Automated Rapid Certification Of Software (ARCOS)

Ray Richards
Program Manager

Proposers' Day

14 May 2019

Agenda

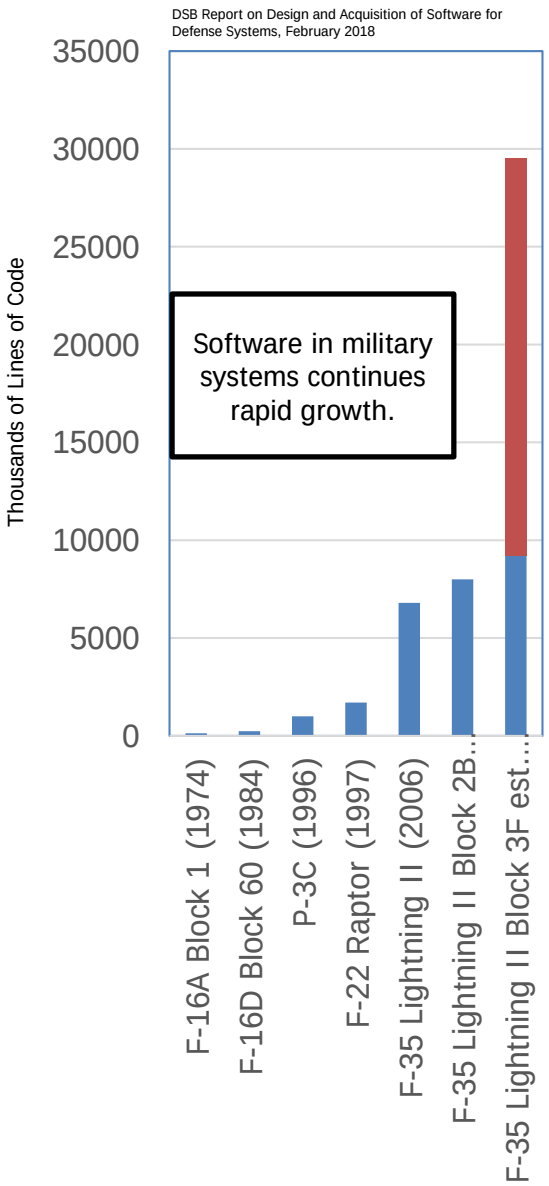
Time	Item
8:30 AM	Registration
9:30 AM	Welcoming Remarks, Dr. Ray Richards
9:35 AM	Security Briefing, DARPA Security
9:40 AM	ARCOS Program Briefing, Dr. Ray Richards
10:00 AM	Software Certification, Dr. John Seel
10:20 AM	Seedling Results, Dr. Gustavo Quiros Araya, Siemens Corporation
10:40 AM	Break and Submit Questions
11:00 AM	Contracts Management Office Briefing , Mr. Mark Jones, DARPA CMO
11:30 AM	Teaming Intro Briefs – 2 min each** (Part 1)
12:00 PM	Lunch Break (on your own)
1:00 PM	Question and Answer Session
2:00 PM	Teaming Intro Briefs – 2 min each** (Part 2)
2:30 PM	Networking Session - Conference room will remain available
3:30 PM	Meeting Adjourns

ARCOS Vision

Automated Rapid Certification Of Software (ARCOS)

Automate the evaluation of software assurance evidence to enable certifiers to rapidly determine that the risk of software deployment is acceptable.

Current software certification practices are unsustainable



- Our ability to produce software has outpaced our ability to certify software
- The cost and time needed to certify software is an impediment to fielding new capability
- Software certification cost is a major consideration in managing a systems lifecycle.
- Certification example: Multi-level secure operating system certified for F22 and F35 in accordance to the Common Criteria
  - Previously certified in safety critical avionics
  - Evaluation underway by April 2006
  - Certificate awarded January 2011

National Information Assurance Partnership

Common Criteria Certificate

is awarded to

Green Hills Software, Inc.

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Versions 2.3, 3.0, 3.1) for conformance to the Common Criteria for IT Security Evaluation (Version 2.3). This certificate applies only to the specific version(s) and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name: INTEGRITY-178B Separation Kernel
Evaluation Platform: INTEGRITY-178B Real Time Operating System (RTOS), version IN-ICR750-0402-GH01_Rel (Version 4.2) running on Compact PCI card, version CPN 944-2021-021 w/PowerPC, version 750CXe
Assurance Level: EAL 6+, High Robustness

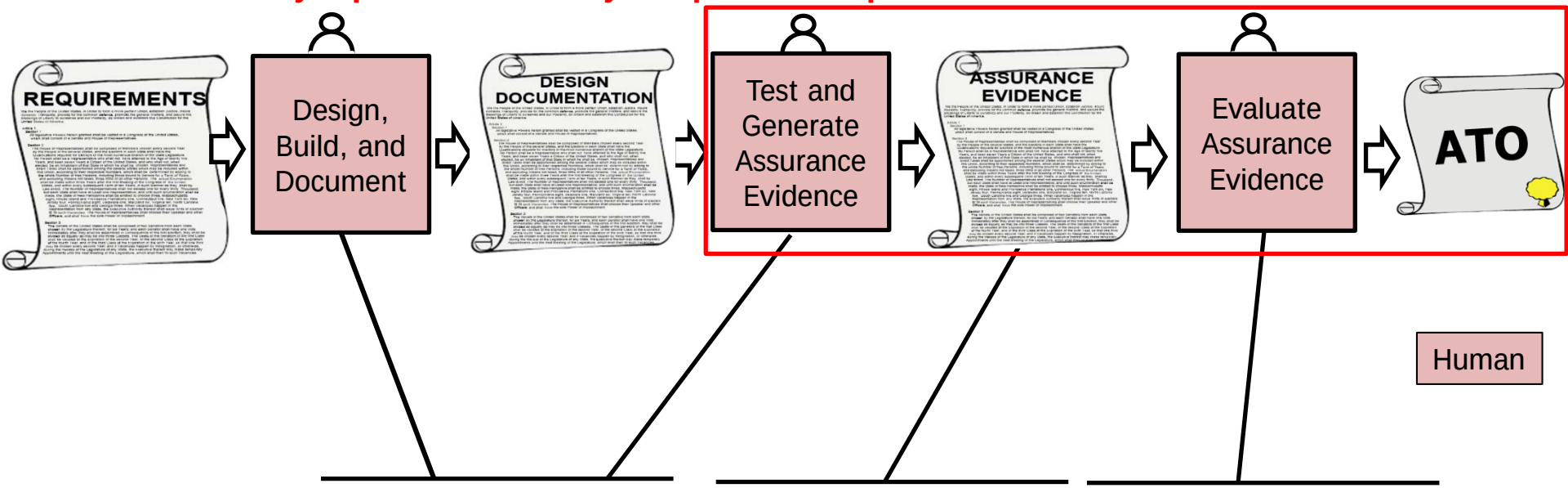
CCTL: Science Applications International Corporation
Validation Report Number: CCEVS-VR-VID10362-2011
Date Issued: 31 January 2011
Protection Profile: US Government Protection Profile for Separation Kernels in Environments Requiring High Robustness, Version 1.03, 29 June 2007

Original Signed By
Director, Common Criteria Evaluation and Validation Scheme
National Information Assurance Partnership

Original Signed By
Information Assurance Director
National Security Agency

Software certifications today

Certifications today: Up to 5 additional years post-development to obtain ATO



Human-driven activities produce implementation and assurance evidence in human readable documents

Assurance evidence captured in human readable documents

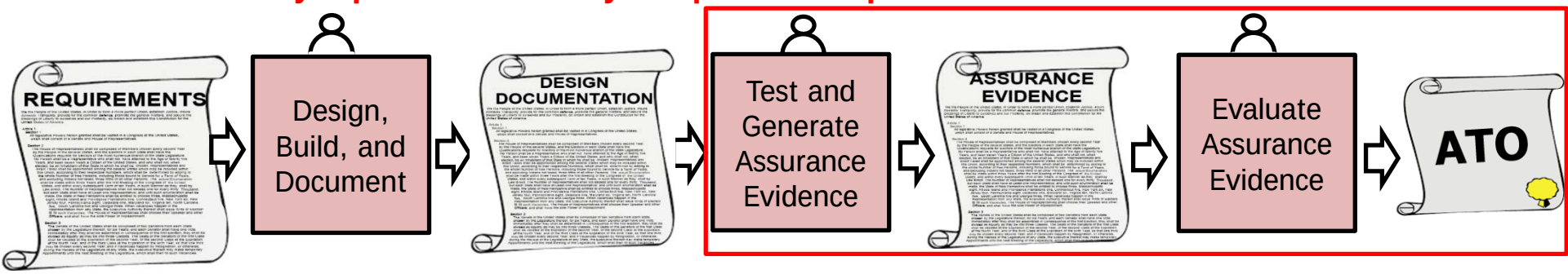
Manual activity evaluates whether or not criteria are met

Evidence:
- Test
- Analysis
- Simulation/Emulation
- Software Quality Assurance (SQA)

ATO: Authority to Operate

Software certifications with ARCOS

Certifications today: Up to 5 additional years post-development to obtain ATO



Certifications with ARCOS: ATO concurrent with development

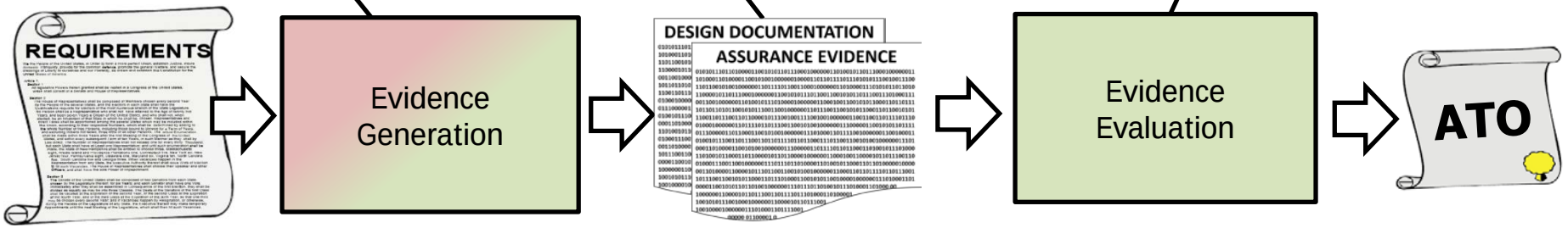
Human

Automated

Co-generation of assurance evidence with documentation and implementation artifacts

Implementation and assurance evidence maintained in binary formats

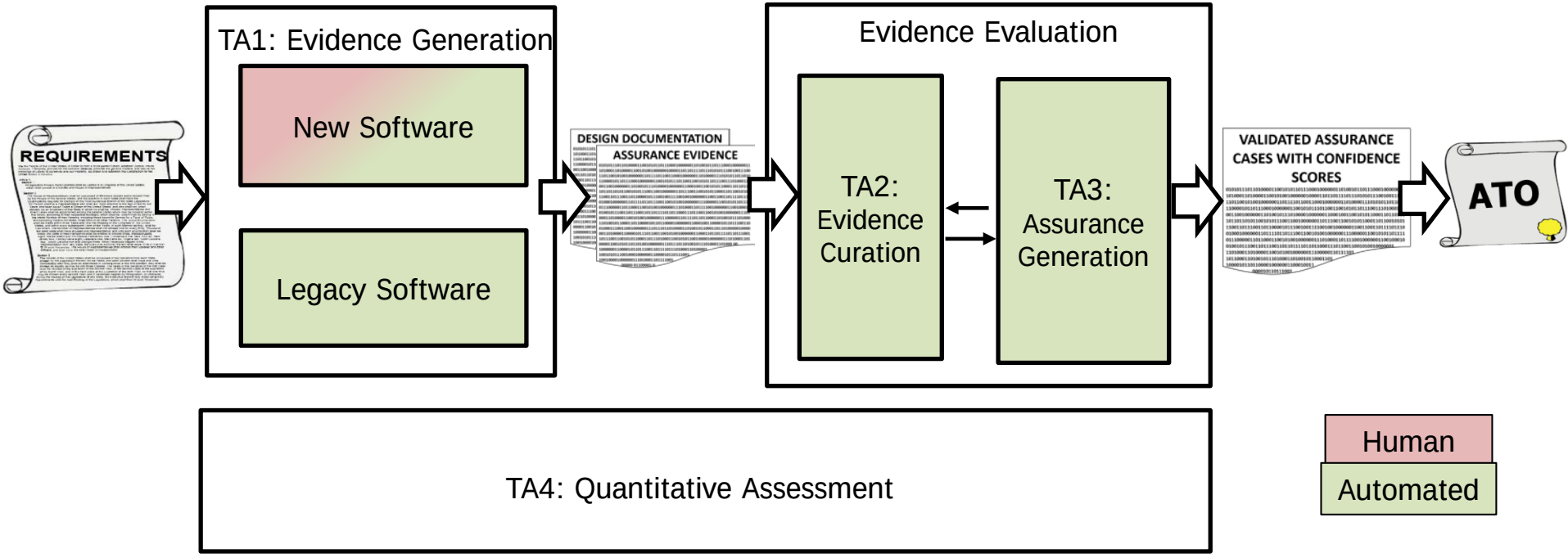
Automated generation and validation of **assurance case arguments**



ARCOS Program Structure

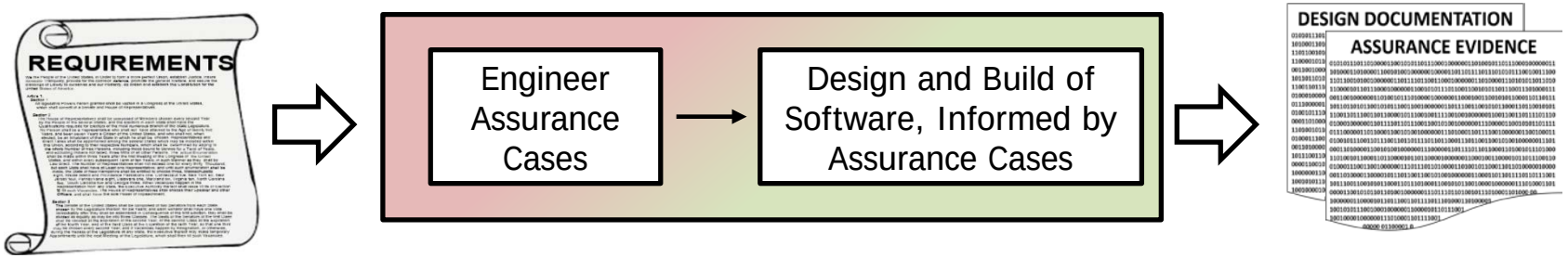
ARCOS Technical Approach and Technical Areas

- TA1: Generation of high quality assurance evidence to support curation and facilitate TA3 analytics
- TA2: Curate a large disparate body of evidence to support TA3 analytics
- TA3: Generate assurance arguments and use data analytics to back the arguments with evidence
- TA4: Provide a series of challenges culminating in the processing of evidence and generation of assurance for a realistic system



TA 1: Evidence Generation for New Software

Goal: Create technologies to construct assurance cases that drive the design and implementation of software



Challenges:

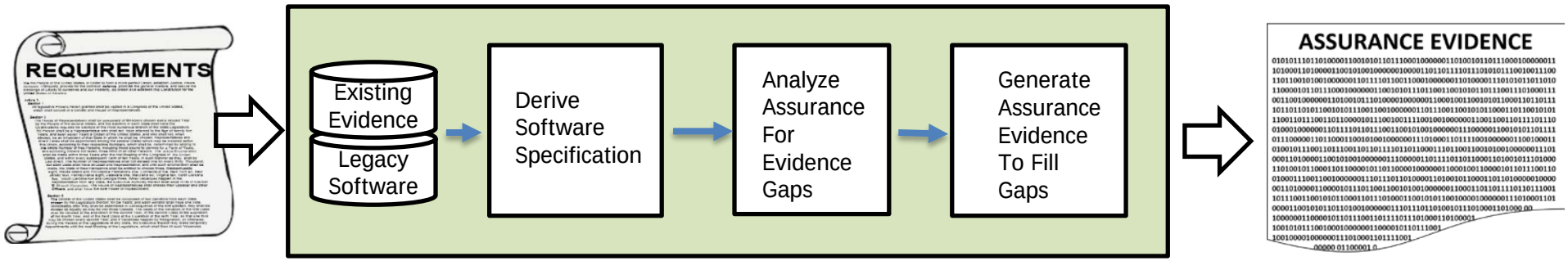
- Develop mechanisms to construct assurance cases, connecting them to software development tools
- Automate the generation of evidence to enable construction of assurance cases
- Capture component interface specifications to support composition

Possible Approaches:

- Invent assurance case languages and tools
- Automate evidence generation through software analysis and test case generation and use
- Extend architectural languages and tools

TA 1: Evidence Generation for Legacy Software

Goal: Create technologies to produce assurance evidence to support certification of existing software



Challenges:

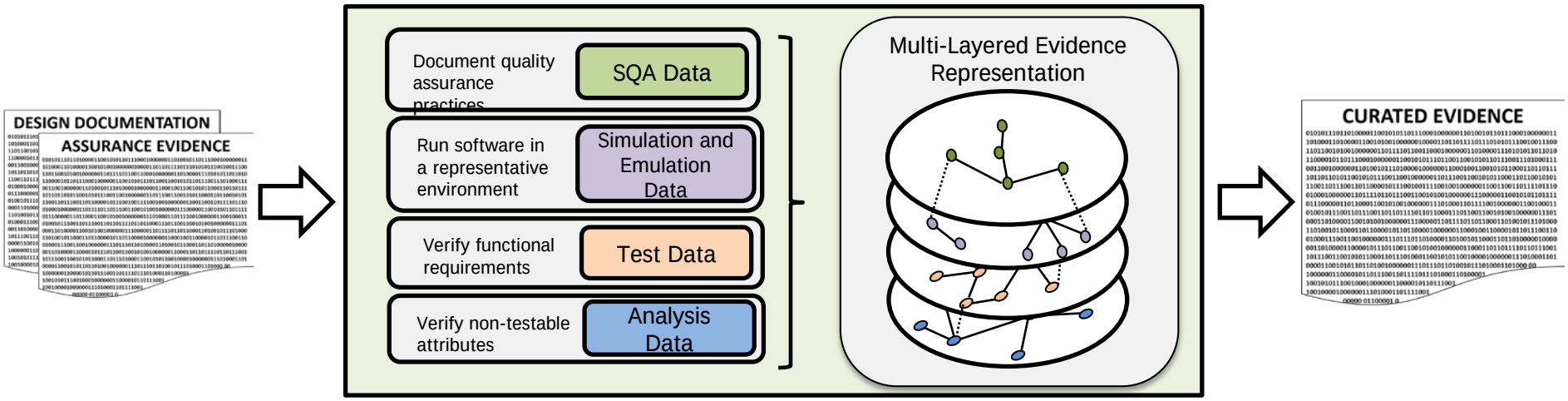
- Generate strong evidence that is focused on certification criteria and assurance cases
- Automate the generation of evidence through test, emulated execution, and analysis

Possible Approaches:

- Extend NLP approaches for the extraction of information
- Invent techniques for the discovery of high-level structures in legacy software
- Create mechanisms to derive specifications for the software using machine learning algorithms
- Automate software analysis, test generation and targeted fuzzing to augment evidence

TA 2: Evidence Curation

Goal: Provide machine readable, common representation of assurance evidence with traceable provenance



Challenges:

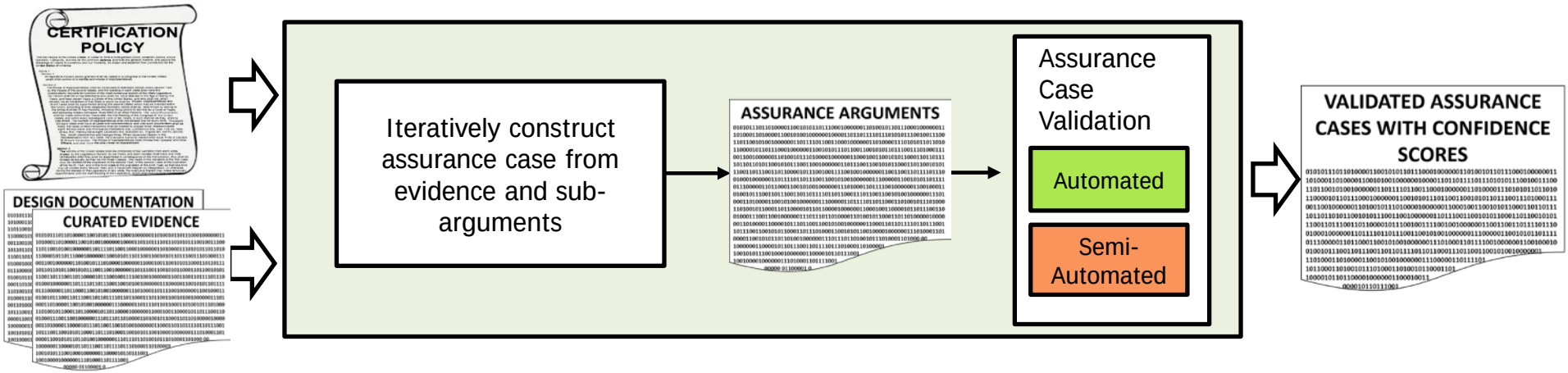
- Develop a representation of evidence from disparate domains that is amenable to analysis
- Developing mapping of evidence to system structure
- Attest to provenance of evidence (chain of custody)

Possible Approaches:

- Create mechanism to make inference from function to structure
- Scale-up the graph-of-graphs representation explored in seedling effort
- Develop provenance trees to attest to integrity of artifacts

TA 3: Assurance Generation

Goal: Create technology to automate generation of assurance cases from curated evidence



Challenges:

- Construct sound assurance arguments
- Substantiate arguments with strongest available evidence
- Evaluate assurance cases to determine soundness and confidence score

Possible Approaches:

- Scale up automated theorem prover technology to construct design-based assurance case arguments
- Develop trained classifiers identify evidence that best fits arguments
- Extend formal methods to demonstrate soundness and correctness of validation algorithms

TA 4: Quantitative Assessment

Goals: Provide a testbed and a series of challenges culminating in demonstrations of processing evidence and
generation of assurance for a realistic system. Perform periodic technology assessments.

Challenges:

- Perform quantitative assessment of ARCOS technologies in coordination with Government evaluators
- Provide a progression of increasingly challenging software systems and data sets that are accessible to research performers
- Demonstrate ARCOS technologies to a military relevant software system in the final phase
- Develop a conservative and sound approach to sample data for evaluation

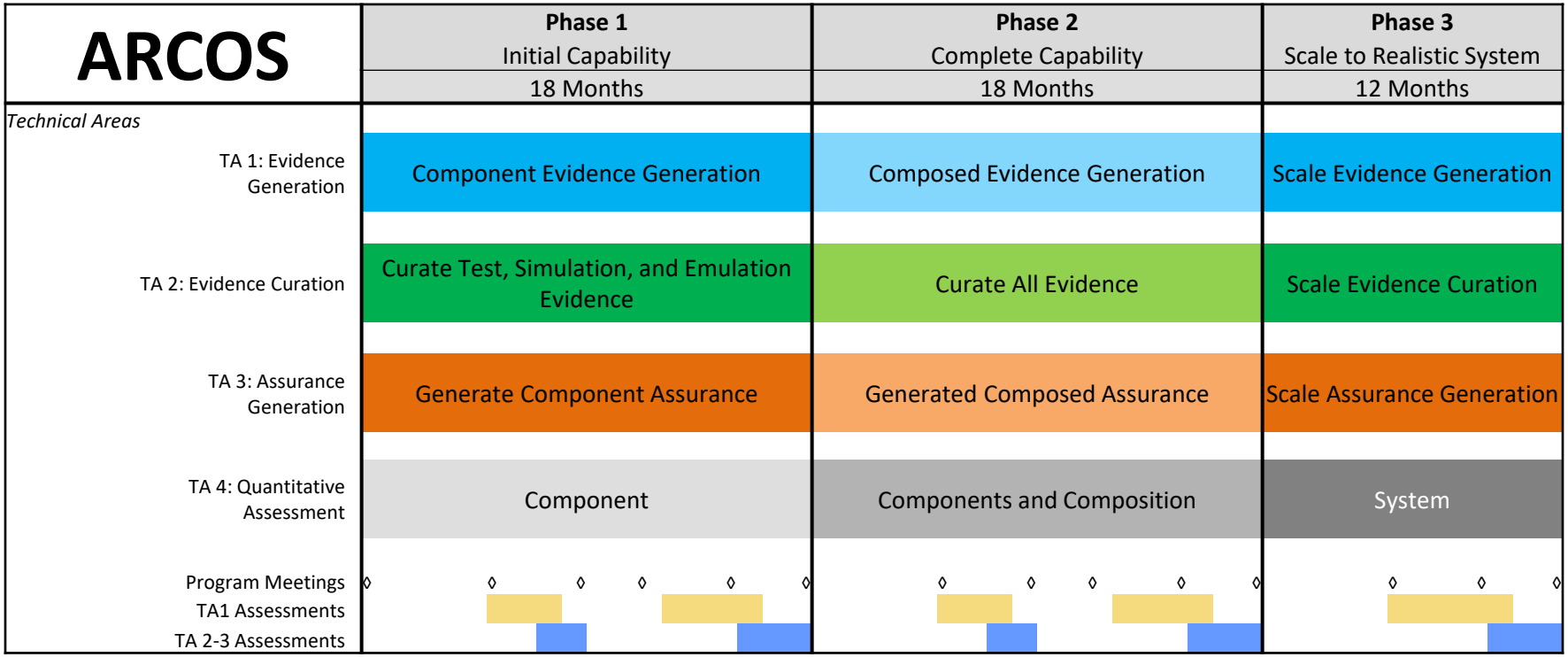
Evaluation (Government Team)

- Provide evaluations for quantitative assessments
  - Evaluate generated evidence and assurance cases
  - Identify and document shortcomings
- End of each phase report on applicability to government C&A practices
- During each phase
  - Provide feedback on the strengths and weakness of performers
  - Compare proposed approaches with the current state of practice
- Team members will include certification experts from across the DoD and Federal Government

ARCOS Goals and Metrics

	Phase 1 (18 Months)	Phase 2 (18 months)	Phase 3 (12 Months)
Scale	One module from Phase 3 system	Set of modules from Phase 3 system	Realistic System
Evidence Domains	Test, Simulation, and Emulation	Test, Simulation, Emulation, Analysis, and SQA	Test, Simulation, Emulation, Analysis, and SQA
Assurance Generation	<4 weeks	<2 weeks	<1 week
TA 1 Legacy Software	3 of 6 evaluators agree with generated evidence	4 of 6 evaluators agree with generated evidence	5 of 6 evaluators agree with generated evidence
New Software	3 of 6 evaluators agree with generated evidence	4 of 6 evaluators agree with generated evidence	5 of 6 evaluators agree with generated evidence
TA 2	100,000+ nodes curated	1,000,000+ nodes curated	10,000,000+ nodes curated
TA 3	3 of 6 evaluators agree with confidence scores	4 of 6 evaluators agree with confidence scores	5 of 6 evaluators agree with confidence scores
TA 4	Performs quantitative assessments with Government Evaluation Team		

Schedule



Awards

- One TA per proposal
- TAs 1 & 3
  - Multiple awards anticipated for each TA
  - Responding to a portion of the TA is acceptable
    - TA 1
      - Legacy Software
      - New Software
    - TA 3
      - Assurance Generation
      - Assurance Validation
  - Addressing the entire TA is encouraged
- TA 2 & 4
  - Single award anticipated for each TA
  - TA 4 performer can not have a conflict of interest with other performers

- Collaborative proposals are encouraged

Important Dates

- Proposers' Day: May 14, 2019
- Abstract Due Date: May 24, 2019, 12:00 noon (EDT)
  - Feedback will be provided as quickly as possible
- Proposals Due / BAA Closing Date: July 9, 2019, 12:00 noon (EDT)

www.darpa.mil