**Assurance Cases**

**Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**

1. **REPORT DATE**
   26 JAN 2015

2. **REPORT TYPE**
   N/A

3. **DATES COVERED**

4. **AUTHOR(S)**
   **Weinstock /Chuck**

5. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
   **Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213**

6. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

7. **PERFORMING ORGANIZATION REPORT NUMBER**

8. **SPONSOR/MONITOR’S ACRONYM(S)**

9. **SPONSOR/MONITOR’S REPORT NUMBER(S)**

10. **DISTRIBUTION/AVAILABILITY STATEMENT**
   Approved for public release, distribution unlimited.

11. **SUPPLEMENTARY NOTES**
   The original document contains color images.

12. **ABSTRACT**

13. **SUBJECT TERMS**

14. **SECURITY CLASSIFICATION OF:**
   a. REPORT unclassified
   b. ABSTRACT unclassified
   c. THIS PAGE unclassified

15. **LIMITATION OF ABSTRACT**
   SAR

16. **NUMBER OF PAGES**
   19

17. **NAME OF RESPONSIBLE PERSON**

18. **REPORT UNCLASSIFIED**

19. **ABSTRACT UNCLASSIFIED**

20. **THIS PAGE UNCLASSIFIED**
Overview

Maturity of Assurance Cases
ISO 15026-2 Assurance Case Standard
Goal Structured Notation
Example from Industry
Confidence Work at the SEI
Other Current Work on Assurance Cases
Closing Thoughts
Maturity of Assurance Case Technology

Developed in late 90s in Europe
Used for safety cases in Europe for over 20 years
The UK Ministry of Defence requires generation of a compelling case to support claims that specific safety requirements are met:

“The safety case shall consist of 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.” [DEFSTAN 00-56 (Part 1)/4]

ISO standard under development (ISO 15026-2)
ISO/IEC 15026-2: Assurance Case

**Claim:** A proposition to be assured (e.g., “The system is safe”)

**Evidence:** A fact, datum, object, claim, or other assurance case

**Argument:** A reason why the set of evidence shows that the claim is true

**Justification:** A reason why a claim has been chosen

**Assumption:** A claim that appears as evidence

An Assurance Case is a quadruple \( a = (c, j, es, g) \) where \( c \) is a claim, \( j \) is a justification, \( es \) is a set of evidence, and \( g \) is an argument which assures \( c \) using \( es \).

The assurance case is to be delivered and maintained with the system

This definition is recursive
Goal Structuring Notation (GSN) – Kelly 1998

A specific notation for an assurance case consistent with 15026-2.

Developed to help organize and structure safety cases in a readily reviewable form.

Used successfully for over a decade to document safety cases for aircraft avionics, rail signaling, air traffic control, and nuclear reactor shutdown.

Shows how claims are broken down into sub-claims, and eventually supported by evidence or while making clear the argumentation strategies adopted, the rationale for the approach (assumptions, justifications) and the context in which claims are stated.
Example: Battery Exhaustion – Part One

C1
Pump is safe for use on patients

S1
Argue over hazards to safe pump operation

Cx1
Hazards: over infusion, under infusion, ...

S2
Argue over hazards causing over infusion

S3
Argue over hazards causing under infusion

Cx4
Hazards: exhaustion of battery power, occlusion of line, faulty pump calibration, ...

C2
The battery exhaustion hazard has been adequately mitigated
Example: Battery Exhaustion – Part Two

**C2**
The battery exhaustion hazard has been adequately mitigated

**C3**
Caregiver is notified sufficiently soon (but not too soon) prior to battery exhaustion

**C4**
When operating on battery power visual and auditory alarms are launched at least \( x \) minutes prior to battery exhaustion but no more than \( x+y \) minutes prior

**S4**
Argue over hazards causing failure to notify caregiver in a timely manner

**Cx3**
A late warning won't give the caregiver time to stop current activities and plug the pump in. An early warning may be ignored. This depends on the clinical setting.

**Cx2**
Caregiver doesn't notice alarm; amount of warning time too little for the anticipated clinical setting

**C5**
Visual and auditory alarms are loud enough to be heard and identified in the anticipated clinical setting

**C6**
\( x \) minutes warning prior to battery exhaustion is sufficient time to allow corrective action in the anticipated clinical setting
The Task

We were asked to assure the safety of a system for guiding aircraft onto ships in bad weather. This was to consider the whole ship/equipment/aircraft system of systems, taking into account:

- Human factors.
- The operating environment.
- Operating procedures.
- Maintenance & Management.

An Operational Safety Case (OSC) was needed.
05 Approach - OSC Safety Strategy

Context
- Safety Targets and Report Requirements
- Definition of Adequately Safe
- Scope

Top Goal
- System is Adequately Safe for Aircraft to Locate & Approach Ship
- Show all elements and interactions are safe

Goals
- System Equipments are Safe to Operate
- System is Safe in Operation
- All System Safety Requirements are Satisfied
- System/Aircraft/Ship Interactions are Safe

Strategy
- System Description
- Aircraft Description
- Ship Description
- Assumptions

What confidence should be placed on an AC?

Given the evidence, how confident should we be in the claim C1? Why?
What does it mean to have confidence in the claim?
What could be done to improve confidence? Why?

```
C1
The system is safe

C2
Hazard A has been eliminated
```

```
C3
Hazard B has been eliminated
```

```
Ev1
Evidence
```

```
Ev2
Evidence
```

```
Ev3
Evidence
```
The Basis for Confidence in a Claim

A classic philosophical problem:

- Justify belief in a hypothesis

Use Induction

- **Enumerative**: Support increases as confirming instances are found

Using past experience as the basis for predicting future behavior
Eliminative Induction

Support for a claim increases as reasons for doubt are eliminated

CLAIM: The light turns on (when the switch is flicked).

Bulb OK?  Power?  Wired?  ?

Confidence increases as doubts are eliminated
What confidence should be placed on an AC?

How confident in C1? Why? (Number of uneliminated doubts)

What does it mean to have confidence? (Lack of doubt)

What could be done to improve confidence? Why? (Elim. more doubts)

- **C1**: The system is safe
  - **C2**: Hazard A has been eliminated
    - **Ev1**: Evidence
  - **C3**: Hazard B has been eliminated
    - **Ev3**: Evidence
Rebutting defeaters (R) attack claim validity

C1.1
The system is secure from sql injection

IR2.1
Unless there is unrestricted user input to a query

Ev3.2
Evidence showing that all user input is properly sanitized before being used in an sql query

IR3.1
If all user input is sanitized then there is no unrestricted user input to a query

Cx2.1a
A parameter is unrestricted if it can cause an unintended modification to the sql query when used

Undermining defeaters (UM) attack evidence validity

UM4.1
But the evidence is based upon faulty sanitation rules

UM4.2
But the evidence is not for the system under consideration

IR4.3
If these reasons are not true, then the evidence is valid

Inference rule (IR) for validating a claim

IR2.2
If user input is properly restricted, then the system is safe from sql injection

UC3.3
Unless there is another way sql injection could occur

Undercutting defeaters (UC) attack rule sufficiency

UC3.3
Unless there is another way sql injection could occur
Key Ideas

Confidence grows as doubts are identified and eliminated

- Doubts about a claim (rebutting defeater)
  - Why claim may be invalid

- Doubts about evidence (undermining defeater)
  - Why evidence may be invalid

- Doubts about reasoning (undercutting defeater)
  - Premise ok; conclusion uncertain
Other State of the Art

John Knight – University of Virginia

• Confidence cases: a confidence argument created in parallel to the safety argument that documents the confidence in the structure and basis of the safety argument.

Tim Kelly – University of York

• Evidence elaboration: modeling evidence to better understand it and its evaluation for the purpose of explicit integration of the source data of evidence and the safety case argument.
Concluding Thoughts

This has been a quick overview of assurance cases and confidence and an introduction to the concept eliminative argumentation as developed by the SEI.

- It is not a comprehensive review of all that is happening in the area.
- The SEI has been applying Baconian probabilities to confidence maps to show how much different portions of the argument contribute to overall confidence – something that may prove useful for incremental certification.

Assurance cases have been proven effective in the safety domain.

- The effectiveness of confidence cases and eliminative induction have yet to be demonstrated in practice.
Contact Information

Charles B. Weinstock
Principal Researcher
Software Solutions Division
Telephone: +1 412-268-7719
Email: weinstock@sei.cmu.edu

U.S. Mail
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA