Digital Instrumentation & Control Training

Module 3.0

Regulatory Concerns

TABLE OF CONTENTS

LIST OF FIGURES

3.0 REGULATORY CONCERNS

Module Introduction:

Welcome to Module 3.0 of the Digital and Microprocessor Control Systems Course! This is the third of five modules available in the Digital Instrumentation & Control Training Course. The purpose of this module is to assist the trainee in understanding the set of regulatory requirements and standards applicable to the acceptance of electronic and digital systems and components for use in nuclear power plant I&C systems. Subject to compliance with existing license commitments, compliance with current applicable regulations, and protection of the public health and safety, the NRC review may consider and use previous interpretations of the regulations as they apply to the application under review. The plant specific aspects of the design must be addressed to ensure that the generic qualification and licensing basis is enveloped in the plant specific design.

The review of any application should involve all of the applicable life-cycle activities. Reviews should confirm the acceptability of system requirements and the adequacy with which the final system meets these requirements. Review of non-digital computer-based system implementation may focus on component and system requirements, design output and validation. Review of computer-based systems should focus on confirming the acceptability and correct implementation of the life-cycle activities.

Section 7.0 of the Standard Review Plan discusses the review of the overall I&C system concept and generic system requirements. Appendices to Section 7.1 discuss the review procedures for each acceptance criterion relevant to I&C systems. Sections 7.2 through 7.9 describe the review of system-specific requirements, system design, and implementation. For computer-based systems or components with embedded computers, Appendix 7.0-A describes a generic process for reviewing the unique aspects of computer-based systems, including hardware/software integration.

The major sections of this module are as follows:

- Section 3.1 Regulatory Roadmap
- Section 3.2: NUREG 0800: Standard Review Plan
- Section 3.3: 10 CFR50.59 and EPRI TR-102348
- Section 3.4: BTP-14 Software V&V
- Section 3.5: BTP-19: Defense-In-Depth and Diversity
- Section 3.6: Regulatory Guidance
- Section 3.7: Tricon Training

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:

Show the relationship between Federal Regulations, Regulatory Guides, and industry standards related to I&C modifications for safety-systems.

Understand the roadmap and flow path through the Standard Review Plan (SRP) Chapter 7, Appendices and all associated Branch Technical Positions.

Understand the 10 CFR 50.59 regulation as applied to I&C modifications and illustrate 10 CFR 50.59 “thresholds” as defined in NEI 96-07. This includes additional guidance given in EPRI TR-102348 Rev. 1 and NRC RIS 2002-22.

Understand and be able to apply the basis for NRC acceptance of software for safety system functions through the guidance in BTP-14.

Understand and be able to apply the basis for NRC acceptance of diversity and defense-in-depth analyses and when they are required, utilizing the graded approach.

Understand the basic requirements in NRC Reg. Guides and associated industry standards referenced as sub-tier documents in SRP Chapter 7.

Understand an example hardware and software design of a PLC platform that has been generically approved by NRC staff in an SER.

3.1 Regulatory Roadmap

The purpose of this section is to show the relationship between Federal Regulations, Regulatory Guides and industry standards and other industry guidance as a basis for acceptance of new digital installations. This same process is followed by the licensee and all associated vendors and provides a stable and reliable basis for all to follow in implementing new digital upgrades and nuclear power plants.

There is a major difference between the types of requirements and your review of a new digital system against these requirements. Overall the levels of guidance are:

- Law:
  - o 10CFR50
- Guidance
  - o Regulatory Guides
  - o NUREGs
- Standards and Guidelines
  - o IEEE
  - o EPRI
  - o IEC, ISO

The law, as documented in 10 CFR 50 is non-negotiable and is a must-do. In all cases, the application of new digital upgrades MUST meet the requirements stated in the law.

Guidance is provided in NUREG 0800 and all associated Reg. Guides. It is important to understand and utilize the guidance in your review of digital systems. This is not the only guidance that can be used to implement a new digital upgrade, including the associated NRC review, but it is a set of guidance that has been followed in the past and found to be acceptable. This is important to provide a stable and proven path, instead of re-inventing the wheel in each new application.

Industry standards are endorsed in some cases and not in others. If an industry standard is endorsed, you should read and understand the Regulatory Guide associated with the standard ahead of time and note any exceptions or restrictions. This is true in some cases, because the industry standard referenced is not a nuclear standard and redefinition of terms, for example, is needed to link this standard to nuclear power plants.

Figure 3-1 provides an overview of the regulatory roadmap as applied to digital instrumentation and I&C upgrades at nuclear power plants. It shows the overall guidance documents and then the sub-tiers of Regulatory Guides and below that, the associated industry standard. This is a good roadmap to keep handy for review of the process and later, for specific reviews of digital upgrades that you are assigned.

3.2 NUREG-0800: Standard Review Plan

The purpose of this module section is to guide the student through the various sections of the Standard Review Plan, Chapter 7, which underwent significant revision in 1997, to incorporate lessons learned in the first number of digital upgrades implemented in the 1980's and 1990's,

The objectives for the student in this section are:

- To be able to find the applicable sections of the SRP for a given issue.
- To use the Branch Technical Position(s) applicable to a given upgrade in determining criteria for hardware and software development.

As an overview, the SRP is:

- Composed of Chapters 1-9
- Chapter 7 covers "Instrumentation and Control"
- Major rewrite of Chapter 7 issued in July 1997 (Now covers digital systems and software)

The purpose of the NRC is to provide a reference for NRC staff to conduct review of:

- New plant designs
- Topical reviews
- License amendment requests

It is used by utilities to understand the expectations of the NRC. It is not a design tool, but can be used to guide the design and to check/review the design.

Figure 3-2,

Figure 3-3 and Figure 3-4 provide an overview of the major sections in the SRP Chapter 7 from Section 7.0 through 7.6 and identifies the major areas addressed in each section.

There is a set of fundamental acceptance criteria applicable to the review process outlined in Chapter 7, as applies to digital I&C systems. The fundamental acceptance criteria are:

- 10 CFR 50.55a (ANSI/IEEE Std 279)
- 10 CFR 50.55a and R.G. 1.153 (IEEE Std 603)
- Appendix A 10 CFR 50
- Appendix B 10 CFR 50

The review process for digital equipment can be differentiated by the review process for other types of design upgrades by some digital specific issues, as follows:

- Minor errors in design and implementation can cause "unexpected behavior"
- Inspection and testing is not enough to "accomplish design qualification at high confidence levels"
- Code, data transmission, data, and hardware "...may be common to several functions to a greater degree than is typical in analog systems"
- System aspects such as real-time performance and on-line testing impact functional requirements

In Appendix 7.0-A of the SRP, the impact of digital I&C on the NRC review process is described as follows:

- "The Staff's approach to the review of design qualification for digital systems focuses…on a high-quality development process…" in addition to inspection and testing
- Review "emphasizes quality and defense-in-depth and diversity as protection against propagation of common-mode failures within and between functions"

In addition to the overall review process, there is a differentiation between systems receiving prior NRC staff generic review and also those more important, when reviewed using the graded approach. These key points, noted in Appendix 7.0-A, are as follows:

- For digital systems "…that the NRC staff has previously approved, the staff review scope would be significantly reduced and would focus only on plant-specific issues."
- "…the complexity and depth of the review can vary substantially depending upon the extent, complexity, and safety significance of the systems involved."

Next, a set of slides is presented to review changes in the initial set of sections in SRP Chapter 7 in the 2007 version, from the 1997 version.

There are several key Branch Technical Positions (BTPs) associated with Chapter 7 of the SRP, these include:

- **BTP HICB-14**:
  Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- **BTP HICB-18**:
  Guidance on Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- **BTP HICB-19**:
  Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems
- **BTP HICB-21**:
  Guidance on Digital Computer Real-Time Performance

The major BTPs and Regulatory Guides will be reviewed in this module along with any associated industry standards that apply.

As an example, Figure 3-5, Figure 3-6, Figure 3-7 and Figure 3-8 provide a visual representation of the various tiers of requirements associated with BTP-14, Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems. Sub-Section 3.1, 3.2 and 3.3 are addressed in more detail in the following slides to overview the levels of requirements and associated source or referenced documents that apply.

3.3 The 10 CFR 50.59 Rule and EPRI TR-102348/Nuclear Energy Institute NEI 01-01

The purpose of this section is to:

- Provide a brief review of the new 10 CFR 50.59 regulation
- Illustrate 50.59 "thresholds" defined in NEI 96-07, Rev. 1
- Summarize guidance given in Revision 1 to EPRI TR-102348 for 50.59 evaluations and NRC Regulatory Issue Summary RIS 2002-22
- Look at how the new 50.59 rule affects digital I&C upgrades

The objectives for the student are to:

- Become familiar with the new 50.59 rule and how it affects digital upgrade evaluations
- Identify key guidance provided in NEI 96-07, Rev. 1, for use of new rule
- Understand the type of guidance available in TR-102348 for performing 50.59 evaluations

The new 10 CFR 50.59 rule became effective at the end of 2000. The major changes are:

- New definitions (no more "USQ" Unresolved Safet Questions)
- Focus on Updated Final Safety Analysis Report UFSAR-described "design functions"
- New terminology ("likelihood" instead of "probability")
- Allows "minimal increase" in likelihood or consequences without prior NRC review

There is an excerpt in the course notebook that we can review along with this section of the module.

Figure 3-2 provides a visual representation of the changes that are evaluated as part of the 10 CFR 50.59 rule. There are modifications for which no evaluations are required as part of the rule. There are changes that require a 50.59 evaluation if they adversely affect UFSAR described design functions. Lastly, there are changes that require prior-NRC approval.

This revised 10 CFR 50.59 rule has 8 criteria (instead of the prior 7) to determine when prior NRC approval is required, as follows:

- More than a minimal increase in likelihood or consequences of an accident
- More than a minimal increase in likelihood or consequences of a malfunction
- New type of accident
- Malfunction with a different result
- Exceed limits for fission product barrier
- Departure from UFSAR-described method of evaluation

NEI 96-07, Revision 1, was issued by the industry to provide general guidance for implementation of the new 50.59 rule. It addresses both the screening process and the 50.59 evaluation process. It was endorsed by the NRC in Regulatory Guide 1.187 in November, 2000.

Figure 3-9 provides an overview of the thresholds defined in NEI 96-07, Rev. 1 – from the category of "trivial effect" to the one of "More than minimal adverse effect," which would require prior approval through a license amendment. EPRI TR-102348, Rev. 1 supplements NEI 96-07, Rev. 1, to define these thresholds as they apply to digital upgrades and gives some examples of small and large (simple and complex) digital modifications.

The impact of the old versus the new 50.59 can be characterized as follows:

- 50.59 Evaluation not necessary for all digital upgrades
- Change screens out if not "adverse"
- Safety-related upgrades can be done under 50.59 as long as adverse effects are "minimal"

As regards digital upgrades, there is a set of key issues that apply in the review of the upgrade to the set of 50.59 questions:

- What is adverse (screening)?
- How to address likelihood of malfunctions?
- How to address results of malfunctions?
- When to treat software common mode failure (is it minimal)?
- What about defense-in-depth and diversity analysis?

Guidance on how to answer the above, in the context of digital upgrades, is provided in EPRI TR-102348, which provides a regulatory framework for performing digital upgrades. It addresses the different methods for 50.59 evaluations and lessons learned in this process. It also discusses other digital issues with regulatory implications, such as diversity and defense-in-depth. Revision 0 of EPRI TR-102348 was issued in 1993 and endorsed by the NRC in Generic Letter 95-02. Revision 1 was issued in March 2002 and is endorsed by NRC RIS 2002-22.

Figure 3-10 provides an overview of the different elements in the implementation of a digital upgrade at a nuclear power plant and the major focus areas in each element or phase.

Next we need to discuss common-mode failure in the context of digital upgrades. The key issues related to this are:

- Single active failures considered in licensing basis
- Single failure criterion in IEEE Std 603, 279, 379
- Plant not designed to cope with common mode failures of hardware (HWCMF)
- Result of design/manufacturing flaws or degradation processes such as wear/corrosion
- Likelihood minimized by design control, qualification, maintenance, testing
- Software failures are a result of design flaw
- Apply similar controls to minimize likelihood

These key points help us answer the following question:

For qualified software-based systems, where is the likelihood of failure in the context of other failures?

Figure 3-11 provides an overview of these various levels of failure and how software CMF fits into this in the context of likelihood of failure. Also, it describes the processes and bases provided by the rigorous approach provided in these NRC and industry guidelines, to provide reasonable assurance of the low likelihood of failure.

Digital upgrade screening has the purpose of identifying adverse effects of implementing the new digital upgrade. Examples of adverse effects per NEI 96-07, Rev. 1 are:

- Decreasing the reliability of a design function
- Adding or deleting an automatic or manual design function
- Converting a feature that was automatic to manual or converting a manual feature to automatic
- Reducing redundancy, diversity, or defense-in-depth, OR
- Adversely affecting the response time required to perform required actions

Figure 3-12 addresses the comparison of the software common mode failure (SWCMF) with the hardware common mode failure (HWCMF).There is specific guidance that applies on the slide to screening out or screening in specific types of digital modifications.

In addressing the likelihood of malfunctions in terms of 10 CFR 50.59, the following major points need to be considered:

- Prior approval if more than a minimal increase in likelihood of occurrence of malfunctions
    - o Digital upgrades to obsolete equipment should result in more dependable systems
- Is likelihood of malfunction increased by software?
    - o Challenge is software reliability is not easily quantified

  - o But methods exist and are being used to assure that digital system design is high quality, high dependability
- Evaluation of quality attributes is needed to assess likelihood of malfunctions due to software

Figure 3-13 addresses the 50.59 evaluation process as it applies to SWCMF and the basis for determining that the increase in likelihood is minimal or not. It is based on the following:

- Determine if reasonable assurance exists that likelihood of software failure is significantly below that of single, active failures
- Qualitative evaluation
  - o Standards, regulations, processes, qualification
- If likelihood is low, then there is no more than a minimal increase
  - o Otherwise, prior NRC review would be required

NEI-96-07, Rev. 1 and EPRI TR-102348 both provide guidance on demonstrating dependability in the design and modification process as follows:

- Per NEI 96-07, Rev. 1: "Qualitative engineering judgment… is typically used to determine if there is more than a minimal increase in the likelihood of occurrence of a malfunction."
- Evaluate complexity, development process, failure management, operating history, and compliance with standards and other industry guidance

In evaluating the results of malfunctions in 50.59 space, prior approval is required if the change creates a possibility for a malfunction with a different result. We need to answer the question:

"Does digital upgrade cause malfunctions with different results?"

In answering this question, the following points should be considered:

- Possible malfunctions are limited to those that are as likely to occur as those described in the UFSAR
- Evaluate failure modes and effects to determine whether credible failures can create different results
- Assess effects of failures at a level consistent with UFSAR (generally at the system level)

NEI 96-07, Rev 1 provides the following guidance on evaluations of the result of the malfunction:

*"…the focus [is] on the **result** of the malfunction rather than the cause or **type** of malfunction."*

*"A new failure mechanism is not a malfunction with a different result if the result or effect is the same as, **or is bounded by**, that previously evaluated in the UFSAR."*

NEI 96-07, Rev. 1, provides the following example review to 10 CFR 50.59:

"If a feedwater control system is being upgraded from an analog to a digital system, new components may be added which could fail in ways other than the components in the original design."

"Provided the end result of the component or subsystem failure is the same as, or is bounded by, the results of malfunctions currently described in the UFSAR (i.e., failure to maximum demand, failure to minimum demand, failure as-is, etc.), then this upgrade would not create a 'malfunction with a different result.'"

Effects of common mode failures are evaluated further. Evaluations should consider the nature of the change and results of the failures, including digital upgrades, as noted in the following from NEI 96-07, Rev. 1:

> *"Thus, for instance, if failures were previously postulated on a train level because the trains were independent, a proposed activity that introduces a cross-tie or credible common mode failure (e.g., as a result of an analog to digital upgrade) should be evaluated further to see whether the likelihood of malfunction has been increased… [or] whether new outcomes have been introduced."*

Figure 3-14 provides an overview of the review of the results of malfunction in 50.59 against the results included in the UFSAR, and consideration of when the results are bounded by the current analysis or not bounded by the current analysis.

As a result of review to the analysis guidance in 50.59 reviewed up to now, prior NRC approval by license amendment may be required. In addition, other reasons for a licensee submitting a license amendment request include:

- Tech Spec changes
- Combining previously separate functions (in a way that creates malfunctions with different results)
- Reducing diversity (using one platform in multiple applications)
- Reducing performance (response time, accuracy, etc.)
- Introducing different failure behavior that affects design function
- Significant Human-System Interface (HSI) changes

Following the graded approach outlined in the SRP Chapter 7, the following guidance and lessons learned from earlier reviews, is provided to the licensees:

- For large-scale Reactor Protectin System (RPS) and Engineer Safety Features Actuation System (ESFAS) upgrades, go in for review
  - o NRC expects this, regardless of 50.59 issues
  - o Often there is a tech spec change anyway
- Whether license amendment or not, communicate with NRC early and often
  - o Experience has shown this pays off

The NRC staff completed a review of EPRI TR-102348, Rev. 1 and issued NRC RIS 2002-22 on November 25, 2002. It endorses the use of TR-102348 for designing and implementing digital replacements. It also endorses the use of TR-102348 for determining whether an upgrade can be done under 50.59 without prior NRC staff approval.

The attachment to RIS 2002-22 recognized the need for industry update of TR-102348 from Rev. 0 to reflect the following changes in the regulatory environment:

- NRC issued NUREG 0800 Chapter 7, June, 1997
- October 4, 1999, NRC published final rule on 50.59
- NEI 96-07, Rev. 1 issued November, 2000
- December 13, 2000, NRC announced the availability of Regulatory Guide 1.187, "Guidance for Implementation of 10CFR50.59, Changes, Tests, and Experiments."

The key points in RIS 2002-22 recognized the revisions to TR-102348 to do the following:

- Existing licensing process including 50.59 updated to reflect the new 50.59, NEI 96-07, Rev. 1 and Reg. Guide 1.187
- Issues associated with digital replacements should be addressed in the context of their potential impact on the system being modified
- Focuses attention on the system functions that are important and how these can be affected by potential failures of the digital equipment

In addition, as noted in RIS 2002-22, the following generic guidelines apply to the review process:

- For RPS and ESFAS, there is no consensus method for determining the likelihood of software malfunctions – therefore, expected these will all receive NRC staff review
- No currently acceptable way to quantitatively establish the reliability of digital systems
- Qualitative approaches are addressed in TR-102348 with regard to software issues, including software common-cause failure issues

In summary the combination of the new 50.59 process along with NEI 96-07, Rev. 1, EPRI TR-102348 and NRC RIS 2002-22 provide a proven roadmap for current and future implementation of digital upgrades at nuclear power plants. The future process is expected to look at and be based on:

- NRC inspection process likely to be looking hard at utility implementation of new 50.59 rule
- EPRI TR-102348, Revision 1, now reviewed and approved by NRC by RIS 2002-22
- 50.59 rule could change again
    - o become “risk-informed”

3.4 BTP-14 Software Verification and Validation

In addressing regulatory concerns, two BTPs rank higher than the others and will be addressed both in this module and in Module 5 with higher emphasis on industry documentation. These are BTP-14 and 19. This section addresses BTP-14 and the next section focuses on BTP-19.

The objectives of this section are to:

- Understand the basis for NRC acceptance of software for safety system functions
- Review BPT-14 and associated industry documents
- Understand scope of V&V reviews – as cradle to grave

As background, the NRC staff’s acceptance of software for safety system functions, as documented in BTP-14 is based upon:

- NRC staff’s acceptance of software for safety system functions, as documented in HICB-14, is based upon:
    - o Confirmation that acceptable plans were prepared by the licensee to control software development activities
    - o Evidence that the plans were followed in an acceptable software life cycle, and
    - o Evidence that the process produced acceptable design outputs

It is important to note that the structure of the review is documented in the SRP Chapter 7, Appendix 7.0-A.

The regulatory basis for BTP-14 is included in the following:

- 10CFR50.55a(h) requires conformance to IEEE Std 279 and/or IEEE Std 603
- 10CFR50, Appendix A, GDC 1, Quality Standards and Records
- 10CFR50, Appendix A, GDC 21, Protection System Reliability and Testing
- 10CFR50, Appendix B, Criterion III, Design Control

As a preliminary, a minimum number of definitions is necessary to discuss the overview of V&V, as follows:

- Activity Group – A collection of software life cycle activities, all of which are related to a specific life-cycle topic.
- Design Output – Documents such as drawings and specifications, that define technical requirements of structures, systems and components
- Documentation – Information recorded about a specific life cycle activity. Forty one activities are recognized by BPT-14. Documentation includes software life-cycle design outputs and software life-cycle process documentation

Figure 3-15 provides an overview of the lifecycle processes that need to be applied for V&V – to each phase in the software lifecycle. The planning characteristics addressed in BTP-14 include the following key points, as well as roles and responsibilities:

- Management – How is the project managed
- Purpose – Why is this being done
- Organization – What structure is used
- Oversight – Methods and application
- Responsibilities – Self evident
- Risks – Methods used to identify, assess and manage
- Security – Methods used to protect information

BTP-14 addresses the main functional characteristics of safety system software and describes the characteristics in detail:

- Accuracy
- Functionality
- Reliability
- Robustness
- Safety
- Security
- Timing

At the same time that functional characteristics are described, we also need to describe good qualities of the software development process that the organization needs to strive for:

- Completeness
- Consistency
- Correctness
- Style
- Traceability
- Un-ambiguity
- Verifiability

Each of these is addressed in BTP-14, as regards software development.

Figure 3-16 provides an overview of the phases of software development and the specific tasks performed in support of each phase, as documented in IEEE Std 1012, which will be covered in Module 5:

- Hazard review
- Risk analysis
- Traceability analysis
- Management review

Figure 3-17 provides an overview of the specific tasks accomplished as part of each phase of software development and how they are related to each other in the "design output" documentation between the specification and implementation in the plant.

Figure 3-18 addresses the key component of system design control that apply to each phase of the software development process from system concept to operation and maintenance support. This is integrated with the hardware specifications which are developed alongside and in close coordination with the software development documentation.

There are a series of standard software life cycle process design outputs that are traceable and auditable to the processes outlined in BTP14:

- Software Requirements Spec. (SRS)
- Hardware and software architecture descriptions (SAD)
- Software design specifications (SDS)
- Code listings
- Build documents
- Installation configuration tables
- Operations manuals
- Maintenance manuals
- Training manuals

In Module 5, we will discuss the software V&V plan development. As a preliminary, the following key points are addressed:

- Issued document – conforming to IEEE Std 1012 and Reg. Guide 1.168
- Includes all characteristics included earlier – Purpose, Organization, etc.
- Description of all required testing, specification, procedures and cases
- Includes traceability matrix – very important!

The traceability matrix is one of the most used and valuable tools in auditing the performance of software verification and validation. The main points to cover related to the traceability matrix are:

- Allow ease of tracing between requirements in SRS, SDD, V&V Plan – and testing and verification activities
- Should allow traceability in both directions
- Living document through design, implementation and validation
- Updated as part of each phase

Finally, a review of the changes incorporated in the 2007 update of BTP 14 is included.

In summary, BTP-14 provides the overall guidance on the process of software verification and validation from initial concept to final implementation. Later sections of the training address more detail on the key points covered in this section.

3.5 BTP-19: Defense-In-Depth and Diversity

The objectives of this section are as follows:

- Understand NRC background and approach to defense-in-depth and diversity analysis

- Review D3 strategies and experience from non-nuclear and international sources
- Identify relevant regulatory documents – NRC developed
- Understand scope of defense-in-depth and diversity (D-cubed) analysis and when it is required
- Understand Graded Approach and NRC review requirements
- Review 2006/2007 TWG update for D3

As background, Figure 3-20is included to show the D3 policy and guidance provided by NRC over the past 20 years. Also, the overall diversity strategy with 4 echelons of defense is shown in Figure 3-21. An international view of the echelons of defense is included in Figure 3-22.

The following provides background on the NRC staff's approach to this area:

- Diversity and defense-in-depth (D3) policy established in 1990's
- Experience to date indicates the need for more specific guidance for assuring adequate diversity and defense-in-depth
- Research on diversity strategies started in late FY 06

The research approach is outlined in Figure 3-23 which shows the importance of the international and domestic safety critical industrial experience and the results of the diversity strategy refinement figure.

The main issue that all discussion on D3 revolves around is:

- Adding diverse systems and/or defense-in-depth features can mitigate the effects of a common cause failure (CCF)
- How much diversity and defense-in-depth are enough? For example
- Are there precedents for good engineering practice?
- Can sets of attributes provide adequate diversity?
- Are there standards that can be endorsed?

The research approach is next outlined, with relation to the D3 Technical Working Group and such documents as NUREG 6303.

Figure 3-24 provides examples of Diversity categories from the European view.

As a result of the NRC Research activities, a set of diversity attributes and criteria were developed, as shown in Figure 3-25. A summary of the application of these diversity attributes in safety critical industries and recent nuclear plant applications is shown in Figure 3-26 and Figure 3-27.

A summary of the results of this attribute research is as follows:

- Avoidance
    - –Produce high-quality (error-free) systems
    - –Minimize common elements
    - –Limit fault propagation
- Mitigation
    - Add defense-in-depth to compensate for failures in other systems
    - Provide diverse systems that will not fail at the same time

Next, a review of the diversity attribute comparison for a number of safety critical system deployments are shown – including the space shuttle, international space station, mission control at Johnson Space Center, the Airbus 320 avionics and the electrical grid.

Finally a summary of the approaches by each safety critical industry is provided to compare and contrast.

Finally, Figure 3-27 illustrates the NRC D3 Research activities.schedule.

3.6 Regulatory Guidance

To begin to review the specifics in BTP-19, the purpose is to provide the following guidance:

To confirm that vulnerabilities to common-cause failures (CCF) have been addressed in accordance with the guidance of SRM on SECY 93-087, specifically:

- To verify that adequate diversity has been provided in a design to meet the criteria established by NRC requirements
- To verify that adequate defense-in-depth has been provided in a design to meet NRC requirements
- To verify that the displays and manual controls for critical safety functions are diverse

The relevant guidance referenced by BTP-19 includes:

- Reg. Guide 1.53 endorses IEEE Std. 379-2000.
- IEEE Std. 379-2000, clause 5.5, identified D3 as a technique for addressing common-cause failure and clause 6.1 identifies logic failures as a type of failure to be considered when applying the single-failure criterion.
- NUREG/CR-6303
- SRM on SECY 93-087

To overview the concept of defense-in-depth and diversity (commonly called D-cubed analysis) the important element is common mode failure, which has the following key points in licensing space:

- NRC position is that software cannot be proven to be error free (e.g., by testing)
- High quality design reduces likelihood of common mode failures
- Still, for RTS and ESFAS functions, need to demonstrate defense against unlikely common mode failure

There are four echelons for defense against common mode failure as noted in BTP-19:

- Control system
- RTS
- ESFAS
- Monitoring and indicators

Each of these is addressed in BTP-19 on the nature of the defense in the order provided.

There are three main points in the NRC position on D-cubed for operating reactors, as noted in BTP-19:

- Licensee should assess defense-in-depth and diversity of the proposed system to demonstrate that vulnerabilities have been addressed
- Demonstrate that each postulated common-mode failure was analyzed for each event in the FSAR
- If a postulated common-mode could disable the safety function, then a diverse means is required to accomplish the same function or a different function

One of the main elements in the upgrade to the SRP Chapter 7 in 1997 addressed the implementation of the graded approach, as related to BTP-19 in the following:

- D-in-D and D analysis required **only** for RTS and ESFAS
  - Primary plant protection systems
  - Key to multi-echelon defense in depth
- Formal analysis not required for other safety-related systems, but:
  - Minimize possibility of common mode failure!
  - Be prepared to discuss what would happen

Next, the upgrade of BTP-19 in 2007 is reviewed as follows:

- Purpose: "This BTP has the objective of confirming that vulnerabilities to common-cause failures have been addressed – following SECY-93-087"
- D3 analysis focus on protection systems, other systems involved as diverse functions
- Definition of "block"
- Postulated Common Cause Failures
- Reference Westinghouse ASIC-Based SER by NRC, Feb. 8, 2001.

Additional guidance on system representation as "blocks" includes:

- "A block is a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment or software."
- Examples: computers, local area networks, and programmable logic controllers

Based on the implementation of a graded approach in both designing and licensing a digital upgrade, the determination of what is ESFAS and included in the ESFAS functions, is critical to determining the required D-cubed analysis. The key points related to this determination are (for the design engineer and NRC reviewer):

- Important to distinguish between primary actuation systems (ESFAS) and other safety-related systems
  - Limit the number of formal analyses required
- Unfortunately, not well-defined
- Check SAR for what it named as part of ESFAS

The requirements for an RTS/ESFAS digital upgrade include the following steps that can be reviewed following BTP-19:

- Perform D-in-D and D analysis to show software common mode failure is addressed (NUREG/CR-6303)
- Analyze effect of failures on mitigation of Chapter 15 accidents using "best-estimate" methods

Details of this analysis of Chapter 15 accidents are provided in Module 5.

The review procedures following BTP-19 should include the following points that should be emphasized in the review:

- System representation as blocks
- Documentation of assumptions
- Identification of alternative trip or initiation sequences
- Identification of alternative mitigation capability

- Justification for not correcting specific vulnerabilities

Additional D3 guidance is provided in industry generated documentation that addresses the integrated CCF strategy as follows:

- Consider all relevant factors, e.g.,
  - Realistic assessment of susceptibility - likely sources of CCF
  - Evaluation of factors that preclude or limit CCF
  - Design features
  - Processes
  - Diversity attributes
  - I&C importance in system and plant context
  - Where will diverse backups improve safety/reliability?
  - Which events are most important?
  - Net safety/reliability gain or loss with proposed solution
- CCF protection comes from combination of design, process and diversity attributes
- Goal is "reasonable assurance" of adequate protection against unsafe CCFs

Figure 3-28 provides an overview of the necessary ingredients of an analysis of digital failures and digital CCFs.

Defensive measures help protect against single channel failures and CCFs including:

- May restrict digital failures to manageable sets of mechanisms
- May preclude, avoid, detect or limit types of failures
- Defensive measures that help protect against CCF:
  - Data validation
  - Procedures that allow changes to only one channel at a time
  - Operating system "blind" to plant transients
  - Time-based cyclic behavior
  - No process-related interrupts
  - Nearly 100% testable
  - Modularity
  - Static allocation of resources

Next, the 2006/2007 D3 TWG progress is reviewed in big picture, and by specifically reading the actual ISG's issued by the date that this class is given.

In summary, the following key points are important:

- D-cubed analysis implemented on a graded approach
- Major effort now to develop lessons learned in the first staff and Region reviews and approvals
- Industry guidelines being developed – covered in Module 5

The background, program elements, scope, schedule and major focus areas will all be addressed in class, as part of this review, following the slides.

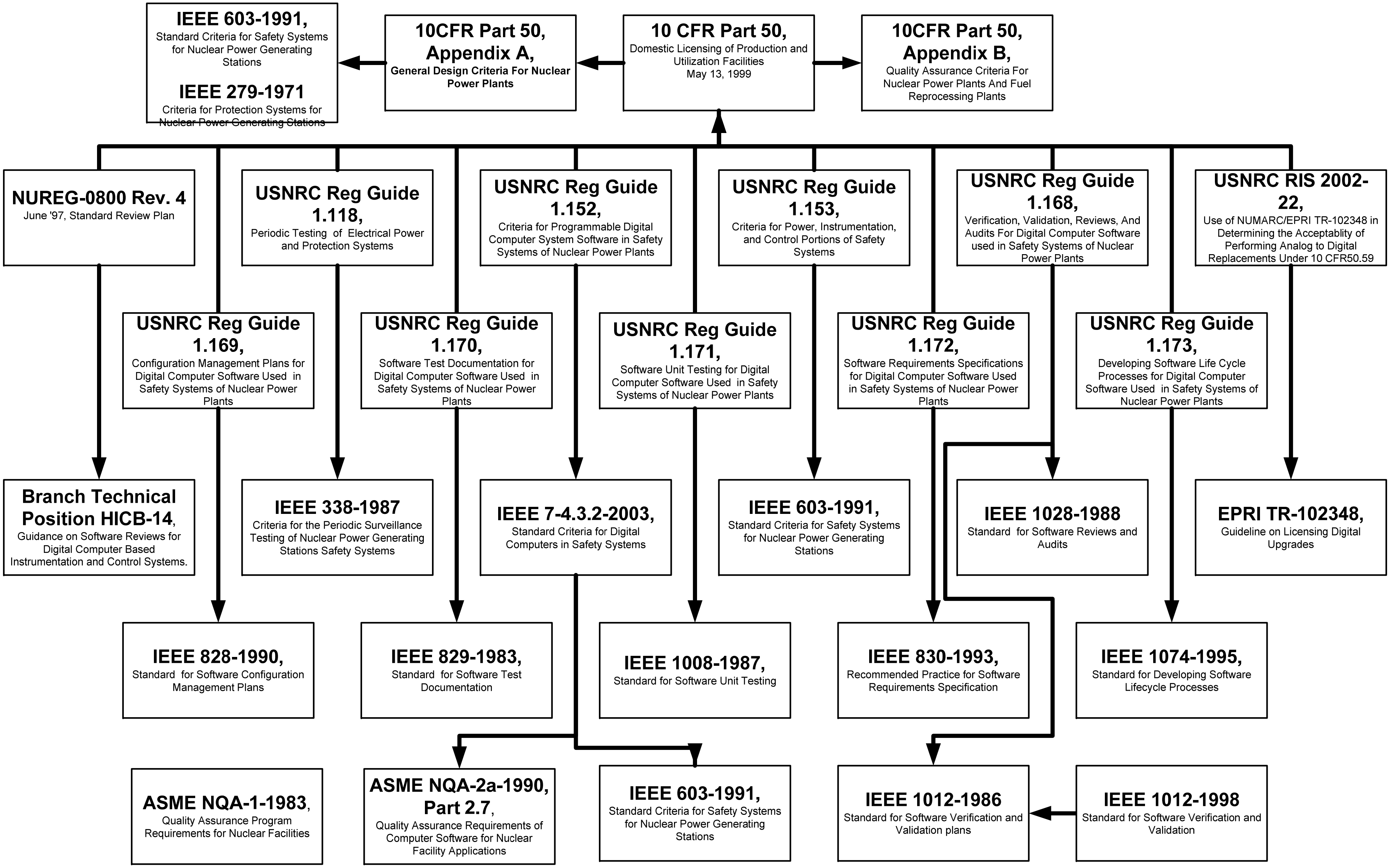

IEEE 603-1991,
Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 279-1971
Criteria for Protection Systems for Nuclear Power Generating Stations
10CFR Part 50, Appendix A,
General Design Criteria For Nuclear Power Plants
10 CFR Part 50,
Domestic Licensing of Production and Utilization Facilities
May 13, 1999
10CFR Part 50, Appendix B,
Quality Assurance Criteria For Nuclear Power Plants And Fuel Reprocessing Plants
NUREG-0800 Rev. 4
June '97, Standard Review Plan
USNRC Reg Guide 1.118,
Periodic Testing of Electrical Power and Protection Systems
USNRC Reg Guide 1.152,
Criteria for Programmable Digital Computer System Software in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.153,
Criteria for Power, Instrumentation, and Control Portions of Safety Systems
USNRC Reg Guide 1.168,
Verification, Validation, Reviews, And Audits For Digital Computer Software used in Safety Systems of Nuclear Power Plants
USNRC RIS 2002-22,
Use of NUMARC/EPRI TR-102348 in Determining the Acceptablity of Performing Analog to Digital Replacements Under 10 CFR50.59
USNRC Reg Guide 1.169,
Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.170,
Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.171,
Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.172,
Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.173,
Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
Branch Technical Position HICB-14,
Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems.
IEEE 338-1987
Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Stations Safety Systems
IEEE 7-4.3.2-2003,
Standard Criteria for Digital Computers in Safety Systems
IEEE 603-1991,
Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 1028-1988
Standard for Software Reviews and Audits
EPRI TR-102348,
Guideline on Licensing Digital Upgrades
IEEE 828-1990,
Standard for Software Configuration Management Plans
IEEE 829-1983,
Standard for Software Test Documentation
IEEE 1008-1987,
Standard for Software Unit Testing
IEEE 830-1993,
Recommended Practice for Software Requirements Specification
IEEE 1074-1995,
Standard for Developing Software Lifecycle Processes
ASME NQA-1-1983,
Quality Assurance Program Requirements for Nuclear Facilities
ASME NQA-2a-1990, Part 2.7,
Quality Assurance Requirements of Computer Software for Nuclear Facility Applications
IEEE 603-1991,
Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 1012-1986
Standard for Software Verification and Validation plans
IEEE 1012-1998
Standard for Software Verification and Validation

Figure 3-1 Regulatory Roadmap – Digital I&C

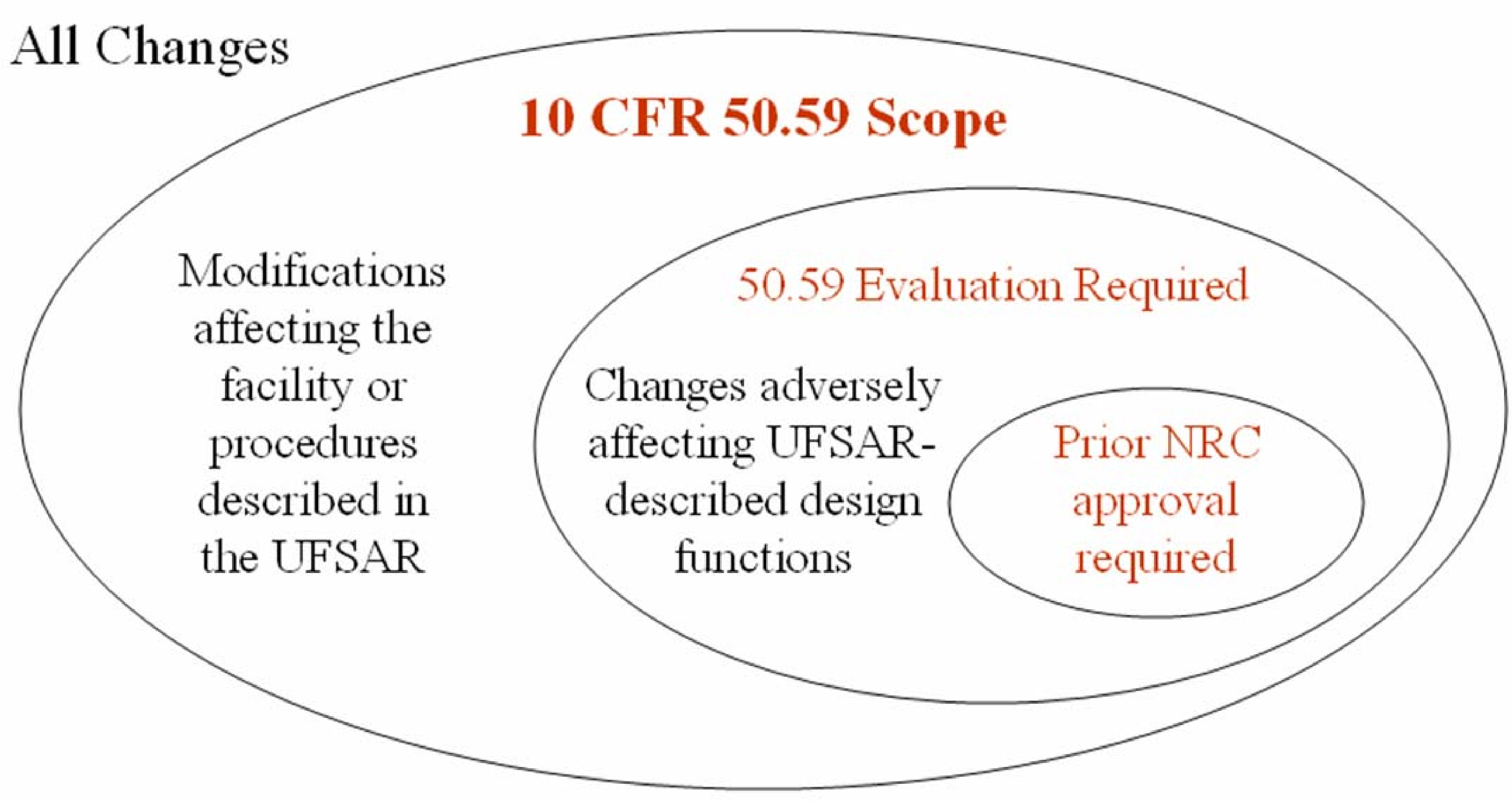
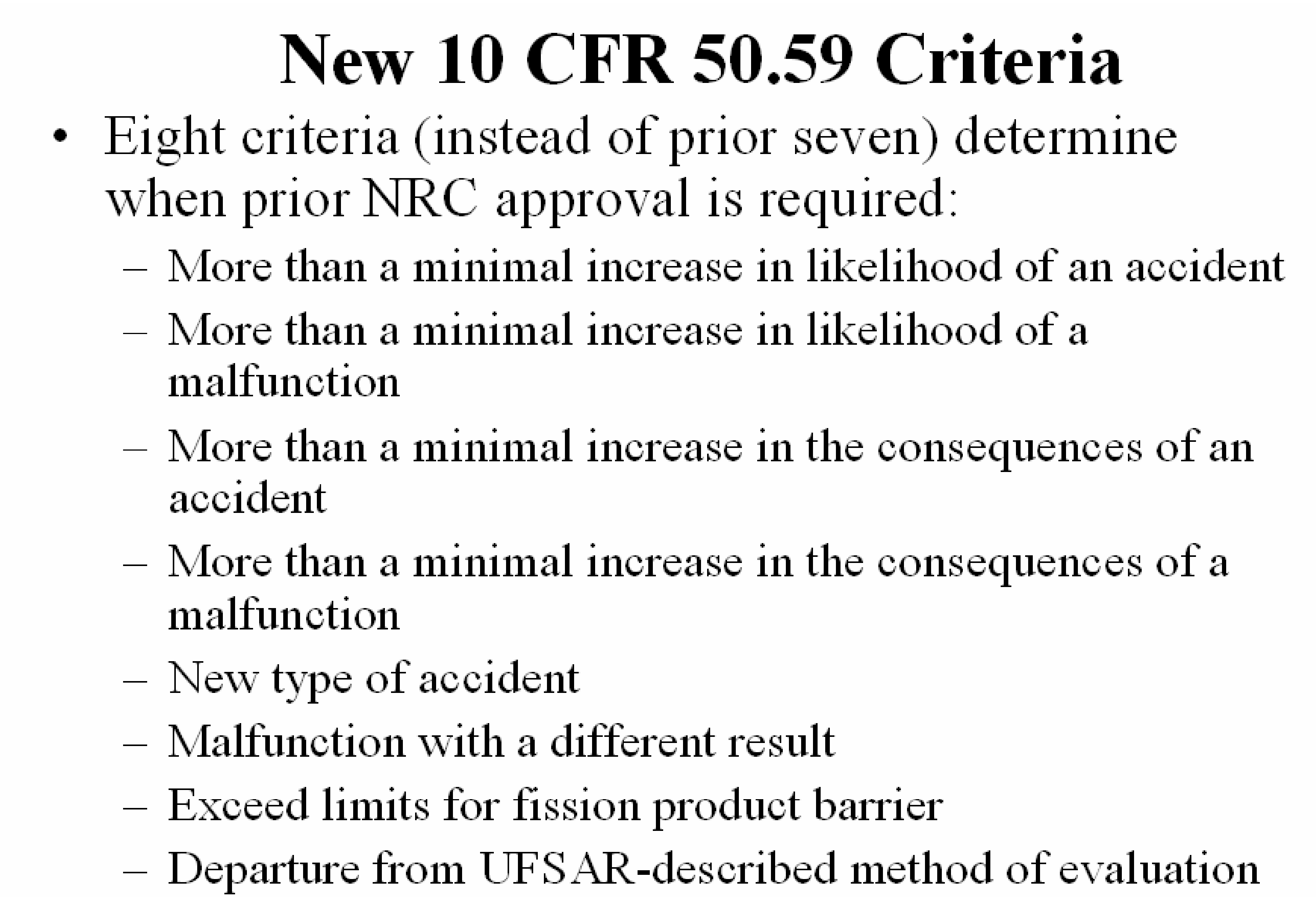

All Changes
10 CFR 50.59 Scope
Modifications affecting the facility or procedures described in the UFSAR
50.59 Evaluation Required
Changes adversely affecting UFSAR-described design functions
Prior NRC approval required

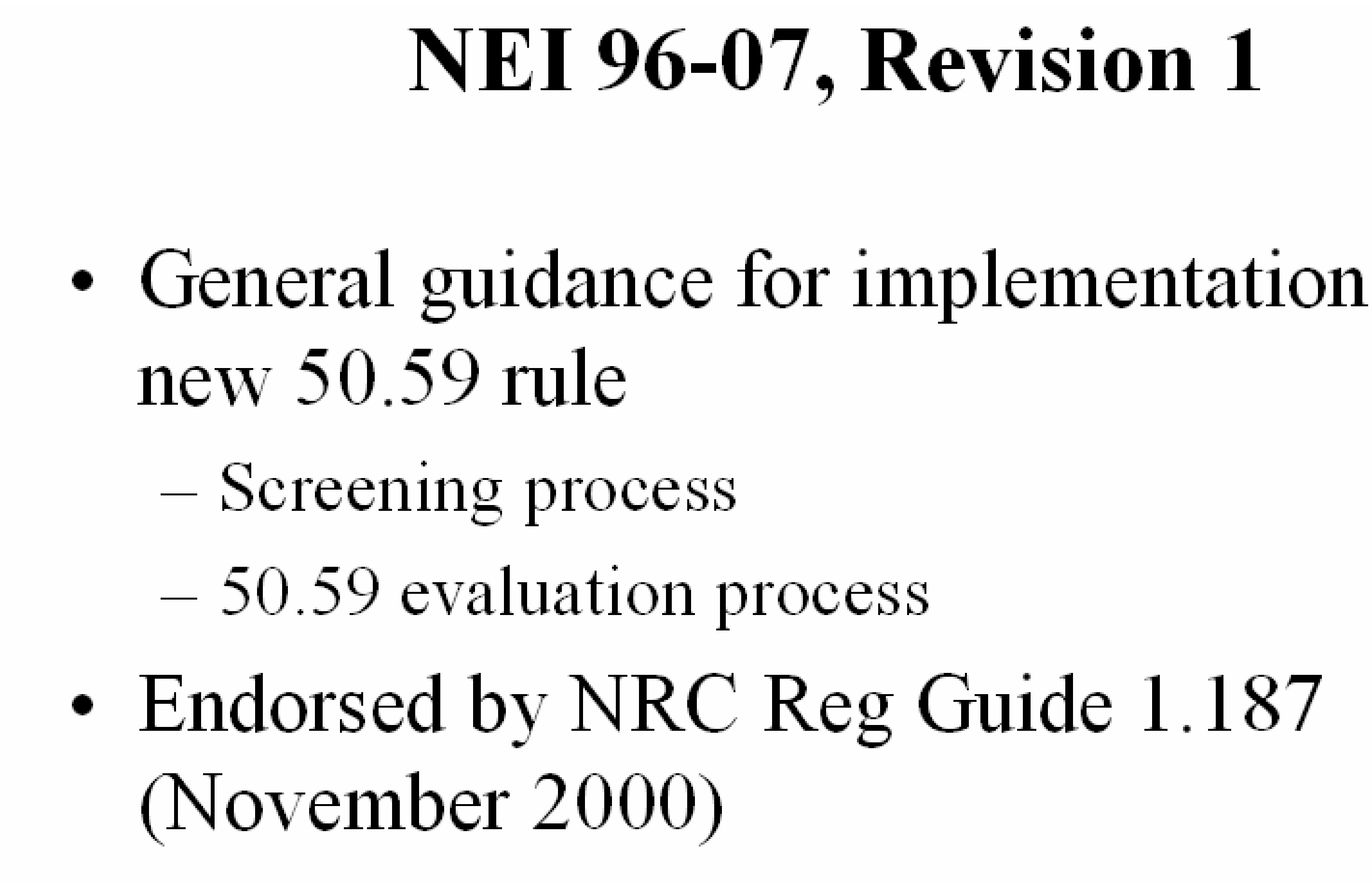
Figure 3-2 **Changes Under 10 CFR 50.59**



New 10 CFR 50.59 Criteria

- Eight criteria (instead of prior seven) determine when prior NRC approval is required:
  - More than a minimal increase in likelihood of an accident
  - More than a minimal increase in likelihood of a malfunction
  - More than a minimal increase in the consequences of an accident
  - More than a minimal increase in the consequences of a malfunction
  - New type of accident
  - Malfunction with a different result
  - Exceed limits for fission product barrier
  - Departure from UFSAR-described method of evaluation

Figure 3-3 New 10 CFR 50.59 Criteria



NEI 96-07, Revision 1

- General guidance for implementation of new 50.59 rule
  - Screening process
  - 50.59 evaluation process
- Endorsed by NRC Reg Guide 1.187 (November 2000)

Figure 3-4 NEI 96-07, Revision 1

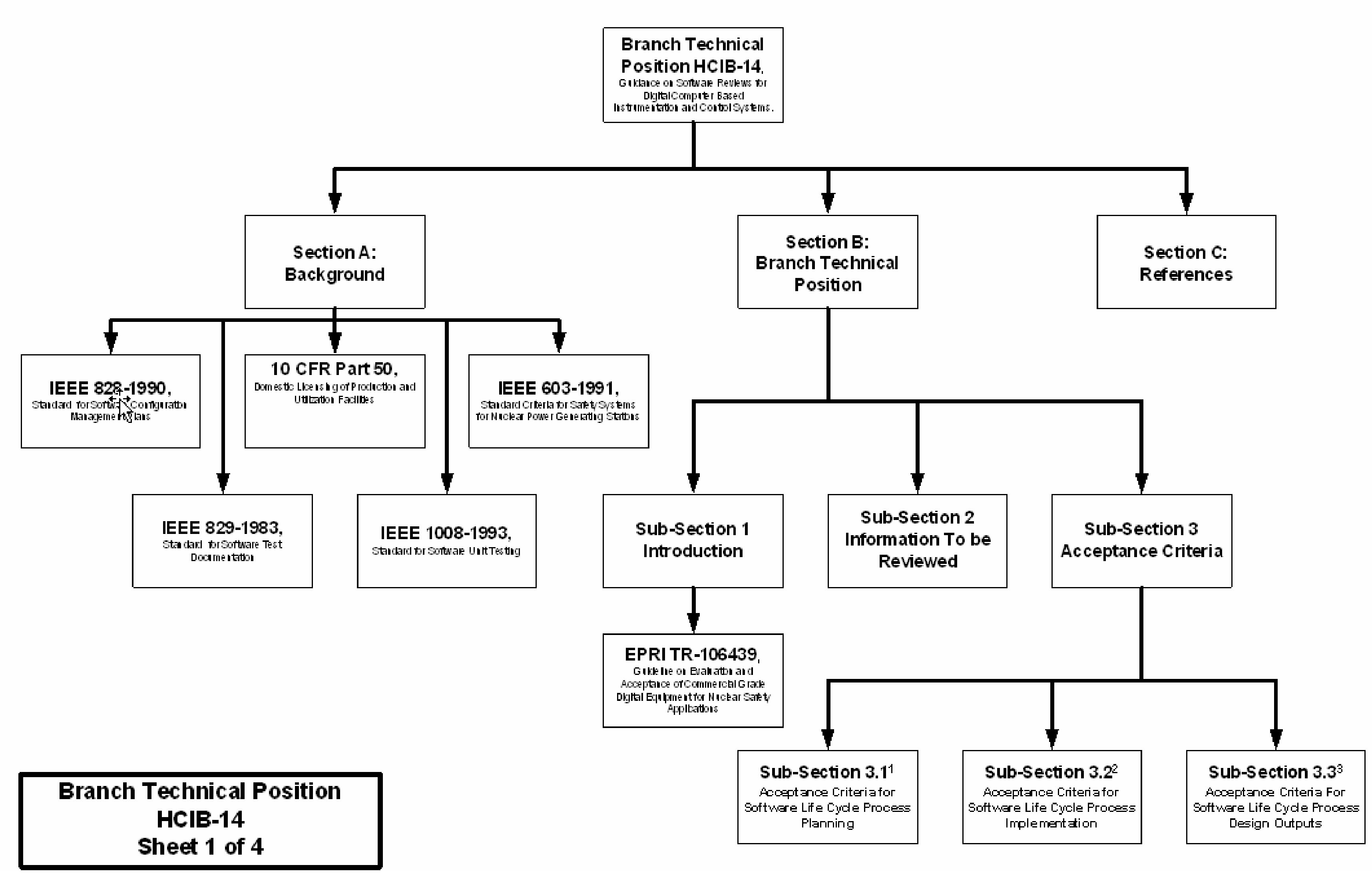

Branch Technical Position HCIB-14, Guidance on Software Reviews for Digital Computer Based Instrumentation and Control Systems.
Section A: Background
Section B: Branch Technical Position
Section C: References
IEEE 828-1990, Standard for Software Configuration Management Plans
10 CFR Part 50, Domestic Licensing of Production and Utilization Facilities
IEEE 603-1991, Standard Criteria for Safety Systems for Nuclear Power Generating Stations
IEEE 829-1983, Standard for Software Test Documentation
IEEE 1008-1993, Standard for Software Unit Testing
Sub-Section 1 Introduction
Sub-Section 2 Information To be Reviewed
Sub-Section 3 Acceptance Criteria
EPRI TR-106439, Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications
Sub-Section 3.1[1] Acceptance Criteria for Software Life Cycle Process Planning
Sub-Section 3.2[2] Acceptance Criteria for Software Life Cycle Process Implementation
Sub-Section 3.3[3] Acceptance Criteria For Software Life Cycle Process Design Outputs
Branch Technical Position HCIB-14 Sheet 1 of 4

Figure 3-5 Branch Technical Position HICB-14 Sheet 1 of 4

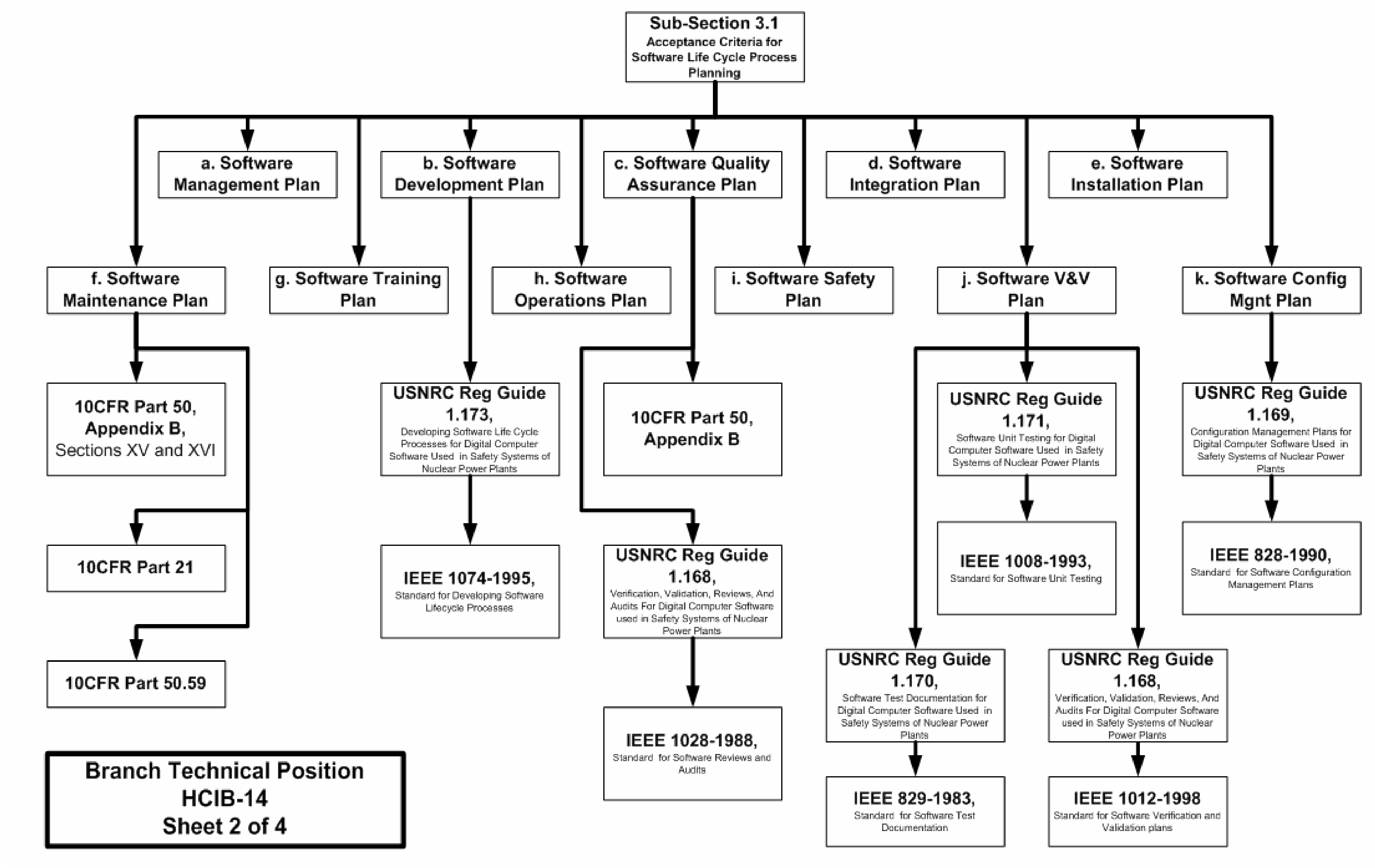

Sub-Section 3.1
Acceptance Criteria for Software Life Cycle Process Planning
a. Software Management Plan
b. Software Development Plan
c. Software Quality Assurance Plan
d. Software Integration Plan
e. Software Installation Plan
f. Software Maintenance Plan
g. Software Training Plan
h. Software Operations Plan
i. Software Safety Plan
j. Software V&V Plan
k. Software Config Mgnt Plan
10CFR Part 50, Appendix B, Sections XV and XVI
10CFR Part 21
10CFR Part 50.59
USNRC Reg Guide 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
IEEE 1074-1995, Standard for Developing Software Lifecycle Processes
10CFR Part 50, Appendix B
USNRC Reg Guide 1.168, Verification, Validation, Reviews, And Audits For Digital Computer Software used in Safety Systems of Nuclear Power Plants
IEEE 1028-1988, Standard for Software Reviews and Audits
USNRC Reg Guide 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
IEEE 1008-1993, Standard for Software Unit Testing
USNRC Reg Guide 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
IEEE 829-1983, Standard for Software Test Documentation
USNRC Reg Guide 1.168, Verification, Validation, Reviews, And Audits For Digital Computer Software used in Safety Systems of Nuclear Power Plants
IEEE 1012-1998 Standard for Software Verification and Validation plans
USNRC Reg Guide 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
IEEE 828-1990, Standard for Software Configuration Management Plans
Branch Technical Position HCIB-14 Sheet 2 of 4

Figure 3-6 Branch Technical Position HICB-14 Sheet 2 of 4

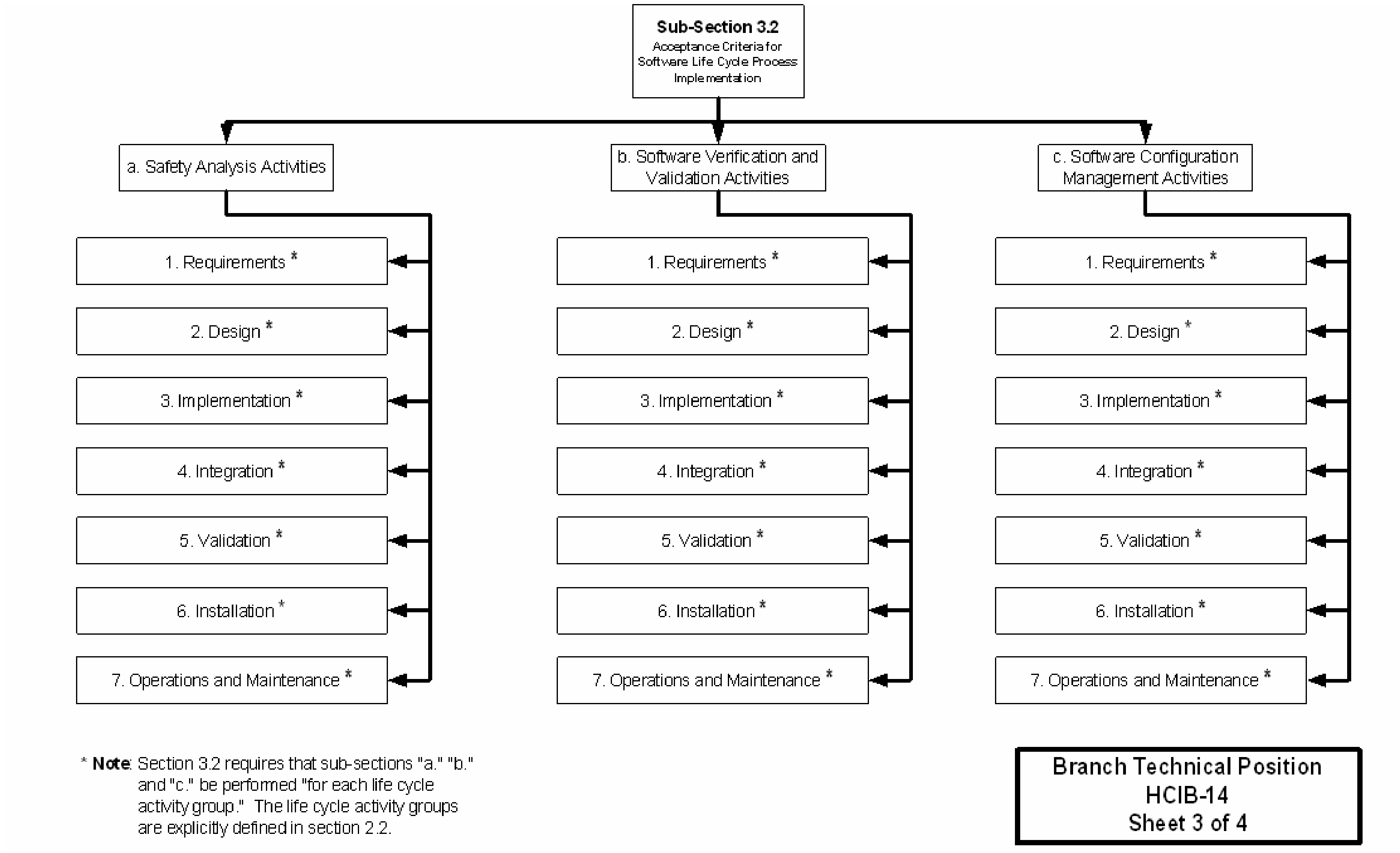

Sub-Section 3.2
Acceptance Criteria for Software Life Cycle Process Implementation
a. Safety Analysis Activities
b. Software Verification and Validation Activities
c. Software Configuration Management Activities
1. Requirements *
2. Design *
3. Implementation *
4. Integration *
5. Validation *
6. Installation *
7. Operations and Maintenance *
* Note: Section 3.2 requires that sub-sections "a." "b." and "c." be performed "for each life cycle activity group." The life cycle activity groups are explicitly defined in section 2.2.
Branch Technical Position
HCIB-14
Sheet 3 of 4

Figure 3-7 Branch Technical Position HICB-14 Sheet 3 of 4

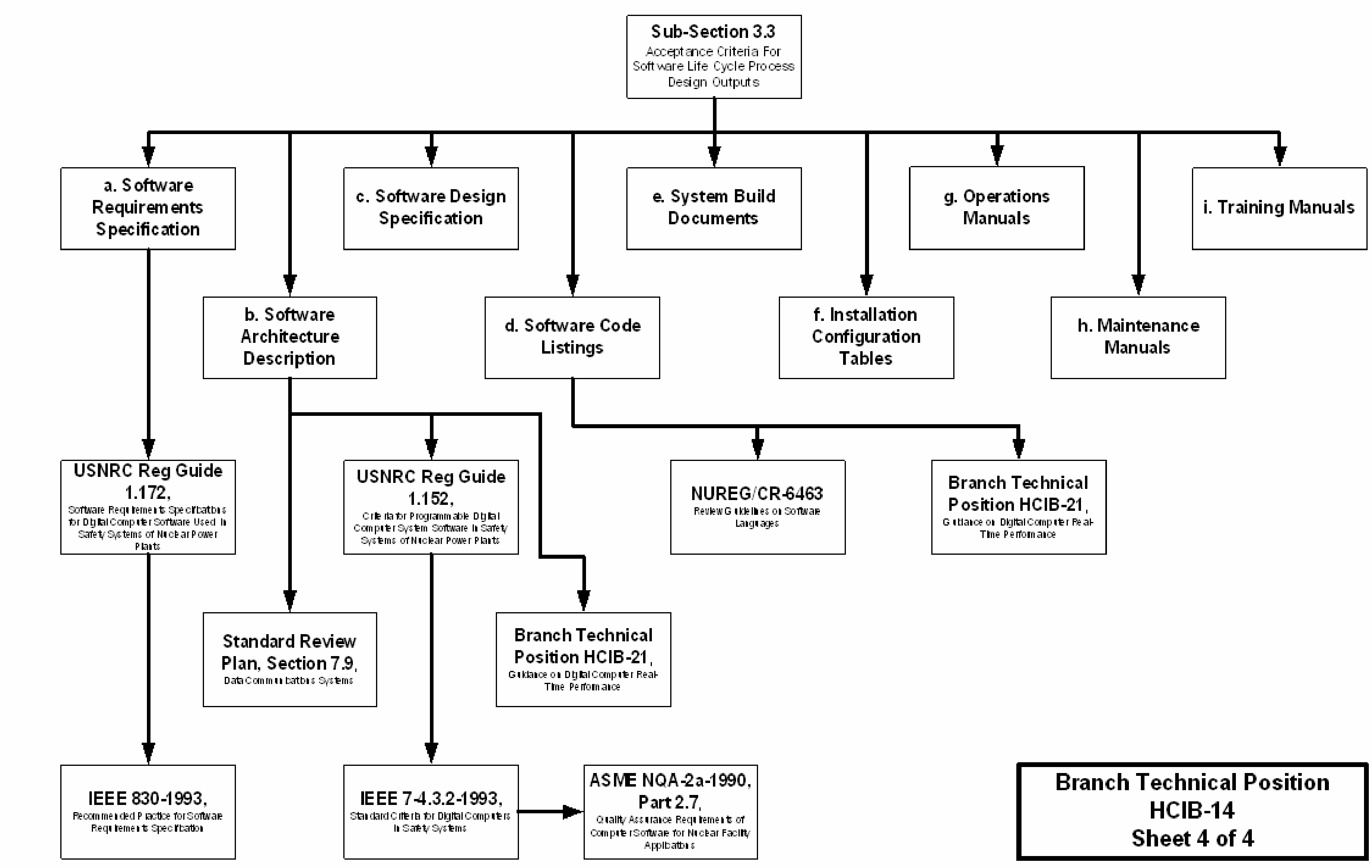
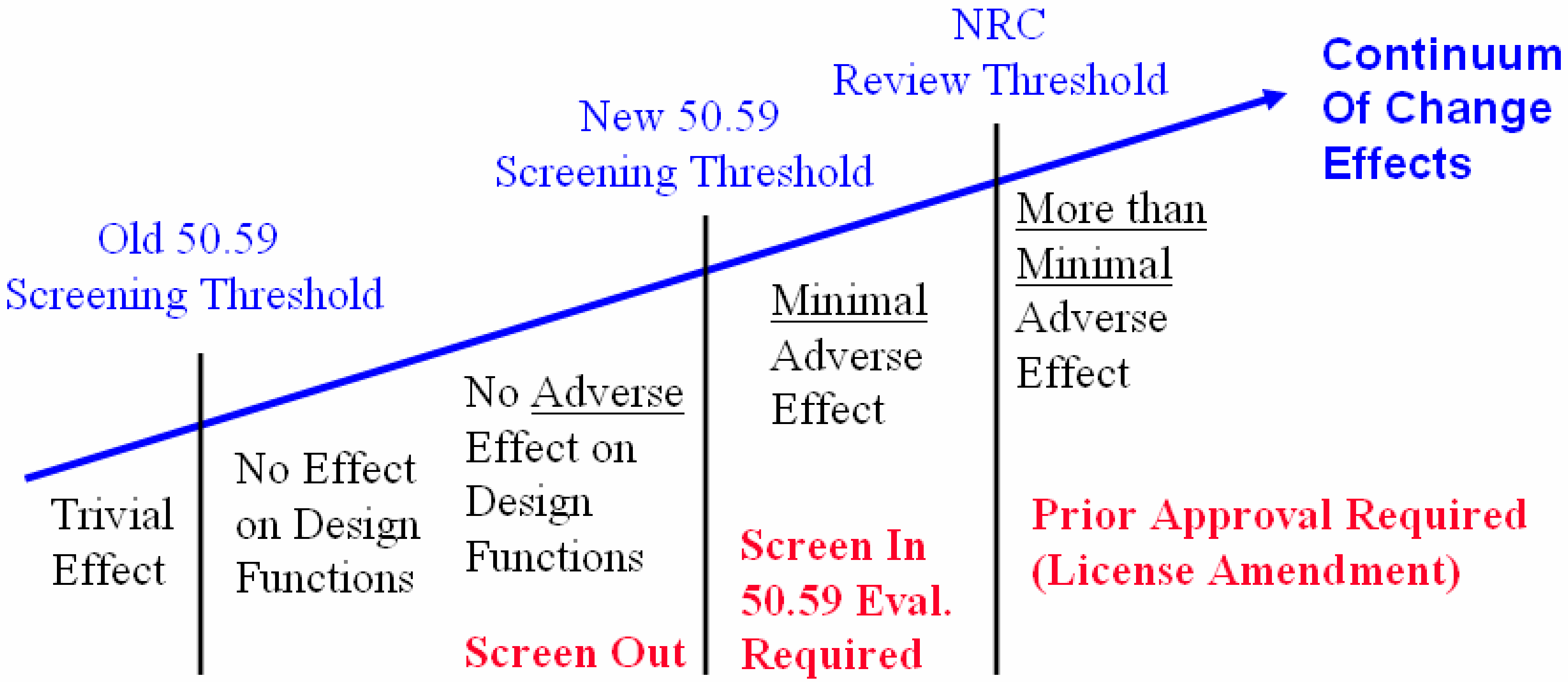

Sub-Section 3.3
Acceptance Criteria For Software Life Cycle Process Design Outputs
a. Software Requirements Specification
b. Software Architecture Description
c. Software Design Specification
d. Software Code Listings
e. System Build Documents
f. Installation Configuration Tables
g. Operations Manuals
h. Maintenance Manuals
i. Training Manuals
USNRC Reg Guide 1.172,
Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
USNRC Reg Guide 1.152,
Criteria for Programmable Digital Computer System Software in Safety Systems of Nuclear Power Plants
NUREG/CR-6463
Review Guidelines on Software Languages
Branch Technical Position HCIB-21,
Guidance on Digital Computer Real-Time Performance
Standard Review Plan, Section 7.9,
Data Communications Systems
Branch Technical Position HCIB-21,
Guidance on Digital Computer Real-Time Performance
IEEE 830-1993,
Recommended Practice for Software Requirements Specification
IEEE 7-4.3.2-1993,
Standard Criteria for Digital Computers in Safety Systems
ASME NQA-2a-1990, Part 2.7,
Quality Assurance Requirements of Computer Software for Nuclear Facility Applications
Branch Technical Position
HCIB-14
Sheet 4 of 4

Figure 3-8 Branch Technical Position HICB-14 Sheet 4 of 4



NRC
Review Threshold

Continuum
Of Change
Effects

New 50.59
Screening Threshold

Old 50.59
Screening Threshold

Trivial
Effect

No Effect
on Design
Functions

No Adverse
Effect on
Design
Functions

Screen Out

Minimal
Adverse
Effect

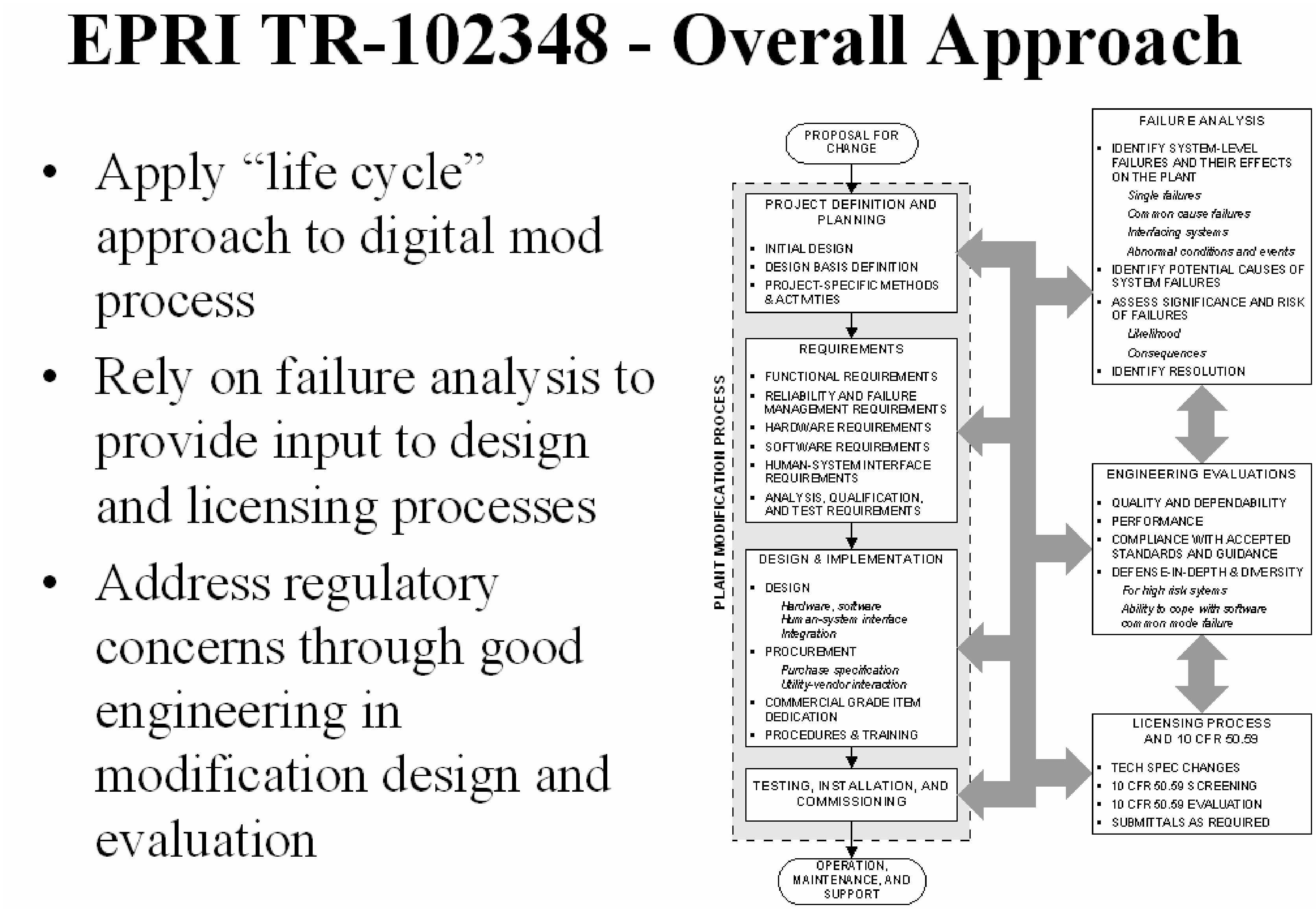
Screen In
50.59 Eval.
Required

More than
Minimal
Adverse
Effect

Prior Approval Required
(License Amendment)

TR-102348, Rev. 1, supplements NEI 96-07, Rev. 1, to define these thresholds for digital upgrades

Figure 3-9 Thresholds Defined in NEI 96-07, Rev. 1



EPRI TR-102348 - Overall Approach

- Apply “life cycle” approach to digital mod process
- Rely on failure analysis to provide input to design and licensing processes
- Address regulatory concerns through good engineering in modification design and evaluation

PROPOSAL FOR CHANGE

PLANT MODIFICATION PROCESS

PROJECT DEFINITION AND PLANNING

- INITIAL DESIGN
- DESIGN BASIS DEFINITION
- PROJECT-SPECIFIC METHODS & ACTIVITIES

REQUIREMENTS

- FUNCTIONAL REQUIREMENTS
- RELIABILITY AND FAILURE MANAGEMENT REQUIREMENTS
- HARDWARE REQUIREMENTS
- SOFTWARE REQUIREMENTS
- HUMAN-SYSTEM INTERFACE REQUIREMENTS
- ANALYSIS, QUALIFICATION, AND TEST REQUIREMENTS

DESIGN & IMPLEMENTATION

- DESIGN
  - *Hardware, software*
  - *Human-system interface*
  - *Integration*
- PROCUREMENT
  - *Purchase specification*
  - *Utility-vendor interaction*
- COMMERCIAL GRADE ITEM DEDICATION
- PROCEDURES & TRAINING

TESTING, INSTALLATION, AND COMMISSIONING

OPERATION, MAINTENANCE, AND SUPPORT

FAILURE ANALYSIS

- IDENTIFY SYSTEM-LEVEL FAILURES AND THEIR EFFECTS ON THE PLANT
  - *Single failures*
  - *Common cause failures*
  - *Interfacing systems*
  - *Abnormal conditions and events*
- IDENTIFY POTENTIAL CAUSES OF SYSTEM FAILURES
- ASSESS SIGNIFICANCE AND RISK OF FAILURES
  - *Likelihood*
  - *Consequences*
- IDENTIFY RESOLUTION

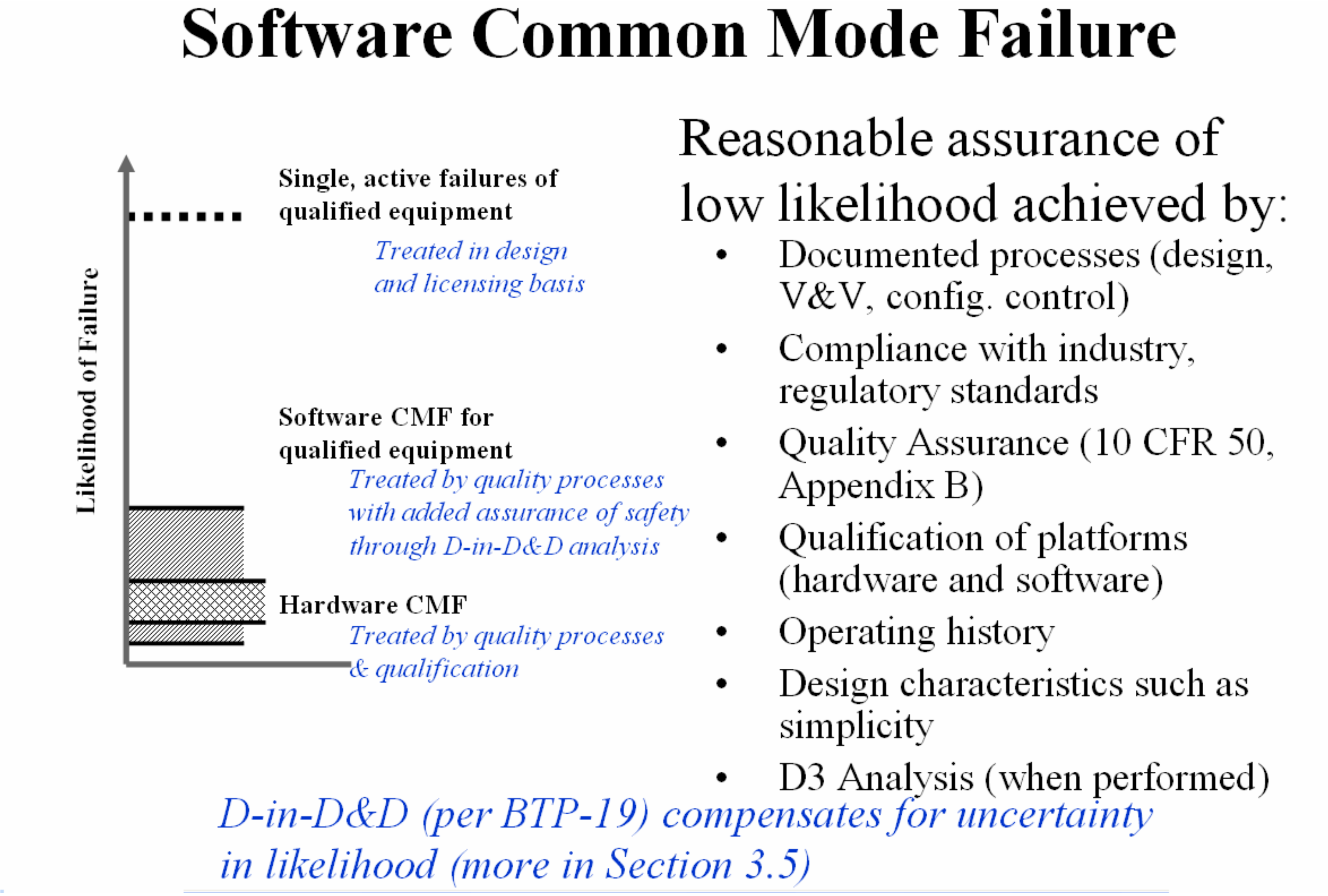
ENGINEERING EVALUATIONS

- QUALITY AND DEPENDABILITY
- PERFORMANCE
- COMPLIANCE WITH ACCEPTED STANDARDS AND GUIDANCE
- DEFENSE-IN-DEPTH & DIVERSITY
  - *For high risk sytems*
  - *Ability to cope with software common mode failure*

LICENSING PROCESS AND 10 CFR 50.59

- TECH SPEC CHANGES
- 10 CFR 50.59 SCREENING
- 10 CFR 50.59 EVALUATION
- SUBMITTALS AS REQUIRED

Figure 3-10 EPRI TR-102348 – Overall Approach



Software Common Mode Failure

Single, active failures of qualified equipment

Treated in design and licensing basis

Software CMF for qualified equipment

Treated by quality processes with added assurance of safety through D-in-D&D analysis

Hardware CMF

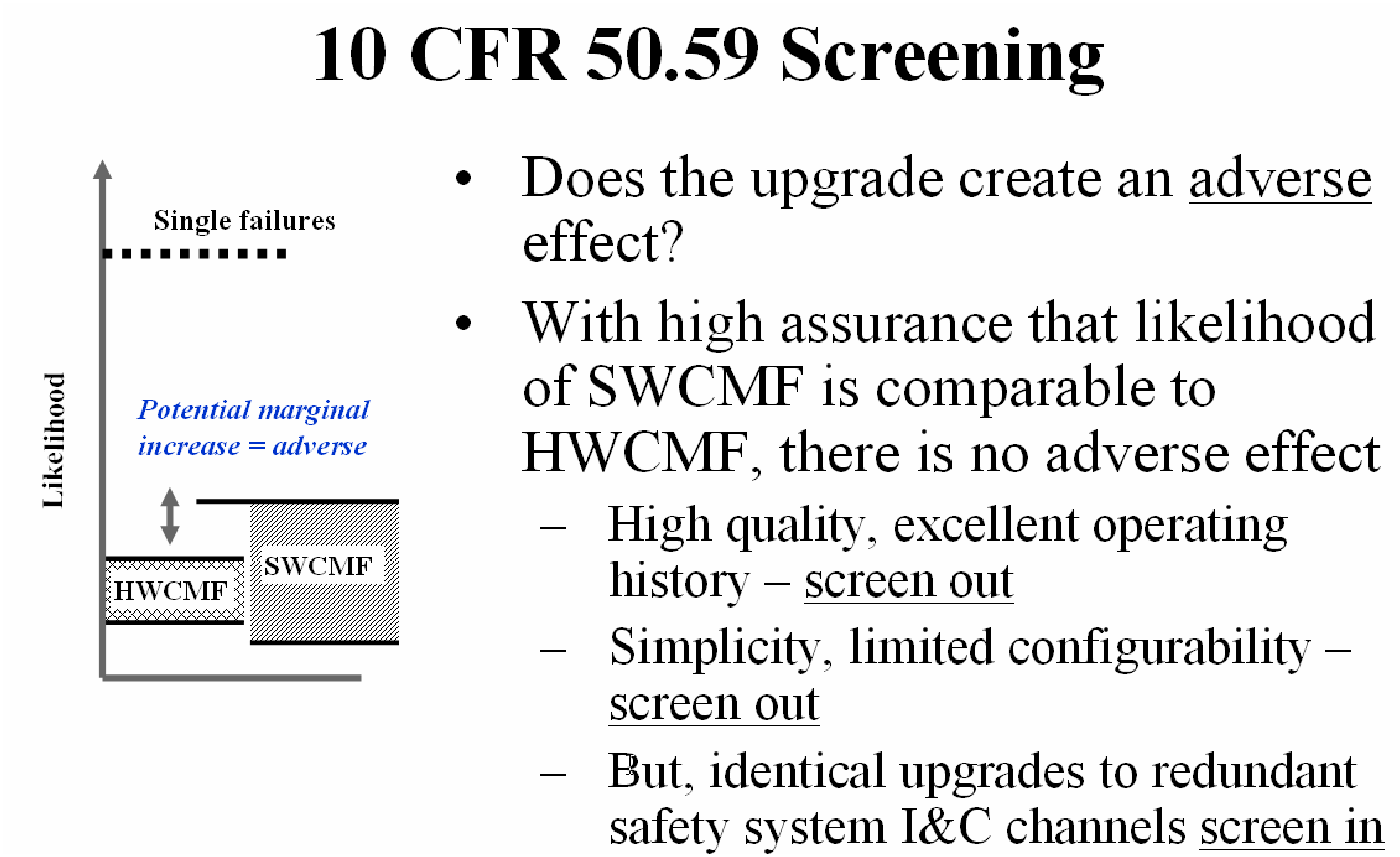
Treated by quality processes & qualification

Reasonable assurance of low likelihood achieved by:

- Documented processes (design, V&V, config. control)
- Compliance with industry, regulatory standards
- Quality Assurance (10 CFR 50, Appendix B)
- Qualification of platforms (hardware and software)
- Operating history
- Design characteristics such as simplicity
- D3 Analysis (when performed)

D-in-D&D (per BTP-19) compensates for uncertainty in likelihood (more in Section 3.5)

Figure 3-11 Software Common Mode Failure

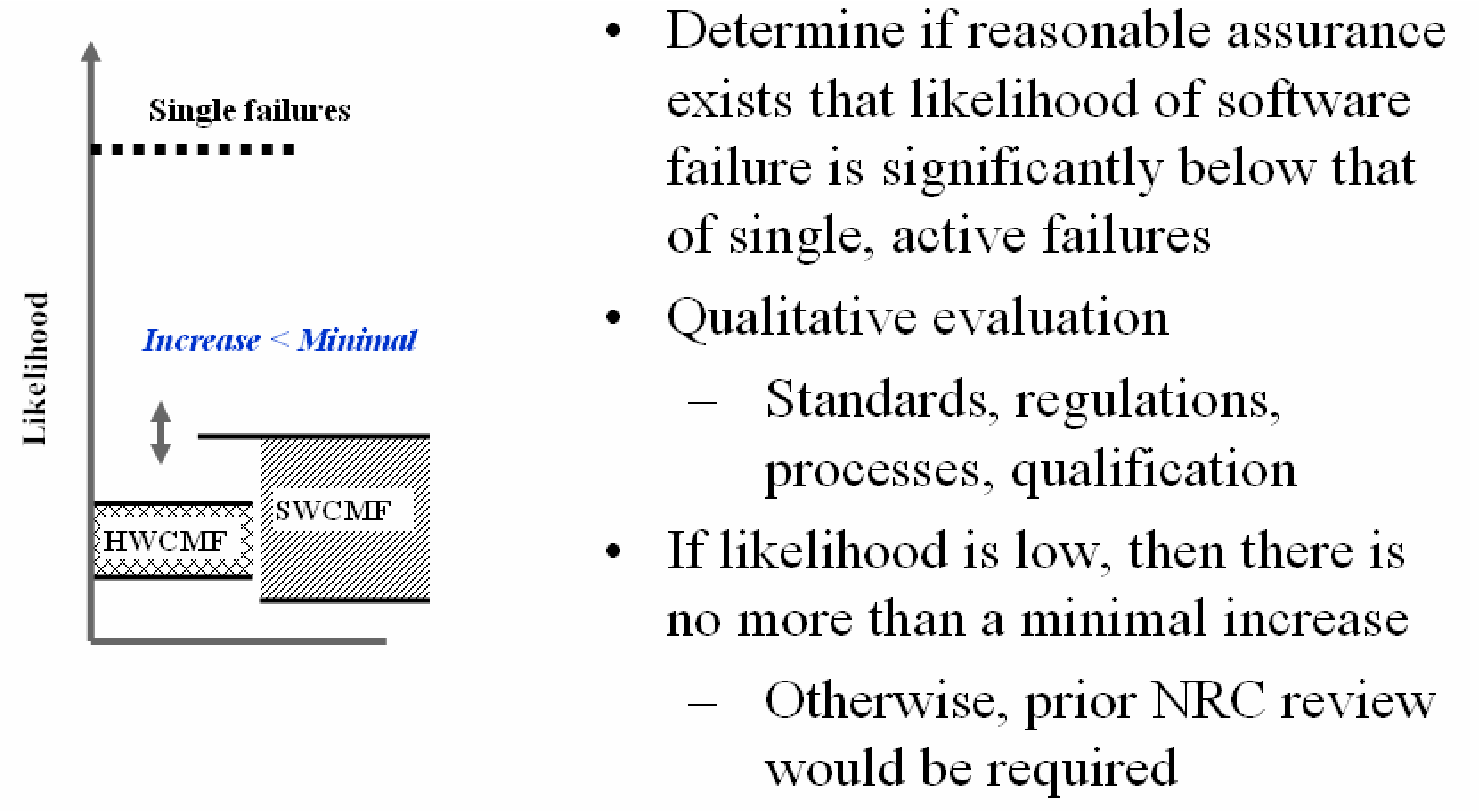


Single failures
Likelihood
Potential marginal increase = adverse
SWCMF
HWCMF

10 CFR 50.59 Screening

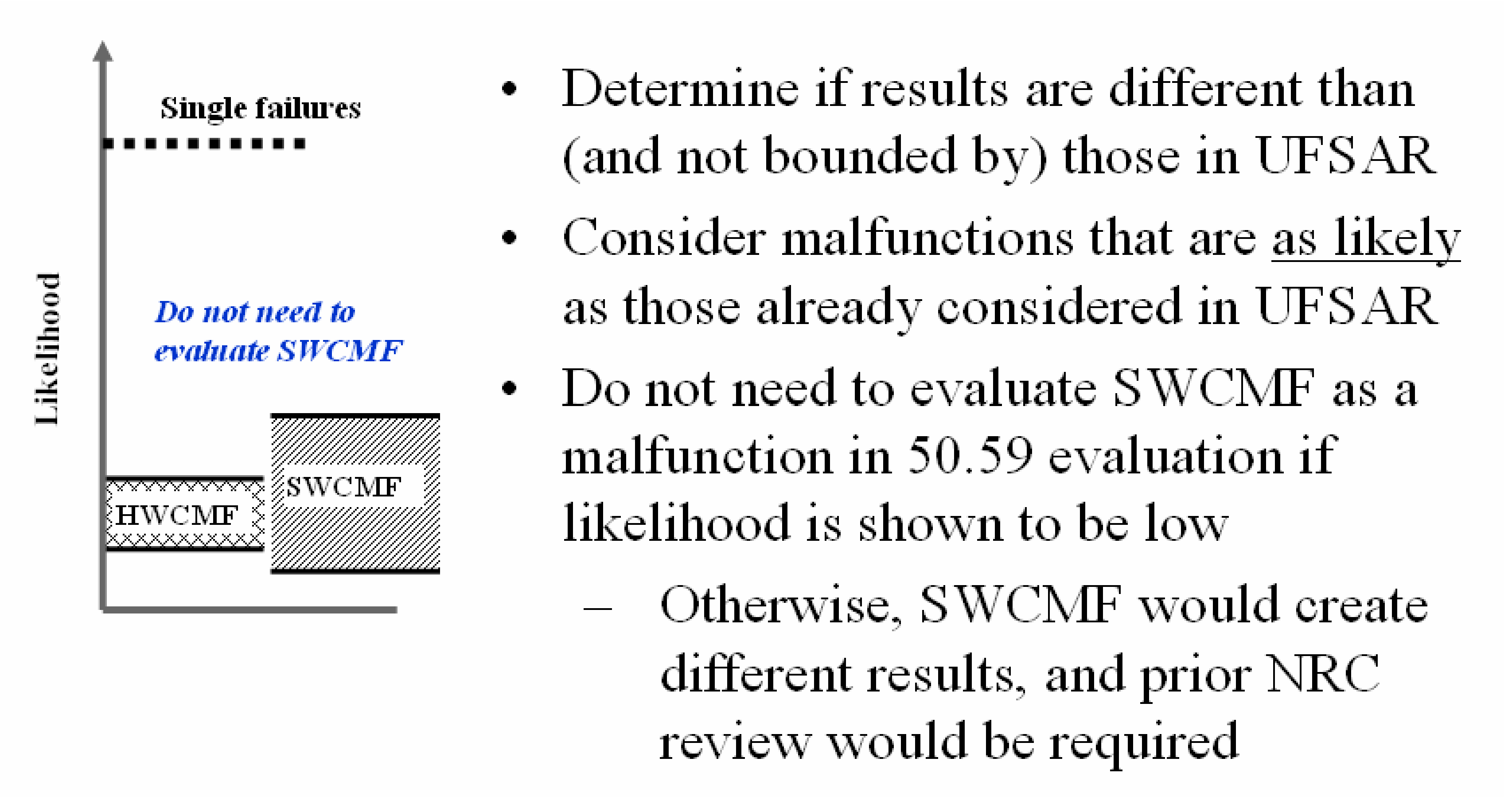
- Does the upgrade create an adverse effect?
- With high assurance that likelihood of SWCMF is comparable to HWCMF, there is no adverse effect
  - High quality, excellent operating history – screen out
  - Simplicity, limited configurability – screen out
  - But, identical upgrades to redundant safety system I&C channels screen in

Figure 3-12 10 CFR 50.59 Screening



- Determine if reasonable assurance exists that likelihood of software failure is significantly below that of single, active failures
- Qualitative evaluation
  - Standards, regulations, processes, qualification
- If likelihood is low, then there is no more than a minimal increase
  - Otherwise, prior NRC review would be required

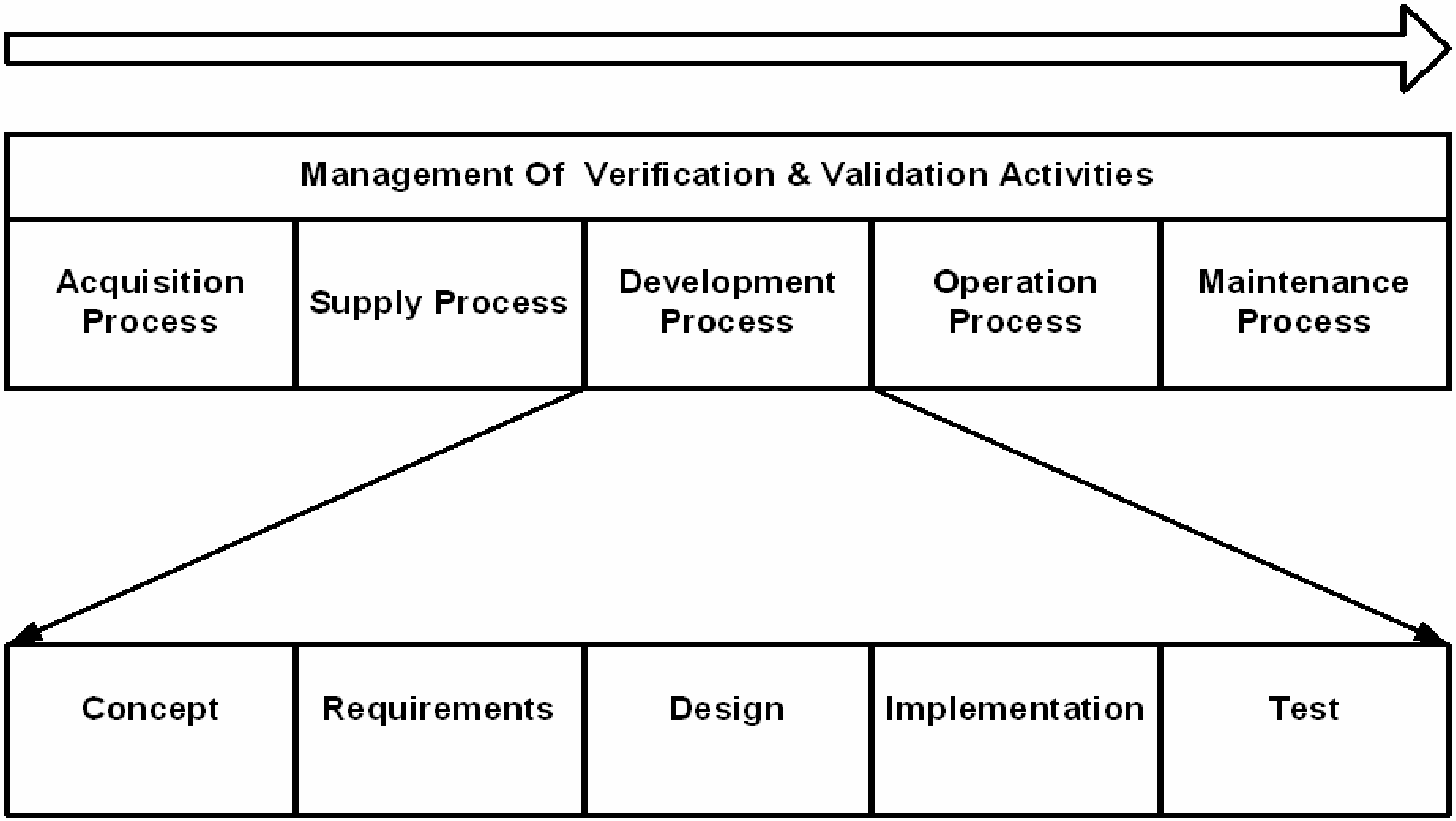
Figure 3-13 Likelihood of Malfunctions in 50.59


Single failures
Likelihood
Do not need to evaluate SWCMF
SWCMF
HWCMF

- Determine if results are different than (and not bounded by) those in UFSAR
- Consider malfunctions that are <u>as likely</u> as those already considered in UFSAR
- Do not need to evaluate SWCMF as a malfunction in 50.59 evaluation if likelihood is shown to be low
  - Otherwise, SWCMF would create different results, and prior NRC review would be required

Figure 3-14 Results of Malfunctions in 50.59

IEEE 1012 - 1998
Standard for Software Verification and Validation
V&V Software Lifecycle Processes



Management Of Verification & Validation Activities

Acquisition Process

Supply Process

Development Process

Operation Process

Maintenance Process

Concept

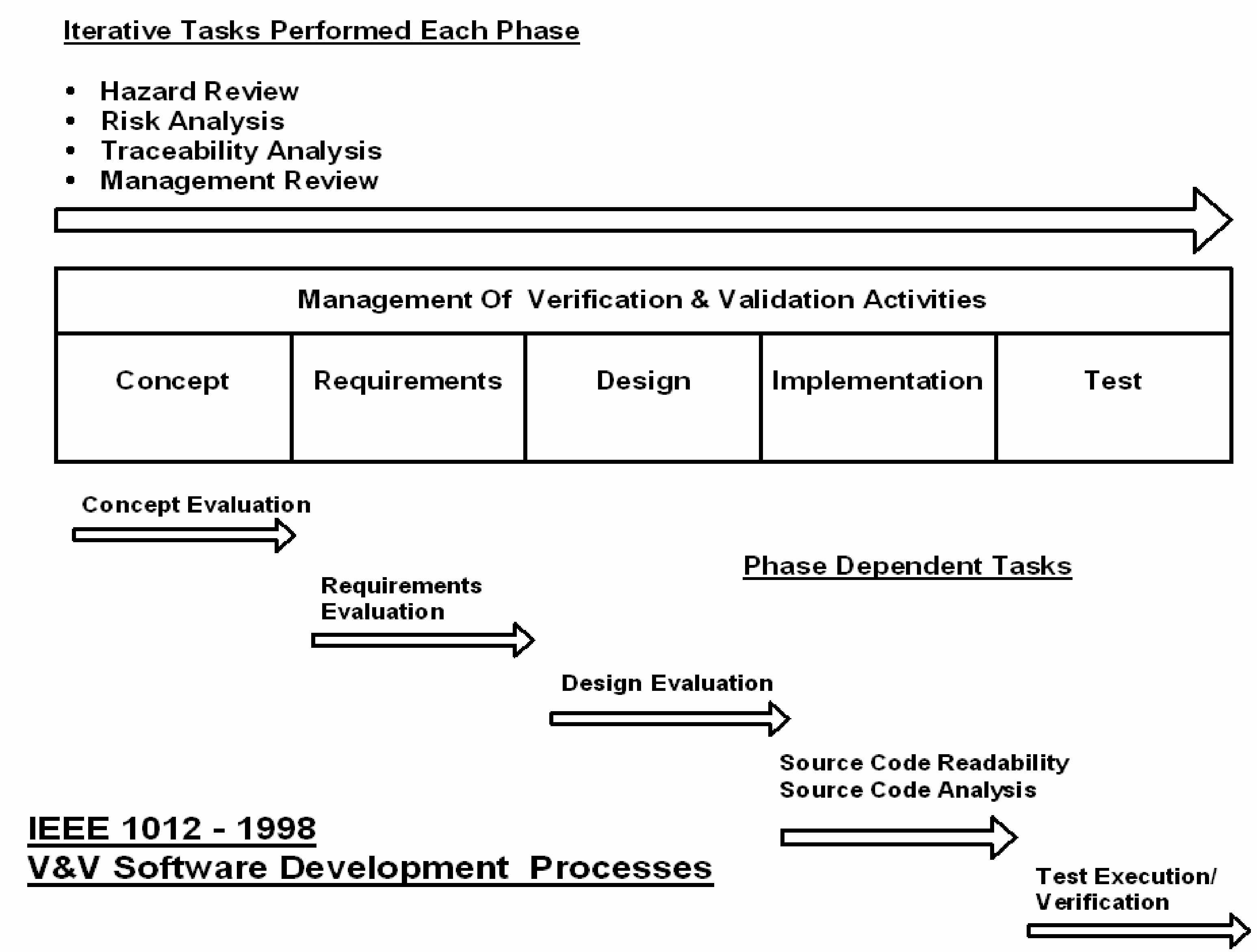
Requirements

Design

Implementation

Test

Figure 3-15 Standard for Software Verification and Validation



Iterative Tasks Performed Each Phase

- Hazard Review
- Risk Analysis
- Traceability Analysis
- Management Review

Management Of Verification & Validation Activities				
Concept	Requirements	Design	Implementation	Test

Concept Evaluation

Requirements Evaluation

Design Evaluation

Source Code Readability
Source Code Analysis

Test Execution/ Verification

Phase Dependent Tasks

IEEE 1012 - 1998
V&V Software Development Processes

Figure 3-16 IEEE Std 1012-1998 V&V Software Development Processes

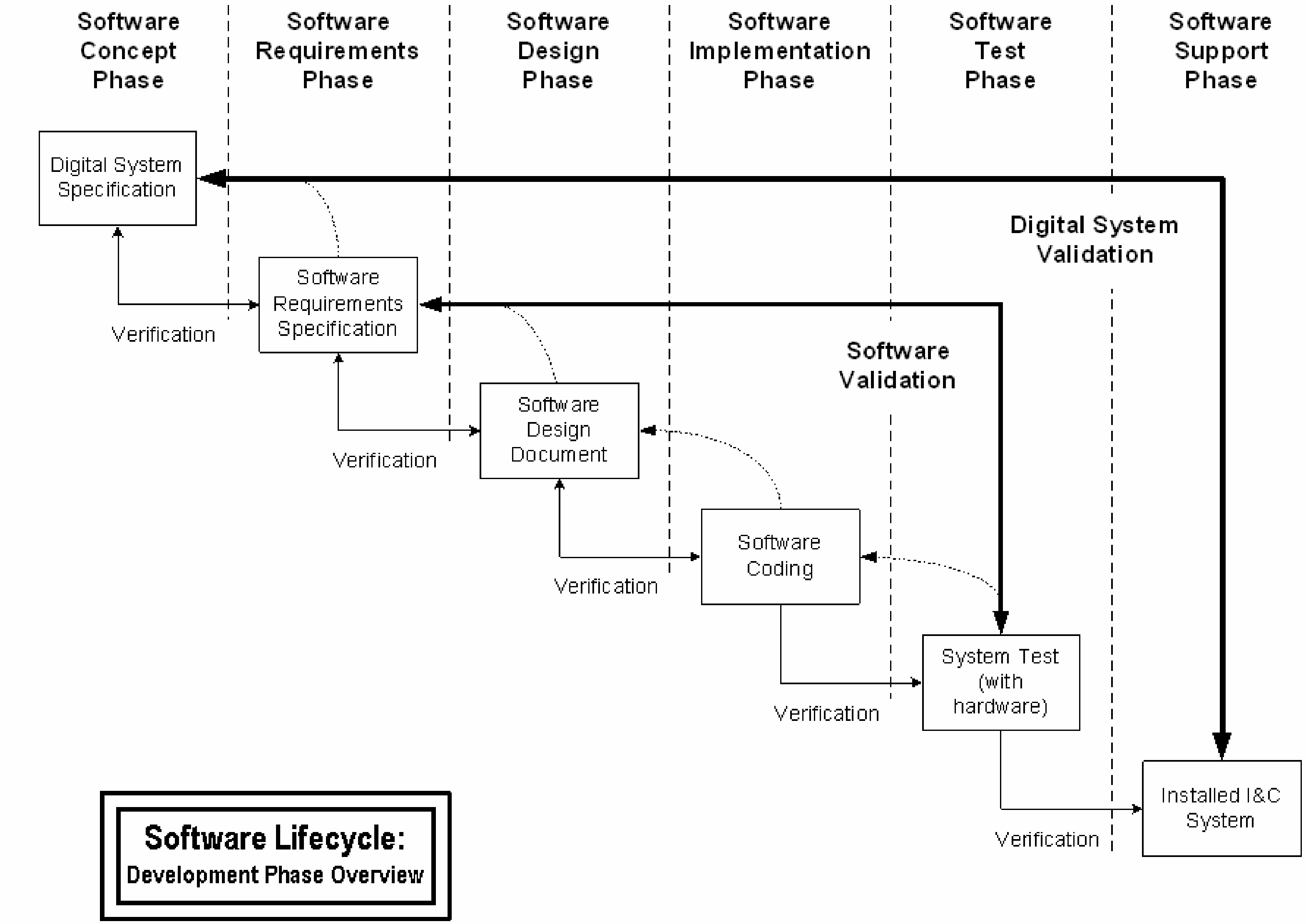


Figure 3-17 Software Lifecycle : Development Phase Overview

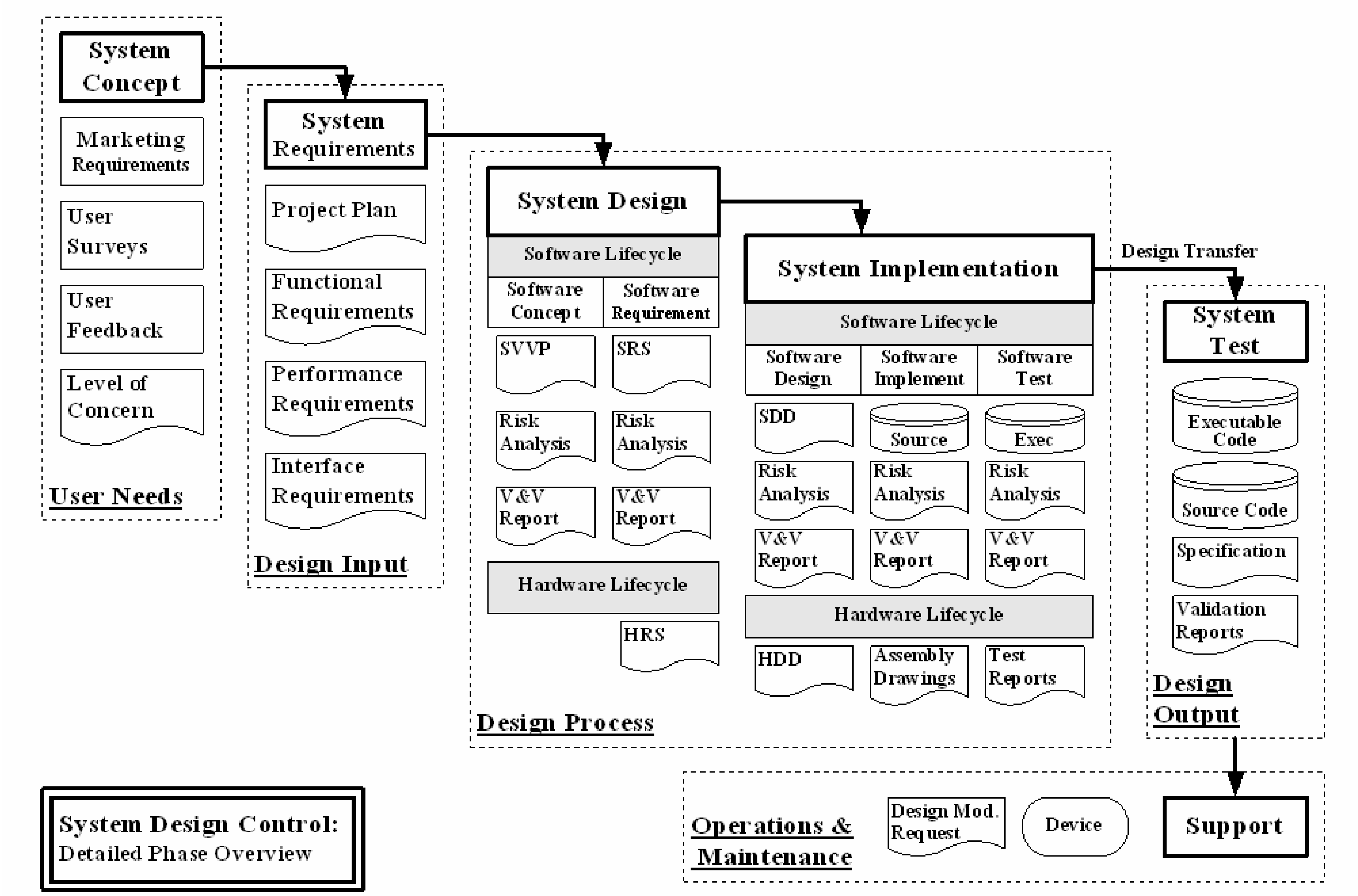
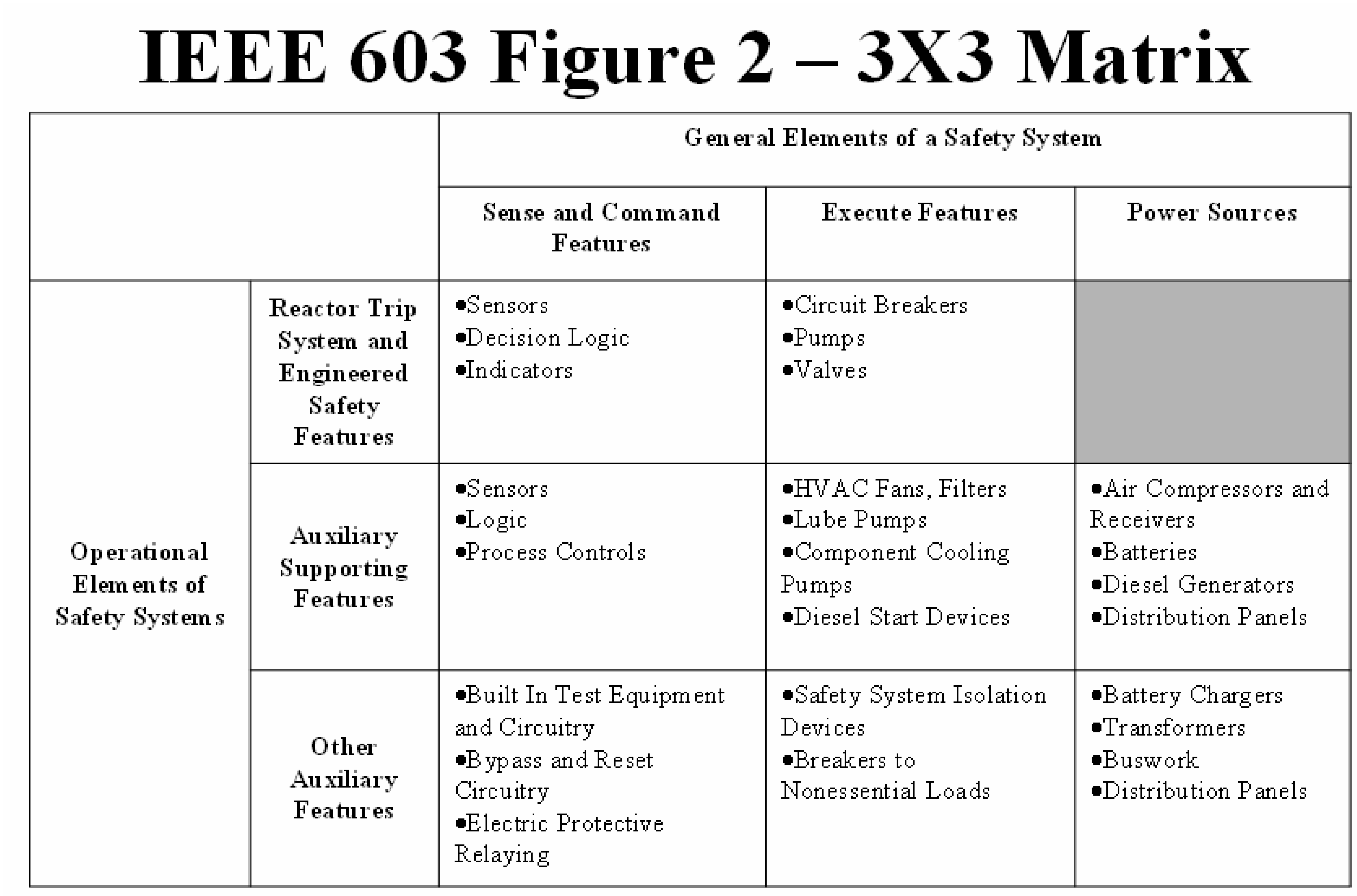


Figure 3-18 System Design Control : Detailed Plan Overview



IEEE 603 Figure 2 – 3X3 Matrix

		General Elements of a Safety System		
		Sense and Command Features	Execute Features	Power Sources
Operational Elements of Safety Systems	Reactor Trip System and Engineered Safety Features	•Sensors •Decision Logic •Indicators	•Circuit Breakers •Pumps •Valves	
	Auxiliary Supporting Features	•Sensors •Logic •Process Controls	•HVAC Fans, Filters •Lube Pumps •Component Cooling Pumps •Diesel Start Devices	•Air Compressors and Receivers •Batteries •Diesel Generators •Distribution Panels
	Other Auxiliary Features	•Built In Test Equipment and Circuitry •Bypass and Reset Circuitry •Electric Protective Relaying	•Safety System Isolation Devices •Breakers to Nonessential Loads	•Battery Chargers •Transformers •Buswork •Distribution Panels

Figure 3-19 IEEE Std 603 Figure 2 - 3x3 Matrix

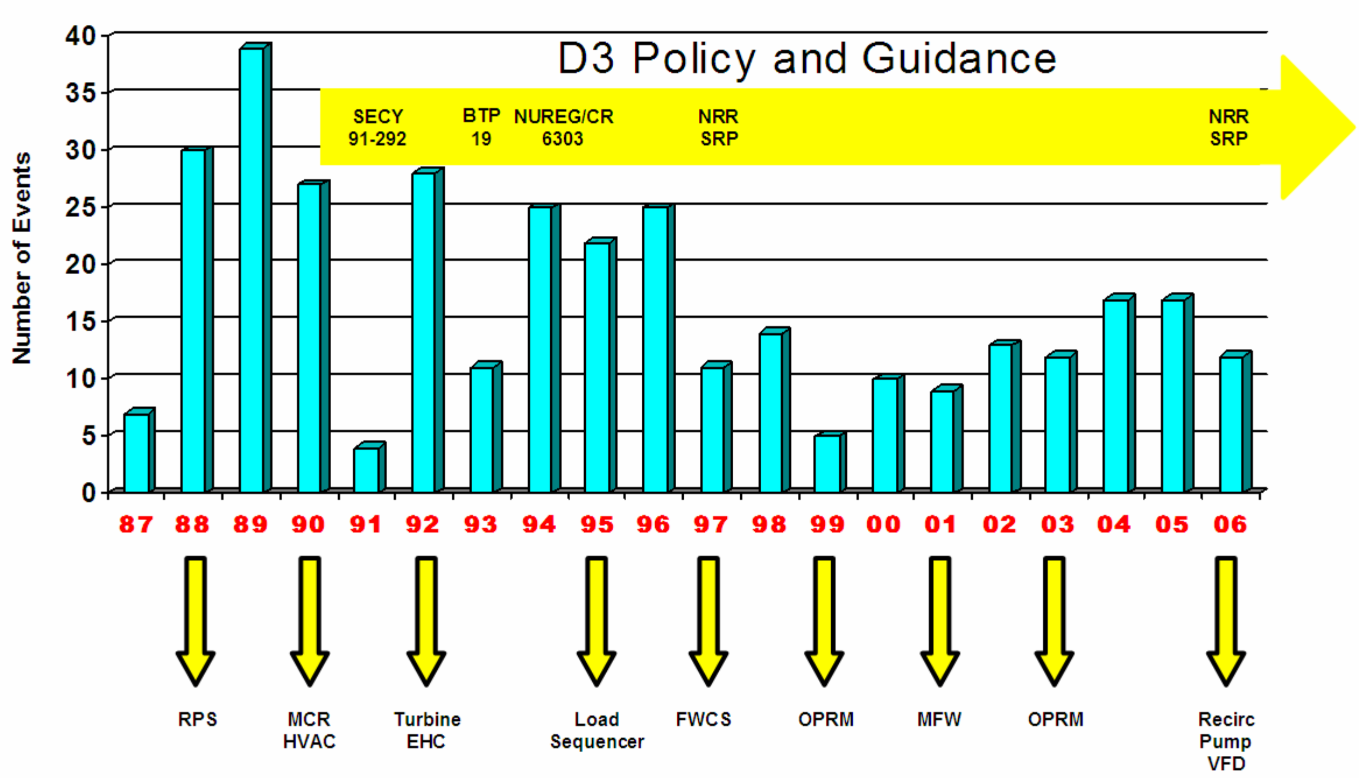
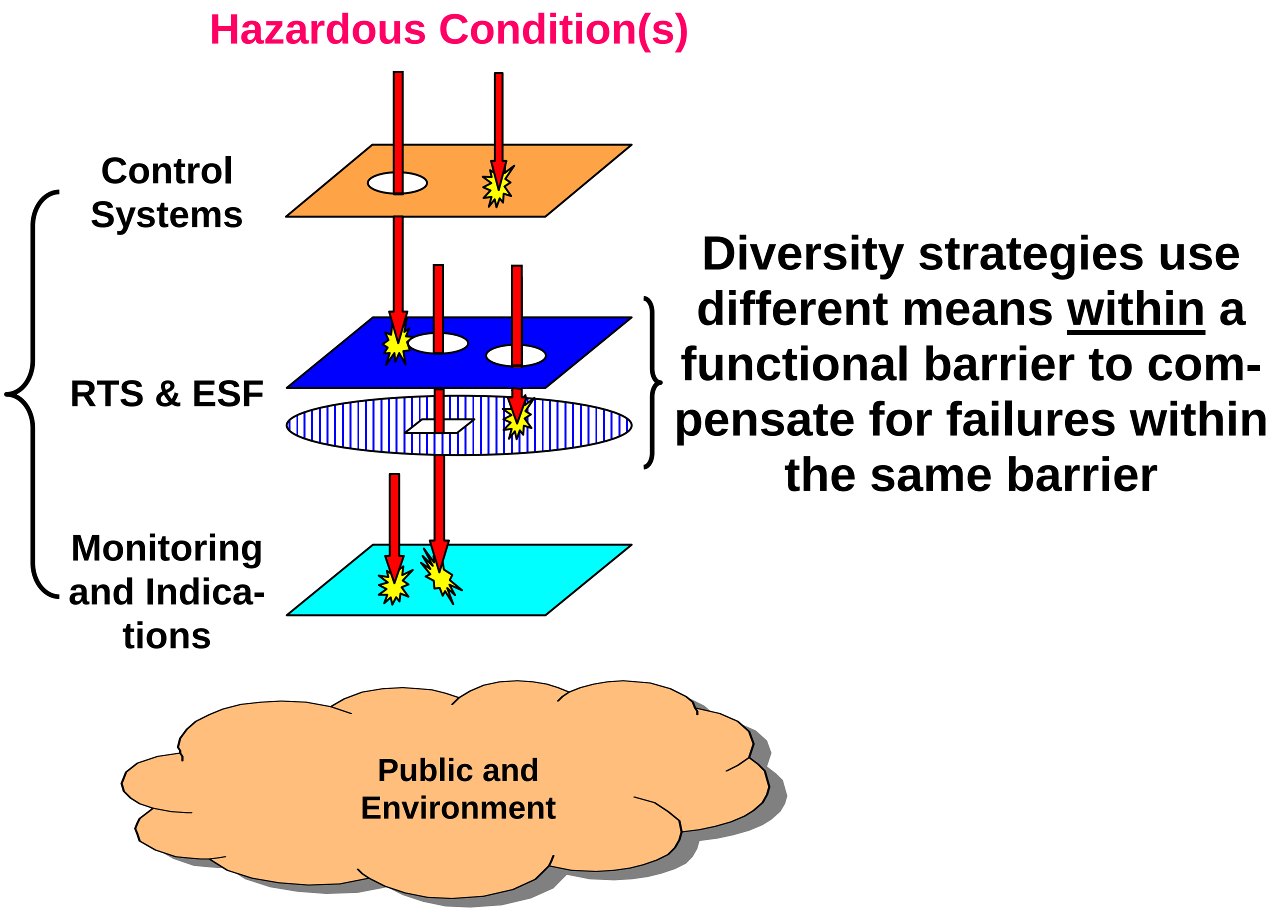


Figure 3-20 D3 Policy and Guidance



Diversity strategies use different means within a functional barrier to compensate for failures within the same barrier

Figure 3-21 Diversity and Defense in Depth Strategies

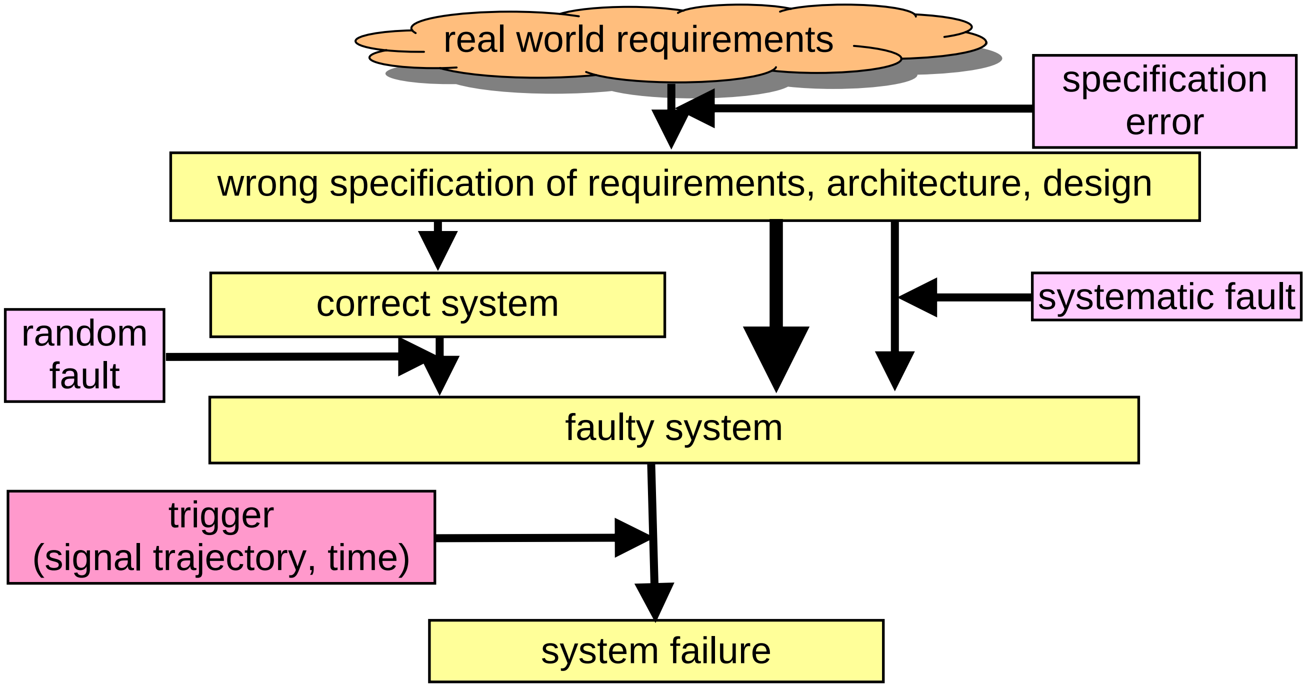


Figure 3-22 System Failure – International View

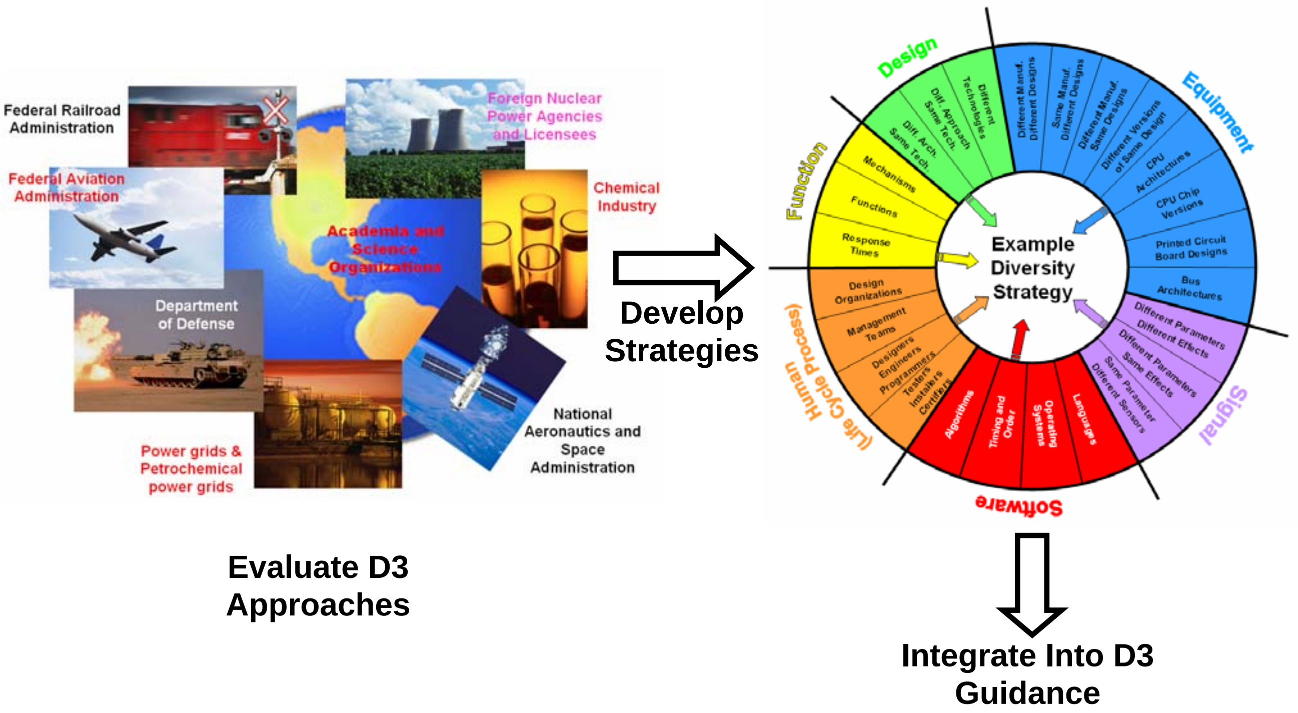
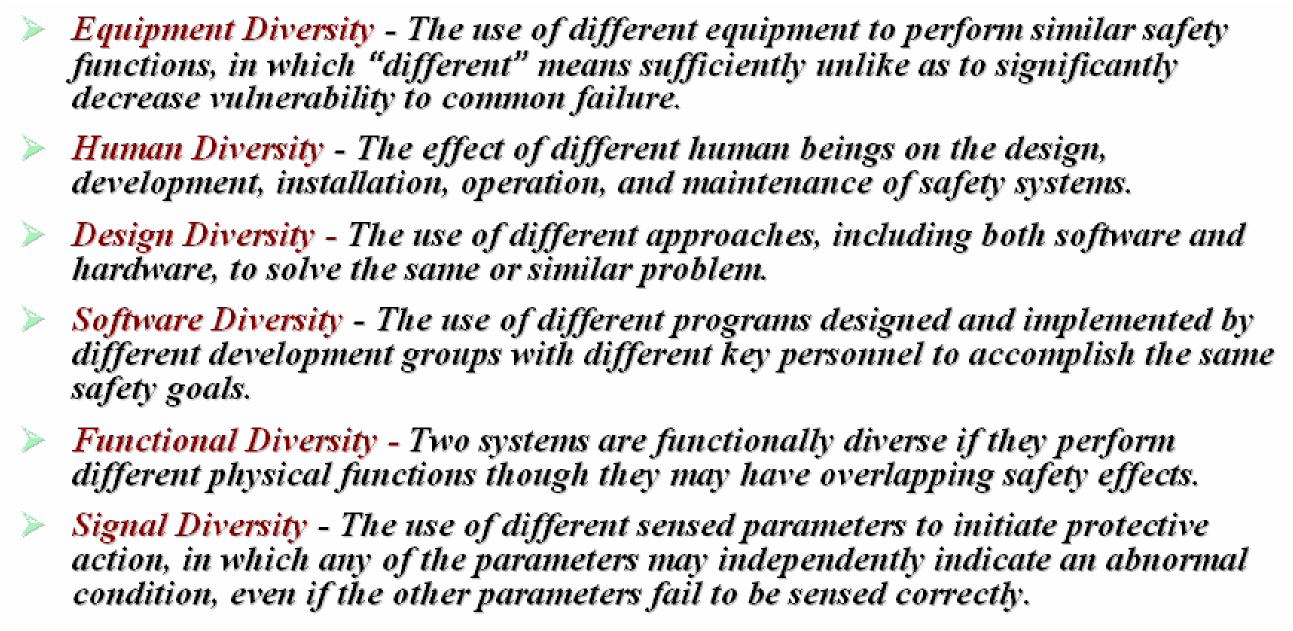

Federal Railroad Administration
Foreign Nuclear Power Agencies and Licensees
Federal Aviation Administration
Chemical Industry
Academia and Science Organizations
Department of Defense
Power grids & Petrochemical power grids
National Aeronautics and Space Administration
Evaluate D3 Approaches
Develop Strategies
Design
Different Technologies
Diff. Approach Same Tech.
Diff. Arch. Same Tech.
Equipment
Different Manuf. Different Designs
Same Manuf. Different Designs
Different Manuf. Same Designs
Different Versions of Same Design
CPU Architectures
CPU Chip Versions
Printed Circuit Board Designs
Bus Architectures
Function
Mechanisms
Functions
Response Times
Example Diversity Strategy
Human (Life Cycle Process)
Design Organizations
Management Teams
Designers Engineers Programmers Testers Installers Certifiers
Software
Algorithms
Timing and Order
Operating Systems
Languages
Signal
Different Parameters Different Effects
Different Parameters Same Effects
Same Parameter Different Sensors
Integrate Into D3 Guidance

Figure 3-23 Research Approach



- Equipment Diversity - The use of different equipment to perform similar safety functions, in which “different” means sufficiently unlike as to significantly decrease vulnerability to common failure.
- Human Diversity - The effect of different human beings on the design, development, installation, operation, and maintenance of safety systems.
- Design Diversity - The use of different approaches, including both software and hardware, to solve the same or similar problem.
- Software Diversity - The use of different programs designed and implemented by different development groups with different key personnel to accomplish the same safety goals.
- Functional Diversity - Two systems are functionally diverse if they perform different physical functions though they may have overlapping safety effects.
- Signal Diversity - The use of different sensed parameters to initiate protective action, in which any of the parameters may independently indicate an abnormal condition, even if the other parameters fail to be sensed correctly.

Figure 3-24 European View

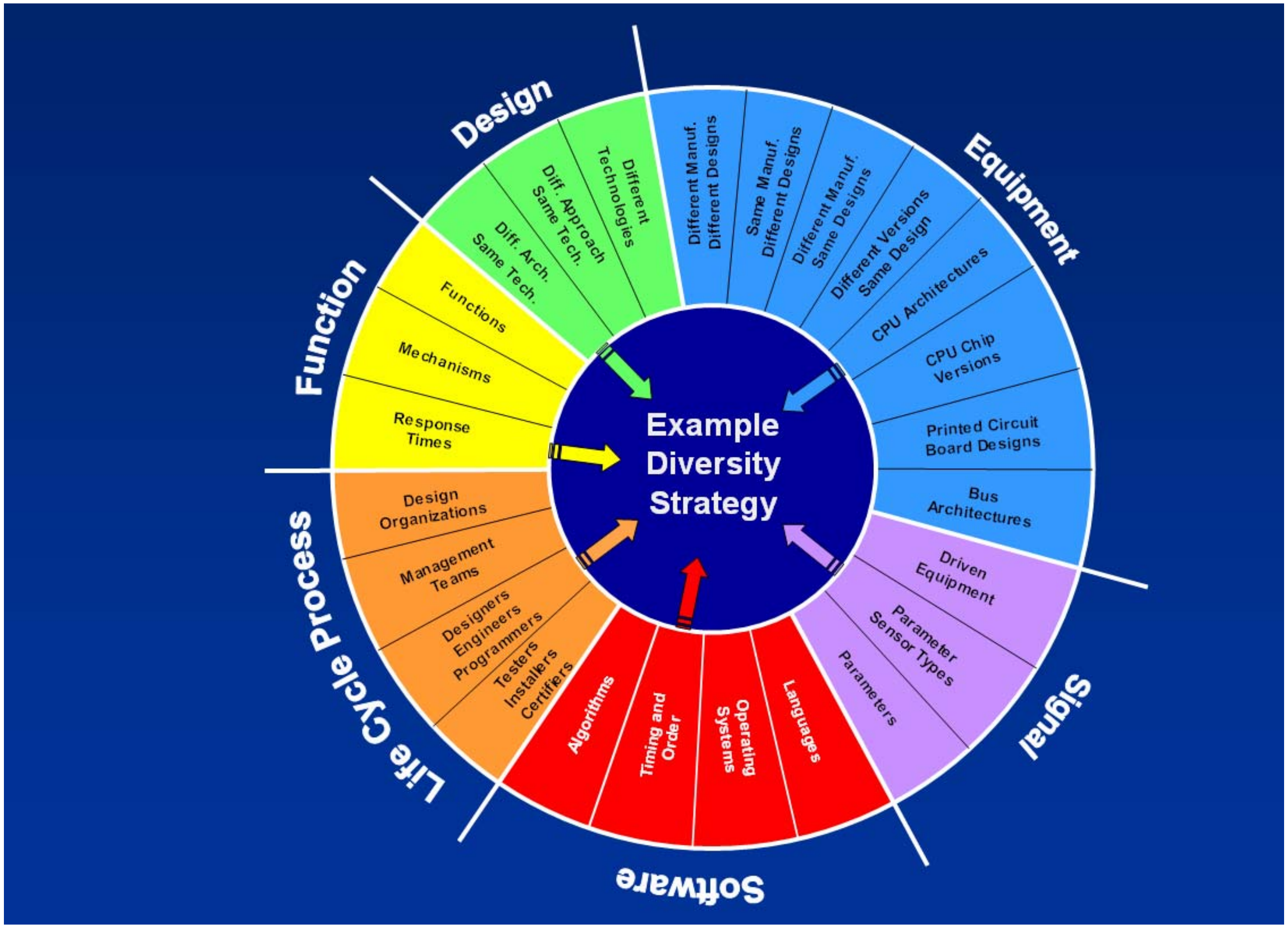
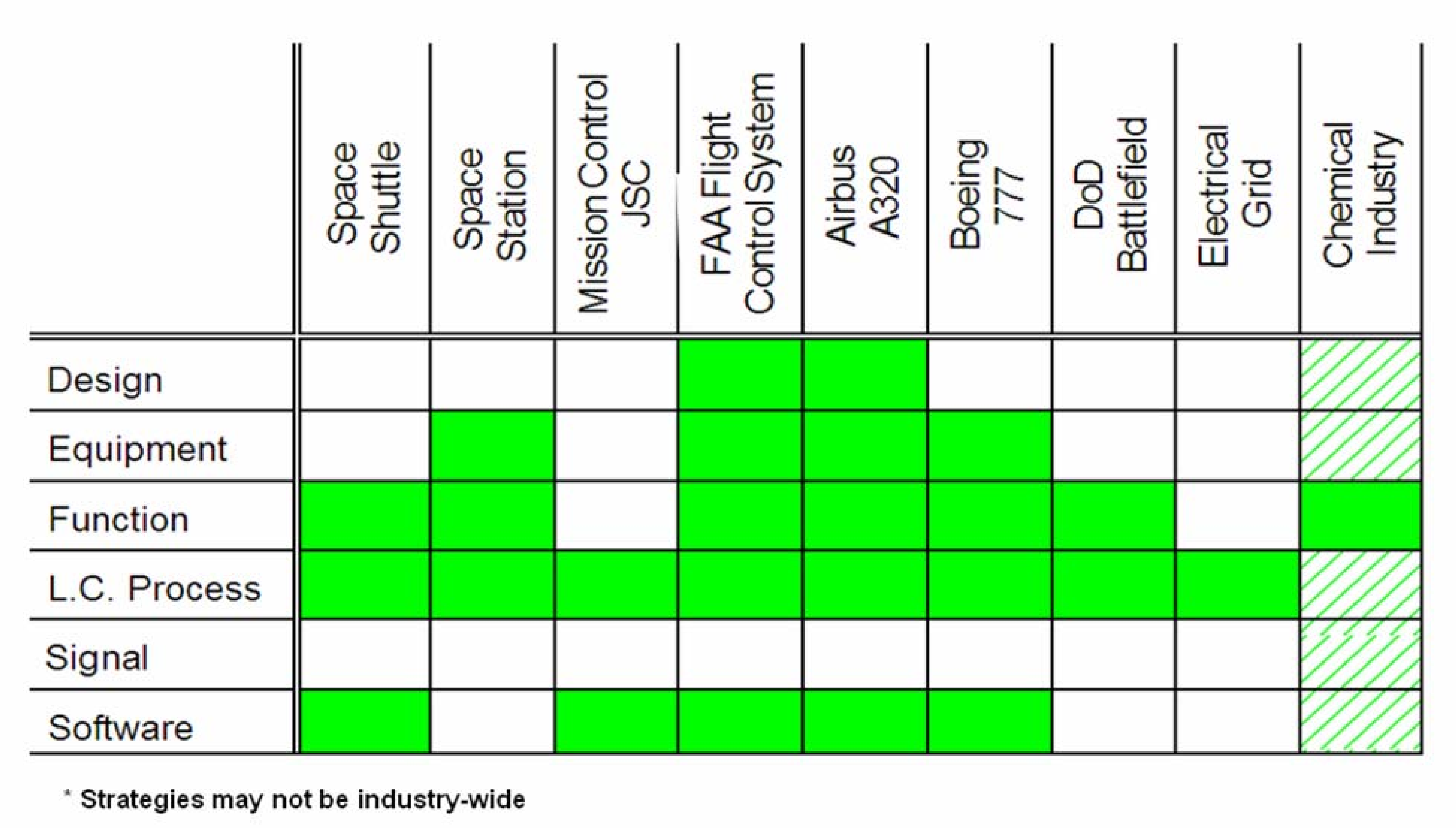


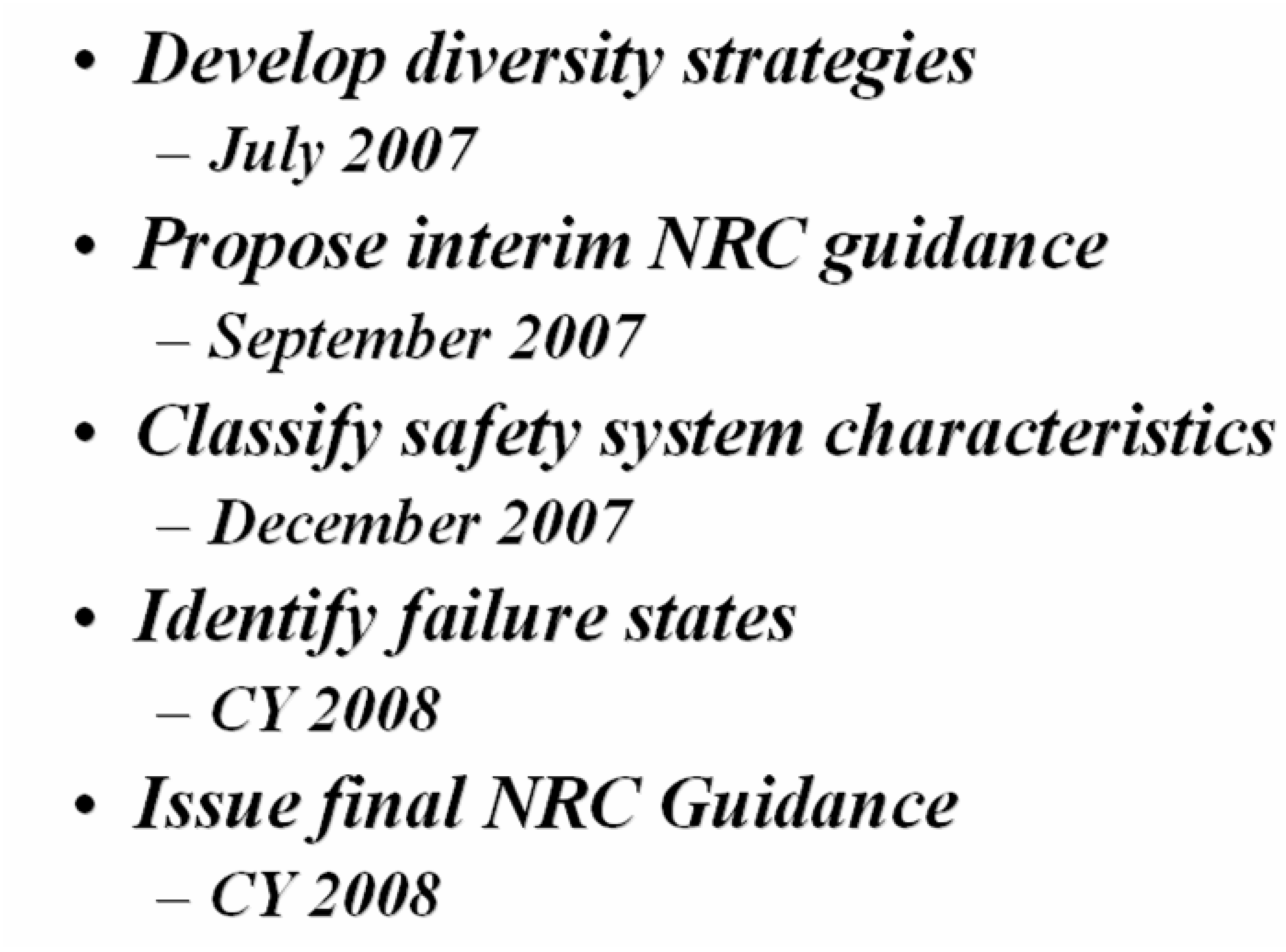
Figure 3-25 Diversity Attributes and Criteria



	Space Shuttle	Space Station	Mission Control JSC	FAA Flight Control System	Airbus A320	Boeing 777	DoD Battlefield	Electrical Grid	Chemical Industry
Design				🟩	🟩				▨
Equipment		🟩		🟩	🟩	🟩			▨
Function	🟩	🟩		🟩	🟩	🟩	🟩		🟩
L.C. Process	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	▨
Signal									▨
Software	🟩		🟩	🟩	🟩	🟩			▨

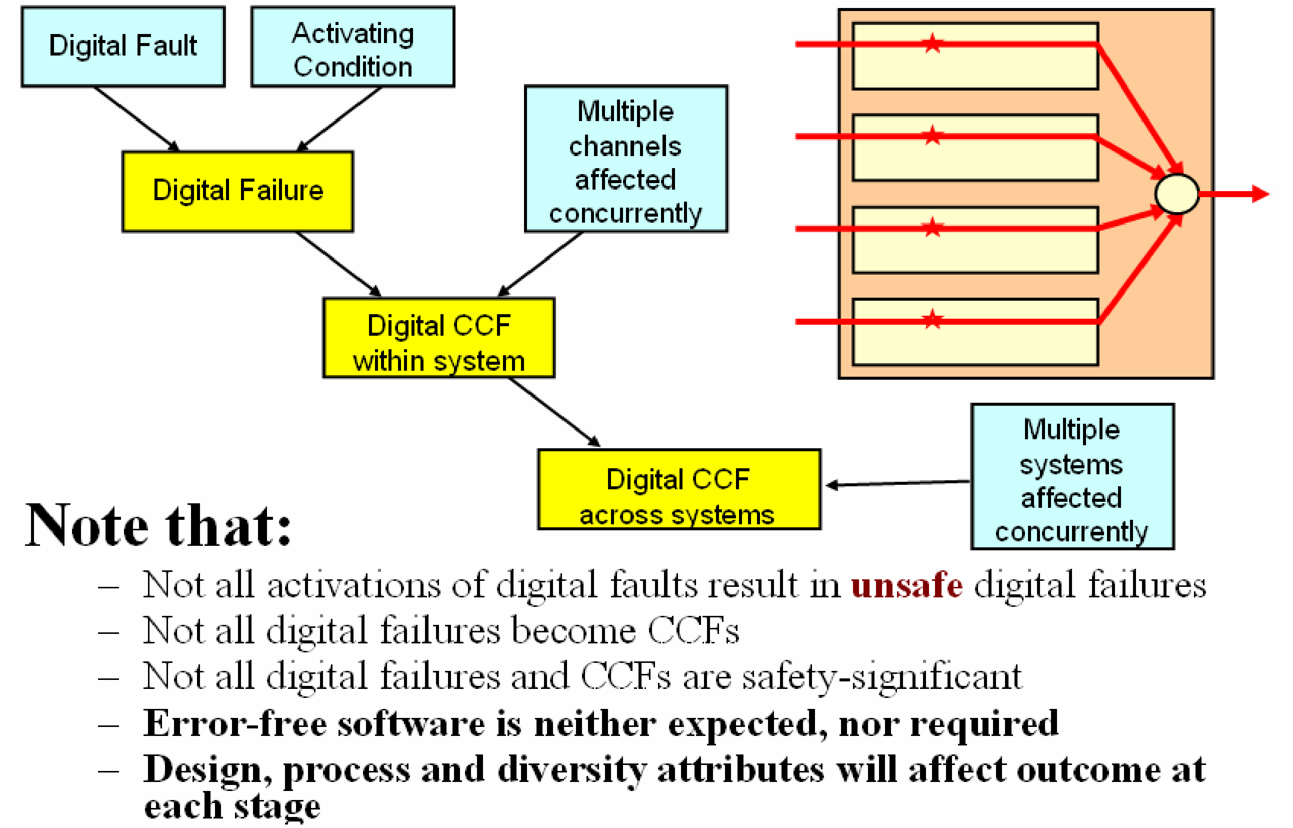
* Strategies may not be industry-wide

Figure 3-26 Summary of Diversity Strategies



- *Develop diversity strategies*
  - *July 2007*
- *Propose interim NRC guidance*
  - *September 2007*
- *Classify safety system characteristics*
  - *December 2007*
- *Identify failure states*
  - *CY 2008*
- *Issue final NRC Guidance*
  - *CY 2008*

Figure 3-27 NRC Research Schedule


Digital Fault
Activating Condition
Digital Failure
Multiple channels affected concurrently
Digital CCF within system
Digital CCF across systems
Multiple systems affected concurrently

Note that:

- Not all activations of digital faults result in **unsafe** digital failures
- Not all digital failures become CCFs
- Not all digital failures and CCFs are safety-significant
- **Error-free software is neither expected, nor required**
- **Design, process and diversity attributes will affect outcome at each stage**

Figure 3-28 Digital Failures & Digital CCFs – Necessary Ingredients