Standardisation efforts overview

A filler before coffee break @ ASSURE 2013

Makoto Takeyama

Kanagawa University

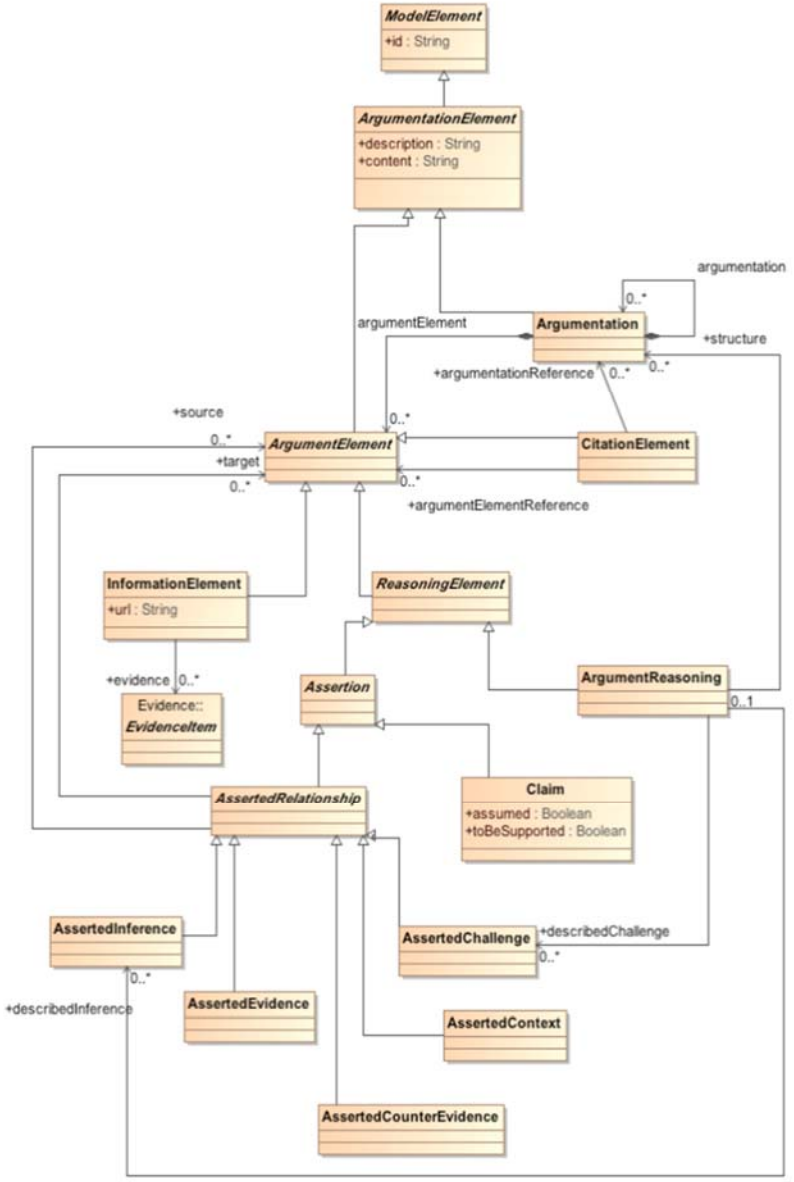
(Research funded by JST CREST DEOS project)

- OMG SACM (Structured Assurance Case Metamodel)
- OMG MACL (Machine-checkable Assurance Case Language)
- ISO/IEC 15026-2:2011
  Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case
- IEC 62741 Ed. 1.0
  Reliability of systems, equipment and components. Guide to the demonstration of dependability requirements. The dependability case

OMG SACM 1.0

- Structured Assurance Case Metamodel
  - Class diagrams, XML schema with (informal) semantics
  - For exchanging AC data among tools
- by System Assurance TF
- Argumentation Metamodel
- Evidence Metamodel
- Version 1.0 released Feb. 2013
- Revision on going

better integration of two parts, GSN support(modules, patterns), Harmonization with ISO/IEC 15026-2, …

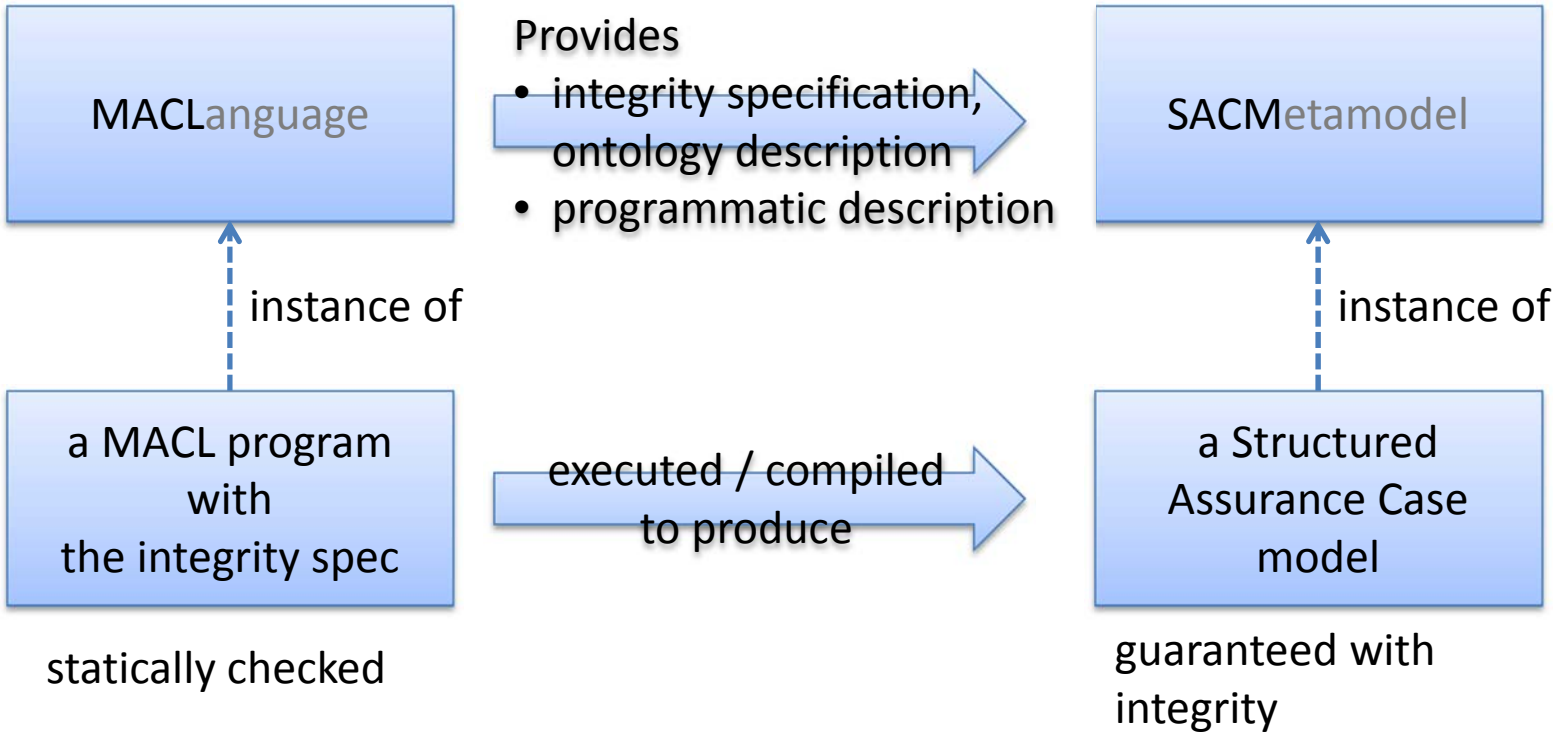


OMG MACL

- Machine-checkable Assurance Case Language:
  a machine-checkable specification- and programming-language for SACM models.
- By System Assurance TF.
- **Specification**:
  - the condition for an argument to be "correct" to have "integrity"
  - w.r.t. the ontological data (term definition, context, sys. model, …) on which the argument is based.
- **Programming**: description of construction of SACM models.
  - programmatic generation of arguments,
  - writing arguments as programs
- **Checkable**: A MACL program can be machine-checked and guaranteed to produce a SACM model satisfying its spec.

OMG MACL

- RFI issued and closed Feb. 2013.
  responses from E. Denney(NASA Ames), Adelard, Nagoya U, U. Eindhoven.
  "Request for Proposals" (spec for spec) targeted Dec. 2013.
- MACL and SACM



ISO/IEC 15026-2:2011

- Systems and software engineering -- Systems and software assurance -- Part 2: Assurance case
- By ISO/IEC JTC1 / SC7 / WG3 (Life cycle management)
- The top-level standard on AC in ISO/IEC std. hierarchy.
- Specifies minimum requirements for the structure and contents of an assurance case:
  Claims, Arguments, Evidence, Assumptions, Justifications
- Conceptual for general applicability.
  Conformance requires explicit mapping between elements in the standard and elements in your assurance case.
- Issued 2011

ISO/IEC 15026-2:2011

IEC 62741 Ed. 1.0 (CD2)

- Reliability of systems, equipment and components
  -- Guide to the demonstration of dependability requirements
  -- The dependability case
- By IEC TC56 / WG3 (Dependability Management)
- From BS 5760-18:2010 of the same title,
  which is from
  UK Defence Standards on Reliability & Maintenance case(?)
- Geared for an acquisition project where
  one customer orders one supplier a system to meet his dependability requirements.
- Guidance on the contents, usages, management of dependability case through the life of project,
- But not much on arguments themselves.
- At a Committee Draft stage.