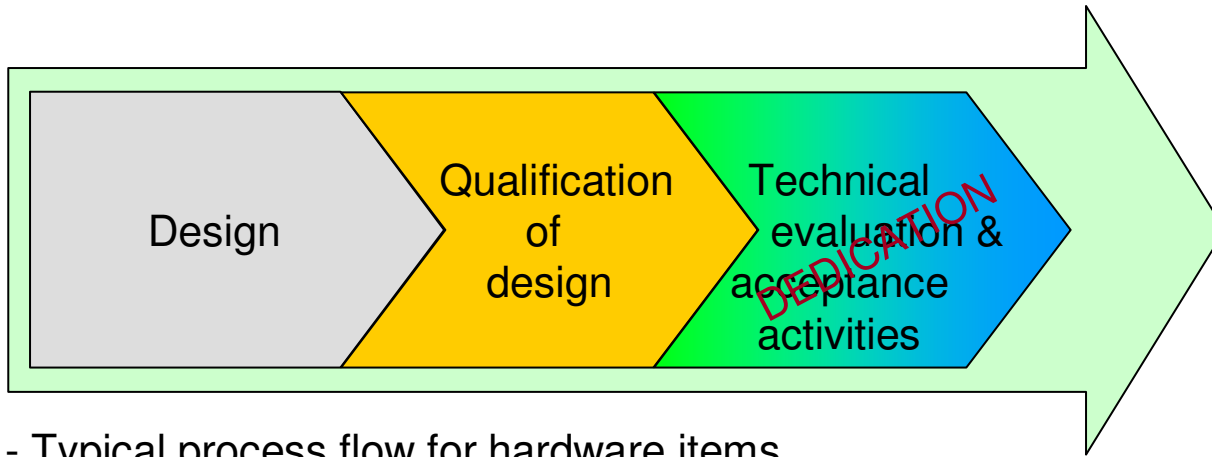


Figure 1 - Typical process flow for hardware items

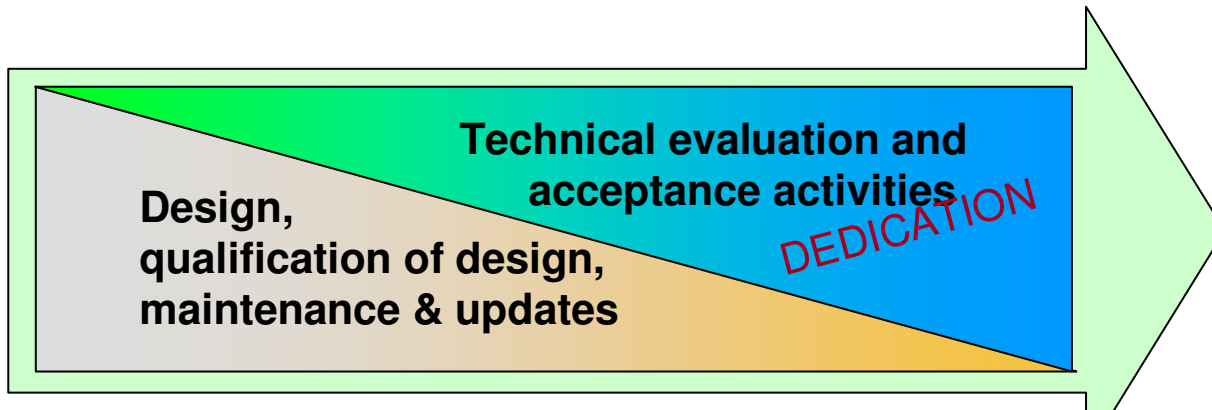


Figure 3 – Overlaying dedication techniques to accept software

Relationship of Design and Acceptance for Software

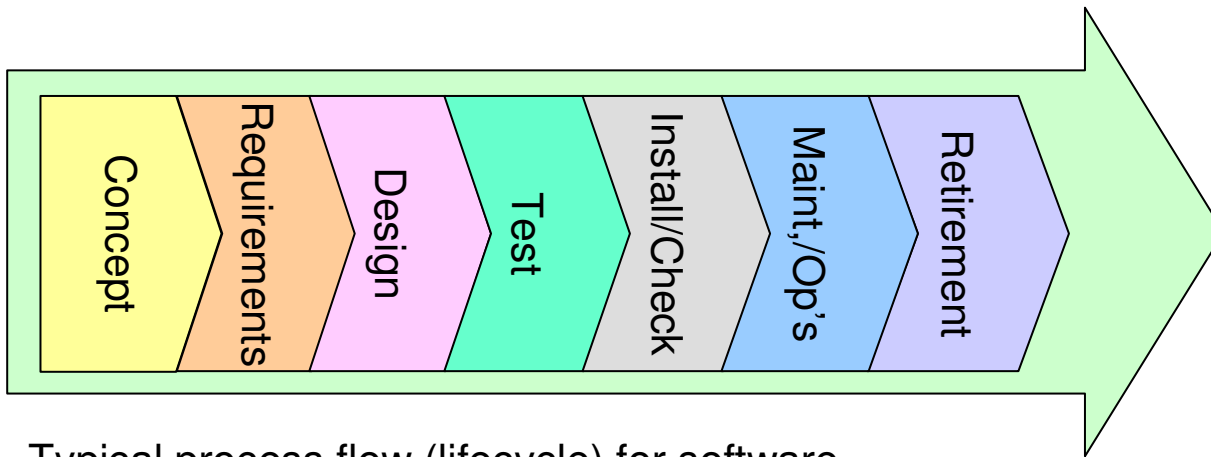


Figure 2 - Typical process flow (lifecycle) for software

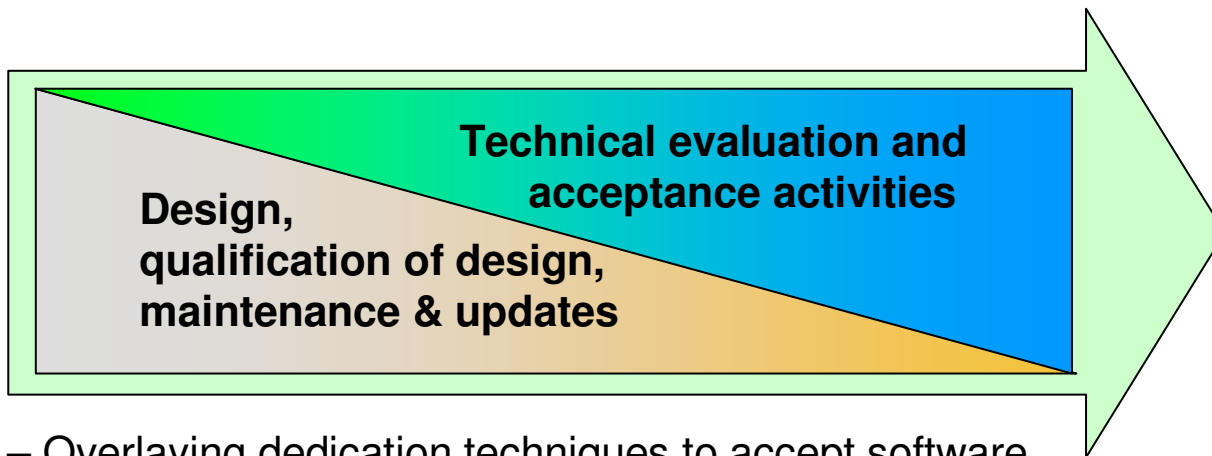
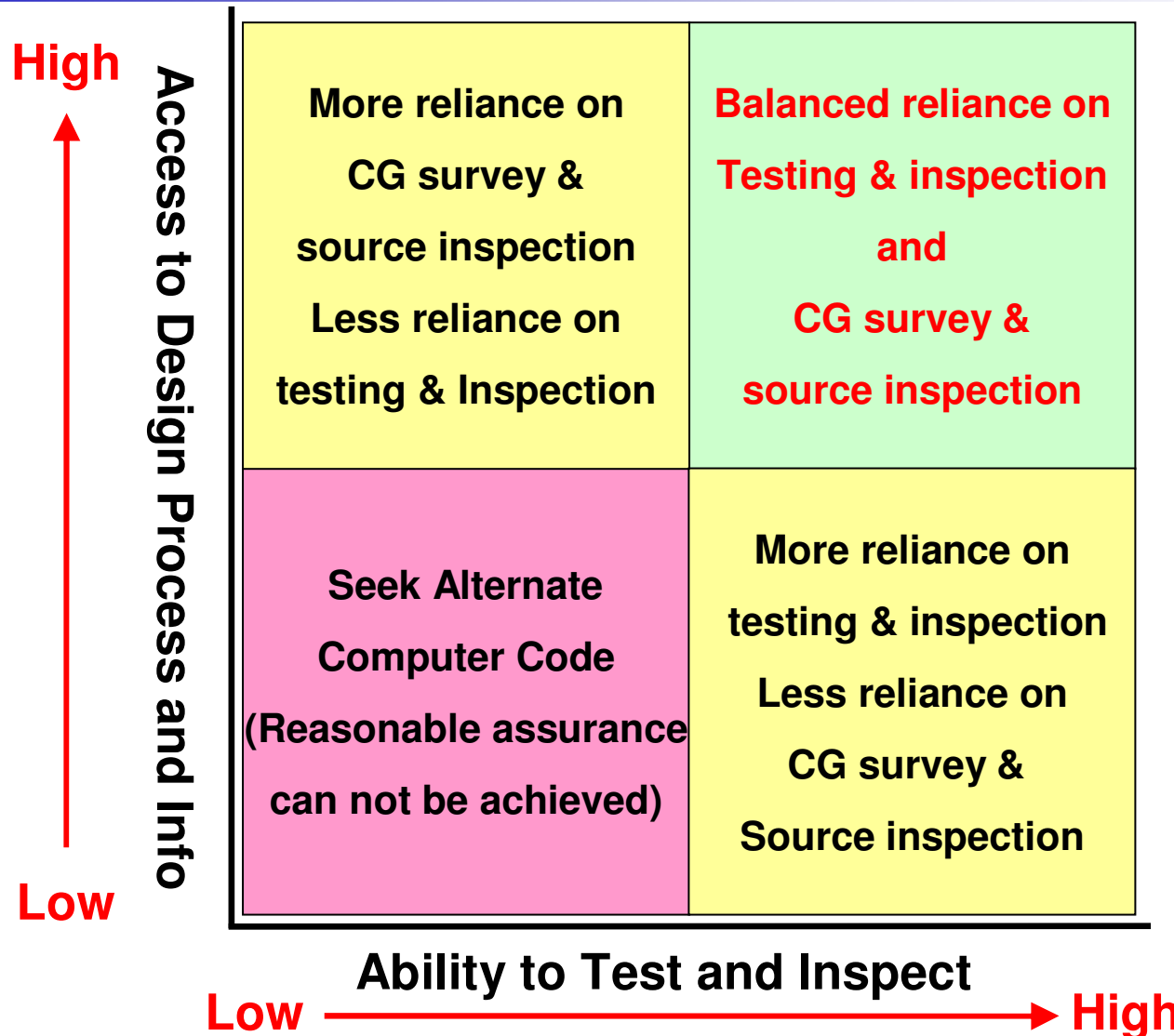


Figure 3 – Overlaying dedication techniques to accept software

Selection of Acceptance Methods



DRAFT



EPRI

**ELECTRIC POWER
RESEARCH INSTITUTE**

Questions?



Together...Shaping the Future of Electricity