

Automated Rapid Certification Of Software (ARCOS)

Ray Richards
Program Manager

Proposers' Day

14 May 2019





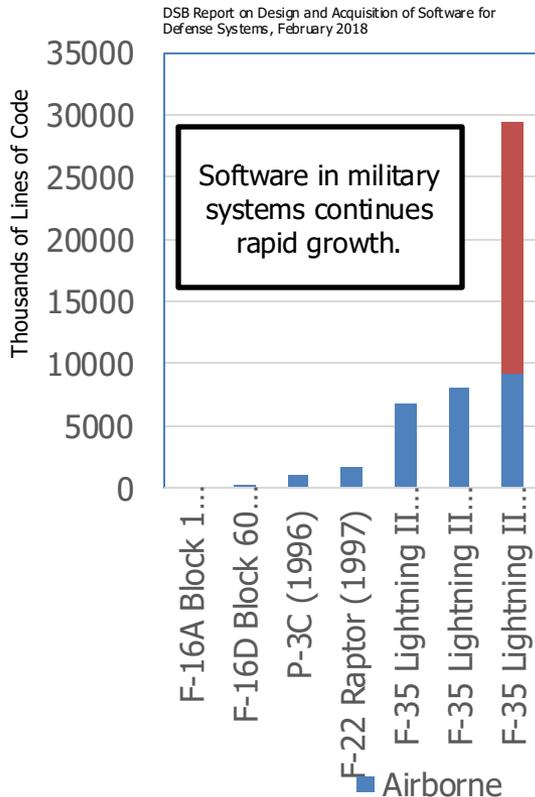
ARCOS Vision



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



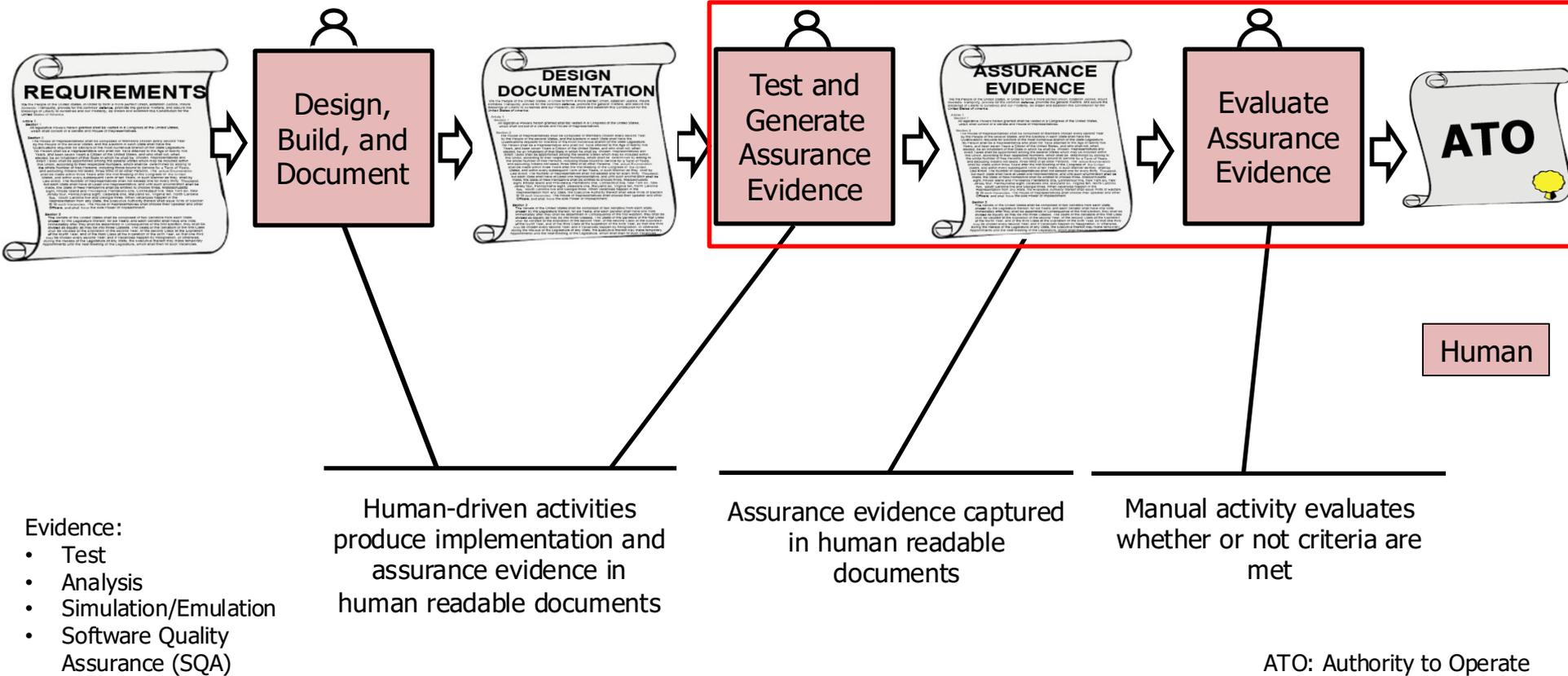
Current software certification practices are unsustainable



- 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



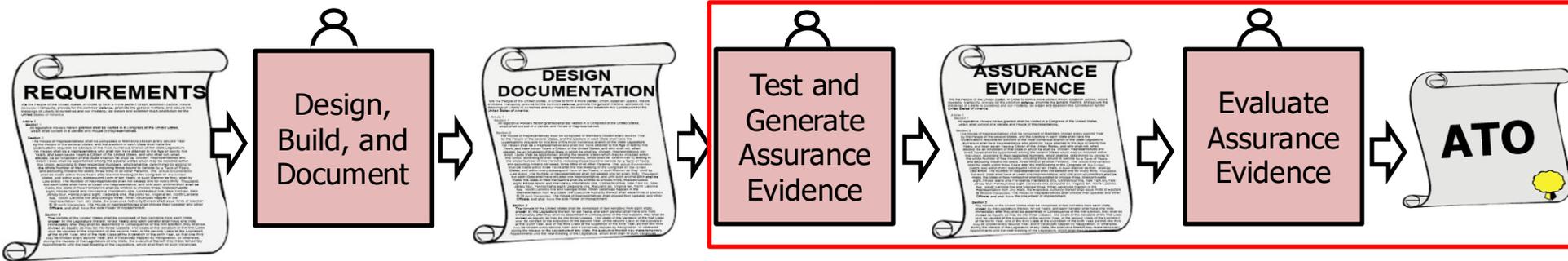
Certifications today: Up to 5 additional years post-development to obtain ATO



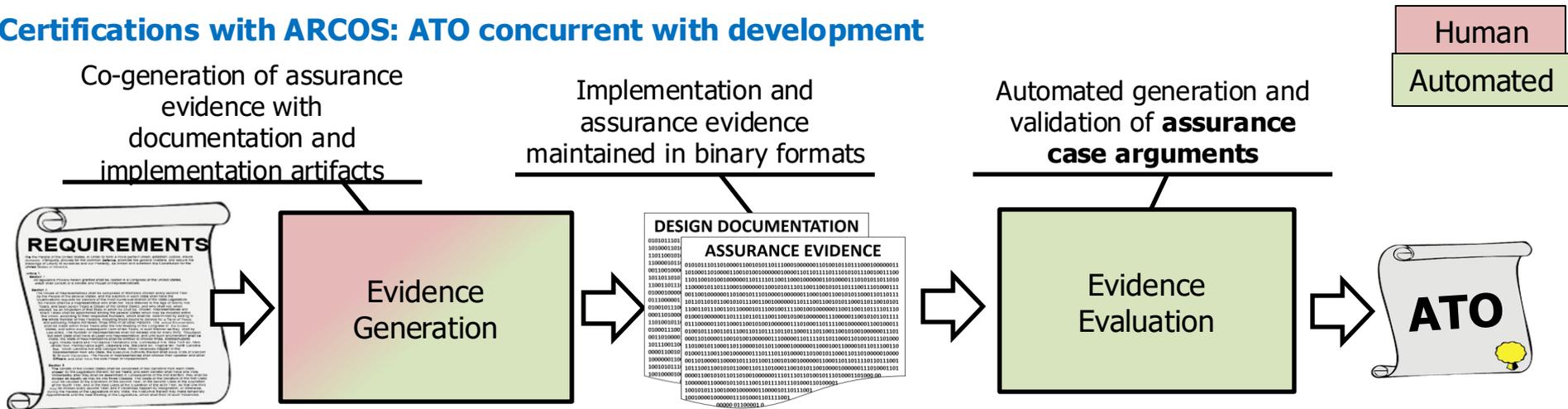


Software certifications with ARCOS

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



Certifications with ARCOS: ATO concurrent with development



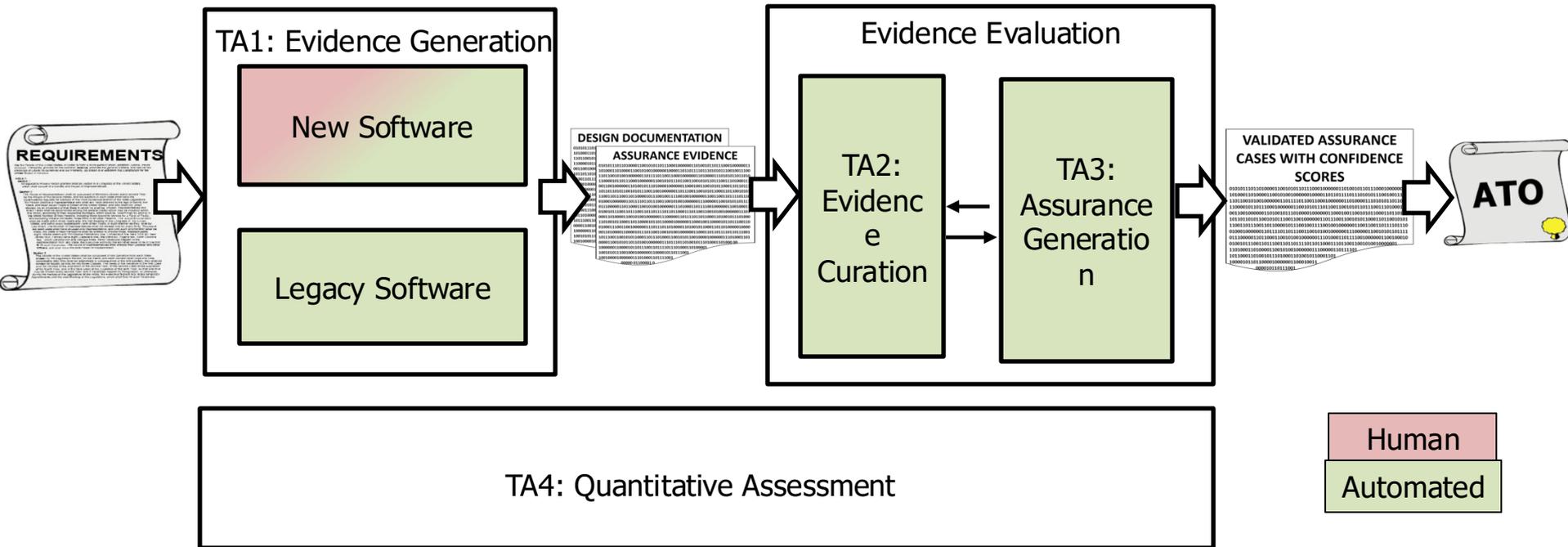
ARCOS Program Structure





ARCOS Technical Approach and Technical Areas

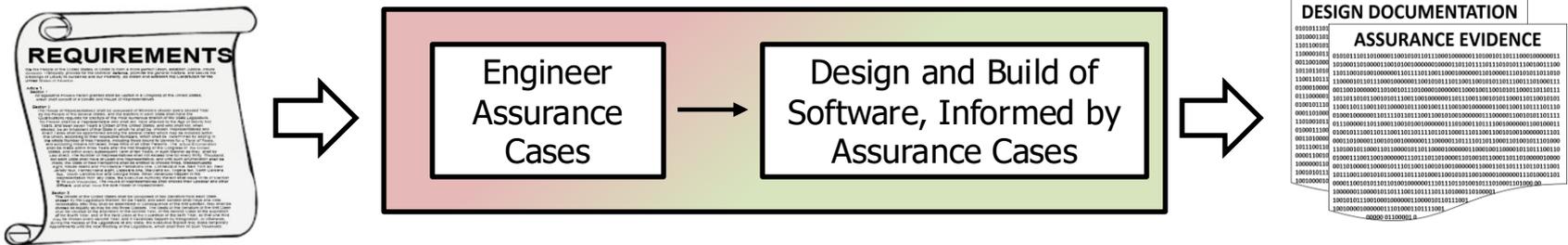
- TA1: Generation of high quality assurance evidence to support curation and facilitate TA3 analytics
- TA2: Curate a large disparate body of evidence to support TA3 analytics
- TA3: Generate assurance arguments and use data analytics to back the arguments with evidence
- TA4: Provide a series of challenges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

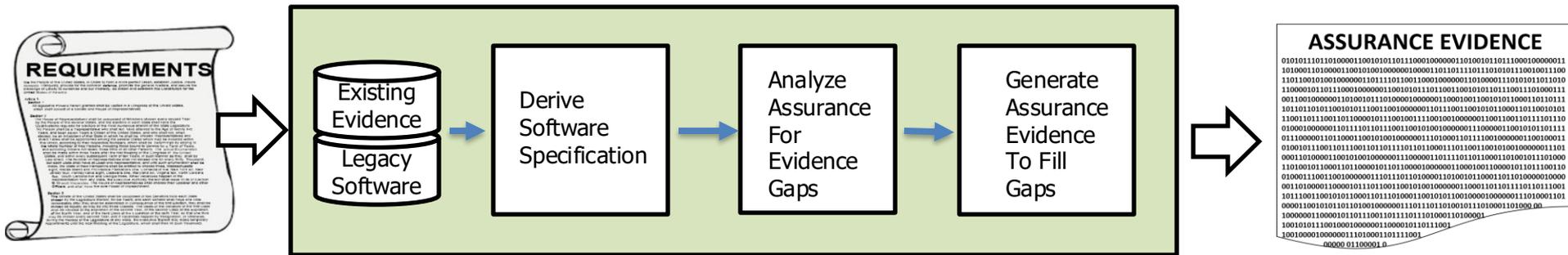
- Develop mechanisms to construct assurance cases, connecting them to software development tools
- Automate the generation of evidence to enable construction of assurance cases
- Capture component interface specifications to support composition

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

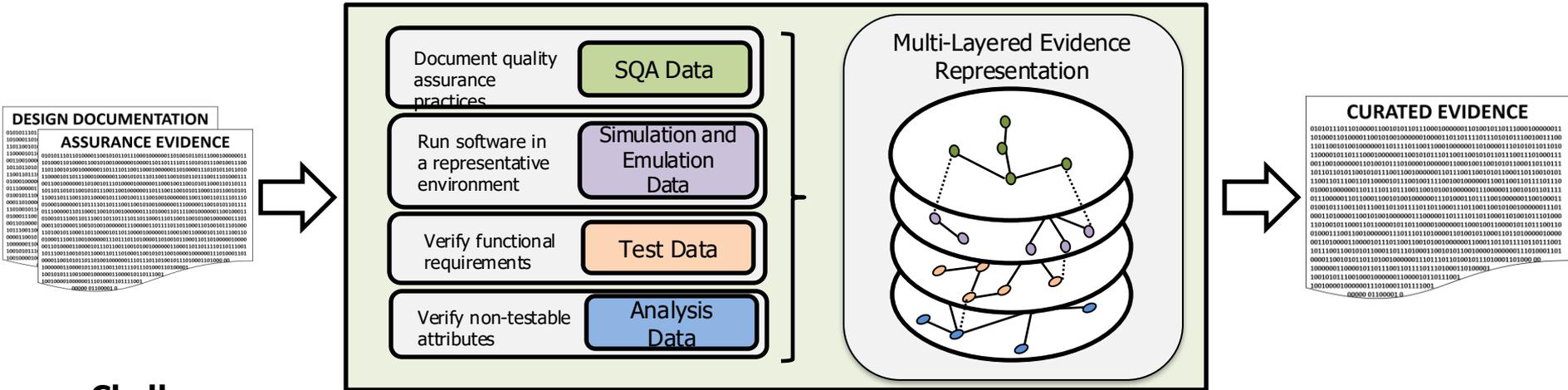
Possible Approaches:

- 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)

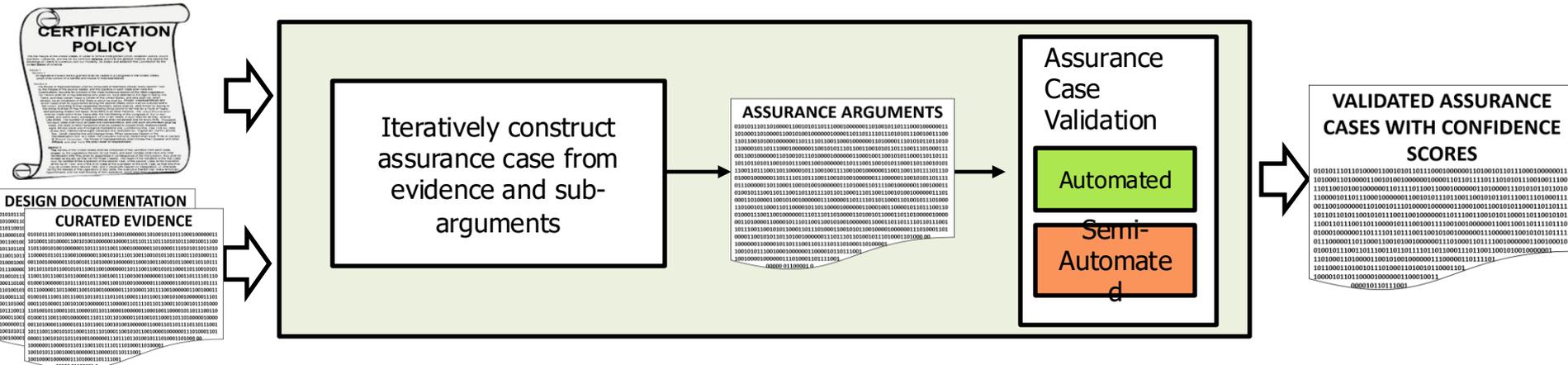
Possible Approaches:

- 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	TMPC, JTT, or F-16 OFPs
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

ARCOS	Phase 1	Phase 2	Phase 3
	Initial Capability 18 Months	Complete Capability 18 Months	Scale to Realistic System 12 Months
<i>Technical Areas</i>			
TA 1: Evidence Generation	Component Evidence Generation	Composed Evidence Generation	Scale Evidence Generation
TA 2: Evidence Curation	Curate Test, Simulation, and Emulation Evidence	Curate All Evidence	Scale Evidence Curation
TA 3: Assurance Generation	Generate Component Assurance	Generated Composed Assurance	Scale Assurance Generation
TA 4: Quantitative Assessment	Component	Components and Composition	System
Program Meetings	◇	◇	◇
TA1 Assessments	◇	◇	◇
TA 2-3 Assessments	◇	◇	◇



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



www.darpa.mil