SOFTWARE CERTIFICATION CONSORTIUM CHARTER

Needs Statement

Critical systems are often subject to certification: a demonstrated assurance that the system has met relevant technical standards and specifications designed to ensure it will not endanger the public, it can be depended upon to deliver its intended service safely and securely and that it is effective. The complexity of software systems, as well as the discontinuous way they behave, renders them extremely difficult to analyze unless great care has been taken with their structure and maintenance.

The goal of certification is to systematically determine, based on the principles of science, engineering and measurement theory, whether an artifact satisfies accepted, well-defined and measurable criteria.

The Software Certification Consortium (SCC) represents a research endeavour, totally devoid of any explicit endorsement by any regulators/companies. Its aim is to understand certification issues with respect to critical systems that contain (significant) software components, and to make recommendations on processes and standards that impact on the certification of such systems. Membership in the consortium by industry, regulators and universities will be encouraged, so that SCC recommendations are practical and effective in the real world. Domains of interest include certification of medical devices, patient management systems, nuclear power plants, automotive and aerospace systems, financial systems, transportation systems and the like. The consortium will serve as a clearing house for sharing knowledge and suggesting research activities related to software dependability leading to certification. The cross domain interest should promote research that not only examines domain specific issues, but also facilitates the sharing of ideas, standards and methods between the different domains and levels of regulation. SCC will aim to disseminate outputs so that they can be taken up in the future by regulator driven open processes and/or standards organizations.

Researchers need to have a direct communication channel with industry practitioners and regulators as to the challenges they are experiencing in certifying software based systems in order to better focus their research efforts. Scalable techniques for engineering and certification of software are required that handle the range of complexity from small devices to complex systems of systems.

The efficacy of techniques used to engineer and certify software needs to be determined through well designed experiments and the collection of operating experience. The resulting empirical data must support the claims made in assurance cases. Root cause analysis of software failures is required to determine areas for improvement in current techniques. A consistent certification framework is required across industry sectors to facilitate sharing of lessons learned. The framework must take into account the varying levels of criticality of software systems. The framework must take into account the needs for re-certification after software maintenance.

The specific competencies of individuals involved with engineering and certifying software need to be specified so that they can be incorporated into the curricula of appropriate university and training programs. Change management is required to accomplish the changes in research program focus, industrial and regulatory practice.

Revision to existing practices and standards are required instead of wholesale re-writes. Commercial-off-the-shelf (COTS) software needs to be certifiable. Tools used for software engineering and certification need to be certified.

Objectives

The SCC is organized to pursue the following objectives:

- To promote the scientific understanding of certification for Systems containing Software (ScS) and the standards on which it is based;

- To promote development and improvement of consensus standards supporting certifiable software-intensive systems and their certification, through transfer of knowledge to existing standards organizations;

- To promote public, government and industrial understanding of the concept of ScS certification and the acceptance of the need for certification standards for software related products;

- To co-ordinate software certification initiatives and activities to further the above objectives.

Goals to Achieve SCC Objectives

Primary Goal

- Develop and document a generic framework for certification, supporting domain specific certification frameworks and criteria.

Detailed Goals

- Use existing knowledge to develop appropriate evidence-based standards and audit points for critical software in specific domains, including hard real-time, safety-critical systems.

- Research and develop improved methods and tools for the development and certification of critical software, conforming to the above standards and audit points.

- Proof of concept: Develop and document software requirements and necessary system requirements and constraints that help developers and regulators in the realization of critical software applications in specific domains.

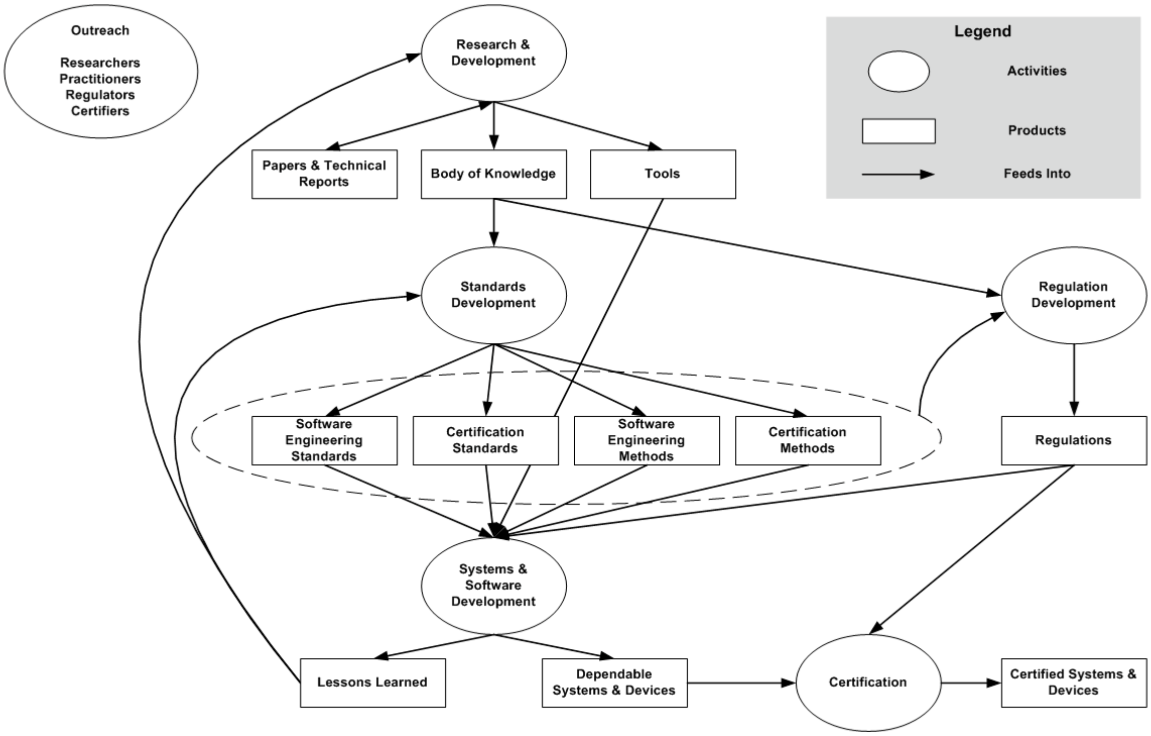
- Scope & Deliverables

The scope of work necessary to accomplish the objectives and goals above involves the coordination of the work program of SCC partners in the areas of, *inter alia*:

1) **Research and Development**:
    a. To produce research papers and technical reports focusing on approaches and techniques in software engineering for certifiable software-intensive systems and their certification,
    b. To develop a structured Body of Knowledge related to the development of certifiable software-intensive systems and their certification, and
    c. To develop knowledge for evaluating tools supporting the development of certifiable software-intensive systems and their certification, including qualification of commercial tools to support development and evaluation of certifiable systems.

2) **Standards Development**: Foster development and improvement of consensus standards supporting certifiable software-intensive systems and their certification, through transfer of knowledge to existing standards organizations.

3) **Experience** in the usage of the Standards, Methods and Tools to document operating experience in the areas of:
    a. Systems and software development,
    b. Certification, and
    c. Licensing approval.



4) **Administration** and coordination of the overall program in terms of:
    a. Planning and coordination of the interdependent initiatives,
    b. Communication with all stakeholders,
    c. Holding Steering Committee and working group meetings, and
    d. Managing SCC funds supporting the initiatives.

5) **Outreach** in order to learn about research needs and to communicate results and collect feedback from:
    a. The research community,
    b. Industrial practitioners, and
    c. Regulatory agencies

Schedule Milestones

The following major milestones have been established:

No.	Milestone	Target Date
1	**RESEARCH & DEVELOPMENT**	
1.1	Understand current state: Assessment of state-of-the-art & state-of-the-practice	June 2011
1.3	Issue Body of Knowledge (Rev 0) required to support improved methods of practice	Dec 2013
1.4	Issue guidance on certification & development practices	Dec 2014
2	**STANDARDS DEVELOPMENT**	
2.1	Identify standards requiring revision or development	Dec 2011
2.2	Engage with standards committees	Dec 2012
3	**EXPERIENCE**	
3.1	Multi-sector lessons learned report	June 2011
3.2	Complete Pacemaker challenge	June 2011
3.3	Publish book on pacemaker challenge	June 2012
3.4	Issue lessons learned report re pacemaker challenge	Dec 2011
4	**ADMINISTRATION**	
4.1	Establish charter and organization for SCC	Dec 2010
4.2	Establish membership rules and regulations	June 2011
4.3	Establish administrative infrastructure	June 2011
4.4	Issue coordinated plan of action	June 2011
5	**OUTREACH**	
5.1	Establish annual conference event	Dec 2011
5.2	Establish technical report series	Dec 2010
5.3	Establish annual mechanism for identifying research needs	June 2011

Resources & Funding

The core means by which the SCC will accomplish its work program is through coordination and focusing of existing work programs within universities, standards organizations and companies involved with development of software intensive systems.

The McMaster Center for Software Certification will fund much of the administration and coordination efforts.

In cases where specific initiatives are identified that are of common interest but not supported with resources, SCC would facilitate the appropriate SCC partners in seeking resources.

Membership

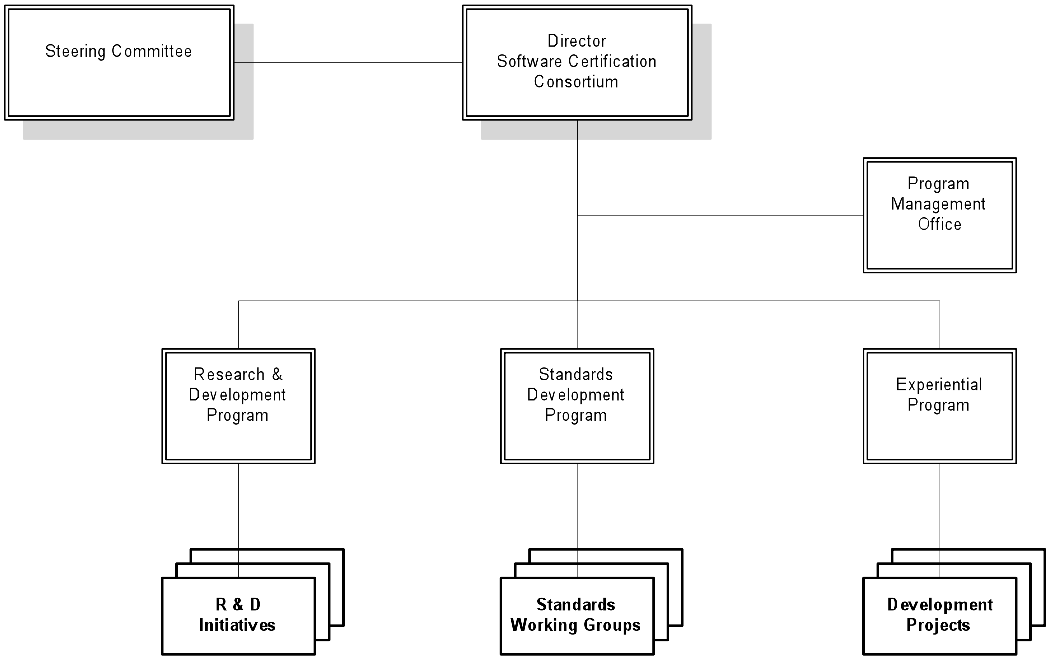
Two categories of membership will be established.

Partners will be individuals who are actively engaged in performing one or more of the elements of the SCC work program.

Members will be individuals who actively participate in SCC workshops.

Authorities & Accountabilities

The figure below shows the organizational structure for the SCC. The authorities and accountabilities for each position are defined below:


Steering Committee
Director Software Certification Consortium
Program Management Office
Research & Development Program
Standards Development Program
Experiential Program
R & D Initiatives
Standards Working Groups
Development Projects

Director – Software Certification Consortium:

- Responsible for the overall SCC work program and its organization
- Accountable to the Steering Committee and informing it as needed

Steering Committee:

- Representation from research, industry and regulators
- Approves governance processes and management practices
- Approves new initiatives into the SCC program
- Sets priorities for the SCC overall program
- Approves membership rules and applications

Program Management Office:

- Proposes the program management practices that will be followed,
- Proposes and supports governance processes,
- Manages schedule and budget at the program level,
- Provides document configuration management,
- Provides centralized support for managing changes and tracking risks and issues.
- Defines and supports execution of the communication plan to keep members and stakeholders informed.

Research & Development Program:

- Set of projects / initiatives working to organize the body of knowledge for software engineering relevant to certification, and supporting tools, to identify gaps in the knowledge, and to identify and promote ways and means to bridge these gaps.

Standards Development Program:

- Set of initiatives to identify gaps in standards and guidelines for software engineering relevant to certification, to identify and promote ways and means to bridge these gaps, and, where needed, to provide the knowledge or technical basis to the appropriate standardization bodies and working groups.

Experiential Program:

- Set of projects / initiatives to evaluate, demonstrate, monitor or track the efficacy of methods and tools relevant to the SCC objectives, e.g. software engineering activities relevant to certification.