20th ANNIVERSARY
CASCON
2010
HONOURING TWO DECADES OF RESEARCH & INNOVATION
Smarter Technologies for a Smarter Planet

Software Certification Consortium

Workshop

SOFTWARE CERTIFICATION CONSORTIUM

November 3rd & 4th

6th SCC Meeting - Welcome

- First SCC Workshop
  - A big thank you to IBM and the CASCON organizers – we did not fit the profile they were looking for, but they have accommodated our needs in spite of that!
- SCC Workshop Organizing Committee
  - John Hatcliff
  - Mark Lawford
  - Tom Maibaum
  - Alan Wassyng
  - Jens Weber

6th SCC Meeting - History

- SCC founded in 2007
  - Mark Lawford, Tom Maibaum, Alan Wassyng (McMaster)
  - Brian Larson (Boston Scientific)
  - Jo Atlee (Waterloo), Marsha Chechik (Toronto), Jonathan Ostroff (York)
- Steering Committee
  - Rick Chapman, Paul Jones (FDA)
  - John Hatcliff (Kansas State), Insup Lee (Pennsylvania)
  - Brian Larson (Multitude Corporation), Bran Selic (Malina Software)
  - Mark Lawford, Tom Maibaum, Alan Wassyng (McMaster)

6th SCC Meeting - History

- The idea
  - A group of researchers/practitioners from industry, regulatory agencies and academia, getting together informally to see how they can improve the dependability of systems that depend on software
  - Share knowledge, discuss approaches, encourage participation/ liaison in standards organizations/committees to help develop more effective ways of building highly dependable software applications, and more effective ways of evaluating the dependability, efficacy, and especially safety of these applications

6th SCC Meeting - History

- Previous meetings
  - August 2007, SEI Offices in Arlington Virginia
    - Original goals & objectives
  - December 2007, University of Minnesota
    - Hurdles, SoftCert paper
  - April 2008, SEI Offices in Arlington Virginia
    - Technical discussion, Direction for SCC
  - May 2010, University of Pennsylvania
    - Draft Charter, Technical discussion
  - August 2010, hosted by NRC, Rockville Maryland
    - Draft Charter, Plan for research, Technical discussion

SCC Objectives (refined)

- 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 such certification 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 (refined)

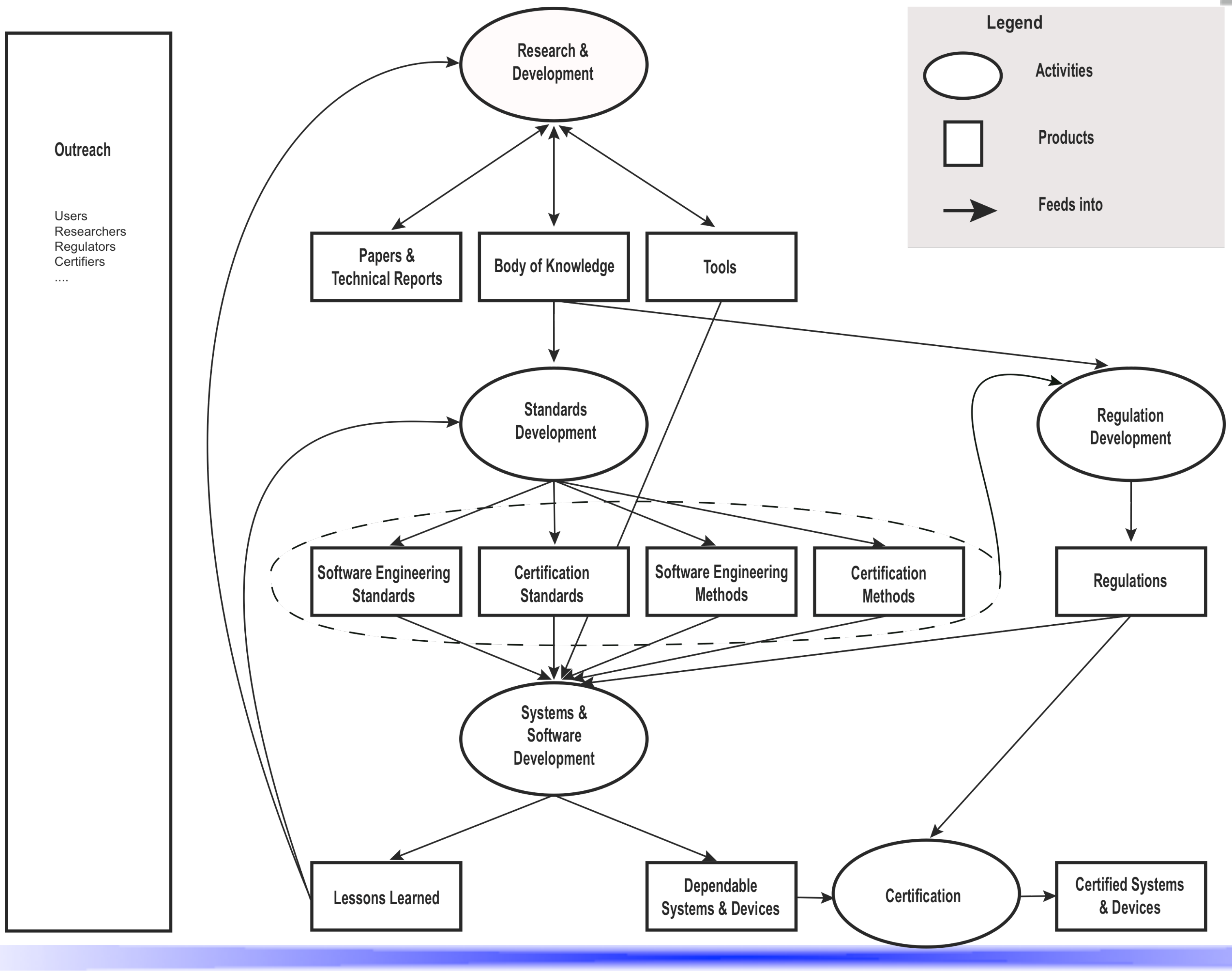
- Primary Goal
  - Develop and document a generic framework for certification, supporting domain specific certification frameworks and criteria
- Detailed Goals
  - Use existing knowledge to develop appropriate evidence-based standards and audit points for critical software in specific domains, including 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 SCC objectives and goals involves the coordination of the work program of SCC partners in the areas of, *inter alia*:

- *Research and Development*:
  - To produce research papers and technical reports focusing on approaches and techniques in software engineering for certifiable software-intensive systems and their certification
  - To develop a structured Body of Knowledge related to the development of certifiable software-intensive systems and their certification
  - 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
  - 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.
- *Experience* in the usage of the Standards, Methods and Tools to document operating experience in the areas of:
  - Systems and software development
  - Certification
  - Licensing approval

Scope & Deliverables



SCC Meeting Schedule

- Three meetings per year
  - Two business oriented meetings with some technical discussion
    - These are likely to be held mainly in the US and probably most often in the Washington DC area
  - One technical workshop (with minimal business sessions)
    - One idea is to attempt to run this as a CASCON Workshop every year
    - Thanks again to IBM and the CASCON organizers

The Time is Right

- We started a software certification initiative in 2004
- Could not get people to take it seriously
- The fact that SCC started off successfully in 2007 was due to the fact that interest in software certification was starting to build
- There are now workshops and tracks at conferences dedicated to software certification
- Many people still think you can develop technology and then bolt-on a certification aspect – it does not work (easily/ effectively)

Principle

- It is reasonably obvious (maybe) – but still needs to be said:

- There are two complementary aspects –
  - Need to determine how to build software applications that can be certified effectively
  - Need to determine how to certify software applications

Wednesday 3rd Nov

20th ANNIVERSARY CASCON 2010 HONOURING TWO DECADES OF RESEARCH & INNOVATION

08:30 – 10:00	**Welcome and Opening Keynote**
08:30 – 09:15	Welcome & Introductions & Background on the Software Certification Consortium (SCC) and its Goals Workshop Organizing Committee
09:15 – 10:00	Invited Talk: The Recent Trend to Assurance Cases – Pros and Cons By Tom Maibaum (McMaster) and Hans Bherer (McMaster)
10:00 – 10:30	***Coffee Break***
10:30 – 12:00	**Session 1: Regulatory Perspectives on Software Certification - Panel**
10:30 – 11:00	Regulatory perspectives on software for nuclear applications By Robert Lojk (Canadian Nuclear Safety Commission)
11:00 – 11:30	Perspectives on certifying software in safety systems for nuclear power plants By Sushil Birla (U.S. Nuclear Regulatory Commission)
11:30 – 12:00	Assurance Cases for Certification of Infusion Pumps By Paul Jones (U.S. Food and Drug Administration)
12:00 – 13:00	***Lunch***
13:00 – 14:00	Panel discussion to end Session 1
14:00 – 14:30	**Session 2: A Specific Instance of Regulation - View from Industry**
14:00 – 14:30	Regulation of Patient Management (eHealth) Software in Canada By James Williams (Blue Pebble) and Jens Weber (U Victoria)
14:30 – 17:00	**Session 3: Tools for Software Certification**
14:30 – 15:00	Smoother Integration of Contract-based Verification into Development Workflows for Certified Systems By John Hatcliff (Kansas State University)
15:00 – 15:30	Workflow Management for Health Care Processes Meets Formal Verification By Fazle Rabbi and Wendy MacCaull (St. Francis Xavier)
15:30 – 16:00	***Coffee Break***
16:00 – 16:30	Assurance Cases for Proofs as Evidence By Arie Gurfinkel (SEI)
16:30 – 17:00	The Tabular Expression Toolbox for Matlab/Simulink By Colin Eles and Mark Lawford (McMaster)

Thursday 4th Nov

08:30 – 10:00	**SCC Business and Keynote**
08:30 – 09:15	SCC Business – Charter and Meeting Schedule
09:15 – 10:00	Invited Talk: The Perceptual and Cognitive Consequences of Aging (and why engineers should care about such things) By Pat Bennett (McMaster)
10:00 – 10:30	***Coffee Break***
10:30 – 12:00	**Session 4: Case Studies in Software Certification**
10:30 – 11:00	Certification of eHealth software By Jens Weber (U Victoria)
11:00 – 11:30	Assurance Cases in Model-Driven Development of the Pacemaker Software By Eunkyoung Jee, Insup Lee, and Oleg Sokolsky
11:30 – 12:00	The Rational Design Process Used for the Darlington Shutdown Systems – Developing Safety-Critical Software for Auditable Certification By Alan Wassyng (McMaster)
12:00 – 13:00	***Lunch***
13:00 – 14:00	**Session 5: Certification of COTS and pre-developed software**
13:00 – 13:30	Measuring and Assessing Software Trustworthiness: Approaches and Challenges By Elizabeth Fong (NIST)
13:30 – 14:00	Software – Friend or Foe By Jeff McDougall, David Tremaine and Tom McCormick (SWI)
14:00 – 15:30	Panel Discussion: The Future of Software Certification
15:30 – 16:00	***Coffee Break***
16:00 – 17:00	Discussion of the SCC's Mandate and Review of the SCC’s Software Certification Roadmap

A Word from Each of the Organizers

John Hatcliff

Mark Lawford

Tom Maibaum

Alan Wassyng

Jens Weber