Managing the Argument-Evidence Interface

Tim Kelly, Linling Sun
University of York

tim.kelly@york.ac.uk

Contents

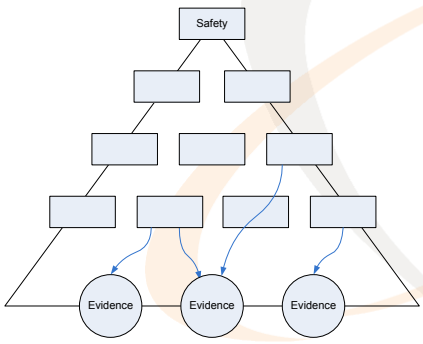
Safety Cases and Evidence

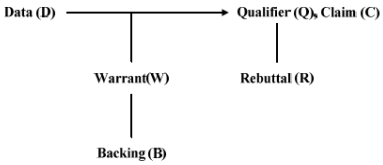
- Role in safety cases
  - "A structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment."

    from DS 00-56
- More attention given to argument than evidence?

Evidence Items

- Artefacts, documents, facts, references or statements of facts?





Notation	Example
Text-based notation (from[100])	Claim 1.1.1: H1 has been eliminated. Evidence 1.1.1: Formal verification
CAE [18]	(Evidence) System X Hazard Log
GSN [5]	Solution_Sn1 Fault Tree for Hazard H1

Evidence in Law, Medicine and Philosophy

- **Definition 1.** That which tends to prove the existence or nonexistence of some fact. It may consist of testimony, documentary evidence, real evidence, and, when admissible, hearsay evidence. (A Dictionary of Law Law and Martin 2009)
- **Definition 2.** The assembled information and facts on which rational, logical decisions are based in the diverse forums of human discourse, including courts of law, and in the practice of evidence-based medicine among many others. (A Dictionary of Public Health Last 2006)
- **Definition 3.** That which raises or lowers the probability of a proposition. The central question of epistemology is the structure of this process and its ultimate rationale. (The Oxford Dictionary of Philosophy Blackburn 2005)

Evidence in Safety Domain

- **Definition 4.** Which is used as the basis of the safety argument. This can be either facts, assumptions, or subclaims derived from a lower-level sub-argument. (Adelard Safety Case Development Manual V1.1 Adelard 1998; Bishop and Bloomfield 1998)
- **Definition 5.** Safety evidence is information, based on established fact or expert judgement, which is presented to show that the safety argument to which it relates is valid. (Safety Case Development Manual EUROCONTROL 2006)
- **Definition 6.** A document or other exhibit that provides justification to a certain claim. (SAEM Working Document 1.0 Beta 1 OMG 2010)

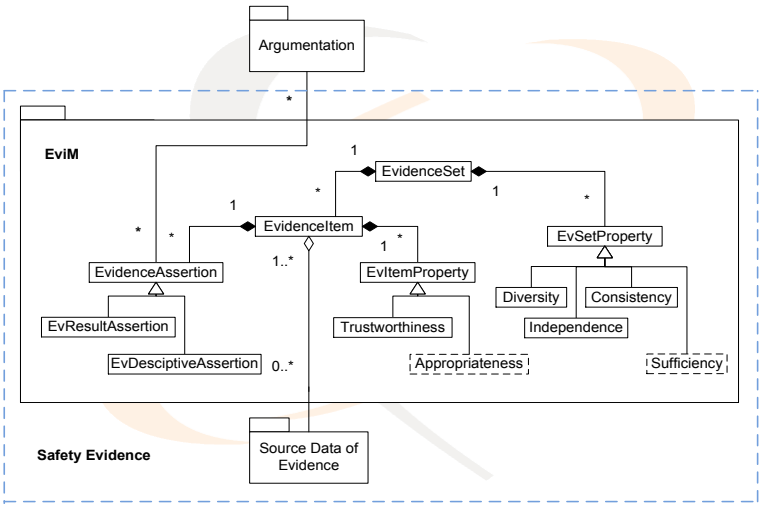
Common Basis

- Evidence is information
- Evidence is not the same as truth
- Evidence does not simply equate to documents or artefacts
- Evidence is the grounds and starting-point of arguments
- Evidence should be examined in context of safety arguments
- The association between evidence and safety claims is a multiplicity relationship
- The association between items of evidence and physical artefacts being cited is a multiplicity relationship

Working Definition

- *Evidence is information that serves as the grounds and starting-point of (safety) arguments, based on which the degree of the truth of the claims in arguments can be established, challenged, and contextualised.*

A Conceptual Model of Evidence
(EviM)



THE UNIVERSITY of York

Evidence Assertions

- OMG ARM and GSN Standard
- *An evidence assertion is a minimal proposition that describes 'factual information' concerning an item of evidence.*
  - *It does not need support from further arguments or evidence and it directly concerns the source data of an item of evidence without involving subjective judgment.*
  - Argument-Evidence Interface Element
- Different from
  - Domain Safety Claims
  - Data Items in the source data of Evidence Items

THE UNIVERSITY of York

Two Sub-Types

- *Evidence result assertion*
  - "What does an item of evidence say"?
    - for justification for domain safety claims
- *Evidence descriptive assertion*
  - "What can we say about an item of evidence according itself other than the evidence result assertions"
    - for providing ground premises or contextual facts for the confidence argument associated with primary safety argument elements

Examples (Evidence result assertion)

Table 1. Examples of evidence result assertion

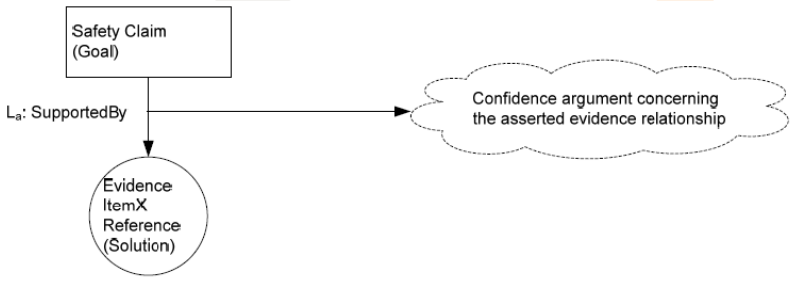
Types of safety evidence	Example of evidence result assertion
FTA (Fault Tree Analysis)	• The probability of failure condition FC_x modelled in FT_x is P_x. • Failure condition FCx modelled in FTx was caused by more than one failure event in FTx. (according to a fault tree model – FT_x)
Software performance test	• The output arrival timing T_o is within the range of $T_a \pm \Delta t$ through the software test STT_x. (according to a software timing test – STT_x) (T_a is the ideal arrival timing in software specification; Δt is the user-defined tolerable difference.)

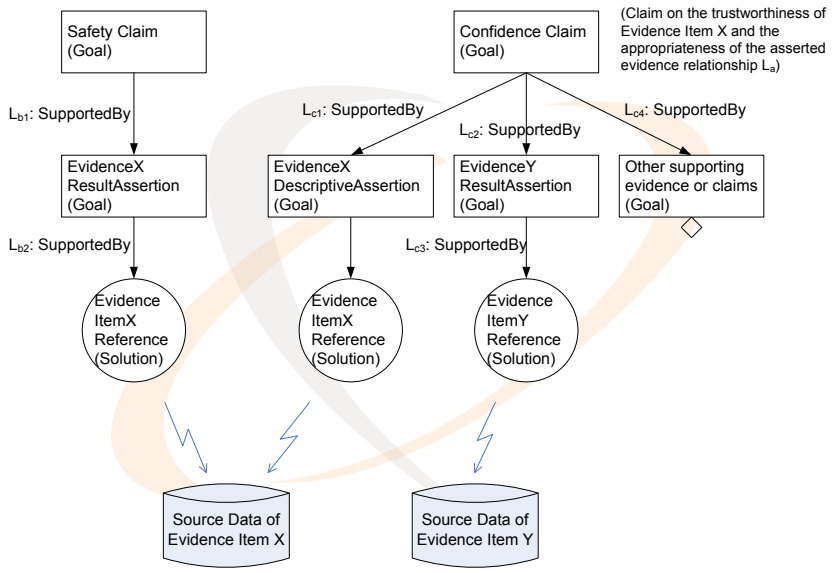
Examples (Evidence descriptive assertion)

Table 2. Examples of evidence descriptive assertion

Types of safety evidence	Examples of evidence descriptive assertion
FTA	• System component C_x is considered in Evidence FT_x
	• Evidence FT_x is created by Engineer E_x.
	• Timing issues are not considered in Evidence FT_x
Software performance test	• Evidence STT_x uses 20 test scenarios.
	• Evidence STT_x is performed by Engineer E_y.

Utilising Evidence Assertions





THE UNIVERSITY of York

Evidence Properties

- Evidence item properties
  - *Trustworthiness*
  - *Appropriateness*
- Evidence set properties
  - *Sufficiency (or coverage)*
  - *Independence*
  - *Diversity*
  - *Consistency*

THE UNIVERSITY of York

Summary

- Clarified *essential meaning* of the concept of evidence, which serves as shared principles and characteristics that apply to *all* objects of evidence in safety cases.
- Explicit integration of the source data of evidence and safety argument through an *interface element* - Evidence Assertion.
- Distinctive evidence *properties* to be considered in *context* of argumentation.