



Frequently Asked Questions

The *exida* 61508 Certification Program

V1 R11 August 12, 2009

exida

Sellersville, PA 18960, USA, +1-215-453-1720

Munich, Germany, +49 89 4900 0547



1 Exida Certification Program

The exida IEC 61508 Certification Program was established in 2005 in response to demand primarily from end users in the process industries and manufacturers of instrumentation products. There was a need to provide high quality technical capability with effective and responsive service.

The exida Certification Program is operated globally by exida.com L.L.C. and its subsidiary companies.

Assessors from exida are assigned on a project basis. Individuals are assigned to do the IEC 61508 assessments such that no one who has worked on a project as a consultant may participate in the assessment. The exida program ensures an independent audit and assessment.

2 Frequently Asked Questions

2.1 Who authorizes exida to perform IEC 61508 certification?

The IEC 61508 standard requires “evidence of competence” of those who perform assessments but does not require they be formally authorized or accredited. However, most end users who purchase IEC 61508 certified equipment demand that the certification be done by a highly competent technical organization with experience in mechanical design, electronic design, software design and probabilistic analysis. The organization doing the work must demonstrate strong competency in these key areas of functional safety.

Product certification programs are often operated per the EN45011 product certification quality program. Although not required by IEC 61508, exida is proceeding with accreditation per EN45011 / ISO-IEC 65. Project audits are in progress for full accreditation to EN45011.

2.2 Is a Nationally Recognized Testing Laboratory (NRTL) required for IEC 61508 certification in the U.S.?

One must not confuse electrical safety with functional safety. Electrical safety certification in the U.S. is recognized by OSHA and must be done by a Nationally Recognized Testing Laboratory (NRTL). An NRTL must meet strict requirements for document control and measurement capability with calibration traceable to the National Institute of Standards and Technology (NIST), www.nist.org.

The ability to accurately assess functional safety as required by IEC 61508 is a very different technical field than the ability to accurately measure electrical currents, voltages, temperatures, etc. To certify that a product meets the requirements of IEC 61508, the certification agency must have full competency in:

- Mechanical design: stress conditions, useful life and systematic design procedures
- Software design procedures and software failure mechanisms
- Electronic hardware design procedures, electronic hardware failure mechanisms
- Hardware Failure Modes, Effects and Diagnostic Analysis (FMEDA)
- Hardware probabilistic failure analysis: stress conditions and useful life
- Hardware and software testing procedures and methods
- Quality procedures, document control and functional safety management



2.3 Is a Notified Body required for IEC 61508 certification in the E.U.?

A Notified Body in the European Union (E.U.) is similar to a NRTL in the U.S. Notified Bodies must also pass strict criteria for measurement and calibration. This is not relevant to IEC 61508 nor is Notified Body status required for an organization to issue IEC 61508 certifications as IEC 61508 is not listed under a specific European Directive but is a Basic Safety Publication applicable to many application areas where no specific functional safety rules exist.

2.4 Does exida have personnel competent to perform assessment to IEC 61508?

The exida 61508 Certification Services team has a combination of over 200 years experience in IEC 61508 assessment and certification. Several of the exida team members are ex-TÜV engineers with decades of functional safety assessment experience. Some team members are mechanical design experts with decades of experience in mechanical design and mechanical failure analysis. Some team members are experienced software designers from instrumentation companies. These people have experience in the design and failure analysis of systematic software failures. Some team members are probabilistic failure analysis experts with decades of failure modeling and analysis experience. **Members of exida have written the majority of text books published worldwide in the area of functional safety.**

2.5 Has exida participated on the IEC 61508 committee?

Several exida team members have been active on the IEC 61508 committee since its inception. These people continue today as the standard progresses through modification. No other certification agency in the world has been more active in the creation of this standard.

2.6 Does exida have project experience in IEC 61508 certification?

People who are now exida team members were the same people who started the functional safety certification process in the late 1980's. Several of our team members have over 20 years of project experience in functional safety. exida has done dozens of projects in co-operation with one of the TÜV organizations. exida has completed over 74 certification projects as of August 2009.

2.7 How should exida IEC 61508 certification differ from other certification schemes?

The IEC 61508 standard is a large specification with each subclause being a requirement. The standard states: "To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified and therefore, for each clause or subclause, all the objectives have been met."

In the opinion of exida, this statement requires a "Safety Case" or "Safety Justification" to the requirements of IEC 61508. A simple certificate and certification report stating general compliance with a standard does not fulfill the IEC 61508 requirements. A full Safety Case lists all IEC 61508 requirements and provides the arguments and justification as to how each project meets the standard. exida does a Safety Case for each certification project.

In addition, the exida Certification program looks at usability of a product from a systems perspective and evaluates the likelihood of unintended misuse. Although this is not part of



many certification programs, the exida End User Advisory Council has strongly suggested this interpretation of IEC 61508 requirements.

2.8 Is exida part of TÜV?

No, exida is wholly owned by independent investors, exida partners and employees. Exida is an independent company. This question is asked because functional safety certifications were first done by one of several German companies collectively known as TÜV per the German standard VDE0801/VDE0801-A1. Since the release of IEC 61508, an international standard, certification companies outside of Germany can perform functional safety certification.

2.9 Who is TÜV?

There is more than one company collectively known in the market as “TÜV.” TÜV is an abbreviation for “Technische Überwachungs Verein” which translates to “Technical Supervision Group.” These are privately held companies and not government owned.

At one time there were several different companies all using a variation of the TÜV name. Names from the past include TÜV Product Service, RWTÜV, TÜViT and others. Several mergers have taken place and there seems to be only three companies doing functional safety today; TÜV Rheinland (www.tuv.com), TÜV Süd (www.tuvglobal.com) and TÜV Nord (www.tuevnord.de). Each has a group that does functional safety assessment for instrumentation products.

2.10 Who are exida Certification Services customers?





2.11 How many certifications has exida done?

As of August 2009 exida has successfully completed over 74 IEC 61508 product certifications of currently marketed products. exida has completed more active IEC 61508 certifications in the process industries than any other organization.

A complete overview of all products that have been assessed to any level is available on the exida web-site. <http://www.exida.com/applications/sael/index.asp>

2.12 Why does an exida certificate list IEC 61508 Parts 1, 2, and 3? Other certificates list IEC 61508 Parts 1 through 7.

All the requirements from the IEC 61508 standard are contained in Parts 1, 2 and 3. Part 4 contains definitions and Parts 5, 6 and 7 contain informative annexes. See Section 3 of this document for more details.

3 IEC 61508 Overview

IEC 61508 is an international standard for the “functional safety” of electrical, electronic, and programmable electronic equipment. This standard started in the mid 1980s when the International Electrotechnical Committee Advisory Committee of Safety (IEC ACOS) set up a task force to consider standardization issues raised by the use of programmable electronic systems (PES). At that time, many regulatory bodies forbade the use of any software-based equipment in safety critical applications. Work began within IEC SC65A/Working Group 10 on a standard for PES used in safety-related systems. This group merged with Working Group 9 where a standard on software safety was in progress. The combined group treated safety as a system issue.

The total IEC 61508 standard is divided into seven parts.

Part 1: General requirements (required for compliance);

Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (required for compliance);

Part 3: Software requirements (required for compliance);

Part 4: Definitions and abbreviations (supporting information)

Part 5: Examples of methods for the determination of safety integrity levels (supporting information)

Part 6: Guidelines on the application of parts 2 and 3 (supporting information)

Part 7: Overview of techniques and measures (supporting information).

Parts 1, 3, 4, and 5 were approved in 1998. Parts 2, 6, and 7 were approved in February 2000.

The standard focuses attention on risk-based safety-related system design, which should result in far more cost-effective implementation. The standard also requires the attention to detail that is vital to any safe system design. Because of these features and the large degree of international acceptance for a single set of documents, many consider the standard to be major advance for the technical world.



3.1 OBJECTIVES OF THE STANDARD

IEC 61508 is a basic safety publication of the International Electrotechnical Commission (IEC). As such, it is an “umbrella” document covering multiple industries and applications. A primary objective of the standard is to help individual industries develop supplemental standards, tailored specifically to those industries based on the original 61508 standard. A secondary goal of the standard is to enable the development of E/E/PE safety-related systems where specific application sector standards do not already exist.

Several such industry specific standards have now been developed with more on the way. IEC 61511 has been written for the process industries. IEC 62061 has been written to address machinery safety. IEC 61513 has been written for the nuclear industry. EN 50128 has been written to address safety-related software for the railroad industry. All of these standards build directly on IEC 61508 and reference it accordingly.

3.2 SCOPE OF THE STANDARD

The IEC 61508 standard covers safety-related systems when one or more of such systems incorporates mechanical/electrical/electronic/programmable electronic devices. These devices can include anything from ball valves, solenoid valves, electrical relays and switches through to complex Programmable Logic Controllers (PLCs). The standard specifically covers possible hazards created when failures of the safety functions performed by E/E/PE safety-related systems occur. The overall program to insure that the safety-related E/E/PE system brings about a safe state when called upon to do so is defined as “functional safety.”

IEC 61508 does not cover safety issues like electric shock, hazardous falls, long-term exposure to a toxic substance, etc.; these issues are covered by other standards. IEC 61508 also does not cover low safety E/E/PE systems where a single E/E/PE system is capable of providing the necessary risk reduction and the required safety integrity of the E/E/PE system is less than safety integrity level 1, i.e., the E/E/PE system is only available 90 percent of the time or less.

3.3 FUNDAMENTAL CONCEPTS

The standard is based on two fundamental concepts: the safety life cycle and safety integrity levels. The safety life cycle is defined as an engineering process that includes all of the steps necessary to achieve required functional safety. The safety life cycle from IEC 61508 is shown in Figure 1.

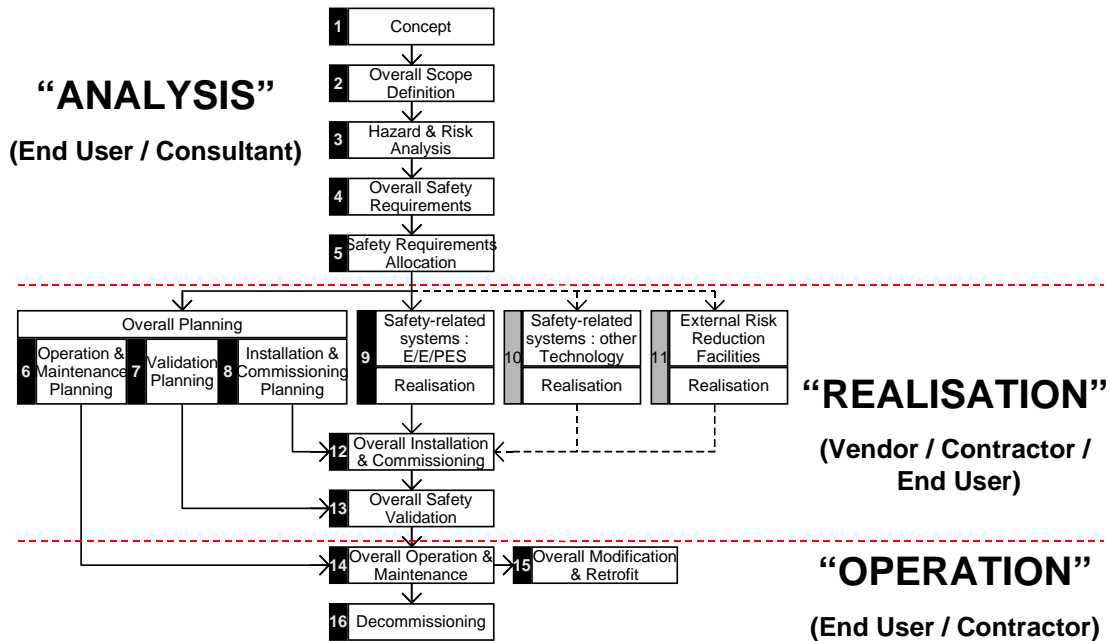


Figure 1: Safety life cycle from IEC 61508.

The basic philosophy behind the safety life cycle is to develop and document a safety plan, execute that plan, document its execution (to show that the plan has been met) and continue to follow that safety plan through to decommissioning with further appropriate documentation throughout the life of the system. Changes along the way must similarly follow the pattern of planning, execution, validation, and documentation. Although the standard is written in the context of a bespoke system, the requirements are applicable to general product design and development.

Safety integrity levels (SILs) are order of magnitude levels of risk reduction. There are four SILs defined in IEC 61508. SIL1 has the lowest level of risk reduction. SIL4 has the highest level of risk reduction. The SIL table for “demand mode” is shown in Figure 2. The SIL table for the continuous mode is shown in Figure 3.

Safety Integrity Level	Probability of failure on demand, average (Low Demand mode of operation)	Risk Reduction Factor
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$	100000 to 10000
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$	10000 to 1000
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$	1000 to 100
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$	100 to 10

Figure 2: Safety integrity levels – demand mode.

Safety Integrity Level	Probability of dangerous failure per hour (Continuous mode of operation)
SIL 4	$\geq 10^{-9}$ to $< 10^{-8}$
SIL 3	$\geq 10^{-8}$ to $< 10^{-7}$
SIL 2	$\geq 10^{-7}$ to $< 10^{-6}$
SIL 1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 3: Safety integrity levels – continuous mode

The mode differences are:

Low demand mode – where the frequency of demands for operation made on a safety-related system is no greater than twice the proof test frequency;

High demand or continuous mode – where the frequency of demands for operation made on a safety-related system is greater than twice the proof check frequency.

Note that the proof test frequency refers to how often the safety system is completely tested and insured to be fully operational.

3.4 COMPLIANCE

The IEC 61508 standard states: “To conform to this standard it shall be demonstrated that the requirements have been satisfied to the required criteria specified (for example safety integrity level) and therefore, for each clause or sub-clause, all the objectives have been met.”

Because IEC 61508 is technically only a standard and not a law, compliance is not always legally required. However, in many instances, compliance is identified as best practice and thus can be cited in liability cases. Also, many countries have incorporated IEC 61508 or large parts of the standard directly into their safety codes, so in those instances it indeed has the force of law. Finally, many industry and government contracts for safety equipment, systems, and services specifically require compliance with IEC 61508. So although IEC 61508 originated as a standard, its wide acceptance has led to legally required compliance in many cases.

3.5 PRODUCT CERTIFICATION

The purpose of product certification is to create a set of documents that demonstrate to the purchaser how a product achieves sufficient safety integrity for use in a safety instrumented function. A product certification is only as good as the documentation produced and the purchaser of such products should review the certification report for the assessment assumptions, safety justification to the individual clauses of IEC 61508 and the resulting conditions for use of the product and shall comply with the specifications of the product “Safety Manual”.

A product assessment done to the requirements of IEC 61508 should include hardware probabilistic failure analysis (FMEDA), field failure analysis, quality system evaluation as well as an assessment of all fault avoidance and fault control measures during hardware and software



development. The process assessment includes a detail study of the testing, modification, user documentation (Safety Manual) and manufacturing processes.

Many of the requirements of IEC 61508 focus on the elimination of systematic faults by use of the best practice product design methods. In order to demonstrate compliance with all requirements of IEC 61508, a product creation process must show extensive use of many fault control and fault avoidance procedures. This applies to hardware, both mechanical and electrical, as well as software.

As an example, the software must be specifically designed to tolerate software faults. The members of the IEC 61508 committee have defined a set of practices that represent good software engineering. They must be applied with different levels of rigor as a function of SIL rating of the instrumentation product.

Full compliance with the requirements of IEC 61508 is seen when a product does not have any significant “restrictions” on usage as documented in the product “Safety Manual.” A large safety manual with a long detailed list of instructions on how to make the product “safe” is a sure sign the manufacturer does not meet requirements unless these restrictions are implemented by the end user.

3.6 The Safety Case Methodology

The Safety Case / Safety Justification methodology provides a systematic and complete way to show compliance to one or more standards. The methodology was established in industries which deal with functional safety of computerized automation in nuclear and avionics [DEF97, BIS98].

For the IEC 61508 standard, all requirements from IEC 61508 were compiled by exida. This compilation was independently audited by TÜV Süd [TUV00]. Each requirement was precisely documented along with the reasoning behind the requirement. The safety case method structures the requirements (parent / child) and in some cases combines like requirements. “Arguments / Solutions” provide a description of how each requirement is met by listing design arguments, verification activities and test cases relevant to that requirement. For full traceability, each design argument and verification / test activity is linked with evidence documents showing the results of the work.

When a safety case for IEC 61508 compliance of a product is completed it must show all requirements along with an argument for each requirement as to how the product meets the requirement. A link to the evidence document that supports the argument is also provided. Additional fields are provided for the independent assessor to record the results of the assessment and to communicate their expectations with other assessors and the certifying persons.

Overall, the safety case concept provides a single place to store compliance information in an organized manner. The use of a safety case provides a systematic means to ensure completeness of any assessment. The Safety Case method supports company learning over multiple projects by establishing a knowledge base consisting of patterns of fundamental requirements and related design arguments. Templates and previous examples of evidence documents provide the ability to reduce effort on subsequent projects.

Note: The term “Safety Case” is being used beyond its original definition [DEF97] in the context of product certification to IEC 61508 and is based on concepts presented and developed earlier [BIS98].



3.7 The exida Open Certification Assessment Process

Manufacturers of safety-related systems / products to be certified and users of such systems / products can get access to the detailed assessment procedures and can buy the supporting safety case and verification tools. This is to provide openness and ensure implementation of the safety requirements by the safety-related system / product.

The manufacturer of safety-related systems / products to be certified can choose between:

- A Functional Safety Management Certificate;
- A Type Approval Certificate;
- A Product Certificate.

The Functional Safety Management Certificate confirms only the compliance of the presented Functional Safety Management System and therefore does not allow for the marking of products with the *exida* Certification mark but does allow the *exida* Certificate to be shown on general company documentation.

The Type Approval Certificate confirms only the compliance of the presented type or prototype and therefore does not allow for the marking of the products with the *exida* Certification mark but does allow the *exida* Certificate to be shown on the product documentation, e.g. Safety Manual.

The Product Certificate confirms the compliance of the product as produced and therefore requires in addition to Type Approval certification, that the product manufacturer's quality assurance system is certified. Product Certification also requires surveillance of the production of the certified product in contrast to Type Approval Certification, allows the marking of the products with the *exida* Certification mark.

A typical assessment (Figure 4) begins with a complete review of the written safety management system (SMS) / Functional Safety Management (FSM) plan. This should be a document or set of documents that describe the process by which a new product is to be developed and modified. The information contained should include all design steps (inputs required, processes to be performed and outputs required), all verification activities, responsibilities and all project documentation generated.

Product requirements and design documents are reviewed next. The documents supplied should match those required in the functional safety management plan. Evidence that the required verification activities have been done shall be included. Competency records must be in place and show that those assigned to the project were competent to perform their specific tasks. When the paper review is complete, the assessment continues with detailed on-site meetings.

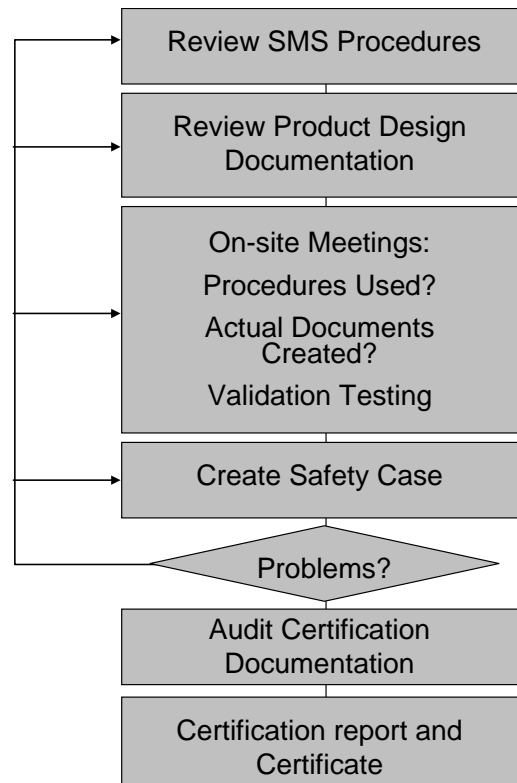


Figure 4: exida Open Certification assessment process

When all relevant documents are reviewed, interviews with the responsible personnel must take place. This is done by visiting the development and manufacturing control site(s). One of the key interview questions is “What process was followed in the design of this project?” and “Have the safety requirements been implemented the product”. It is surprising how often the answer varies from the process described in the functional safety management plan or from the documented safety concept. Any discrepancies must be justified and documented by modifications to the “project specific functional safety management plan” and safety concept. The site visit must also include witnessed validation testing often including specific fault injection tests.

If all documentation for both the process and the product are complete and seem fit, a safety case document is created. This step provides a systematic method to ensure that no requirements of the standard(s) are missed. Often missing requirements are identified and the assessment must return to a previous step to correct the problem. When the safety case is judged to be accurate and complete, the certification report describing all assessment activities and their results is written. The documentation is given to an independent auditor to verify.

When the audit is complete and the independent auditor supports the certification, the certificate (Figure 6) is issued.



Figure 6: exida IEC 61508 Certificate

3.8 The exida Assessment and Certification Report

The exida Assessment and Certification Report shall give the user of the product detailed information to support his confidence in the product and its certification and shall support his safety-related application of the product. The exida Assessment and Certification Report is structured as follows:

Management summary

- 1 Purpose and Scope
- 2 Description of the product / system
- 3 Project management
 - 3.1 Assessment of the development process
 - 3.2 Assessment of the technical safety properties of the product
 - 3.3 Roles of the parties involved
- 4 Results of the Functional Safety Assessment
 - 4.1 Technical safety aspects of the product / system
 - 4.1.1 Safety Functions of the product / system
 - 4.1.2 Safety Integrity Functions and failure behavior of the product / system



- 4.1.3 Safety-related timing behavior of the product / system
- 4.2 Functional Safety Management
 - 4.2.1 Applicable Safety Life Cycle phases
 - 4.2.2 FSM planning
 - 4.2.3 Documentation
 - 4.2.4 Training and competence recording
 - 4.2.5 Configuration Management
 - 4.2.6 Tools (and languages)
- 4.3 Safety Requirement Specification
 - 4.3.1 Safety Requirement Specification and traceability into design
- 4.4 Change and modification management
 - 4.4.1 Change and modification procedure
- 4.5 Hardware Design
 - 4.5.1 Hardware architecture design
 - 4.5.2 Hardware Design, FMEDA and Probabilistic properties
- 4.6 Software Design
 - 4.6.1 Software architecture design
 - 4.6.2 Software Design methods, design analysis and static code analysis
- 4.7 Verification
 - 4.7.1 SW related Verification activities
 - 4.7.1 HW related Verification activities
- 4.8 Validation
 - 4.8.1 HW related Validation activities
- 4.9 Safety Manual
 - 4.9.1 Operation, installation and maintenance requirements
- 5 Reference documents
- 6 Status of the document
 - 6.1 Releases of the document

4 REFERENCES

[DEF97] Defence Standard 00 – 55, Parts 1 and 2, Issue 2, August 1997, U.K. Ministry of Defence.

[BIS98] Peter G. Bishop and Robin E. Bloomfield, "A Methodology for Safety Case Development", in Safety-Critical Systems Symposium, Birmingham, UK, February 1998. <http://citeseer.ist.psu.edu/bishop98methodology.html>

[TUV00] Requirements Database Review, Report #: eS 70177T, TÜV Product Service Inc., October, 20, 2000.

[IEC00] IEC 61508, Functional Safety of electrical / electronic / programmable electronic safety-related systems, Geneva: Switzerland, 2000.



5 Terms and Definitions

COTS	Commercial Off The Shelf
FIT	Failure In Time (1x10 ⁻⁹ failures per hour)
FMEA	Failure Modes Effects Analysis
FMEDA	Failure Modes, Effects and Diagnostic Analysis
FSM	Functional Safety Management
IEC	International Electro-technical Commission
NIST	National Institute of Standards and Technology
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System – Implementation of one or more Safety Instrumented Functions. A SIS is composed of any combination of sensor(s), logic solver(s), and final element(s).
SMS	Safety Management System
SRS	Safety Requirements Specification

6 Status of the document

Releases

Version:	V1
Revision:	R11
Version History:	V1, R11: Updated organization questions, numbers, August 12, 2009
	V1, R10: Updated numbers, July 2009
	V1, R9: Updated numbers, July 15, 2008
	V1, R8: Edited descriptions, updated numbers, Oct. 19, 2007
	V1, R7: Incorporated comments from end users, October 9, 2007
	V1, R6: Added more customer names, certs, August 20, 2007
	V1, R5: Updated more certifications, minor edits
	V1, R4: Updated more certifications June 18, 2007
	V1, R3: Added more certifications
	V1, R2: Released; February 5, 2007
	V1, R1: Released; February 2, 2007
	V0, R1: Internal Draft; February 1, 2007
Authors:	William M. Goble, Rainer Faller
Review:	V1, R2: William Goble
	V1, R1: Rainer Faller
	V0, R1: Iwan van Beurden, Greg Sauk

Future Enhancements

As required.



Release Signatures

A handwritten signature in black ink, appearing to read "William M. Goble". The signature is written in a cursive style and is positioned above a solid black horizontal line.

Dr. William M. Goble, Principal Partner