

Software Certification Consortium

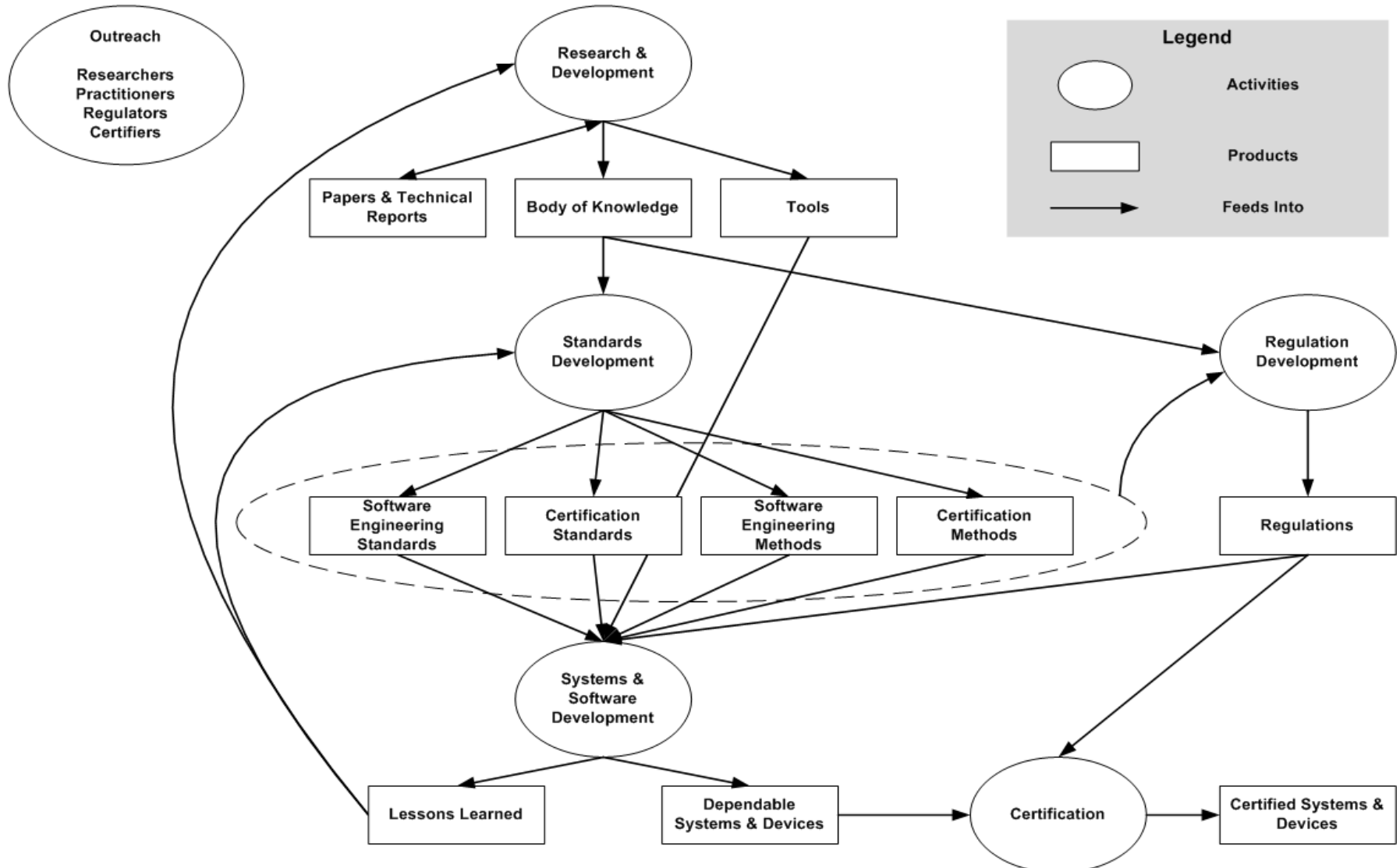
Meeting #12
October 28 - 29, 2013



Welcome & Introductions

- **Alan Wassyng**
- **Sushil Birla**
- Workshop Participants
- Remote Participants

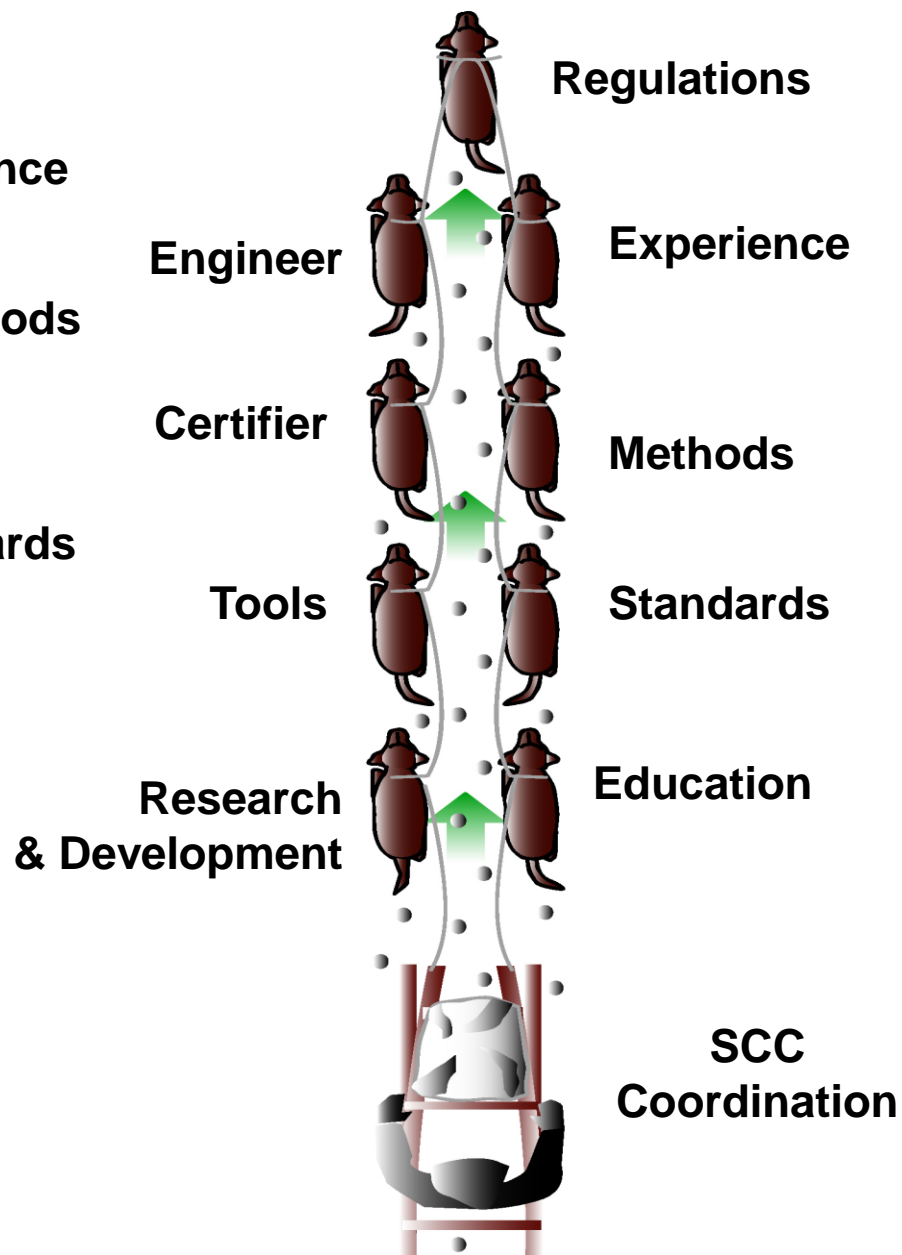
Scope & Deliverables





Dog Sled - Not Aligned

Same Effort but Progress



Dog Sled - Aligned

Workshop Theme

System Safety Requirements

Methods for their Development and Validation

Agenda

<u>MONDAY</u>	
08:30 – 09:00	Introductions & Context
09:00 – 09:30	Nancy Leveson – MIT Introduction To A Systems Approach To Requirements Generation For Safety
09:30 – 10:00	John McDermid – University of York The "Classical" Approach To Deriving Safety Requirements
10:00 – 10:15	<i>Coffee</i>
10:15 – 11:00	Discussion 1
11:00 – 11:30	Sushil Birla – US NRC Evaluating Hazard Analysis Of A Distributed Digital System For Nuclear Reactor Safety
11:30 – 12:00	Paul Jones – US FDA What The FDA Looks For In Submitted System Safety Requirements
12:00 – 13:00	<i>Lunch</i>
13:00 – 13:45	Discussion 2
13:45 – 15:30	Breakout #1 & Coffee
15:30 – 16:30	Report Back
17:30 – 18:30	<i>Social at TBD</i>
18:30 – 21:00	<i>SCC Dinner at P.F. Changs – White Flint Mall – 11201 Rockville Pike</i>

Agenda

<u>TUESDAY</u>	
08:30 – 09:00	Donald Firesmith – SEI The Four Types Of Safety-Related Requirements And Their Relationships To Other Types Of System Requirements
09:00 – 09:30	Tom Maibaum – McMaster University Quality, Measurement (and Assurance Cases)
09:30 – 09:45	<i>Coffee</i>
09:45 – 10:30	Discussion 3
10:30 – 11:00	Peter Feiler – SEI Architecture-centric Strategies for Addressing Challenges in Software-reliant Safety-critical Systems
11:00 – 11:30	John Thomas – MIT Generating Executable Software Requirements Through Hazard Analysis
11:30 – 12:00	Connie Heitmeyer – NRL Specifying Requirements for Safety-Critical Systems
12:00 – 13:00	<i>Lunch</i>
13:00 – 13:45	Discussion 4
13:45 – 15:00	Breakout #2 & Coffee
15:00 – 16:00	Report Back
16:00 – 16:30	Summary & Wrapup

Breakout #1

Establishing System Safety Requirements

1. What are the existing methods for establishing system safety requirements?
2. What are the outstanding issues associated with this set of methods?
 - Are the issues domain specific?
3. What are the actions required to address the issues?
 - Are you already working on these actions?
 - Would you like to work on them?
 - Who would you like to work with?

Breakout #2 – Certification

- 1) What are the means for:
 - gaining confidence that the system safety/security requirements are complete and correct?
 - Including requirements necessary to deal with hazards introduced during the design of the system
 - gaining confidence that the system safety/security requirements are adequately implemented?
- 2) What are the issues associated with the above means?
- 3) What are the actions required to address the issues?
 - Are you already working on these actions?
 - Would you like to work on them?
 - Who would you like to work with?

Action Items