Comparison of ISO 9000 and Recent Software Life Cycle Standards to Nuclear Regulatory Review Guidance

G. G. Preckshot
J. A. Scott

Version 3.0

January 20, 1998
Comparison of ISO 9000 and Recent Software Life Cycle Standards to Nuclear Regulatory Review Guidance

Version 3.0

Prepared by:
G. G. Preckshot
John A. Scott

Prepared for
U.S. Nuclear Regulatory Commission

FESSP
Fission Energy and Systems Safety Program
Lawrence Livermore National Laboratory
Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy, and performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.
Comparison of ISO 9000 and Recent Software Life Cycle Standards to Nuclear Regulatory Review Guidance

Version 3.0
Manuscript date: January 20, 1998

Prepared by
G. G. Preckshot
John A. Scott

Lawrence Livermore National Laboratory
7000 East Avenue
Livermore, CA 94550
Prepared for
U.S. Nuclear Regulatory Commission
Abstract

Lawrence Livermore National Laboratory is assisting the Nuclear Regulatory Commission with the assessment of certain quality and software life cycle standards to determine whether additional guidance for the U.S. nuclear regulatory context should be derived from the standards. This report describes the nature of the standards and compares the guidance of the standards to that of the recently updated Standard Review Plan.
Figures

Figure 1. A standards framework based on U.S. regulation, standards used in the U.S. nuclear industry, and IEEE software engineering standards ........................................ 6
Figure 2. A standards framework based on applicable regulation and IAEA, ISO, and IEC standards ........................................................................................................... 7
Figure 3. Topics in the ISO 9000 Standards Suite. ISO 9001, ISO 9002, and ISO 9003 are nested to indicate the relationships of their scopes ....................................................... 8
Figure A1-1. Categories of Standards in the ISO 9000 Suite ..................................... 18

Tables

Table 1. Regulatory Guides on Software Engineering Standards ............................... 4
Table 2. Endorsement Topics for ISO 9001/9000-3 .............................................. 12
Table A2-1. Generic Quality Assurance Subjects .................................................. 25
Table A2-2. Criteria for ISO 9001 Contract Compatibility with 10 CFR 50, Appendix B 28
Table A2-3. Endorsement Positions for ISO 9001/9000-3 ..................................... 30
Table A3-1. Software Life Cycle Subjects for Comparison of Standards ................. 31
Table A3-2. Software Life Cycle Comparison Notes ............................................. 35
Executive Summary

The use of accepted standards has long been a part of U.S. nuclear engineering practice and several key standards covering design criteria and quality assurance have been important to nuclear power plant design in the U.S. At present, there are several emerging international standards on quality and software engineering that are relevant to nuclear safety I&C systems, but their relationship to, and usage within, the current U.S. regulatory context has not been investigated. These are the ISO 9000 suite of quality standards and new standards on software engineering practice: EIA/IEEE J-Std-016, ISO/IEC 12207, and its U.S. adaptation. This report compares these standards with the guidance in the newly updated Standard Review Plan and considers whether new or modified regulatory guidance is appropriate, given the content of the standards.

The approach used was to review the standards and classify key clauses classified under topic headings developed concurrently. The associated reviewer comments were then sorted and merged according to classification, which juxtaposed comments on clauses from different standards that addressed similar topics. Conclusions were drawn from comparing standards and regulations based on sorted topic headings, and are given in Chapters 4 and 5.

It was concluded that it may be possible for the NRC to develop guidance regarding the conditions under which products developed to the requirements of ISO 9001 would meet the requirements of 10 CFR 50 Appendix B. However, since the requirements of ISO 9001 are tailorable according to the contract covering the development of a particular product, it might be more appropriate for developers of ISO 9001-compliant products to prepare a demonstration that the quality assurance provisions of 10 CFR 50 Appendix B have been met for that product. The information provided in this report would be useful to the reviewers of such a demonstration. The key issues are discussed in Chapter 4. It is not recommended that the NRC issue guidance on ISO 9000-3, the guideline for the application of ISO 9001 to software, since this document is under revision to address shortcomings found in initial use of the guideline.

It was also concluded that the software life cycle standards addressed in this report should not be endorsed at this time. These standards are still evolving and do not add significant new material, with respect to software development, beyond what is already in the SRP. The 12207 standards are unique in addressing additional process areas, such as software process improvement, and integrating these into overall guidance for the software life cycle process. However, although aspects of these processes that are important to safety have been addressed in the SRP, some trial use and feedback of experience is necessary before the NRC considers enlarging its guidance to endorse these additional processes.
1.0 Introduction

The topics of general design criteria for nuclear power plants (NPP) and quality assurance (QA) criteria for NPPs are addressed in the regulations of the U.S. Nuclear Regulatory Commission in 10 CFR 50 Appendix A and 10 CFR 50 Appendix B. The use of accepted standards has long been a part of U.S. nuclear engineering practice, and several key standards covering design criteria and quality assurance have been important to nuclear power plant design in the U.S. The advent of digital technology and its importance to NPP instrumentation and control (I&C) systems have made standards on various aspects of software engineering increasingly important to the nuclear community. At present, there are several emerging international standards on quality and software engineering that are relevant to nuclear I&C safety systems, but their relationship to, and usage within, the current U.S. regulatory context has not been investigated. In particular, wide attention is focused on the ISO 9000 suite of quality standards and on EIA/IEEE J-Std-016, ISO/IEC 12207, and its U.S. adaptation, which deal with software engineering practice.

The goals of this study are to:

1. Compare the QA requirements of ISO 9001 with those of 10 CFR 50, Appendix B and compare the software QA requirements of ISO 9000-3 with those of the newly updated Standard Review Plan (SRP), Chapter 7.
2. Compare the EIA/IEEE J-Std-016, ISO/IEC 12207, and the EIA/IEEE version of ISO/IEC 12207 (referred to herein as US 12207) with the newly updated SRP.
3. Recommend new or modified regulatory guidance, if appropriate.

This study addresses the following questions:

1. How does the guidance in the emerging standards on software practice compare with the Standard Review Plan (Chapter 7 and its related branch technical positions) and with relevant NRC regulatory guides? Are there any aspects of this guidance that should be added to the recent update of NRC guidance? This could include either the addition of new regulatory guides or updates to the SRP, its branch technical positions, or existing regulatory guides.
2. What does compliance with the general quality requirements of ISO 9001 imply about potential compliance with Appendix B?
3. What does the use of the ISO 9000-3 guideline imply about compatibility with the Standard Review Plan (Chapter 7 and its related branch technical positions) and with relevant NRC regulatory guides?

1.1 Research Methods

The standards under study were reviewed and clauses were classified under topic headings that were developed concurrently. After classification, the associated reviewer comments were sorted and merged according to classification, which juxtaposed comments on clauses from different standards that addressed similar topics. Summaries of these studies are contained in the appendices. Conclusions were drawn from comparison of standards and regulations based on sorted topic headings.
1.2 Acronyms

ANSI American National Standards Institute
ASME American Society of Mechanical Engineers
ASQC American Society for Quality Control (now the ASQ)
BTP Branch Technical Position
CEN European Committee for Standardization
CFR Code of Federal Regulations
CMM Capability Maturity Model
EIA Electronic Industries Association
I&C Instrumentation and Control
IEC International Electrotechnical Commission
IEEE Institute of Electrical and Electronics Engineers
ISO International Organization for Standardization
NPP Nuclear Power Plant
NRC Nuclear Regulatory Commission
PESP Pre-Existing Software Product
QA Quality Assurance
RG Regulatory Guide
SEI Software Engineering Institute
SRP U.S. NRC Standard Review Plan
SSC Systems, structures, and components

1.3 Report Organization

Chapter 2 describes the regulatory context within which the comparisons of this report were performed. Chapter 3 provides a summary of the standards evaluated and Chapters 4 and 5 contain the results of the comparisons. Because of the amount of information associated with Chapters 3, 4, and 5, the details are presented in Appendices A1, A2, and A3. This permits the body of the report to focus on the results. A summary of the conclusions is given in Chapter 6.

2.0 Regulatory Background

2.1 Established Regulation and Guidance

2.1.1 10 CFR 50

10 CFR 50.55a (a)(1), “Codes and Standards,” [10 CFR 50, 1994] requires in part that structures, systems, and components be designed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR 50.55a(h) requires protection systems to meet the requirements of IEEE Std. 279-1971. Section 4.3 of IEEE Std. 279 requires in part that quality levels be achieved through specification of requirements known to promote high quality. Regulatory Guide 1.153, Rev. 1, endorses IEEE Std. 603-1991 as an acceptable alternative to IEEE Std. 279-1971.
Section 5.3 of IEEE Std. 603 requires in part that safety system equipment be designed, inspected, tested, and maintained in accordance with a prescribed quality assurance program.

10 CFR 50 Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants,” requires licensees to develop programs to assure the quality of nuclear power plant design, construction, and operation. It was implemented in 1970 and contains 18 criteria that must be part of the quality assurance program for safety-related systems and components. These criteria were based on experience from military, the National Aeronautics and Space Administration, commercial nuclear projects, nuclear reactor experience of the Atomic Energy Commission [NUREG-1055, 1984]. All of the 10 CFR 50 Appendix B criteria are important for the discussions on quality assurance and software life cycle processes in this report. In the latter area, several of the criteria are particularly important. Appendix B, Part I, “Organization,” and Part II, “Quality Assurance Program,” require an applicant to establish a quality assurance program for structures, systems, and components that prevent or mitigate accidents. Part III, “Design Control,” requires that measures be established so that applicable regulatory requirements and the design basis are correctly translated into specifications, drawings, procedures, and instructions. Part X, “Inspection,” requires that a program of inspection be established to verify conformance with instructions, procedures, and drawings. Part XI, “Test Control,” requires that a test program be established and that testing required to demonstrate that structures, systems, and components will perform satisfactorily in service is identified and performed with acceptable results. Finally, Part XVII, “Quality Assurance Records,” requires that sufficient records be maintained to furnish evidence of activities affecting quality.

2.1.2 Standard Review Plan and Regulatory Guides

The Standard Review Plan (SRP) [NUREG-0800 Chapter 7, 1997] provides guidance to an NRC reviewer on reviewing a license application, license amendment, permit, renewal, extension, design certification, or topical report. Branch technical positions provide additional guidance to the reviewer on key, specific topics and are packaged within the SRP. Regulatory guides (RG) describe methods acceptable to the NRC staff for complying with the Commission’s regulations.

The primary regulatory guide covering digital NPP safety systems is RG 1.152 Rev. 1, which endorses IEEE Std. 7-4.3.2-1993 (see Figure 1). IEEE Std. 603-1991, endorsed by RG 1.153 Rev. 1, provides general design guidance that is applicable to all safety systems, including digital safety systems.

2.2 Recent Guidance Updates

The SRP and its branch technical positions were recently revised to account for the impact of digital systems technology. New regulatory guides were issued on acceptable ways to conduct particular software processes that are important for software quality.

2.2.1 Chapter 7 of the Standard Review Plan

Major revisions were made to SRP Chapter 7, “Instrumentation and Controls,” in 1997. The introduction and Section 7.1 provide a general discussion of digital safety systems and strategies for their review. A new appendix to this section describes the review process for digital systems in detail. This appendix is supported by new branch technical positions, and refers to the new regulatory guides as examples of methods acceptable to the NRC staff for implementing certain software processes. Two new sections were added on diverse
actuation systems and digital data communication, and the remaining sections were updated to account for the impact of digital systems.

2.2.2 BTP HICB-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”

BTP HICB-14 was added to provide the reviewer with detailed information and acceptance criteria on the software elements of digital systems. It is organized into discussions on planning software related activities, implementation of the planned activities, and the design outputs produced by the software life cycle processes.

2.2.3 Other Branch Technical Positions

Several other new BTPs were produced that focus on digital system issues that, while they are important considerations in software development, are not directly related to the emerging standards that are the subject of this report. These address the topics of diversity and defense-in-depth, self-test and surveillance testing, the use of programmable logic controllers, and the evaluation of digital system architecture and real-time performance.

2.2.4 Regulatory Guides on Software Engineering Standards

Six new regulatory guides endorsing eight software engineering standards were developed by the NRC staff. The standards endorsed are part of the standards framework shown in Figure 1 and are not specific to nuclear power plants. The regulatory guides endorse the standards, with certain exceptions, as methods acceptable to the NRC staff for accomplishing certain key software engineering activities. These new regulatory guides complement RG 1.152, Rev. 1. The endorsed standards and corresponding new regulatory guides are listed in Table 1.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Subject</th>
<th>Reg. Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Std. 1012-1986</td>
<td>Verification and Validation Plans</td>
<td>1.168</td>
</tr>
<tr>
<td>IEEE Std. 1028-1988</td>
<td>Software Reviews and Audits</td>
<td></td>
</tr>
<tr>
<td>IEEE Std. 828-1990</td>
<td>Software Configuration Management Plans</td>
<td>1.169</td>
</tr>
<tr>
<td>IEEE Std. 1042-1987</td>
<td>Software Configuration Management Guide</td>
<td></td>
</tr>
<tr>
<td>IEEE Std. 830-1993</td>
<td>Software Requirements Specifications</td>
<td>1.170</td>
</tr>
<tr>
<td>IEEE Std. 1008-1987</td>
<td>Software Unit Test Plans</td>
<td>1.171</td>
</tr>
<tr>
<td>IEEE Std. 829-1983</td>
<td>Software Test Documentation</td>
<td>1.172</td>
</tr>
<tr>
<td>IEEE Std. 1074-1995</td>
<td>Software Life Cycle Development</td>
<td>1.173</td>
</tr>
</tbody>
</table>

3.0 Background on Standards

The standards reviewed in this report have a substantial prior history, and several of them underwent name or designation changes during development. It is important to identify the standards being reviewed for endorsement, and their antecedents, to provide context for the comparisons of this report. The following sections summarize the historical context of the
two sets of standards reviewed and identify the probable future evolution of these documents; a more detailed discussion is given in Appendix A1. Conclusions regarding compatibility with NRC guidance are given in Chapters 4 and 5.

3.1 Standards Frameworks

Frequently, standards dealing with quality or software processes do not stand alone. Instead, the subjects covered are related to the coverage of other standards in a suite of standards. The suite is structured, to some extent, to minimize overlap and inconsistency among the members of the suite [Scott, Preckshot, 1996]. Such a suite is called a standards framework in this document.

Individual standards from different frameworks often have different coverage and levels of detail although the nominal subject may be the same or nearly the same. This is true of the standards frameworks depicted in Figures 1 & 2 for digital computers and software used in nuclear power plants. To use a combination of standards drawn from the two frameworks, significant gaps and overlaps in guidance and scope would have be resolved. ISO member nations, including the U.S., are working to resolve differences, which could potentially lead to a single guidance framework. There seems to be strong sentiment to move toward the ISO framework; with respect to ISO/IEC 12207, a U.S. version is being developed that adds significant additional material.

The analysis of standards in this document is based on a snapshot of the current versions of the standards reviewed. Therefore, the conclusions and data of this report have a limited lifetime.
Figure 1. A standards framework based on U.S. regulation, standards used in the U.S. nuclear industry, and IEEE software engineering standards
Figure 2. A standards framework based on applicable regulation and IAEA, ISO, and IEC standards

3.2 The ISO 9000 Quality Standards

ISO is an international standards organization comprised of member nations, each represented by a standards organization from that nation. The American National Standards Institute (ANSI) is the ISO member body representing the U.S. ISO develops standards on a wide range of topics with the goal of facilitating international trade and cooperation; those ISO standards dealing with quality assurance and quality management are known as the ISO 9000 standards.

The structure of the ISO 9000 series of standards is complex and is described in detail in Appendix A1. For the purposes of this discussion, it should be noted that (1) the three ISO 9000 quality standards have a nested scope, as illustrated in Figure 3, with ISO 9001 being the only one encompassing design and development, and (2) the guideline, ISO 9000-3, provides guidance on applying ISO 9001 to software.
ISO 9001 focuses on standardized supplier quality assurance practices upon which the purchaser evaluates whether products will meet the purchaser’s quality requirements. Formal certification by third party registrars is used to increase purchaser confidence that the supplier is in compliance with ISO 9001.

### 3.2.1 ISO 9001, ISO 9000-3, and Software Development

The ISO 9000-3 guideline is structured differently from the ISO 9001 standard. Because of resulting confusion, the former is currently being revised, with one objective being to make the connection between the guide and standard more obvious. Neither document deals with software process in any depth. ISO 9000-3 attempts to fit the ISO 9001 orientation of control of manufactured product to the development of software products. It is not clear if or how the revision will deal with software process issues.

There is a key difference between ISO 9000-3, a quality guideline, and software engineering standards such as ISO/IEC 12207, namely, the former addresses software from a quality perspective while the latter address quality from a software processes perspective. This distinction helps to explain the difference in level of software process detail found between ISO 9000-3 and the software engineering standards.
3.2.2 Variability Issues

ISO 9001 has some variability in application, especially for companies producing software. There are a variety of reasons for this, including: (1) the fact that many of its provisions are general and can be interpreted differently, (2) different national standards bodies can develop their interpretation and certification mechanisms for their national application of the standard, (3) variability in certification audits because of confusion over the relationship of ISO 9000-3 to ISO 9001, and (4) variability in certification audits because of pressures on the auditing organizations.

3.2.3 Contract Orientation of ISO 9000

ISO 9001 is designed for suppliers who contract to supply goods or services to purchasers as described by specification in the contract. The intended quality level and functions supplied are contained in the contract; ISO 9001 certification only certifies that the supplier has the quality assurance programs in place to meet contract specifications. Therefore, ISO 9001 certification does not, by itself, imply a minimal level of quality. The contract provisions must be known before this can be determined.

3.2.4 Relationship to NRC Guidance Structure

The NRC guidance with which ISO 9001 and ISO 9000-3 are most directly comparable is Appendix B of 10 CFR Part 50. Both documents cover the quality subjects listed in Table A2-1 of Appendix A2. ISO 9000-3 can also be compared to BTP HICB-14 of Chapter 7 of the SRP and NRC regulatory guides on software engineering standards. However, the utility of ISO 9000-3 is dependent upon the compatibility of ISO 9001, as applied under a given contract, with Appendix B.


ISO 9001 covers all of the quality-related activities of an organization, regardless of the technologies involved. For software engineering, standards have evolved to assist in producing high-quality systems and components; however, their requirements must be consistent with the overall quality plan of the organization. Such technology-specific standards should not be considered to be “stand-alone” quality plans.


3.3.1 Purpose and Structure

ISO/IEC 12207 blends the contractual viewpoint of ISO 9001 and the software life cycle process viewpoint of IEEE 1074, and adds material on roles related to software

¹ This standard is in draft as of this writing.
development, such as the roles of acquirer and organizational management. EIA/IEEE US 12207\textsuperscript{2,3} adopts this broader perspective and adds considerable detail, in part, through its references to supporting software engineering standards\textsuperscript{4}. Part 0 of EIA/IEEE US 12207 is ISO/IEC 12207 in its entirety with six added annexes, four of which are normative. Part 1 is a guide on software life cycle data and Part 2 provides guidance on the implementation of Part 0. The U.S. version ‘tightens’ the standard considerably; however, it has not been approved by consensus ballot as of this writing.

In contrast to ISO 9001, which views quality from the traditional statistical process control standpoint, the 12207 standard reflects a view that controlling software life cycle processes underlies software quality. The 12207 standard is oriented toward acquirer–supplier agreements and is applicable to software development life cycles in support of an agreed level of software quality assurance. The 12207 standard cites ISO 9001 as a normative reference, and supports ISO 9001 as an adjunct standard.

EIA/IEEE J-Std-016 is also based on the importance of software life cycle processes but focuses primarily on the developer role. There is some feeling that EIA/IEEE J-Std-016 exists primarily to support legacy software QA programs for embedded military systems, and to support defense contractors with software development infrastructures designed to the Mil-Std-2167A environment. It was “published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of an EIA/IEEE Standard.” This standard was issued, by the IEEE, as a trial use standard in 1995. Trial use standards are automatically withdrawn by the IEEE two years following their issue.

It is unclear how long these standards will exist in their present forms considering the differences between the ISO/IEC and U.S. versions of 12207 and the fact that the J-Std-016 is an interim standard.

### 3.3.2 Relationships to the NRC Guidance Structure

The primary elements of SRP Chapter 7 related to the areas covered by these standards are BTP HICB-14, SRP Chapter 7 Appendix 7.0-A (“Review Process for Digital Instrumentation and Control Systems”), and Regulatory Guides 1.168 through 1.173. BTP HICB-14 presents acceptance criteria for software planning, implementation and design outputs. The regulatory guides address specific software topics by endorsing certain software engineering standards and ensure compatibility of the endorsed standard with Appendix B quality requirements. Of particular interest is RG 1.173 on IEEE Std. 1074-1995, which addresses the development of a software life cycle for a particular software effort.

The software life cycle standards considered in this report allow for two situations: one in which the software and its computer hardware comprise the entire system, and another in which the software under development is part of a larger computer-based system, such as

\textsuperscript{2} The past designations of these standards causes some confusion. The existing EIA/IEEE J-Std-016 was also known as IEEE Std. 1498 or EIA 640. Past drafts of the document intended to become US 12207 were labeled as revisions of EIA/IEEE J-Std-016. The document that will become the three-part US 12207 was variously known as IEEE Std. P1448 and EIA PN3764.

\textsuperscript{3} In the remainder of this document, references to “the 12207 standard” refer to the content of ISO/IEC 12207, which is also Part 0 of EIA/IEEE US 12207. References to the specific standards will be made when necessary.

\textsuperscript{4} Over 50 standards are referenced, including standards from the IEEE, ISO, ISO/IEC, and ASTM (American Society for Testing and Materials).
an embedded control system. The latter is typically the case for NPP I&C systems. Since the life cycle standards are not specific to an industry, the system-level aspects can only be addressed in generic ways. The comparisons in this report are made with an understanding that guidance on nuclear system design derives, in part, from the U.S. standards IEEE Std. 279-1971, IEEE Std. 603-1991, and IEEE Std. 7-4.3.2-1993. Also, in this context, the role of the higher-level quality standard, ISO 9001, cited by ISO/IEC 12207, is replaced by the applicable version of the nuclear quality standard, ASME NQA-1.

4.0 Comparison of ISO 9001/9000-3 to NRC Guidance

Appendix A2 contains the details of the review of ISO 9001 compared to 10 CFR 50, Appendix B and of ISO 9000-3 compared to BTP HICB-14. This section summarizes the findings of Appendix A2, the most important of which is that it may be possible for the NRC to develop guidance on ISO 9001 but, since the implementation of ISO 9001 is dependent on the governing contract, it may be more appropriate that developers of a given ISO 9001 product demonstrate that the requirements of 10 CFR 50, Appendix B, have been met. The comparisons made in this report would be helpful in reviewing such a demonstration. It is premature to consider endorsement of ISO 9000-3.

4.1 ISO 9001 and 10 CFR 50, Appendix B

ISO 9001 cannot be changed to make it directly equivalent to Appendix B. This is because the ultimate quality requirements that motivate an ISO 9001 supplier are those in a contract, while the Appendix B motivation for quality comes from reactor safety considerations delineated by regulation. However, ISO 9001 is still useful if the terms of the contract are acceptable. Appendix B and the provisions of ISO 9001 were compared using the subjects of Table A2-1 as points of comparison. Table A-2 summarizes the issues that would need to be addressed in a contract between an applicant/licensee and an ISO 9001 supplier to ensure that the regulations in 10 CFR 50, Appendix B were met. Table A2-2 was also compared with a study done by Virginia Electric and Power Company [Carter, 1996] and the ultimate conclusion is the same: the differences between ISO 9001 and 10 CFR 50, Appendix B are small enough to be surmountable.

4.2 ISO 9000-3 and BTP HICB-14

ISO 9000-3 and BTP HICB-14 both present criteria for software quality, but BTP HICB-14 is substantially more detailed and is organized in a life cycle activities format. ISO 9000-3 addresses staged development to a limited extent, but does not detail activities to the extent found in BTP HICB-14 or IEEE Std. 1074-1995. Other guidelines in the 9000 suite address specific topics (e.g., ISO 10007 on configuration management, ISO 9004-4 on quality improvement, ISO 10005 on quality plans, and ISO 10006 on project management). None of these additional guidelines is specifically addressed to software or digital systems.

ISO 9000-3 cannot be used without ISO 9001. Since it is expected that ISO 9000-3 will be revised to reconcile its structure with that of ISO 9001, any potential endorsement of ISO 9000-3 would depend upon showing how the ISO 9001-certified product meets the

---

6 IEEE Std. 7-4.3.2-1993 is endorsed by NRC Regulatory Guide 1.152, Revision 1.
7 NQA-1-1983 was endorsed by NRC Regulatory Guide 1.28 at a time when the NQA standards (NQA-1, NQA-2, and NQA-3) existed as separate entities. In the 1994 revision, these separate entities were combined and the aggregate was renamed NQA-1.
requirements of 10 CFR 50 Appendix B, as well as on the final form of ISO 9000-3. Table 2 identifies topics needing special consideration in developing an endorsement for ISO 9000-3.

### Table 2. Endorsement Topics for ISO 9001/9000-3

<table>
<thead>
<tr>
<th>Topic</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Acceptance criteria, design bases, regulatory requirements.</td>
</tr>
<tr>
<td>Safety Orientation</td>
<td>Safety analyses, corrective action notification requirements, research and development of new technical approaches, environmental qualification, tying quality to safety, applicability of QA program to identified SSCs.</td>
</tr>
<tr>
<td>Independence</td>
<td>Independence of verifiers and checkers, inspectors, and QA auditors. Authority and freedom from cost and schedule pressures of management responsible for quality activities.</td>
</tr>
<tr>
<td>Testing</td>
<td>Testing environments, procedures for non-conforming SSCs in test and inspection.</td>
</tr>
<tr>
<td>Control</td>
<td>Applicable codes and standards, personnel qualification, design change control commensurate with control on original design.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Location, retention, and availability of quality records.</td>
</tr>
</tbody>
</table>

### 4.3 Conclusions

Given the widespread interest in the ISO 9000 series of quality standards, it may be useful for the NRC, and for developers of ISO 9000-compliant nuclear products, to understand their relationship to the U.S. nuclear regulatory context. The comparisons above indicate that establishing the correspondence, subject to a review of the contract governing ISO 9001 implementation, between ISO 9001 and 10 CFR 50 Appendix B is possible but that ISO 9000-3 will be more difficult to address until ISO 9000-3 is revised.

### 5.0 Comparison of Software Process Standards to NRC Guidance

#### 5.1 Software Life Cycle Standards Review

Appendix A3 contains a detailed summary of a keyword comparison of three software life cycle standards: ISO/IEC 12207, EIA/IEEE US 12207 Draft (US 12207), and EIA/IEEE J-Std-016 (J-Std-16). The three standards were compared with NRC guidance contained in SRP Chapter 7, Appendix 7.0-A, BTP HICB-14, and Regulatory Guides 1.168 through 1.173. The topics used as points of comparison are given in Table A3-1 and the comparison notes, arranged by topic, are given in Table A3-2.

#### 5.2 Conclusions

##### 5.2.1 ISO/IEC 12207

It appears that this standard, particularly as it evolves, will have an important impact on international acceptability of software products. The scope of the standard is broader than
most and recognizes areas that frequently receive too little emphasis, e.g., operation and maintenance and the topic of software process improvement. Feedback of experience, indicating general acceptance of these aspects of the standard, is needed before considering NRC adoption of such guidance. For this and a variety of other reasons discussed in Appendix A3, including compliance, level of detail, and the normative reference to ISO 9001, it is not recommended that this standard be considered for regulatory guide endorsement at this time. The development of NRC guidance on ISO 9001 will address the latter concern. The standard will still be a useful reference for safety critical software developments, in part because of its focus on acquirer, supplier, operations and maintenance, and management processes.

5.2.2 EIA/IEEE US 12207 Draft

This standard has not been issued as of this writing and there is no experience with its use. Its incorporation of material beyond that of ISO/IEC 12207 helps to address the issues associated with level of detail and compliance. Other issues associated with ISO/IEC 12207, such as the acceptability of the broader scope and the normative reference to ISO 9001, still exist. It is also unclear how ISO/IEC 12207 might evolve based on US 12207 and other country-specific implementations. The standard is largely compatible with NRC regulatory guidance and could be endorsed at the proper time, given that it is considered part of an overall framework of standards to be employed for the development of high-integrity software. It is premature to consider endorsement at this time.

5.2.3 EIA/IEEE J-Std-016

Since this standard does not add anything substantially different than US 12207 and since the future of the standard is uncertain, it should not be considered for endorsement at this time. In addition, since its material is organized quite differently than the SRP, it is likely that a regulatory guide would become enmeshed in information mapping and interpretations, possibly adding more confusion than value.

6.0 Summary

Since ISO 9001 is receiving considerable attention and use, it is likely that the NRC will need to evaluate products developed to its guidance. Since the impact of ISO 9001 requirements are determined in part by the acquirer-supplier contract, it is recommended that developers of ISO 9001-compliant products demonstrate that the requirements of 10 CFR 50, Appendix B, have been met for the products in question. The material in this report will be useful in reviewing such a demonstration.

The planned future version of ISO 9000-3 should be evaluated after it is issued. Endorsing ISO 9000-3 alone is not recommended for three reasons:

1) It is a guide, not a normative standard
2) It is currently under revision
3) The normative standard is ISO 9001. Endorsing ISO 9000-3 could be seen as endorsing ISO 9001 for software only, a position that would be difficult to support

As noted in section 5.2, there appears to be little benefit in developing endorsements of the ISO/IEC 12207, EIA/IEEE US 12207, or EIA/IEEE J-Std-16 software life cycle standards at this time, but there is a longer-term possibility that US 12207 might be endorsed depending on how the standard evolves. Depending on the future feedback of experience, it may be appropriate to incorporate guidance into the SRP on new roles recognized in the
12207 standard, such as the acquirer, or on the general topic of software process improvement. The direction of evolution is uncertain because of the large difference between the US version of 12207 and the international version.
References


Appendix A1 - ISO 9000 and the Software Life Cycle Standards

A1-1.0 The ISO 9000 Quality Standards

ISO is an international standards organization comprised of member nations, each represented by a standards organization from that nation. The American National Standards Institute (ANSI) is the ISO member body representing the U.S. ISO develops standards on a wide range of topics with the goal of facilitating international trade and cooperation; those ISO standards dealing with quality assurance and quality management are known as the ISO 9000 standards.

A1-1.1 History

The ISO 9000 suite of standards traces its roots back to a 1959 Department of Defense quality standard, MIL-Q-9858 [Bamford and Deibler, 1993]. NATO adopted the program and issued its own series of standards, AQAP1, AQAP4, and AQAP9. The British Standards Institute (BSI) issued commercial versions of the NATO standards as BS 5750, Parts 1–3. These three standards eventually became, with evolutionary changes, ISO 9001, ISO 9002, and ISO 9003 in 1987, and were updated in 1994.

A1-1.2 Purpose and Structure

The ISO 9000 series addresses quality issues from two viewpoints [ISO, 1994 p14]: (1) the viewpoint of a purchaser interested in gaining confidence in the supplier’s quality systems (external quality assurance) and, (2) the viewpoint of the supplier seeking to achieve purchaser satisfaction (quality management). From a regulatory perspective, the external quality assurance viewpoint is a primary consideration. The constituent standards of the ISO 9000 series, and their numbering scheme (which is not intuitively obvious) have evolved over the last ten years, but they can be grouped into the general areas of quality assurance, quality management, and quality technology as shown in Figure A1-1, with the ISO 9000-1 guideline providing guidance on applicability of the various standards.
None of the ISO 9000 standards is specific to nuclear power plants. The topic of each element of the ISO 9000 suite is depicted in Figure 3 of the main report.

The elements of the suite that are of primary importance with respect to organizational quality assurance are the standards dealing with quality assurance requirements (ISO 9001, 9002, and 9003). The primary quality assurance requirements standard of interest for this report is ISO 9001 since it is the only standard in the suite that includes design control within its scope. ISO 9002 and ISO 9003 address subsets of the ISO 9001 topics. ISO 9002 is identical to ISO 9001 except that all quality system requirements for design control have been deleted. Of the 9000-x guidelines, ISO 9000-3 is of interest to this report since it provides guidance for applying ISO 9001 to software elements of products. Guides in the technology category (for example, project management, configuration management, quality plans) cover subjects important to software development, but which are applicable generally to all product categories.

ISO 9001 focuses on standardized supplier quality assurance practices upon which the purchaser can evaluate whether products will meet the purchaser’s quality requirements. The use of formal certification by third party registrars is used to increase purchaser confidence that the supplier is in compliance with ISO 9001. Reciprocity holds; registrars recognized by one nation’s national standards body are recognized by the national standards bodies of other, participating nations.
The three QA requirements standards are the ones used by registrars for judging whether an applicant for ISO 9000 registration meets the requirements for registration. ISO 9001 is the most general of these, addressing design, development, production, installation, and servicing. ISO 9002 addresses production, installation, and servicing. ISO 9003 addresses final inspection and test. ISO 9001 is intended to be used where a contract between a supplier and a purchaser requires the demonstration of the supplier’s capability to design, develop and supply the specified product(s). ISO 9002 is intended to be used where a contract between a supplier and a purchaser requires the demonstration of the supplier's capability to control the processes that determine the acceptability of the specified product(s). ISO 9003 is intended to be used where a contract between a supplier and a purchaser requires the demonstration of a supplier’s capability to detect and properly dispose of any product non-conformance during final inspection and test. Of the three organizational quality assurance standards, only ISO 9001 is applicable to software development because it alone addresses design.

ISO 9004 is a series of guides for implementing quality management functions and is of primary interest to those concerned with the quality management viewpoint. These guides serve the three primary standards by providing guidance on a variety of general quality system management topics. The 10000 series guidelines cover quality technology topics that are generally useful for quality systems (such as measuring equipment) but which are not specifically management topics. Some guidelines that were originally numbered in the ISO 9004 series have been renumbered in the 10000 series.

A1-1.2.1 ISO 9001, ISO 9000-3, and Software Development

The standard that applies to a contract to develop any product is ISO 9001. ISO 9000-3 is a guide for applying ISO 9001 to software products. The guide is structured differently from the standard. As a result of the mismatch in organization between ISO 9000-3 and ISO 9001, the former is currently being revised. One of the objectives of the revision is to make the connection between the guide (ISO 9000-3) and the normative standard (ISO 9001) more obvious. Also, neither document deals with software process in any depth. ISO 9001 comes from a background concerned with statistical control of manufactured product, where design and manufacturing are separate processes. ISO 9000-3 attempts to fit this orientation to the development of software products, where the closest approximation to manufacturing is duplication of finished software product onto delivery media. It is not clear if or how the revision will deal with software process issues.

Considerable effort has been expended in comparisons of the SEI software capability maturity model (CMM) with the software guidance provided by ISO 9000-3. For example, see Bamford and Deibler [1993]. Comparisons have been at the certification level by comparing certification questions or issues. These comparisons define areas of overlap as well as differences in scope and serve to underscore a key difference between ISO 9000-3, a quality guideline, and software engineering standards such as ISO/IEC 12207: the former addresses software from a quality perspective while the latter address quality from a software processes perspective. This distinction helps to explain the difference in level of software process detail found between ISO 9000-3 and the software engineering standards.

A1-1.2.2 Variability

ISO 9001 has some variability in application, especially for companies producing software. There are a variety of reasons for this, including: (1) the fact that many of its provisions are general and can be interpreted differently, (2) different national standards bodies can develop their interpretation and certification mechanisms for their national application of the standard, (3) variability in certification audits because of confusion over the relationship of
ISO 9000-3 to ISO 9001, and (4) variability in certification audits because of pressures on the auditing organizations.

Regarding national implementations of the standards, it is the intent of ISO, expressed in Annex C of ISO 9000-1:1994, that national or regional implementations not modify the requirements of the standard itself. However, this compliance is voluntary and driven primarily by market pressures. The U.S. implementation of ISO 9001, ANSI/ASQC Q9001-1994, corresponds word-for-word with the international standard. Even if the standard is adopted without modification, additional requirements may be added. For example, in the European Union, additional product certification requirements may apply, such as those required to obtain the CE Mark⁸. Similarly, the UK has developed the TickIT interpretation of ISO 9001 for software. The certification mechanisms themselves can also add variability. Certification as an ISO 9001 supplier takes approximately two years and can be a relatively expensive process. Maintaining a certification means performing internal audits and submitting to surveillance audits by the registrar. This means that interpretation of what it means to be an ISO 9001 supplier is, to some extent, under control of the certifying agencies.

Registrars are nominally under control of a national standards body. In the U.S., this top-level body is the American National Standards Institute (ANSI), and in other countries the top-level body can be a national or regional body such as the European Committee for Standardization (CEN).

Software certification audits vary since there is no one-for-one correspondence between the clauses of ISO 9000-3 and the clauses of ISO 9001. Although a table in the current version of ISO 9000-3 gives a mapping of section numbers, it is not clear from this table how or which provisions of ISO 9001 were translated to produce the guidelines of ISO 9000-3. This has resulted in interpretations of ISO 9000-3 which may not be entirely consistent with ISO 9001, and some confusion among registrars as to whether the standard, ISO 9001, or the guideline, ISO 9000-3, is the normative reference for software. Walker [1997] notes that “There is little commonality in the approach to auditing software companies against the requirements of ISO 9001,” and “Remarkably there is no internationally (or nationally) agreed checklist against which compliance of software systems to the requirements of ISO 9001 can be assessed.” Bamford and Deibler [1997] note that “Since 1991, it has been virtually impossible for the reader to trace the complete relationship between ISO 9001 and ISO 9000-3.”

ISO 9000-3 is intended to be guidance for applying ISO 9001 to suppliers of software. Because it is guidance, it is not mandatory, and compliance is supposed to be judged by the degree to which provisions of ISO 9001 are met. In spite of this, because of the mismatch in organization between ISO 9001 and ISO 9000-3, provisions of ISO 9000-3 are sometimes independently applied by registrars, making this guidance ade facto mandatory standard.

Finally, there appears to be some variability in audits as a result of pressures placed on the third party auditors. Bamford and Deibler [1997] identified pressures originating from the business environment and from the audited clients. In the former, there are pressures to reduce the costs of audits that can affect the adequacy of the audits performed. In the latter, clients can focus on pleasing an auditor rather than on implementing the quality systems themselves.

---

⁸ The CE, “Conformite European,” Mark signifies that a product has met all certification requirements for marketing the product in the European Union. These requirements are likely to include a registered ISO 9000 quality assurance system as well as various European Union directives (EN directives).
A1-1.2.3 Contract Orientation of ISO 9000

The ISO 9000 suite of standards is widely used in Europe and use is increasing in the U.S. because of competitive pressure for selling products in Europe. Because of the internationalization of commerce, the NRC may encounter increasing number of submissions citing ISO 9001 compliance.

ISO 9001 is designed for suppliers who contract to supply goods or services to purchasers as described by specification in the contract. The intended quality level and functions supplied are contained in the contract; ISO 9001 certification only certifies that the supplier has the quality assurance programs in place to meet contract specifications. If the supplier is unable to meet contract requirements, the supplier is supposed to determine this fact by contract review and decline the contract.

This means that ISO 9001 certification does not, by itself, imply a minimal level of quality. The contract provisions must be known before this can be determined. An ISO 9001-certified supplier could agree to supply product of which individual examples only had an 80% chance of meeting functional specifications, if this were in the supply contract. As long as deliveries of product continued to meet the statistical contract specification, the supplier would be delivering conforming product.


ISO/IEC 12207-1995, “Information Technology—Software Life Cycle Processes,” EIA/IEEE US 12207, “U.S. Implementation of ISO/IEC 12207 International Standard,” and EIA/IEEE J-Std-016-1995, “Standard for Information Technology Software Life Cycle Processes Software Development, Acquirer-Supplier Agreement (Issued for Trial Use),” are specific to software engineering and address top-level software engineering issues by focusing on software life cycle processes. The use of these standards can be supported and enhanced with the use of subordinate standards addressing specific software engineering topics, such as software configuration management or software requirements specifications (EIA/IEEE J-Std-016 differs somewhat in that much of this detailed information has been included in Annexes to the standard.) The importance of software life cycle standards in standards frameworks is illustrated in Figures 1 and 2 of the main report.

A1-2.1 History

ISO/IEC 12207 was influenced, to some extent, by both the ISO 9000 series standards and the IEEE software engineering standards, in particular by IEEE Std. 1074, which is endorsed in RG 1.173. The 12207 standard blends the contractual viewpoint of ISO 9001 and the software life cycle process viewpoint of IEEE 1074, and adds a significant amount of material on roles related to software development, such as the acquirer, the supplier, the developer, and organizational management. EIA/IEEE US 12207 adopts this broader perspective (by incorporating as Part 0 the unmodified ISO/IEC 12207) and adds considerable detail (in Parts 1 and 2), in part, through its references to supporting software engineering standards.

Like the ISO 9000 series, EIA/IEEE J-Std-016 has military standards in its ancestry. It was also influenced by a desire to be compatible with ISO/IEC 12207. The military standards influencing EIA/IEEE J-Std-016 were a series of efforts to improve quality by having some control over software life cycle. The earliest was Mil-Std 1679, which led to the two DoD standards, DoD-Std 2167, and later, DoD Std 2167A. Two other standards (DoD Std 7935A and NSA 1703) covered approximately the same subjects but for somewhat
different application environments. The two DoD standards were consolidated in Mil-Std 498, in favor of which the National Security Agency eventually retired NSA 1703. Several of the EIA/IEEE J-Std-016 normative annexes contain format and content preparation guidance for specific software life cycle design output specifications that appears to have been derived from the Data Item Descriptions referenced by Mil-Std 490 which, in turn, was referenced by DoD Standard 2167A.

A1-2.2 Purpose

In contrast to the ISO 9000 series, which views quality from the traditional statistical process control standpoint, the 12207 standard starts with a view that controlling software life cycle processes underlies software quality. It is designed to be used between two parties, the supplier and the acquirer, and assumes either an informal agreement about what is to be supplied, or a legally binding contract. The life cycle processes are the responsibility of both the supplier and acquirer, and if the supplier acquires software items for inclusion in a product, then the supplier fills the role of acquirer for the purchased items.

The design of the 12207 standard is compatible with the purpose of the ISO 9000 series to enhance international trade. It references ISO 9001-1994 as the normative quality standard, consistent with its place in the ISO standards framework. When digital systems in nuclear power plants are involved, IEC 880 and IEC 987 are applicable nuclear industry standards. These latter standards do not reference the ISO 9000 series or ISO/IEC 12207, but are likely to in future revisions.

EIA/IEEE J-Std-016 is also based on the importance of software life cycle processes. The focus of the 1995 version is primarily on the developer role, in an acquirer-supplier context, of the 12207 standard; other roles, such as the operator or maintainer, are planned for inclusion in future revisions. This standard has been issued as a trial use, interim standard. Therefore, the standard notes that it has been “published at the request of the originating Committee without necessarily following the rigorous public review and resolution of comments which is a procedural part of the development of an EIA/IEEE Standard.”

A1-2.3 Structure and Content

All three standards are software life cycle standards, although the 12207 standard currently has a broader scope. Part 0 of EIA/IEEE US 12207 is ISO/IEC 12207 in its entirety with six added annexes, four of which are normative. Part 1 is a guide addressing software life cycle data and contains references to various other standards dealing with topics related to that data. Part 2 provides guidance on the implementation of Part 0 and contains guidance that may only be appropriate for use within the U.S. EIA/IEEE J-Std-016 focuses mainly on the developer role of the 12207 standard. It is unclear how long these standards will exist in their present forms considering the differences between the ISO/IEC and U.S. versions of 12207 and the fact that the J-Std-016 is an interim standard.

ISO/IEC 12207 covers:

- Primary processes: acquisition, supply, development, operation, and maintenance
- Supporting processes: documentation, configuration management, quality assurance, verification, validation, joint review, audit, and problem resolution
- Organizational processes: management, infrastructure, improvement, and training
- A tailoring process prescribed in a normative annex
• Informative annexes addressing tailoring, processes and organizations, and a bibliography

EIA/IEEE US 12207 adds:
• Five annexes to ISO/IEC 12207:
  Guidance on basic concepts underlying the standard (informative)
  Compliance (normative)
  Objectives of life cycle processes (normative)
  Life cycle data objectives (normative)
  Relationships to other standards (informative)
  Errata (normative)
• A new part (Part 1) providing guidance on software life cycle data
• A new part (Part 2) providing guidance on implementation considerations

EIA/IEEE J-Std-016 addresses software development in the system context (e.g., discusses hardware/software integration and software/system testing). It has annexes that address:
• Tailoring
• Development strategies
• Acquirer information on deliverables
• Reuse
• Normative information on the format and contents of plans and software design outputs
• Documentation requirements
• Product evaluations
• Problem reporting
• Joint management reviews

A1-2.4 Orientation, Applicability, and Future Evolution

The 12207 standard is oriented toward acquirer–supplier agreements, similar to ISO 9000’s contractual orientation, although the former permits informal agreements. The standards are applicable to software development life cycles in support of an agreed level of software quality assurance. Although ancestral standards primarily addressed software life cycle activities, the 12207 standards address additional related topics, such as processes for acquisition, supply, process improvement, and management. The U.S. version ‘tightens’ the standard considerably; however, it has not been approved by consensus ballot as of this writing. The 12207 standard cites ISO 9001 as a normative reference, and supports ISO 9001 as an adjunct standard as shown in Figure 2 of the main report.

Future evolution of the 12207 standards is difficult to predict. The U.S. implementation is more restrictive about compliance and provides significantly more detail, some of which is specific to the U.S. software experience. It is not known whether other, country-specific versions of 12207 will emerge. The evolution is impossible to predict except that the next revision will be available in the year 2001.

EIA/IEEE J-016 is a commercial standard, based on previous military software standards (2167A), and updated for current practice. There is some feeling that it exists primarily to support legacy software QA programs for embedded military systems, and also to support
defense contractors with software development infrastructures designed to the 2167A environment. EIA/IEEE J-016 became commercial with the DoD decision to encourage the use of commercial standards, but because of the drive to reconcile standards frameworks and the existence of ISO/IEC 12207, it is not known whether EIA/IEEE J-016 will evolve further. It should also be noted that this standard was issued, from the IEEE side, as a trial use standard in 1995 and that such standards are automatically withdrawn by the IEEE two years following their issue.
Appendix A2 - Review of the ISO 9000 Series Standards

A2-1.0 Comparison of ISO 9001/9000-3 to Regulation

A2-1.1 Quality Assurance Subjects

ISO 9001 covers the generic quality assurance subjects listed in Table A2-1. These are subjects found in most quality assurance standards or requirements, including Appendix B of 10 CFR Part 50. Differences usually lie in the details or rigor with which each topic is treated, and how the subjects are related to each other. Comparison of different quality assurance approaches can be made by examining how each approach deals with each subject area.

Table A2-1. Generic Quality Assurance Subjects

<table>
<thead>
<tr>
<th>Subject</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance Criteria</td>
<td>A set of criteria that an item or process must meet to be acceptable. That is, so that it can fulfill its part in meeting design requirements.</td>
</tr>
<tr>
<td>Activities</td>
<td>An activity or activities covered by QA.</td>
</tr>
<tr>
<td>Applicability</td>
<td>Any statement of to what or to whom or when all, several, or one QA requirement applies.</td>
</tr>
<tr>
<td>Authority</td>
<td>An assignment of authority or requirement to document authority of persons or organizations performing QA functions.</td>
</tr>
<tr>
<td>Compatibility</td>
<td>Measures taken or arrangements to ensure that one organization or development phase can and will talk to the other.</td>
</tr>
<tr>
<td>Complaints</td>
<td>Customer or purchaser indications that a product does not meet expectations.</td>
</tr>
<tr>
<td>Contracts</td>
<td>The primary means of specifying requirements and QA levels under ISO 9001.</td>
</tr>
<tr>
<td>Control</td>
<td>Control of conditions, material, design, configuration, processes, procurement, or procedures. Control measures include identification, marking, documentation, and disposition.</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>Action taken to correct a deficiency or eliminate a non-conformity.</td>
</tr>
<tr>
<td>Design Bases</td>
<td>Any mention of design bases, an NPP-specific, or at least nuclear-facility-specific concept. In ISO 9001, the closest approximation to this concept.</td>
</tr>
<tr>
<td>Documentation Requirements</td>
<td>Any specific item required to be documented by a standard or QA program requirement.</td>
</tr>
<tr>
<td>Environmental Conditions</td>
<td>Conditions required for inspection or test or to meet environmental qualification criteria.</td>
</tr>
<tr>
<td>Handling, Storage, and Shipping</td>
<td>Anything to do with handling, storage, or shipping conditions or procedures that may affect quality or the eventual safety of an item being handled, stored, or shipped.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identification</td>
<td>Singling out or finding an item or procedure that meets certain criteria. The act of labeling or tagging an item.</td>
</tr>
<tr>
<td>Independence</td>
<td>Not dependent on, as in not having common factors. Usually refers to the independence of assurance activities from development activities, but can refer to segregation of system components.</td>
</tr>
<tr>
<td>Inspections</td>
<td>Comparison of an actual item, procedure, or organization with specifications, design criteria, or performance requirements. Generally distinguished from testing because the inspector views, while the tester tests.</td>
</tr>
<tr>
<td>Non-conforming Material, Parts, or Components</td>
<td>Material, parts, or components that do not meet specifications, test criteria, inspection criteria, or procurement documents.</td>
</tr>
<tr>
<td>Preventive Action</td>
<td>Action taken to prevent the occurrence or recurrence of conditions adverse to quality.</td>
</tr>
<tr>
<td>QA Functions</td>
<td>What QA people are supposed to be doing; i.e., checking, auditing, inspecting, witnessing, or documenting.</td>
</tr>
<tr>
<td>QA Plan</td>
<td>Any mention of a plan or description or documentation of a QA program, as differentiated from records and documentation of specific QA actions.</td>
</tr>
<tr>
<td>Records</td>
<td>As distinguished from documentation, the item, not the content. Records are the individual documentation items required by other sections. As records, these items are managed as units of distinguishable classes, and retained or disposed of by class, time, and obsolescence criteria.</td>
</tr>
<tr>
<td>Regulatory Requirements</td>
<td>Any mention of regulations or requirement to conform to regulations, usually NRC regulations, but includes “Applicable Regulations” in ISO 9001.</td>
</tr>
<tr>
<td>Research and Development</td>
<td>R &amp; D necessary to demonstrate that a particular approach or engineering design will meet safety or functional requirements. Any investigation necessary to establish that a method, product, or process has desired characteristics.</td>
</tr>
<tr>
<td>Resources</td>
<td>Personnel, money, materials, or equipment.</td>
</tr>
<tr>
<td>Responsibility</td>
<td>An assignment of responsibility.</td>
</tr>
<tr>
<td>Reviews</td>
<td>A requirement for a review or reviews, generally to determine the status of a design or program execution at a point in time.</td>
</tr>
<tr>
<td>Root Cause Determination</td>
<td>Finding the real reason, rather than the apparent reason, that something happened.</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>A requirement for, or mention of, safety analyses.</td>
</tr>
<tr>
<td>Skills</td>
<td>Any requirement for skills, education, training, or qualifications.</td>
</tr>
<tr>
<td>Testing</td>
<td>Any requirement for or discussion of testing.</td>
</tr>
<tr>
<td>Timeliness</td>
<td>Any requirement for timely execution.</td>
</tr>
<tr>
<td>Tools</td>
<td>Any discussion of tools, their acquisition, adequacy, or qualification.</td>
</tr>
<tr>
<td>Subject</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Updating Methods</td>
<td>Changing or improving development or quality assurance methods, typically to reflect advances in the industry. This is an ISO 9001 concept.</td>
</tr>
<tr>
<td>Verification</td>
<td>Any method of verifying that a product meets requirements, or a standard requirement for verification. Verification includes intermediate design or performance requirements, as well as acceptance criteria.</td>
</tr>
</tbody>
</table>

A2-1.2 Comparisons

A2-1.2.1 ISO 9001, ISO 9000-3 and Appendix B

ISO 9001 and 10 CFR 50, Appendix B both describe general quality systems and cover the quality subjects listed in Table A2-1. ISO 9000-3 is a guideline, and does not have the force of a standard. Consequently, ISO 9001 is reviewed here using ISO 9000-3 as a guide for how to apply the requirements of ISO 9001 to a software product.

A major philosophical difference between ISO 9001 and Appendix B is that the ISO 9001 is designed to demonstrate a quality assurance capability that is required by a contract between a supplier and a purchaser. In contrast, Appendix B describes a quality program required of anyone supplying, constructing, erecting, operating, or maintaining structures, systems, or components essential to the safety of a 10 CFR Part 50 nuclear facility. In the former case, the quality program and the acceptance criteria can be tailored by contractual agreement; in the latter case, the quality program and acceptance criteria are dictated by safety impact. ISO 9001 compliance does not automatically guarantee high quality, but it does restrict the number of quality issues to be resolved to a small set. This is a commercial standard; the purchaser is allowed to purchase the level of quality assurance the purchaser deems appropriate. For the NRC to endorse ISO 9001, the most accessible mechanism available to the NRC staff to assure ISO 9001 supplier compliance with Appendix B is acceptance criteria for contracts between an applicant/licensee and an ISO 9001 supplier. This mechanism would fall under the regulatory provisions of 10 CFR 50, Appendix B, Part VII, “Control of Purchased Material, Equipment, and Services” during the NRC’s oversight of an applicant or licensee that proposed to use the ISO 9001 supplier.

Appendix B has specific requirements for documents, records retention and availability to the NRC staff and nuclear power plants. The quality level is high and is tied to nuclear safety. ISO 9001 permits document availability, records retention, and quality level to be controlled by contract. The supplier is required to have a documented quality assurance program, but not required to make documentary evidence available or to meet specifications other than what is required by contract or required to demonstrate that contractual acceptance criteria have been met. There is no mention of nuclear safety, and only one mention of “applicable” regulatory requirements.

As mentioned above, ISO 9000-3 references ISO 9001 as the normative standard and is an interpretation of ISO 9001 in the context of software development. There is one significant difference with Appendix B that is emphasized in the software development arena. Software maintenance is a significant line item. Appendix B does not address maintenance as part of a supplier/constructor’s responsibility, although Appendix B is applicable to maintenance programs in nuclear power plants. There are no requirements of ISO 9001 that

---

9 The feasibility of this should be reviewed by the NRC Office of General Counsel.
are either expanded or deleted by ISO 9000-3. It is expected that the next revision of ISO 9000-3 will make its correspondence with ISO 9001 explicit by section number.

ISO 9001 cannot be adapted to make it directly equivalent to Appendix B. This is because the ultimate quality requirements that motivate an ISO 9001 supplier are those in a contract, while the Appendix B motivation for quality comes from reactor safety considerations as delineated by regulation. However, ISO 9001 is still useful if the terms of the contract are acceptable. Appendix B and the provisions of ISO 9001 were compared using the subjects of Table A2-1 as points of comparison. Table A2-2 summarizes the issues that would need to be addressed in a contract between an applicant/licensee and an ISO 9001 supplier to ensure that the regulations in 10 CFR 50 Appendix B were met.

Table A2-2. Criteria for ISO 9001 Contract Compatibility with 10 CFR 50, Appendix B

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contract Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptance Criteria</td>
<td>Contracts with an ISO supplier must include acceptance criteria that are selected to ensure that SSCs being procured fulfill their safety functions. ISO 9001 does not include specific regulatory safety criteria.</td>
</tr>
<tr>
<td>Applicability</td>
<td>Contracts with an ISO 9000 supplier should identify structures, systems, and components, major organizations, and the functions of those organizations covered by the QA program. A project QA plan pursuant to ISO 9001 is acceptable and would be required. Example contractual identified subjects: reactivity control devices, mitigation devices, instrumentation and control systems, reactor physics, stress, thermal, hydraulic, and accident analyses; materials compatibility, accessibility for in-service inspection, maintenance, and repair, acceptance criteria for inspections and tests.</td>
</tr>
<tr>
<td>Authority</td>
<td>Contracts should specify that persons doing QA shall report to managers having sufficient authority and organizational independence from cost and schedule that safety (of SSCs) is not impacted.</td>
</tr>
<tr>
<td>Contract</td>
<td>Contracts don’t appear in Appendix B, but contain the acceptance criteria and specifications to which the ISO 9000 supplier has agreed to work. Contractual items include validation (acceptance criteria), maintenance, schedule, responsibility for purchaser hardware and software, scope, availability of skilled personnel, records requirements, and quality assurance criteria. Contract review should resolve differences and determine if supplier can meet specs.</td>
</tr>
<tr>
<td>Control, Change</td>
<td>The contract should specify that changes shall be subject to control measures commensurate with the measures applied to the original design and approved by the original designers or designated successors.</td>
</tr>
<tr>
<td>Control, Processes</td>
<td>Appendix B is more explicit about qualification of personnel (e.g. welders) to construction standards and codes. Otherwise the same. Contract may need to specify code qualification if this is necessary to meet regulatory requirements or applicant/licensee commitments. ISO 9000 is more explicit about control of measuring and test equipment. Also, ISO 9000 considers statistical process control, which Appendix B does not mention directly.</td>
</tr>
<tr>
<td>Subject</td>
<td>Contract Criteria</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>Regulatory notification requirements need to be in the contract or referenced as part of required corrective action procedures.</td>
</tr>
<tr>
<td>Design Basis</td>
<td>Regulatory requirements and design bases need either be stated or referenced in contracts with ISO 9000 suppliers.</td>
</tr>
<tr>
<td>Documentation Requirement</td>
<td>Design basis and regulatory requirements are contract provisions. Location of quality records is at the ISO 9000 supplier’s discretion unless specified by contract. Contract would have to specify quality record locations matching NRC requirements. Documentation requirements of ISO 9000 otherwise a superset of Appendix B.</td>
</tr>
<tr>
<td>Independence</td>
<td>Contracts should specify that persons doing QA shall report to managers having sufficient authority and organizational independence from cost and schedule that safety (of SSCs) is not impacted. Additional criteria: Verifying and checking designs shall be performed by someone other than the designer; Inspections shall be performed by other than those who did the work; Audits shall be carried out by personnel not directly responsible for the area being audited. Since ISO 9001 uses different terminology, the contact should make it clear that Appendix B requirements are met.</td>
</tr>
<tr>
<td>Regulatory Requirements</td>
<td>Regulatory requirements would need to be referenced in the contract.</td>
</tr>
<tr>
<td>Research and Development</td>
<td>R&amp;D requirements would need to be stated in the contract, because ISO 9000 mentions only R&amp;D to identify and develop necessary measurement techniques: identification of any required measurement technique that exceeds the state of the art and needs to be developed. Appendix B requires prototyping to verify design or construction features whose properties have an uncertain effect on safety.</td>
</tr>
<tr>
<td>Safety Analysis</td>
<td>The safety analysis approach of the NRC, 10 CFR 50, NUREG-800, and other documents would need to be referenced in the supplier’s contract. Specific safety analyses for which the supplier had responsibility would need to be enumerated. The issue of environmental qualification would need to be addressed.</td>
</tr>
<tr>
<td>Testing</td>
<td>Contract should include most adverse design conditions for test and acceptance criteria, and what to do about non-conformance. Since ISO 9001 uses different terminology, the contact should make it clear that Appendix B requirements are met.</td>
</tr>
</tbody>
</table>

Table A2.2 was compared with a study done by Virginia Electric and Power Company [Carter, 1996] and substantial agreement was found. Differences existed in the subject areas of design interface control, training, shipping, handling, and storage, and incoming inspection (in which this report found no essential difference between Appendix B and ISO 9001), and acceptance criteria, design bases, regulatory requirements, applicability, corrective action, and safety analyses (which this report found should be addressed in contracts with ISO 9001 suppliers). The Virginia Power study did not address the contractual nature of ISO 9001, which accounted for a significant part of the differences. Due to the different topics selected for comparison, there were differences in outcome, but
the ultimate conclusion is the same: the differences between ISO 9001 and 10 CFR 50, Appendix B are small enough to be surmountable.

**A2-1.2.2 ISO 9000-3 and BTP HICB-14**

ISO 9000-3 and BTP HICB-14 both present criteria for software quality, but BTP HICB-14 is substantially more detailed and is organized in a life cycle activities format. ISO 9000-3 addresses staged development to a limited extent, but does not detail activities to the extent found in BTP HICB-14 or IEEE Std. 1074-1995. Other guidelines in the 9000 suite address specific topics (e.g., 10007 on configuration management, 9004-4 on quality improvement, 10005 on quality plans, 10006 on project management). None of these additional guidelines is specifically addressed to software or digital systems.

ISO 9000-3 cannot be used without ISO 9001, which underlies ISO 9000-3. The analysis results presented in Table A2-3 are based solely on comparison of Appendix B requirements and requirements listed in ISO 9001, and represent only a preliminary list of differences. A final list of concerns identified by the NRC staff in establishing a position on ISO 9001 (if such a position were to be established) would need to be addressed prior to endorsing ISO 9000-3 (as a guide for software development under ISO 9001). Since it is expected that ISO 9000-3 will be revised to reconcile its structure with that of ISO 9001, the endorsement of ISO 9000-3 would depend upon endorsement of ISO 9001. ISO 9000-3 bears a similar relation to ISO 9001 as NQA 2a, Part 2.7 does to NQA-1. Table A2-3 gives positions that would be candidates to be addressed in an endorsement.

**Table A2-3. Endorsement Positions for ISO 9001/9000-3**

<table>
<thead>
<tr>
<th>Position</th>
<th>Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criteria</td>
<td>Acceptance criteria, design bases, regulatory requirements.</td>
</tr>
<tr>
<td>Safety Orientation</td>
<td>Safety analyses, corrective action notification requirements, research and development of new technical approaches, environmental qualification, tying quality to safety, applicability of QA program to identified SSCs.</td>
</tr>
<tr>
<td>Independence</td>
<td>Independence of verifiers and checkers, inspectors, and QA auditors. Authority and freedom from cost and schedule pressures of management responsible for quality activities.</td>
</tr>
<tr>
<td>Testing</td>
<td>Testing environments, procedures for non-conforming SSCs in test and inspection.</td>
</tr>
<tr>
<td>Control</td>
<td>Applicable codes and standards, personnel qualification, design change control commensurate with control on original design.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Location, retention, and availability of quality records.</td>
</tr>
</tbody>
</table>

**A2-2.0 Conclusions**

Given the widespread interest in the ISO 9000 series of quality standards, it may be useful for the NRC, and for developers of ISO 9000-compliant nuclear products, to understand its relationship to the U.S. nuclear regulatory context. The comparisons above indicate that establishing the correspondence, subject to a review of the contract governing ISO 9001 implementation, between ISO 9001 and 10 CFR 50 Appendix B is possible but that ISO 9000-3 will be more difficult to address until ISO 9000-3 is revised.
Appendix A3  Review of Software Process Standards

A3-1.0  Software Life Cycle Subjects for Comparison of Standards

Information on important provisions of the software life cycle standards was collected and a keyword was assigned to represent the category in which the information fell. The collected information was then analyzed with respect to a number of common software subjects that were derived from the keywords. These are shown in Table A3-1. The results of these analyses are presented below and summarized in Table A3-2 in terms of the software topics for which key observations were made.

Table A3-1. Software Life Cycle Subjects for Comparison of Standards

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>Activities performed by an acquirer of software or software-based products.</td>
</tr>
<tr>
<td>Audits and Reviews</td>
<td>Anything relevant to the performance of the various audits and reviews conducted during the software life cycle.</td>
</tr>
<tr>
<td>Compliance</td>
<td>Any aspect of, or requirement for, claiming compliance with a standard. Includes the activity of tailoring a standard’s requirements.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Any software configuration management activity.</td>
</tr>
<tr>
<td>Cost &amp; Schedule</td>
<td>References to or provisions for adjusting requirements based on cost or schedule considerations.</td>
</tr>
<tr>
<td>COTS/PESP</td>
<td>Anything related to commercial off-the-shelf or pre-existing software products.</td>
</tr>
<tr>
<td>Documentation</td>
<td>Any aspect of the documentation of software plans, design outputs, or supporting activities.</td>
</tr>
<tr>
<td>Framework</td>
<td>References to, or implied use of, sets of complementary standards.</td>
</tr>
<tr>
<td>Independence</td>
<td>Any aspect of the independent performance of supporting software activities such as software quality assurance, verification &amp; validation, or software safety analyses.</td>
</tr>
<tr>
<td>Level of Detail</td>
<td>The amount of detail with which an activity or product requirement is described.</td>
</tr>
<tr>
<td>Life Cycle</td>
<td>References to the system or software life cycle.</td>
</tr>
<tr>
<td>QA/SQA process</td>
<td>Any reference to quality assurance activities.</td>
</tr>
<tr>
<td>Problem Reporting / Corrective Action</td>
<td>Any aspect of detecting and correcting problems with software-based products.</td>
</tr>
<tr>
<td>Process Improvement</td>
<td>Any reference to activities specifically designed to assess and improve project or organization software processes.</td>
</tr>
<tr>
<td><strong>Topic</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>Any aspect of the requirement for capturing and retaining records of the software development process.</td>
</tr>
<tr>
<td>Scope</td>
<td>The range of applicability of a standard or the set of topics addressed by the standard.</td>
</tr>
<tr>
<td>Software Safety</td>
<td>Any activity related to ensuring the safety of developed software systems.</td>
</tr>
<tr>
<td>SW Requirements</td>
<td>Any reference to determining and documenting software requirements. See SW Phase Activities &amp; Design Outputs.</td>
</tr>
<tr>
<td>SW Phase Activities &amp; Design Outputs</td>
<td>Any reference to the various categories of software activities (phases) or the design outputs produced by them, e.g., software requirements.</td>
</tr>
<tr>
<td>SW Project Management</td>
<td>Any aspect of software project management.</td>
</tr>
<tr>
<td>System Issues</td>
<td>Any references to activities or issues that are at the system level that affect, or are influenced by, software.</td>
</tr>
<tr>
<td>Testing</td>
<td>see V&amp;V</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>Any reference to verification or validation activities or work products.</td>
</tr>
</tbody>
</table>

### A3-1.1 ISO/IEC 12207 vs NRC Regulatory Context

Appendix 7.0-A, BTP HICB-14, and RG 1.173, which endorses IEEE Std. 1074-1995 with exceptions, all provide guidance on software life cycle activities. IEEE Std. 1074 provides high level guidance on software processes and activities and on the informational relationships among them. This standard is intended to assist with the design of software life cycles for organizations or projects and can be used with any software life cycle model, such as the spiral or waterfall model. RG 1.173 relates this guidance to the NPP environment. IEEE Std. 1074 references other software standards that treat specific software topics in more detail, thus serving as a higher level software standard in an overall standards framework.

ISO/IEC 12207 is similar to this guidance in that it includes high-level guidance on the same life cycle processes and activities; however, it has a somewhat broader scope covering topics such as the software acquirer’s activities and management activities such as software process improvement. The inclusion of these activities is a strong point of the standard, particularly its inclusion of guidance on operation and maintenance processes. These latter topics are addressed in BTP HICB-14 and in RG 1.173 but detailed guidance is not included in the regulatory guides on software engineering standards. The standard does not discuss information flow among processes and activities nor does it provide references to standards treating specific software topics in more detail. It would be possible to use ISO/IEC 12207 as the top standard in a software standards framework, with IEEE Std. 1074 and its referenced standards providing information of the design of software processes consistent with ISO/IEC 12207’s requirements.

---

10 This viewpoint is also expressed in the IEEE Harmonization Action Plan for ISO/IEC IS 12207, EIA/IEEE J-Std-16, and IEEE 1074 [IEEE, 1996].
A number of issues would need to be addressed in considering the use of ISO/IEC 12207 in the NRC regulatory context, the two most important being the definition of compliance with the standard and the mandatory use of ISO 9001 as the governing high-level quality assurance standard. Regarding compliance, ISO/IEC 12207 presents a full range of activities but does not provide any minimum set of required activities and, in fact, requires that the standard be tailored, as part of the acquirer–supplier agreement, by selecting those activities to be performed. Use of this standard in the nuclear regulatory environment would necessitate a determination of the minimum required activities in the NPP context. For any software products for which ISO/IEC 12207 compliance is claimed, the implications of this compliance can only be determined by examining the acquirer–supplier agreement under which the development was performed.

ISO/IEC 12207 requires that the clauses of ISO 9001 be met “as specified in the contract.” The requirement for use of ISO 9001 is particularly effective if organizational quality processes exist and software processes are being defined with the intent of applying the existing organizational processes to individual projects as applicable. It may not be as useful in the other direction, i.e., if project processes are being defined and a new high-level quality assurance program is needed. The implications of the use of ISO 9001 in the NRC regulatory context, including its contract basis, are discussed in Chapter 4 and Appendix A2 of this report.

Both BTP HICB-14 and ISO/IEC 12207 (through its normative reference to ISO/IEC 9126) address the topic of software quality characteristics. The requirements are similar but do not map one-to-one. Incorporation of this guidance into the NRC regulatory context would require considerable discussion to interpret and clarify relationships between the two sources of guidance.

Various other issues exist regarding consistency with NRC regulatory guidance. ISO/IEC 12207 does not address minimum configuration management activities as does RG 1.169, and treats verification and validation with less rigor than does RG 1.168. In fact, ISO/IEC 12207 makes these processes optional. In the NRC context, the guidance on software reuse provided in the SRP, and its reference to the NRC Safety Evaluation Report on EPRI 106439, would take precedence over the ISO/IEC 12207 guidance. BTP HICB-14 and the regulatory guides provide considerable information on software life cycle design outputs, but ISO/IEC 12207 provides little detail in this area. The important SRP topics of consideration of regulatory requirements in software life cycle processes and of software safety analyses are given little attention in the standard. As in Regulatory Guides 1.168 through 1.173, discussion of issues such as independence, record keeping, and relation of the standard’s guidance to nuclear system engineering processes would be required to incorporate ISO/IEC 12207 guidance into the NRC regulatory context.

A3-1.2 US 12207 vs NRC Regulatory Context

The current draft of US 12207 is the U.S. implementation of ISO/IEC 12207 and, therefore, its scope is also broader than the SRP. Many of the issues discussed above still apply, e.g., the normative reference to ISO 9001 (strengthened to delete “as specified in the contract”) and the question of software reuse. However, additions made in the U.S. implementation have the effect of ‘tightening’ the standard and moving it much closer to compatibility with the SRP.

Compared to ISO/IEC 12207, US 12207 presents a much more conservative viewpoint on tailoring of the standard’s requirements, i.e., selecting activities to perform, by stressing that tailoring should be considered to be a process of identifying non-applicable requirements. The tailoring activity is still required. US 12207 also notes that regulatory
requirements may exist in high-integrity arenas and that the regulator might need to establish a minimum set of activities and processes needed in order to claim compliance.

The lack of detail in ISO/IEC 12207 has been addressed to a considerable extent with the inclusion of specific objectives for life cycle processes and life cycle data, and with the inclusion of references to more detailed supporting standards. This additional detail is very similar to the SRP and the NRC software engineering regulatory guides. However, a potential regulatory guide would need to devote considerable discussion to relating the guidance to the SRP context. The referenced standards are similar to those included in IEEE Std. 1074 but also include relevant ISO and ISO/IEC standards. US 12207 takes an approach similar to the NRC’s regulatory guide approach, in that documented ‘alternative methods’ are allowed provided that the methods meet the life cycle goals and that other processes specified in the standard are not compromised.

A3-1.3 EIA/IEEE J-Std-016 (J-Std-16) vs NRC Regulatory Context

EIA/IEEE J-Std-16 is primarily focused on the ISO/IEC 12207 software development process (and on the supplier acting as the developer) although the introductory material states the intent to develop it into fuller compatibility with ISO/IEC 12207 processes. This intent puts the long-term viability of EIA/IEEE J-Std-16 somewhat in doubt, since it does not make much sense to maintain two separate, almost identical, standards. This standard is similar to US 12207 in level of detail but includes the detail in normative annexes. Much of this material appears to be based on the data item descriptions (DIDs) referenced by the Mil-Std-2167A standard. This material is quite detailed and similar in content to the SRP. However, it is organized quite differently from the SRP and the NRC software engineering regulatory guides; use of this guidance would necessitate significant exceptions on the mapping of information. Unfortunately, a tailoring provision is included that could be interpreted quite loosely. Therefore, the question of compliance and minimum required provisions to be met in the NRC regulatory context is also an issue with this standard.

Configuration management is addressed but is probably given insufficient attention for use in high-integrity software. In particular, the standard’s use of the terms of ‘higher-level configuration management’ and ‘as-built software’ would need clarification for the NRC regulatory context. Also, the standard calls for developer participation in determining configuration items, whereas, in RG 1.169, the items to be controlled are specified.

EIA/IEEE J-Std-16 devotes considerable attention to audits and reviews, tracing, and testing but some of the activities that might be included in the more general topic of verification and validation, such as interface analyses, are omitted. This area would need expansion to be consistent with the SRP and regulatory guides. EIA/IEEE J-Std-16 also requires the evaluation of reusable software and provides an annex interpreting the use of the standard for this type of software. In the NRC context, the guidance on software reuse provided in the SRP, and its reference to the NRC Safety Evaluation Report on EPRI 106439, would take precedence over the EIA/IEEE J-Std-16 guidance.

J-Std-16 is more conscious of the need for safety and security analyses than the 12207 standards; however, its guidance is still brief and would need the same type of amplification as included in RG 1.173. A strong point in EIA/IEEE J-Std-16 that bears on safety and security is its emphasis on the inclusion of the software developer in system-level activities.

As with Regulatory Guides 1.168 through 1.173, discussion of issues such as independence, record keeping, and relation of the standard’s guidance to nuclear system engineering processes would be needed to incorporate EIA/IEEE J-Std-16 into the NRC
regulatory context. EIA/IEEE J-Std-16 requires independence but in a slightly more limited way than the SRP.

**A3-2.0 Summary Table of Software Life Cycle Comparison Notes**

The comparison of the software life cycle standards with the SRP is summarized in Table A3-2.

<table>
<thead>
<tr>
<th>Topic</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquisition</td>
<td>The 12207 standards devote more attention to acquisition in terms description of the process. J-16 is not focused on this topic. The SRP addresses only the specific aspects of acquisition necessary to ensure safety, e.g., adequacy of COTS/PESP products.</td>
</tr>
<tr>
<td>Audits and Reviews</td>
<td>Audits and reviews are stressed in all of the standards as well as in the SRP.</td>
</tr>
<tr>
<td>Compliance</td>
<td>ISO/IEC 12207 requires a downward tailoring process and makes many requirements contingent upon contract; no minimum requirements are provided. US 12207 tightens this considerably but does not provide minimum acceptance criteria. J-16 also allows liberal tailoring. BTP HICB-14 and the regulatory guides provide acceptance criteria and minimum acceptance criteria where necessary.</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>ISO/IEC 12207 does not provide minimum configuration management activities nor a minimum list of configuration items, as do the Regulatory guides. The importance of configuration management is stressed in the SRP.</td>
</tr>
<tr>
<td>Cost &amp; Schedule</td>
<td>The software life cycle standards consider cost and schedule to be among the valid criteria for process tailoring. Since the nuclear context is focused on safety, the SRP, BTP HICB-14, and the Regulatory guides stress that cost and schedule considerations should not impact safety considerations.</td>
</tr>
<tr>
<td>COTS/PESP</td>
<td>The 12207 standard gives minimal requirements for COTS incorporation into software products and US 12207 Part 2 provides evaluation criteria. J-16 requires evaluation per criteria placed in the Software Development Plan and provides information on applying J-16 to PESP. The SRP is much more specific in its reference to the NRC Safety Evaluation Report on EPRI 106439, which was developed for the nuclear safety environment.</td>
</tr>
<tr>
<td>Documentation</td>
<td>ISO/IEC is weak in this area; the U.S. version adds considerable information on documentation in its Annex on life cycle data objectives and in its added Part 1 on life cycle data. J-16 also provides considerable detail in its annexes. Documentation, in a form appropriate to the software methods used, is stressed in the SRP.</td>
</tr>
<tr>
<td>Framework</td>
<td>All of the life cycle standards are generic and therefore lack system detail for the nuclear area. Each would have to be folded into the nuclear context. J-16 is stronger than 12207 in making more explicit the need for software personnel involvement in system level activities. The SRP is designed for the nuclear context.</td>
</tr>
<tr>
<td>Topic</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Independence</td>
<td>The life cycle standards recognize the need for independence of SQA and possibly for V&amp;V but provide few requirements. J-16 is stronger than 12207 in requiring independence for some testing but is still short of 10 CFR 50 Appendix B requirements for independence. The SRP is much stronger in this area.</td>
</tr>
<tr>
<td>Level of Detail</td>
<td>The SRP and US 12207 address this through informative references to appropriate standards. J-16 includes significant detail in its Annexes. ISO/IEC provides high-level information only.</td>
</tr>
<tr>
<td>Life Cycle</td>
<td>None of the standards, nor the SRP, prescribe the use of any life cycle model. J-16 provides some informative guidance on the use of several life cycle models, including the evolutionary model which may not be appropriate for nuclear safety I&amp;C systems.</td>
</tr>
<tr>
<td>QA/SQA Process</td>
<td>The 12207 standard requires compliance with ISO 9001. The SRP has Appendix B as its quality process requirements. J-16 does not reference organizational QA programs. All guidance addresses SQA to some extent. All have a “say what you do and do what you say” orientation.</td>
</tr>
<tr>
<td>Problem Reporting / Corrective Action</td>
<td>Problem reporting and corrective action is a common theme in all standards and the SRP. Regulatory notification requirements would have to be included by agreement or contract.</td>
</tr>
<tr>
<td>Process Improvement</td>
<td>The 12207 standards provide specific requirements for a software process improvement process. J-16 and the SRP provide less in this area but do include guidance on software measurements, which support process improvement efforts. Despite published results for software process improvement, this continues to be a controversial topic.</td>
</tr>
<tr>
<td>Record Keeping</td>
<td>The 12207 standards do not provide much detail on record keeping but require availability of records to the acquirer. J-16 is more detailed and refers to maintenance of records for the life of the project. The SRP reflects 10 CFR 50 requirements on records, which are more stringent.</td>
</tr>
<tr>
<td>Scope</td>
<td>ISO/IEC 12207 has the broadest scope since it includes ancillary processes such as acquisition and process improvement. The SRP addresses items in these areas if there is a nuclear safety concern but BTP HICB-14 and the regulatory guides do not describe the overall processes. The J-16 scope is similar to BTP HICB-14 and the regulatory guides.</td>
</tr>
<tr>
<td>Software Safety</td>
<td>Little attention is given to safety analyses in the 12207 standards. J-16, given its military background, is more conscious of this but gives brief guidance. These standards seem to consider the details of safety considerations to be a special topic outside the scope of the document. BTP HICB-14 and RG 1.173 stress the need for safety analyses for NPP safety software.</td>
</tr>
<tr>
<td>SW Project Management</td>
<td>All standards and the SRP require software activities to be managed using proven project management practices.</td>
</tr>
<tr>
<td><strong>Topic</strong></td>
<td><strong>Notes</strong></td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>System Issues</td>
<td>All of the life cycle standards are generic and therefore do not address the nuclear industry. J-16 has the most explicit recognition of software processes within a systems engineering context. The SRP addresses both system and software issues for the U.S. nuclear context.</td>
</tr>
<tr>
<td>V&amp;V</td>
<td>ISO/IEC 12207 treats V&amp;V in less detail and allows the implementer to determine if V&amp;V is necessary. J-16 gives extensive treatment to testing but glosses over other possible V&amp;V techniques. V&amp;V gets much more complete emphasis in the SRP.</td>
</tr>
</tbody>
</table>