OMG – International Standards for Assurance Cases

Luke Emmet – loe@adelard.com

Overview

- Existing notations for safety/assurance cases
- Standardisation at OMG
- SACM – Structured Assurance Case Metamodel
  - Status
  - Relationship to ISO 15026

Existing notations and standards

- Requirements for safety cases well established in UK
  - Most regulated sectors
    - —*A structured argument supported by a body of evidence to establish …*
  - Role of case to communicate safety strategy
  - Focus for meaningful safety challenge
  - A living document over the lifecycle
- Generalise from *Safety Case* to *Assurance Case*
  - Can cover security or other assurance attributes
  - Often we may talk of *case based approaches*

Existing notations

- Notations are well established:
  - —Claims-Arguments-Evidence (CAE)
  - —Goal Structuring Notation (GSN)
  - Both based on work by Stephen Toulmin
  - Some minor differences in emphasis
  - But basically the same key concepts
    - —A structured argument comprises of a graph of claims
    - —Important to show reasoning and contextual information
    - —Ultimately supported by evidence
- Tools provide a de-facto interchange standard
  - Some based on open standards (e.g. ASCE XML format)

Object Management Group – OMG

- Community based standards body, open participation process
- Most well-known standards:
  - UML, SysML
- Technical interoperation specifications
  - i.e. data exchange between tools
  - Open standards seen to de-risk tool adoption

System Assurance Task Force

- Increasing interest in cyber security
  - Software assurance “ecosystem”
- System Assurance Task Force (SysA) goals
  - Facilitate the development of a specification for a Software Assurance Framework
  - Enable industry to improve visibility into the current status of software assurance during development of its software
  - Enable industry to develop automated tools that support the common framework

SysA standards

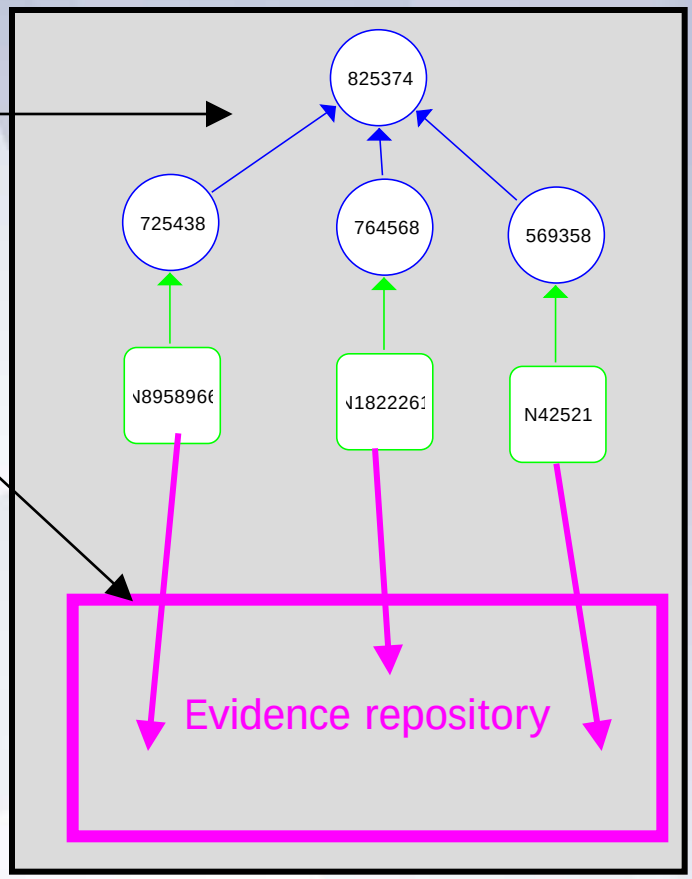
- Existing standards – KDM (knowledge discovery metamodel)
  - A vendor neutral way of exchanging static analysis models
- Developing standards for Assurance Cases
- Some UK Participation sponsored in part by MoD SSEI programme (Software Systems Engineering Initiative) - 2011
  - Benefits of promulgating UK safety policy perspective
  - Adelard LLP, University of York

SACM

- SACM – Structured Assurance Case Metamodel
  - Combines previous OMG specifications
    - ARM (Argument Metamodel)
    - SAEM (Software Assurance Evidence Metamodel)
- ARM led by Adelard and University of York
  - Harmonises common elements from GSN and CAE
  - A structured argument comprises a graph of assertions (claims), ultimately supported by evidence
    - Links are asserted relationships between claims, context and evidence
      - “supported by”, “in context of”, “has evidence”

SAEM and ARM

- Looking at developing models for interchange of information for
  - Claims and arguments to go on top - ARM
  - Evidence repository metamodel - SAEM
- ARM – argument metamodel
- SAEM – the evidence repository
  - Expressing attributes about software artefacts and relations between them
    - Containment
    - Concretisation of models
    - Library dependencies
    - Versioning
    - ...
  - And be extensible in the future



Status of SACM

- Version 1.0 is a recommended OMG specification for adoption
  - —http://www.omg.org/spec/SACM/
- Tool support available
  - —ASCE, NASA GSN tool, others coming
- Standard now in revision (RTF process)
  - —Aim to simplify further to increase adoption
  - —Reduce overlaps
- Version 1.1 due 2014

- Future – may offer to ISO for fast-track acceptance

Related international standardisation

- ISO 15026-2
  - Part 2: Assurance Case
    - —Provides requirements and framework
  - Not a technical interop standard, conceptual approach not dissimilar to UK safety case concept
    - —00-56, CAP 670 SW01
  - Fits well with SACM – can think of SACM as a technical standard to exchange data when working within ISO 15026
- Open Group Assurance Case standard
  - Dependability through Assuredness ™ Standard
  - Again, more at the process level

Thanks for listening.