APEGGA

Guideline for Professional Responsibilities in Developing Software

V1.0
February 2006

The Association of Professional Engineers, Geologists and Geophysicists of Alberta

FOREWORD

An APEGGA guideline presents procedures and practices that are recommended by APEGGA. In general, an APEGGA Member should conform to the recommendations in order to be practising in accordance with what is deemed to be acceptable practice. Variations may be made to accommodate special circumstances if they do not detract from the intent of the guideline.

Guidelines use the word *should* to indicate that among several possibilities, one is recommended as particularly suitable without necessarily mentioning or excluding others; or that a certain course of action is preferred but not necessarily required; or that (in the negative form) a certain course of action is disapproved of but not prohibited *(Should equals is recommended that)*. The word *shall* is used to indicate requirements that are mandatory and must be followed *(Shall* equals is required to). The word may is used to indicate a course of action permissible within the limits of the guideline *(May* equals *is permitted).*

PARTICIPANTS

APEGGA's Practice Standards Committee (PSC) publishes practice standards and guidelines to promote high levels of professional service. A PSC subcommittee with the following membership prepared the draft guideline:

Mr. D.H. (Dave) Currie, P.Eng., Chair
Mr. A.L. (Larry) Adorjan, P.Geoph.
Mr. K. (Ken) Chapman, ISP
Mr. M. (Tex) Gamvrelis, P.Eng.
Mr. R.J. (Rich) Isaac, P.Eng.
Mr. D.D. (Dion) Lux, P.Eng.
Mr. R.H. (Hugh) McLeod, P.Eng.
Mr. B.R. (Bruce) Palmer, P.Geol.

The final development of the guideline was greatly assisted through significant contributions of time and expert knowledge by:

Mr. S. (Shawn) Abbott
Mr. B.G. (Barry) Brown, P.Eng
Mr. P.R. (Paul) Brown, P.Eng.
Mr. P. (Peter) Davenport
Mr. R. (Bob) Fabian, ISP
Mr. J. (John) Harauz, P.Eng.
Dr. R.C. (Ron) Hinds, P.Geoph.
Mr. R.S. (Richard) Huntrods, P.Eng.
Mr. C.S. (Chris) Jones, P.Geol.
Mr. M.P.J. (Martin) Kratz, LLB, ISP
Mr. J.L. (Jamie) Marriott, P.Eng.
Mr. S. (Steve) McConnell, MSE
Dr. I. (Iain) Robertson
Mr. R.F. (Ron) Starman, P.Eng.
Mr. C.S. (Carl) Turner, P.Eng.
Mr. R.P. (Ross) Vogt, P.Eng.
Mr. J.D. (John) Voth, P.Eng.

Canadian Information Processing Society (CIPS)
Institute of Electrical and Electronics Engineers Computer Society's (IEEE-CS) Professional Practices Committee
Software Human Resources Council (SHRC) of Canada

Substantial technical comments were also received from the following individuals:

Mr. D.J. (David) Allen, P.Eng.
Mr. V.N.S. (Vincent) Chiew, P.Eng.
Mr. P. (Peter) Chrapchynski, P.Eng, PMP
Dr. A.D. (Allan) Hiebert, P.Eng., MBA
Mr. M.D. (Murray) Kachmar, P.Eng.
Mr. N.H. (Norm) Kalmanovitch, P.Geoph.
Ms. K.J. (Kim) Kelly, P.Eng.
Mr. G. (Geoff) Kneller, P.Eng, MBA
Dr. P.B.P. (Philippe) Kruchten, P.Eng.
Dr. F. (Frank) Mauer
Mr. S.R. (Simon) Orrell, P.Eng., PMP
Ms. M.D. (Mona) Trick, P.Eng.

Comments that would help to improve this document or questions regarding the interpretation of this guideline should be addressed to:

Ms. L.M. (Lianne) Lefsrud, P.Eng.
Assistant Director, Professional Practice, APEGGA
1500 Scotia One, 10060 Jasper Avenue
Edmonton, Alberta T5J 4A2
E-mail: llefsrud@apegga.org
Fax: (780) 426-1877

TABLE OF CONTENTS

1 OVERVIEW

Governments grant the privilege of self-governance and the associated responsibility to regulate professional matters to selected professions. In enacting the *Engineering, Geological, and Geophysical Professions Act,* the Alberta Government granted self-governance to engineers, geologists, and geophysicists. A key expectation of members of self-governing professions is to accept legal and ethical responsibility for their work and to hold the interest of the public and society as paramount. Other legislation and regulations recognize and rely upon Professional Members' responsibility, either directly or indirectly, to protect the public interest.[1] As the regulator of the professions of engineering, geology and geophysics in Alberta, APEGGA's role is to maintain appropriate standards and guidelines of professional practice to uphold the protection of public interest.

There is a need to provide proactive means to defend public interest, safety, and security as it may be affected by software failure. This guideline sidesteps the 'software engineering' versus 'computer science' debate by narrowing the focus to the professional responsibilities of APEGGA members in developing and using engineering, geological, and geophysical software in Alberta. This guideline reinforces our regulatory jurisdiction while pragmatically protecting the public interest in this area.

1.1 SCOPE

It is recognized that the professional engineer, geologist, or geophysicist is most often part of a software development team that includes others such as Information Systems Professionals (ISP)[2], computer scientists, and technologists. However, this document focuses specifically on the role of APEGGA Members who assume professional responsibility for projects involving engineering, geological, or geophysical software, that are developed in Alberta. Examples are given of such software that requires authentication, and the manner in which it is to be authenticated.

- This document reviews the professional responsibilities of Professional Members of APEGGA to ensure that public interest is protected, by:
- recognizing professional and ethical[3] responsibilities with software development and use, especially safety and security considerations;
- accepting professional responsibilities in product delivery (i.e., final review and stamping);
- delineating responsibilities for multi-disciplinary projects (i.e., hardware and software interfaces such as piping and instrumentation diagrams); and

1 Examples of legislation relying upon Professional Members to protect the public interest are the *Alberta Building Code*, *Occupational Health and Safety Code*, *Canadian Securities Administrators NI 51-101* (*Standards of Disclosure for Oil and Gas Activities*) and *NI 43-101* (*Standards of Disclosure for Mineral Projects*).

2 Information Systems Professional of Canada (ISP), a certification designation granted by Canadian Information Processing Society (CIPS) provincial bodies, as professions are regulated on a provincial basis). CIPS is a Canadian professional association that provides leadership in information systems and technologies by developing and promoting quality standards and practices, research, certification, and professional development while safeguarding the public interest. http://www.cips.ca

3 In addition to APEGGA's *Code of Ethics*, there is a documented software engineering code of ethics, which both the IEEE Computer Society and Association for Computing Machinery (ACM) have endorsed (also endorsed by many companies) that should be mentioned. http://computer.org/computer/code-of-ethics.pdf and http://www.acm.org

- recognizing professional responsibilities of Members in the different software development roles and during the various stages of software development.

The scope of this guideline and, hence, the enforceability has been necessarily limited to the professional responsibilities of APEGGA Members developing software in Alberta. Software that is developed and/or used out of Alberta is outside the jurisdiction of APEGGA; Professional Members should consult with those authorities having jurisdiction for their guidelines and standards of practice.

This is not meant to be a technical document. APEGGA cannot hope stay abreast of this rapidly developing industry and so defers to other authors[4] and agencies who have already developed excellent standards and best practices (i.e., ANSI/UL,[5] COBIT,[6] ITIL,[7] CSA,[8] IEEE-CS,[9] ISO,[10] IEC,[11] SEI-CMM/CMMI®,[12] SAE,[13] RTCA,[14] SEG[15]). Professional Members are advised to direct themselves to these other references, as required.

---

4 Ian Sommerville, *Software Engineering 7th edition (International Computer Science Series)* (Addison Wesley, 2004).

5 American National Standards Institute (ANSI) is a premier source for timely, relevant, actionable information on national, regional, international standards and conformity assessment issues. http://www.ansi.org . Underwriters Laboratory Inc. (UL) has developed more than 800 Standards for Safety to help insure public safety and confidence, reduce costs, improve quality and market products and services. http://www.ul.com

6 The *Control Objectives for Information and related Technology (*COBIT) framework is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with Information and related IT. The COBIT Framework outlines IT Governance Controls and audit objectives to enable development of clear policies and practices in controls for IT services, including development of software. http://www.ITgovernance.org or http://www.isaca.org

7 IT Infrastructure Library (ITIL) is an industry best practice framework for IT Service Management that establishes best practice and a standard of IT service quality that customers should demand and providers should seek to supply. It was developed by the CCTA (now the OGC - Office of Government Commerce) in collaboration with subject experts, practitioners, consultants and trainers to help organizations improve the way they use IT. http://www.itsmf.ca or www.itsmf.com

8 Canadian Standards Association (CSA) is a not-for-profit membership-based association serving business, industry, government and consumers in Canada and the global marketplace. CSA works in Canada and around the world to develop standards that address real needs, such as enhancing public safety and health. http://www.csa.ca

9 Institute of Electrical and Electronics Engineers (IEEE) is the world's largest technical society. The IEEE is organized into 37 technical societies, including the Computer Society (CS), which develops and maintains technical standards for software development. IEEE-CS maintains approximately 50 standards in computing science and engineering. http://www.ieee.org

10 International Organization for Standardization is a network of the national standards institutes of 156 countries. It is a non-governmental organization, occupying a special position between the public and private sectors. http://www.iso.ch

11 International Electrotechnical Commission (IEC) develops international standards and conformity assessment for government, business and society for all electrical, electronic and related technologies. http://domino.iec.ch/

12 Carnegie Mellon University's Software Engineering Institute (SEI) has developed the Capability Maturity Model for Software (also known as the CMM and SW-CMM) which has been a model used by many organizations to identify best practices useful in helping them increase the maturity of their processes. In 2000, the SW-CMM was upgraded to CMMI® (Capability Maturity Model Integration). http://www.sei.cmu.edu/cmmi/models/

13 Society of Automotive Engineers (SAE), promotes standards development, events, and technical information and expertise used in designing, building, maintaining, and operating self-propelled vehicles for use on land or sea, in air or space. http://www.sae.org/

14 Organized in 1935 as the Radio Technical Commission for Aeronautics (RTCA) today includes roughly 250 government, industry and academic organizations from the United States and around the world. RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. http://www.rtca.org/

15 Society of Exploration Geologists (SEG) is a not-for-profit organization that promotes the science of geophysics and the education of applied geophysicists. SEG, founded in 1930, fosters the expert and ethical practice of geophysics in the exploration and development of natural resources, in characterizing the near surface, and in

1.2 PURPOSE

Engineering, geological, and geophysical software - either directly or indirectly - may affect the safety, security, and financial welfare of the public. The purpose of this document is to outline the ethical and professional responsibilities of APEGGA Members to ensure that the public interest is protected. This document also provides guidance for others interfacing with Professional Members who are developing software, such as clients and owners who are acquiring ready-made software or specifying requirements for new software. This guideline should be regarded as an addition to, but not a substitute for, specialized software training.

The purpose of this guideline is also to remind Professional Members of their ethical obligation to respect intellectual property rights. It is recognized that the development of engineering, geological, and geophysical software is very competitive and, therefore, proprietary in nature. The purpose of this guideline is not to undermine the competitiveness of Albertan software, but to protect the public first and foremost. However, by requiring the involvement of Professional Members in the development of engineering, geological, and geophysical software, this may prove to be a value-added proposition for Albertan software companies.

1.3 REFERENCES

This guideline is to be read in conjunction with the following documents:

Guideline for Ethical Practice V2.0, APEGGA, March 2003.

Practice Standard for Authenticating Professional Documents V2.0, APEGGA, April 2002.

Guideline for Relying on Work Prepared by Others V1.0, APEGGA, June 2003.

Guideline for the Development of Consulting Rate Structures and Contracts V1.0, APEGGA, February 2005.

Guideline for the Management of Risk in Professional Practice V1.0, APEGGA. May 1989.

1.4 DEFINITIONS

For the purposes of this guideline the following terms and definitions apply and are capitalized throughout. Other references (i.e., CAN/CSA-ISO/IEC 15288:04) provide technical definitions.

Act
The *Engineering, Geological and Geophysical Professions Act*, R.S.A. 2003, c. E-11.1.

Association
The Association of Professional Engineers, Geologists and Geophysicists of Alberta (APEGGA).

Authentication
Application of the Professional Member's stamp, signature, and date.

mitigating earth hazards. The Society, which has more than 25,000 members in 129 countries, fulfills its mission through its publications, conferences, forums, Web sites, and educational opportunities. http://www.seg.org

Professional Member
A professional engineer, professional geologist, professional geophysicist, registered professional technologist (engineering), registered professional technologist (geological), registered professional technologist (geophysical), licensee or permit holder entitled to engage in the practice of engineering, geology, or geophysics under the Act.

Professional Document (s)
Documents that express a professional opinion upon which someone else may rely; both hard copies and electronic copies of design documents, requirements, specifications; including documentation of an operating environment (compiler, software versions, etc.); testing specifications; test procedures for critical components of software interfaces; interpretation of test results; implementation procedures/guides; user guides; reports or other documents that express engineering, geological or geophysical work as contemplated in the Act (sections 3, 6 and 8) or Regulations (section 54), or reproductions of same.

Regulations
The *Engineering, Geological and Geophysical Professions Act* General Regulation consisting of Alberta 150/99 and 37/2003, and Registered Professional Technologist (Geological) and Registered Professional Technologist (Geophysical) Regulation consisting of Alberta Regulation 36/2003.

2 PROFESSIONAL PRACTICE ISSUES FOR ENGINEERS, GEOLOGISTS, AND GEOPHYSICISTS

2.1 PROFESSIONAL RESPONSIBILITY

Developing software is an inherently risky proposition – interpreting the needs of clients and consumers, balancing budget and schedule constraints, and ensuring the efficiency, effectiveness, integrity, security, privacy, safety, and quality of the software. The software development process is a complex undertaking comprised of specifying, designing, implementing, and testing. Professional Members contribute to the success of software development projects. However, APEGGA is primarily concerned with their responsibility for minimizing the risk of failure and protecting the public interest.

Typically, the software project is usually aligned with larger programs intended to fulfill a system or business need. Project failure is then directly related to a failure to achieve the required or desired change, within the available time and resource constraints of the project. It is uncommon to find a software project where failure can be measured in purely technical terms. In addition to technical failure, there also may be change, service, and/or market failure:

- Technical Failure – The project faced challenging technical requirements with clearly defined technical objectives. Failure was due to an inability to meet the technical challenge.
- Change Failure – The project involved work with software, but its objective was to achieve some organizational change. Failure to achieve that change caused the project to fail.
- Service Failure – The project worked on a software-based service. Its objective was to achieve a specified level of service. Failure to meet service commitment caused project failure.

- Market Failure – The project worked on a software product. Its objective was to achieve a certain market impact and level of customer satisfaction. Failure to achieve that market impact caused the project to fail.

There is a need to provide proactive means to defend public safety and security as it may be affected by software failure – especially technical and/or service failure. “Many companies building safety-critical software are not using proper procedures from a software-engineering and safety-engineering perspective”.[16] There are many instances of software failure leading to data or identity theft, fraud, economic losses, damage to physical property, and even loss of life. Market forces, the legal system, and other authorities are usually relied upon to defend public welfare. However, these act after the fact.

The law of civil obligation (torts) may be applicable in these kinds of cases. That increases the importance of providing guidance to Members who wish to be software developers in the need for proposed care and attention in the design, programming, testing, implementation and use of software systems and for such Members in taking such care.

Professionals are reminded of APEGGA’s *Code of Ethics*, which states that they “shall, in their areas of practice, hold paramount the health, safety and welfare of the public, and have regard for the environment”.[17] Also, professionals must ensure that appropriate action or notification of the proper authorities occurs in any instance where they believe that public safety or the environment is endangered, or where required by relevant legislation, regulations, approvals, or orders.

In some instances, APEGGA Members may be the only employees in a company, agency, government department, or other entity who have a legal obligation to protect the public interest.[18] The courts expect a higher standard of care from professionals than from the public at large. Professionals also share corporate responsibility for the quality of products and services delivered. Under Canadian legislation an individual can be deemed to be a party to an offence if he or she acquiesced in the commission of the offence.[19] Therefore, Professional Members must assess the risk of software failure as a function of the probability and consequences of such failure[20] and provide necessary safeguards.[21] An example of this is the design of Programmable Logic Controls (PLCs) with mechanical redundancies that mitigate the risk of failure.

2.2 INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights arise in software development and should be respected. Professionals are reminded that several forms of intellectual property may arise during software development. There will likely be copyright in the form of the software itself.

16 Nancy Leveson and Clark S. Turner “An Investigation of the Therac-25 Accidents”, *IEEE Computer*, Vol. 26, No. 7, July 1993, pp. 18-41. http://courses.cs.vt.edu/~cs3604/lib/therac_25/therac_1.html

17 *Guideline for Ethical Practice* APEGGA, April 2003. http://www.apegga.com

18 As noted above, there may also be other professionals such as ISP holders present or working on the project.

19 *Plain Language Guide: Bill C-45 - Amendments To The Criminal Code Affecting The Criminal Liability Of Organizations* [Justice Canada; Last updated Feb. 3, 2004]. The amended Act came into force on March 31, 2004. http://canada.justice.gc.ca/en/dept/pub/c45/

20 *Risk Management: A Guideline for Managers, A National Standard for Canada*, CAN/CSA-850-97 (reaffirmed 2002).

21 Richard Feynman has summarized of the risks associated with the shuttle system. http://www.ranum.com/security/computer_security/editorials/dumb/feynman.html

The algorithms used and underlying knowledge framework used in a software development project may be confidential information. The algorithms and processes used may also be inventive and potentially patentable.[22]

In addition the professional should keep in mind not only the rights being created by the software development process, but also the rights of others that might be used (or infringed) during that development. For example, the use of open source software in one's project remains subject to copyright protection and may only be used in accordance with the terms of its license and applicable law. Similarly the professional should avoid direct or inadvertent misuse of the rights of others.

The basic rules on ownership of copyright in Canada depend on whether or not there is an agreement dealing expressly with the ownership of the copyright. If not then the general rule for most works is that the author who creates the copyrighted work retains the copyright in the work unless it is expressly assigned to another in writing. An exception to this general rule arises where the professional is an employee working in the scope of employment in developing the software. Then absent an agreement to the contrary the employer is the first owner of the copyright. As this is a complex area further review of these issues is encouraged to avoid unnecessary conflict.[23]

In a case where the professional develops the software for another and, due to the ownership rules retains the copyright in the work, then the party who engaged the professional also has important rights. Of course it is best to avoid conflict if the parties agree on these issues. If that did not occur, then the courts will seek to interpret what the reasonable expectation of the parties was. Often the most likely result in such a case is that the engaging party has an implied license to use the software for the purposes the parties contemplated. It is very important for the professional to remember that in such engagements the engaging party may also have provided confidential information and other works to the professional that cannot be misused. As this is an area where conflict can arise it is important to document the relationship properly and get legal advice when needed.

In addition to legal obligations the professional also has important ethical and professional obligations. Following are excerpts from APEGGA's *Guideline for Ethical Practice,* which discuss intellectual property rights.

- Process information and/or all confidential information received during professional service should be considered the exclusive property of its owner and should not be disclosed to others except with the owner's specific approval. Particular care should be taken regarding trade practices that may be unique and practices that identify the owner's special attributes.
- When Professional Members use designs supplied by clients, the designs remain the property of the clients and should not be duplicated by the Professional Members for others without the express permission of the first client.

22 For a review of other applicable rights and more background, see Martin P.J. Kratz, *Canadian Intellectual Property Law* (Carswell, 1998).

23 For more detailed analysis of the rules for several types of copyright works, see Kratz, *supra*. In the context of the Internet, see Alan M. Gahtan, Martin P.J. Kratz, and J. Fraser Mann, *Internet Law: A Practical Guide for Legal and Business Professionals* (Carswell, 1998); Lesley Ellen Harris, *Digital Property: Currency of the 21st Century* (McGraw-Hill, 1998); or Barry B. Sookman, *Computer, Internet and Electronic Commerce Law* (Carswell, 2000).

- Professional Members may contemplate engaging in new work that would require the application of confidential knowledge that was obtained through other projects. However, they should not promote such work or employment, or negotiate for it without the consent of all parties connected with the prior projects that were of a confidential nature.

2.3 RESPONSIBILITIES FOR ENGINEERING AND GEOSCIENCE SOFTWARE

Responsibility and accountability is twofold, between professionals who are involved in: 1) the development (specifying, designing, implementing, testing, and support) and 2) the use of engineering, geological, and geophysical software. First, the Professional Members responsible for the software development process must ensure that the software is fit for use by others. Fitness for use is not limited to functionality – but must also give due regard to reliability, usability, security, and privacy concerns. Second, as users, the Professional Members shall be responsible to ensure that the software is used within its parameters and with an understanding of the underlying engineering/geoscience principles, assumptions, limitations, design constraints, and validity/reliability of results.

The following listings of responsibilities may be used by Professional Members who acquire ready-made software for their field of practice, and who could benefit from having a checklist of what to demand from their vendors. These listings may also be used by those who want to specify software to be developed for them and who would benefit from knowing what to request on a process quality perspective from their potential software developer or consultants. Lastly, these listings may be used by those Professional Members who develop software that is safety-critical or mission-critical.

Professional Members involved in developing software should:

- explicitly document and explain the purpose and context of the software, the methodologies and input parameters, as well as the limitations of the software systems;
- disclose the scope of testing, particularly in terms of functionality which was proven out and the extent to which internal and field testing has indeed provided confirmation of suitability to purpose;
- provide realistic sample data and verified results to allow end users to test the reliability, functions, features, and performance of the software for themselves;
- provide conformance statements to applicable standards plus integration with the encompassing software system;
- provide clear and understandable documentation and procedures to users, including highlighting any limitations, risks, or cautions on the use of the software, or in respect of the format, content, input, or processing of the data and interpretation of processed results;
- review and directly disclose to the users any limits on the liability of the software developer and identify where there may be a need for use of back up or double checking procedures to verify proper operation of the software;
- provide, where required by agreement, for timely releases to software users of important bug fixes or software corrections that may affect the performance, reliability or accuracy of the software;

- provide, where required by agreement, timely continuing maintenance and support services for the software or provide sufficient design documentation to allow the client to perform maintenance;
- provide, where required by agreement, timely continuing educational and training services for the users of the software;
- be prepared to provide timely access to source code for the software under suitable contractual terms (i.e., source code escrow arrangements) where needed by users who must be able to rely on the proper functioning and maintenance of the software;
- conduct their programming activities in accordance with applicable software industry guidelines or standards;
- maintain their programming activities in accordance with software industry best practices; and
- join, support, and participate in continuing educational programs of applicable industry associations and professional associations applicable to software development, such as CIPS, ACM, IEEE-CS, for example.

The software developers and clients are free to negotiate the scope of work including these 'shoulds', any warranties, and the apportioning of liability through their contractual agreement. Refer to APEGGA's *Development of Consulting Rate Structures and Contracts* for a more detailed discussion of contractual agreements.

Additionally, Professional Members involved in developing software shall:

- ensure that appropriate action or notification of the proper authorities occurs in any instance where they believe that public safety or the environment is endangered, or where required by relevant legislation, regulations, approvals, or orders; and
- assess the risk of software failure as a function of the probability and consequences of such failure and provide necessary safeguards.

These listings of the responsibilities of Professional Members developing software could be made longer. However, the purpose of these listings is to emphasize that there are many obligations that the Professional Member who wishes to develop software should be prepared to undertake, regardless of the development methodology used.

It is recognized that engineering, geological, and geophysical software used in Alberta, may not have been developed in Alberta and not be Authenticated by a Professional Member. Professional Members may Authenticate Professional Documents containing results obtained from such software. However, it is recommended that Professional Members follow the due diligence procedures outlined in APEGGA's *Relying on Work Prepared by Others* when using such software. Professional Members in applying software for professional purposes shall:

- critically assess the fitness of software products for the purpose at hand, considering the systems requirements for functionality, reliability, usability, security, and privacy;
- examine, understand, document, and communicate to all stakeholders the methodologies and input parameters, as well as the limitations of the results obtained;
- verify, where appropriate, new software releases against available standards for general use (e.g., SCADA systems against a security standard such as ISO/IEC 15408, or structural design software against hand calculations);

- take any necessary training available to understand the proper use of the software;
- maintain and use the software in accordance with the published documentation for the software; and
- apply sound technical and professional judgment based upon their experience and expertise that the results being provided by the software are reasonable.

2.4 ENGINEERING, GEOLOGICAL, AND GEOPHYSICAL SOFTWARE REQUIRING AUTHENTICATION

Software may interpret and incorporate engineering, geological, and/or geophysical principles, upon which someone else may rely. Refer to the definitions of the practice of engineering, geology, and geophysics presented in Appendix A. As such, the software may be an engineering, geological, or geophysical product which requires Authentication as per the Act and the Regulations under the Act. Examples of such software may include, but are not limited to:

- Data acquisition, processing, and interpretation software for:
  - Remote sensing, Geographic Information Systems (GIS), photogrammetry, geospatial data, geometrical correction, data visualization and editing
  - Seismic data conversion, data processing and viewing, refraction and reflection interpretation
- Modeling and design software for:
  - Thermal modeling
  - Air dispersion modeling
  - Geographic Information Systems (GIS) modeling
  - Petroleum resource appraisal systems and reservoir simulation
  - Ore reserves estimation and grade control systems
  - Slope stability analysis, structural analysis, pipe stress analysis
  - Electrical and other facility design
- Deployment and control software, such as:
  - Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logic Controllers (PLCs) design or modification that impacts original design parameters
  - System protection (i.e., power, telecommunications, oil and gas)
  - Industrial operation and control (i.e., nuclear facilities, process control for refineries or mills, robotics control systems, radar controlled aircraft landing systems, automated traffic management systems)

Part two of the Act defines an exclusive scope for the practice of engineering, geology, and geophysics. Refer to Appendix A for these definitions. Only Professional Members may take responsibility for engineering, geological, or geophysical software developed in Alberta. Companies who develop engineering, geological, and geophysical software in Alberta must have a permit to do so. Software development activities may be included under an existing permit to practice.

Professional Members often develop software that is not engineering, geological, or geophysical related (i.e., business, financial, or tax software; e-commerce software; database analysis software; gaming software). Such software does not require Authentication as part of Professional Members' regulatory obligations.

However, Professional Members must recognize that their professional and ethical responsibilities remain the same, even if Authentication is not required. Professional Members should seek to familiarize themselves with the legal, ethical, and other responsibilities they may have in such cases. This may include, for example, studying and/or seeking the ISP designation or other internationally recognized relevant computing professional designation.

2.5 AUTHENTICATION PROCESS

How is software to be authenticated? APEGGA's Council has determined that the Regulations concerning the Authentication of Professional Documents shall be interpreted to mean "all originals and all copies of final documents shall include a signed and dated professional stamp or a facsimile thereof".[24]

Software

The original version or modifications of the program or code (either written or electronic) shall be authenticated.[25] The software may be Authenticated by Authenticating the equivalent of the 'cover page' or introduction to that software.

Review of Software and Associated Professional Documents

A Professional Member who has thoroughly reviewed and accepts responsibility for software and the associated Professional Documents prepared by another person shall Authenticate them. The thorough review should include sufficient research, calculations and other professional work so that the professional member is satisfied that the work is safe and meets appropriate codes and standards. The Professional Member's Authentication will be regarded in the same manner as if he or she was the original author. A thorough review does not necessarily imply a complete rework. The test that should be applied is "Does the work meet the acceptable professional and regulatory standards?", not "Is this the way that I would have performed the work?". The Professional Member should describe, either in notes or attached documents, what the review consisted of and how extensive it was.

Professional Documents

Professional Documents (either in electronic or hard copy form) associated with but separate from engineering, geological or geophysical software shall be Authenticated if they contain engineering, geological, or geophysical work of a professional nature. This may include the following design, testing, and commissioning documents:

- design documents, requirements, specifications; including documentation of operating environment (compiler, software versions, etc.)
- physical models of PLC and SCADA systems (i.e., process drawings, mechanical drawings)
- artifacts produced during the course of design and development (i.e., tradeoff analysis, prototypes, analysis elements)
- risks being identified, engaged, mitigated (i.e., by source code control system or version control) and contingency plans
- testing specifications

24 APEGGA Council minutes, April 27, 2000.
25 *Practice Standard for Authenticating Professional Documents V2.0*, APEGGA, April 2002. http://www.apegga.com

- test procedures of software and its interfaces with critical components
- interpretation of test results
- verification by an independent body/organization (e.g., security)
- implementation procedures and guide
- user guides
- training materials and aids
- development and maintenance documents, tools, and aids

Revisions

If engineering, geological, or geophysical software undergoes continuous evolution (as is the case for most commercial software), then the Professional Member responsible for authorizing a release must label and Authenticate the software and/or the Professional Documents that are part of that release. A Professional Document or software that has been revised shall be Authenticated in a manner that clearly indicates a Professional Member's acceptance of responsibility for the revisions. Care should be taken in documenting the revisions to clearly identify the boundary of professional responsibility between the original and revised software and/or documents.

The appearance of a Professional Member's stamp on a Professional Document is taken as indicative of a Professional's involvement and acceptance of responsibility for that work contained in that software or document. Refer to APEGGA's Authentication Practice Standard for a more detailed discussion.

2.6 PROFESSIONAL RESPONSIBILITIES FOR MULTI-DISCIPLINARY PROJECTS

For multi-disciplinary projects, the involved Professional Members shall inform other members of the design team (including non-APEGGA professionals such as ISPs) of design decisions that will affect their disciplines, check for conflicts between disciplines, and clarify areas where responsibilities are unclear. For example, there may be a need to clarify the responsibilities between the disciplines of two or more involved professionals with the following actions:

- responsibility for coordinating the work of technical specialists;
- interface among disciplines (e.g., software requirements for mechanical controls such as developing piping and instrumentation diagrams);
- clearly define responsibilities between the respective areas;
- normalize design criteria and assumptions to ensure consistency among the different areas within the discipline; and
- identify stakeholders of the software in terms of any design constraints being imposed upon the software or environmental conditions that place limitations upon the software.

> A Professional Member, as required under the Code of Ethics, must only undertake work in his or her profession for which he or she is competent and qualified. Therefore, the project manager is entitled to assume that if a Professional Member undertakes an assignment for a portion of the work within the discipline, then the specialty Professional Member is assumed to be competent and qualified. However, if evidence arises that suggests the specialty Professional Member is not competent or qualified, then the manager must undertake such additional work to ascertain whether the person is competent and qualified.

2.7 SAFETY AND SECURITY CONSIDERATIONS

Safety concerns necessarily increase the rigour of the software engineering process and verification is an especially important consideration. Also, extra effort is required for a safety-related system because of additional processes that may be required (e.g., hazards analysis, risk management, use of formal techniques, need for specialized tools etc.).

NASA's new standard provides an example of the integrated approach that is required for software safety.[26]

> "Software safety requires a coordinated effort among all organizations involved in the development of NASA software. This includes program/project/facility managers, hardware and software designers, safety analysts, quality assurance, and operations personnel. Those conducting the software safety activities will also interface with personnel from disciplines such as reliability, security, IV&V, human factors and environmental. The responsibility for development of a safe system, including the software elements, belongs to the program/project manager in conjunction with the local safety and mission assurance organization."

There may also be concerns regarding personal, corporate, and national security. More and more software projects are connecting into our information infrastructure. There is clear international recognition that the information infrastructure is the most critical element in a nation's critical infrastructure – failure of the information infrastructure could bring down all of the elements in the nation's critical infrastructure. It is possible that Canadian government may impose additional legal or regulatory requirements on those organizations with significant connections to Canada's information infrastructure.

Members must familiarize themselves with federal and provincial legislation that regulates electronic information, as required. PIPEDA (Personal Information Protection and Electronic Documents Act)[27] supports and promotes electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions. Alberta's Personal Information Protection Act (PIPA) came into force as of January 2004.[28] The purpose of PIPA is to govern the means by which private sector organizations handle personal information in a manner that recognizes both the right of an individual to have his or her personal information protected and the need of organizations to collect, use or disclose personal information for purposes that are reasonable. For systems storing personal data that are contemplated by PIPEDA or PIPA, a privacy audit or security/vulnerability assessment by a third party is advisable and, in many cases, required.

Specific industry sectors have developed software safety and security standards to be referenced by Professional Members, as required. These standards include, but are not limited to:

- ANSI/UL 1998, *Standard for Software in Programmable Components*. The scope of the standard applied to software whose failure could result in a risk of injury to persons or loss of property. The standard is intended for the evaluation of products

---

26 Section entitled 'Software Safety Management' added to NASA-STD-8719.13B w/ Change 1, *Software Safety Standards*, July 8, 2004. http://www.hq.nasa.gov/office/codeq/doctree/871913.htm

27 http://laws.justice.gc.ca/en/P-8.6/

28 http://www.oipc.ab.ca/pipa/

that rely on software and microelectronics to perform safety-related functions. It is not intended to be used as the sole basis for reviewing safety-related functions, but to be used in conjunction with an application specific standard, directive, regulation or purchasing specification.

- ISO/IEC 61508, *Functional safety of electrical/electronic/programmable electronic safety-related systems.*[29] There are seven parts to this standard covering: general and specific requirements, determination of safety integrity levels, techniques and measures, etc.
- IEC 60880, *Software for computers in the safety systems of nuclear power stations.*[30] This standard discusses software system principles and requirements.
- ISO13485:1996, *Quality systems - Medical devices & ISO 13485:2003, Requirements for regulatory purposes.*[31] Specifies, requirements for the design/development and, when relevant, installation, servicing, and quality management system for medical devices.
- RTCA DO-178B, *Software Considerations in Airborne Systems and Equipment Certification.*[32] This document discusses software considerations for developers, installers, and users, when aircraft equipment design is implemented using microcomputer techniques.
- SAE AS9100, *Aerospace Basic Quality System Standard.*[33] This is the quality system requirements for suppliers to the aerospace industry issued August 2001. The Standard has approximately 80 additional requirements plus other requirements and 18 amplifications of the ISO 9001:2000 Standard.[34]

2.8 VARIOUS ROLES IN THE SOFTWARE DEVELOPMENT TEAM

APEGGA Members may assume many and various roles in the software development team. Note that the number of individuals required to support the following functions will vary with the degree of complexity, the project schedule, the size of the company, and the scope of the professional services offered. Also note that depending on skill sets of the software development team, the allocation of responsibilities, accountability, and authority amongst personnel will vary - these roles will not be uniform from company to company. As an example, the following table lists various specialty roles, and the relative prevalence based upon company and project size.[35]

---

29 Available for purchase at http://domino.iec.ch/
30 Available for purchase at http://domino.iec.ch/
31 Available for purchase at http://www.iso.org
32 http://www.the-as9100-store.com/
33 Available for purchase at http://www.sae.org/
34 *ISO 9001:2000, Quality Management Systems — Requirements*. This standard specifies requirements for a quality management system where an organization: needs to demonstrate its ability to consistently provide product that meets customer and applicable regulatory requirements; and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable regulatory requirements [adapted from the standard's abstract]. The "family" of quality management standards is sometimes colloquially called "ISO 9000". http://www.iso.org
35 Excerpt from Steve McConnell, *Professional Software Development – Shorter Schedules, Higher Quality Products, More Successful Projects, Enhanced Careers*, p. 91 (Addison Wesley, 2003).

Specialty	Number of Software Employees <10	<100	<1,000	<10,000	Ratio Specialists: Generalists
Proportion of Specialists	0%	10-25%	15-35%	20-40%	
Architecture			X	X	1:75
Configuration Control			X	X	1:30
Cost Estimating			X	X	1:100
Customer Support		X	X	X	1:25
Database Administration		X	X	X	1:25
Education and Training				X	1:250
Function Point Counting			X	X	1:50
Human Factors				X	1:250
Information Systems				X	1:250
Integration				X	1:50
Maintenance and Enhancement	O	X	X	X	1:4
Measurement			X	X	1:50
Network		X	X	X	1:50
Package Acquisition				X	1:150
Performance				X	1:75
Planning				X	1:250
Process Improvement				X	1:200
Quality Assurance	O	X	X	X	1:25
Requirements			X	X	1:50
Reusability				X	1:100
Standards				X	1:300
Systems Software Support		X	X	X	1:30
Technical Writing	O	X	X	X	1:15
Testing	O	X	X	X	1:8
Tool Development				X	1:250

O = Occasionally Present; X = Usually Present

Comprehensively defining professional responsibilities for each of these roles is a book-length topic and is outside the scope of this guideline. A detailed discussion of the responsibility, accountability, and authority associated with each role is discussed in detail by others, including but not limited to the following:

- *SWEBOK Guide*[36]
- Occupational Skills Profile Model developed by the Canadian Software Human Resources Council (SHRC)[37]
- IEEE 1490, *A Guide to the Project Management Body of Knowledge*[38]
- ISO/IEC 12207, *Information technology - Software life cycle processes*[39]

2.9 PROCEDURAL GUIDELINES

The choice of software development methodology depends on the culture of the company, the experience and background of staff, and the type of software to be developed. As the learning curve for a development methodology is steep, once a certain methodology is chosen, it may be refined but rarely changed. Whatever development methodology is chosen there should be a clear understanding of why it was chosen and the benefits and pitfalls of choosing it.

Therefore, this guideline does not specify what development methodology or combination of methodologies is to be used or preferred. The only requirement is that organizations must choose a reliable, proven methodology, and put appropriate controls/processes in place that minimize any inherent risks within the chosen methodology.

As the software industry is relatively immature, critics would argue that there is no completely reliable, proven methodology for developing software. Or, conversely, if software developers are restricted to only using 'reliable and proven' methodologies, this would restrict the creation or adoption of improved practices. It is recognized that the world of software is rapidly evolving and that Professional Members must also evolve to stay competent in their technical abilities. However, using new and unproven methodologies may require additional quality assurance/control measures to minimize the associated risks.

There are many procedural guidelines and best practices to assist Professional Members that are readily available online via purchase or open-access. These standards include, but are not limited to:

36 *Guide to the Software Engineering Body of Knowledge*, © IEEE 2004. This body of knowledge and recommended practices was compiled by the IEEE Software Engineering Coordinating Committee as 'generally recognized' knowledge by practitioners. SWEBOK Guide may be used for such purposes as accreditation of academic programs, development of education and training programs, certification of specialists, or professional licensing. http://www.swebok.org

37 The Software Human Resource Council (SHRC) is a not-for-profit sector council, working with industry, education, associations and government to address employment issues that affect information technology workers at all points of their career paths, in all sectors of the Canadian economy. The SHRC has developed the Occupational Skills Profile Model (OSPM), in response to an urgent need for standardized skills in the Canadian IT sector, the public sector and educational institutions. http://www.shrc.ca

38 http://www.ieee.org

39 http://www.iso.ch

- IEEE 1233, *Guide for Developing System Requirements Specifications*
- IEEE 830, *Recommended Practice for Software Requirements Specification*
- IEEE 1058, *Standard for Software Project Management Plans*
- IEEE 1016, *Recommended Practice for Software Design Descriptions*
- IEEE 1063, *Standard for Software User Documentation*
- IEEE 829, Standard for Software Test Documentation
- IEEE 1008, *Standard for Software Unit Testing*
- IEEE 1012 and 1012a, *Standard for Software Verification and Validation*
- IEEE 1061, *Standard for a Software Quality Metrics Methodology*
- ISO/IEC 12207, *Software Life Cycle Processes*
- ISO/IEC 15288, *System Life Cycle Process*
- ISO/IEC 15939, *Software Measurement Process*
- ISO/IEC 16085 (aka IEEE 1540), *Software Risk Management Process*
- Agile Manifesto[40]

3. SUMMARY

Professional Members may be involved in the development and/or usage of engineering, geological, geophysical or other software. Software failure may pose risks to public safety and security. Members must be aware of these risks and of their ethical and professional responsibilities to protect the public.

Many others have developed best practices, guidelines, and standards – some of which are listed here. Professional Members are advised to direct themselves to these other references, as required.

40 http://www.agilemanifesto.org

APPENDIX A - DEFINITIONS OF THE PRACTICE OF ENGINEERING, GEOLOGY, AND GEOPHYSICS

Definitions of "practice" as per the *Engineering, Geological, and Geophysical Professions Act*

1(q) "practice of engineering" means

- (i) reporting on, advising on, evaluating, designing, preparing plans and specifications for or directing the construction, technical inspection, maintenance or operation of any structure, work or process
  - (a) that is aimed at the discovery, development or utilization of matter, materials or energy or in any other way designed for the use and convenience of humans, and
  - (b) that requires in that reporting, advising, evaluating, designing, preparation or direction the professional application of the principles of mathematics, chemistry, physics or any related applied subject, or
- (ii) teaching engineering at a university;

(r) "practice of geology" means

- (i) reporting, advising, evaluating, interpreting, geological surveying, sampling or examining related to any activity
  - (a) that is aimed at the discovery or development of oil, natural gas, coal, metallic or non-metallic minerals, precious stones, other natural resources or water or that is aimed at the investigation of geological conditions, and
  - (b) that requires in that reporting, advising, evaluating, interpreting, geological surveying, sampling or examining, the professional application of the principles of the geological sciences, or
- (ii) teaching geology at a university;

(s) "practice of geophysics" means

- (i) reporting on, advising on, acquiring, processing, evaluating or interpreting geophysical data, or geophysical surveying that relates to any activity
  - (a) that is aimed at the discovery or development of oil, natural gas, coal, metallic or non-metallic minerals or precious stones or other natural resources or water or that is aimed at the investigation of sub-surface conditions in the earth, and
  - (b) that requires in that reporting, advising, evaluating, interpreting, or geophysical surveying, the professional application of the principles of the geophysical sciences, or
- (ii) teaching geophysics at a university;