Software Certification Consortium
Meeting #10
January 7 - 8, 2013

EVIDENCE REQUIRED FOR HIGHEST INTEGRITY LEVEL SYSTEMS

DAY 1

8:45 – 9:00	Introduction
Session 1	**Evidence that the system requirements are correct, complete and understandable**
9:00 – 9:30	**Rance Cleaveland**, University of Maryland / Fraunhofer USA Analyzing Consistency and Completeness of Requirements: A Model-Based Approach
9:30 – 10:00	**Ramesh S.**, GM Global R&D Formal Methods Based Requirement Engineering for Automotive Embedded Systems
10:00 – 10:30	Discussion
10:30 – 10:45	*Coffee*
10:45 – 12:00	Breakout Session 1
12:00 – 12:30	Report Back from Breakouts
12:30 – 1:30	*Lunch*
Session 2	**Evidence that the implementation meets its requirements**
1:30 – 2:00	**John Knight**, University of Virginia Finally: Practical Formal Verification of Large Software Systems
2:00 – 2:30	**Daniel Jackson**, MIT Self evidently true: rethinking software design
2:30 – 2:45	*Coffee*
2:45 – 3:15	**Elizabeth Fong**, NIST Software Assurance Tools to Improve Evidence Strength
3:15 – 3:45	Discussion
3:45 – 5:00	Breakout Session 2
5:00 – 5:30	Report Back from Breakouts

DAY 2

Session 3	**Evidence that the operational and maintenance requirements and constraints are identified correctly and satisfied**
9:00 – 9:30	**Oleg Sokolsky & Insup Lee**, University of Pennsylvania Understanding Evidence: Lessons from the GPCA Case Study
9:30 – 10:00	**Norbert Carte**, US Nuclear Regulatory Commission Evidence that the Operational and Maintenance Requirements and Constraints are Identified Correctly and Satisfied
10:00 – 10:30	Discussion
10:30 – 10:45	*Coffee*
10:45 – 12:00	Breakout Session 3
12:00 – 12:30	Report Back from Breakouts
12:30 – 1:30	*Lunch*

Session 4	**Analysis & Future Work**
1:30 – 2:45	Breakout Session 4
2:45 – 3:00	*Coffee*
3:00 – 4:30	Report Back from Breakouts
4:30 – 5:00	Action Items
5:00 – 5:15	Concluding Session

BREAKOUT Session #1 – Evidence that the system requirements are correct, complete and understandable

1) Identify the item(s) of evidence that would capture the system requirements

2) Identify the acceptance criteria for each item of evidence identified in 1)

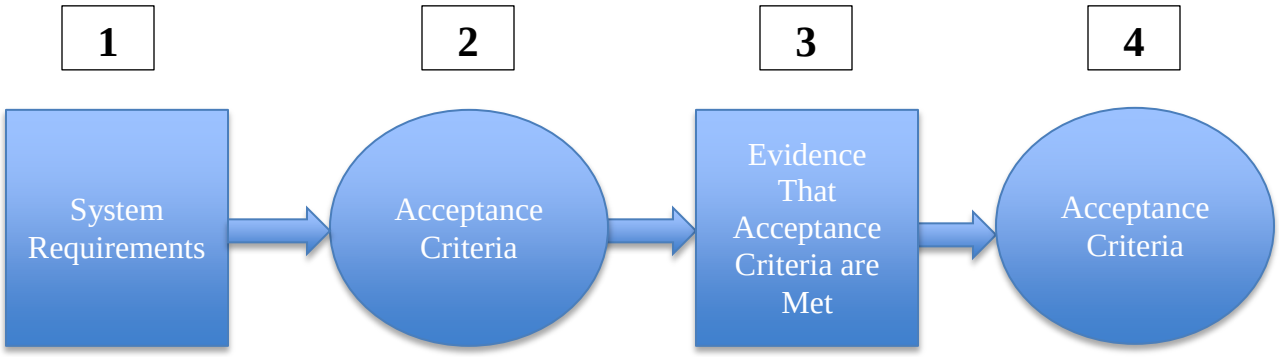
3) Identify what evidence is required to provide assurance that the acceptance criteria for the System Requirements identified in 2) have been met with an adequate degree of confidence for a high integrity system
    a. Provide rationale for each item of evidence identified
    b. Provide rationale for why the set of items of evidence are "complete"

4) For each item of evidence identified in 3) list the acceptance criteria that would be used to determine if the evidence is acceptable

5) For each acceptance criterion identified in 2) and 4) identify whether there is general consensus on the acceptance criterion, or if further research is required to provide a basis for consensus, or if there is actual disagreement on the value of the acceptance criterion

6) For each item in 5) where there is not general consensus, identify the scope of work necessary to provide a basis for consensus

7) For each item in 6) identify who would be good candidates to perform the work.



BREAKOUT Session #2 – Evidence That the Implementation Satisfies the Requirements with the Appropriate Degree of Confidence for a Safety Critical Application

1) Identify the relevant item(s) of evidence that result from implementation

2) Identify any acceptance criteria for each item of evidence identified in 1) that is prerequisite to gaining confidence that the implementation satisfies the system requirements

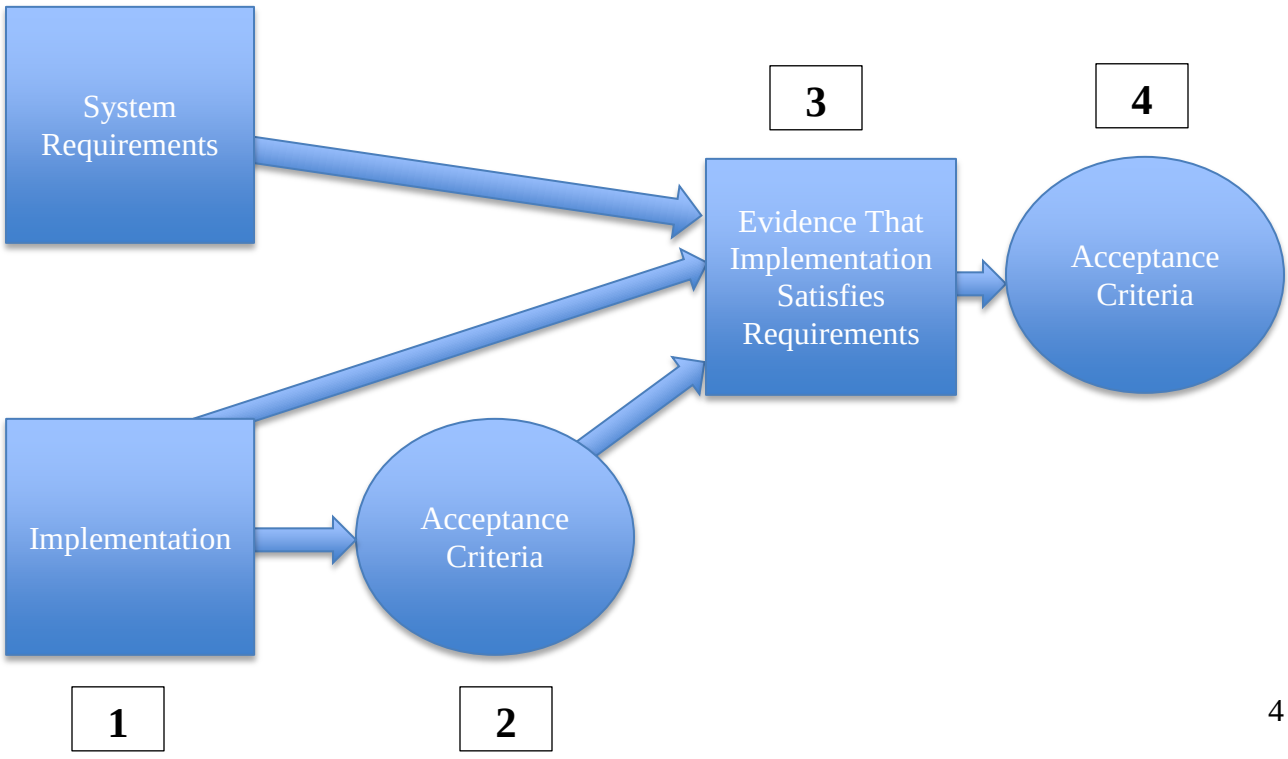
3) Identify what evidence is required to provide assurance that the Implementation Satisfies the System Requirements with the Appropriate Degree of Confidence for a Safety Critical Application

4) For each item of evidence identified in 3) list the acceptance criteria that would be used to determine if the evidence is acceptable

5) For each acceptance criterion identified in 4) identify whether there is general consensus on the acceptance criterion, or if further research is required to provide a basis for consensus, or if there is actual disagreement on the value of the acceptance criterion

6) For each item in 5) where there is not general consensus, identify the scope of work necessary to provide a basis for consensus

7) For each item in 6) identify who would be good candidates to perform the work.



BREAKOUT Session #3 – : Evidence that the operational and maintenance requirements and constraints are identified correctly and satisfied

1) Identify the item(s) of evidence that capture the operational and maintenance requirements and constraints, including resources.

2) Identify the acceptance criteria for each item of evidence identified in 1)

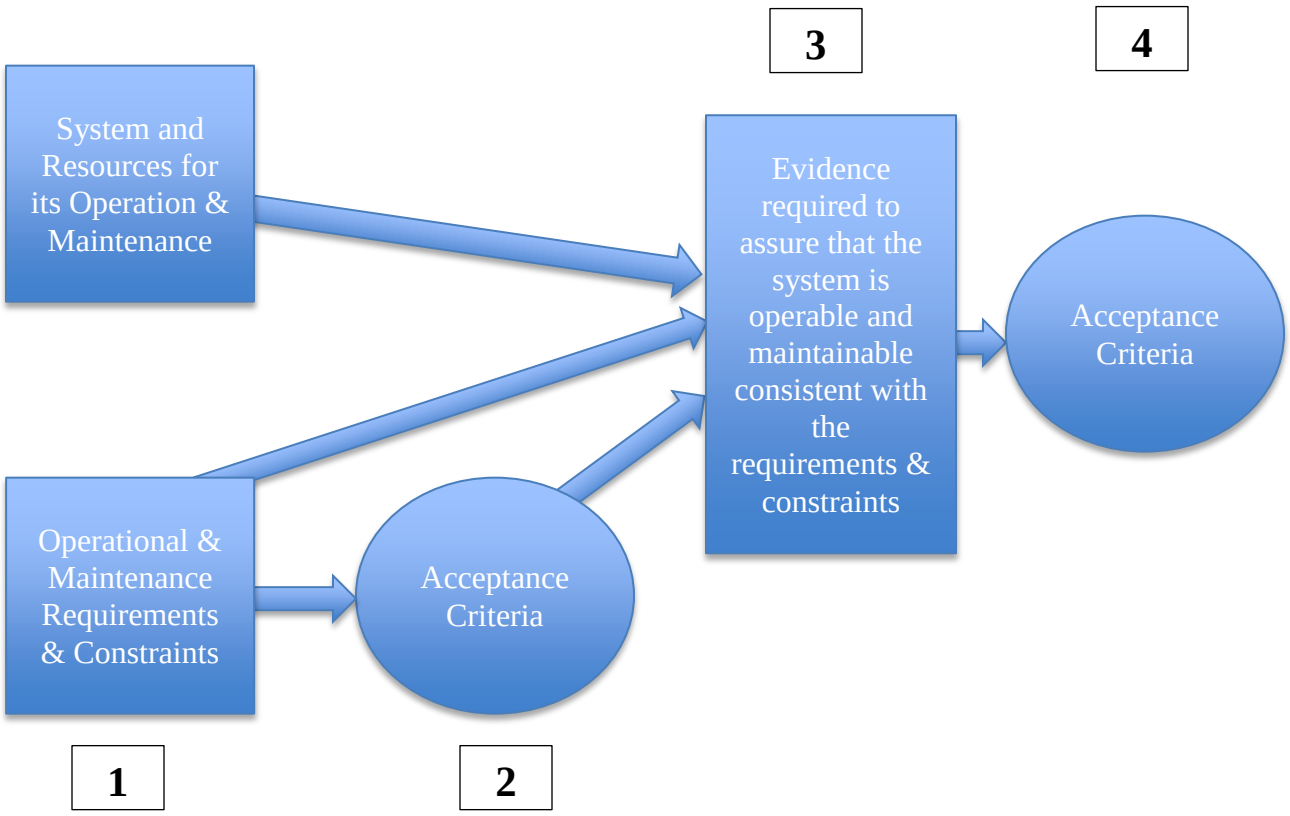
3) Identify evidence required to assure that the system is operable and maintainable consistent with the requirements & constraints identified in 1)

4) For each item of evidence identified in 3), define criteria for its acceptance.

5) For each acceptance criterion identified in 4) identify whether there is general consensus on the acceptance criterion, or if further research is required to provide a basis for consensus, or if there is actual disagreement on the value of the acceptance criterion

6) For each item in 5) where there is not general consensus, identify the scope of work necessary to provide a basis for consensus

7) For each item in 6) identify who would be good candidates to perform the work.



Breakout Session #4 - Planning for Future SCC Work

1) From the work items identified in breakout sessions 1, 2 and 3, select the top 10 and rank them.

2) For each scope of work in the top 10, identify if there are existing work programs that adequately address the same scope of work

3) For the top 10 scopes of work where there is inadequate existing work ongoing, estimate the funds required to carry out the scope of work

4) If possible, identify the willingness of the candidates to perform their work as part of a coordinated SCC work program (if they are in the room)
5) Rank the top 5 items of work where there is inadequate work ongoing

6) Identify potential participants for each item

7) Estimate funding required for each item.