Research Review 2017

Execution Model, Session II FAA-Sponsored Research on Complexity and Safety

Purpose of Research Effort

Federal Aviation Administration (FAA) regulates to ensure safety of air travel

Concerned that, as system complexity keeps increasing, they might not be able to certify newer aircraft as safe

Asked, How complex is too complex to be able to assure safety?

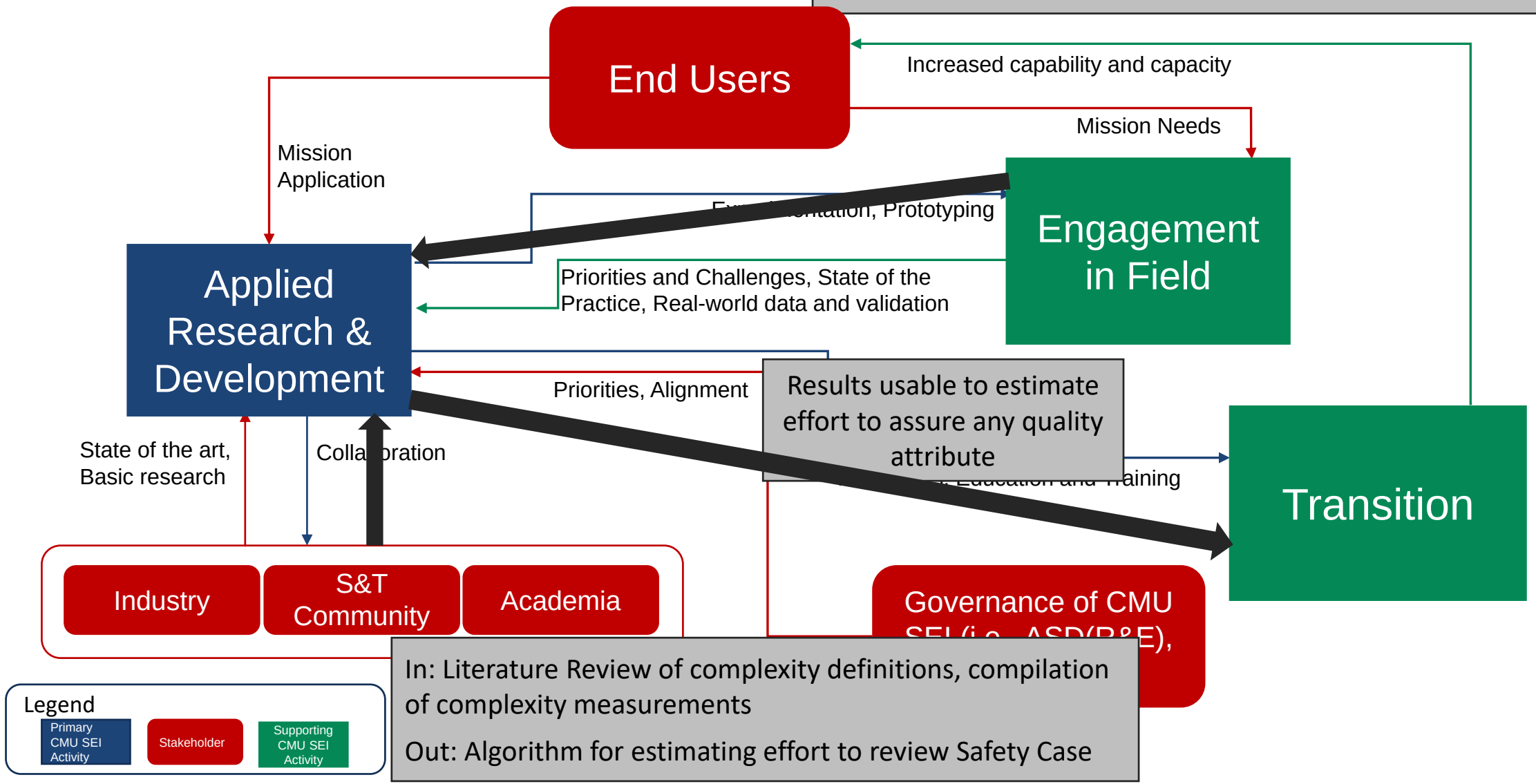
More general gap: Difficulty predicting overall properties of increasingly complex systems

- DoD also concerned about assuring safety and other qualities
- All are more difficult to prove with highly complex systems

FAA may choose to request aircraft manufactures create and provide safety cases

CMU SEI Execution Model

Measuring Complexity for System Safety Assurance: FAA-funded research project (FY2015-2016)



Results and Value to DoD

Results: SEI delivered algorithm and method for estimating complexity and therefore assurance effort, once architecture (including components and interconnections) has been determined

Alternatives considered: Measuring design complexity (number of parts and connections) but 1) no obvious connection to safety 2) difficult to get design detail

Innovative aspects: Estimating complexity of safety case, in terms of number of ways a failure can propagate within an architecture, and available early

Value to DoD now:

- Many items “too complex to certify”
- Possible to estimate safety from architecture
- *Choose measure of complexity directly relevant to required quality attributes*

Desired future research: Test algorithm against larger systems; Validate with failure data; Combine with virtual integration body of knowledge; Precedence (recertification, regression testing)

Insights & Observations

Separate:

- *causes* of complexity (design, stakeholders, requirements, technology change, etc.)
- *effects* of complexity (Confusion, error, and difficulty designing, planning, predicting properties, identifying problems, verify and validate, maintain, etc.)

Complexity needs to be specified as the complexity *of* something, such as a system, an environment …or a task

Complexity measurement, to be useful, needs to be available in design phase

Measurement is useful when complexity ties to something that makes a difference. Here: assurance effort. Also: Risk

Complexity is inherently not simple → problematic to seek one measure that captures it (even composite)

Algorithm can be used to estimate quality assurance effort, maybe testing strategy

Assumptions needed to calculate potential error propagations

Assurance and certification cost time, money, and complexity

Reports

http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=483758

The FAA Research Project: Effects of System Complexity on Aircraft Safety

Definition and Measurement of Complexity in the Context of Safety Assurance *(*overall report)

5 previous and more detailed reports:

- Complexity Definition Literature Review
- Candidate Complexity Metrics
- Impact of Complexity on Safety
- Estimating Complexity of Safety Argument
- Testing the Identified Metrics

Principal Investigator and Contributors

Principal Investigator

Dr. Sarah Sheard

Principal Engineer, Systems Engineering

Email: sheard@sei.cmu.edu

Telephone: +1 412.268.7612

Contributors

Dr. Mike Konrad, mdk@sei.cmu.edu

Dr. Chuck Weinstock, weinstock@sei.cmu.edu

Dr. Bill Nichols, wrn@sei.cmu.edu

Greg Such, gsuch@sei.cmu.edu

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0705