Overview (this presentation)

- Who are we?
- Approaches to Assurance
- Assurances cases – requirements
- Assurance Case lifecycle
- Notations for argumentation
- Example Assurance Cases
- Use of ASCE for Assurance Case development and maintenance
- Conclusions
Adelard

20 years in software and systems assurance
- Research in dependability, safety, security etc.
- Policy, standards, guidance...
- Independent safety audit/assessment/advice
- Software assurance
  - Formal methods
  - Static analysis
  - Software criticality analysis
- Human factors
- Hazard and risk identification, analysis, management
- Domains
  - Security
  - Defence
  - Air traffic management
  - Nuclear
  - Road/rail transport
  - Space

ASCE
- The Assurance and Safety Case Environment
Approaches to assurance

- The safety justification triangle

- Goal Based

- Vulnerability assessment

- Standard and guidelines
Standards based assurance

- Historical approach
- Can work well in stable environments with established best practice
- Does not easily support change and innovation
- “Check box” approach
- May not demonstrate explicit assurance properties
- In the event of a mishap
  - Standards may be deemed deficient
  - Perception of regulatory responsibility
Goal based assurance

- Specific assurance goals established
- Progressively more detailed sub-goals (or claims)
  - supported by argument and evidence

The Assurance Case

- Vulnerability approach
  - bottom-up analysis of issues and risks
  - can complement goal based approach
Assurance Cases - issues

- Increasingly required by law/regulation/standards
- Emergence of goal-based standards
  - cf evidence based assurance
  - encourages innovation, but requires more focus on achievement
  - Assurance Case is the key assurance information repository
- Complexity
  - vast amount of data to be integrated - information overload
  - complexity of argument
- Comprehension
  - Assurance Cases need to be independently audited
  - many stakeholders require different views of the Assurance Case
- Supply chain
  - geographically and culturally diverse suppliers
- Range of risks associated with Assurance Case 'failure'
Some Definitions

“A documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment.”

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 environment. Def Stan 00-56 issue 4

A security assurance case uses a structured set of arguments and a corresponding body of evidence to demonstrate that a system satisfies specific claims with respect to its security properties. BSI Portal

“An assurance case is a formal method for demonstrating the validity of a claim by providing a convincing argument together with supporting evidence.”

FDA - Infusion Pump - Premarket Notification [510(k)] Submissions DRAFT GUIDANCE, April 2010

Copyright © Carnegie Mellon University 2005-2007
Assurance Case Requirements

- UK:
  - Defence
  - Offshore and on-shore process industries
  - Rail
  - Air
  - Nuclear
  - Even ‘exempt’ areas are choosing to deliver Assurance Cases

- Other:
  - IEC 61508:
    - Functional safety assessment
  - DO178:
    - Software accomplishment summary
  - MilStd 882
    - Technical data package
Overview

- Standards are moving from prescriptive approaches to *goal based*
- That is, it says *what* you must do, not *how* you must achieve it
- In an assurance context you must not only achieve adequate assurance, you must demonstrate your achievement

- The top-level goals are:

  1. Identify the assurance requirements
  2. Show that the assurance requirements are met
Key Assurance Case requirements

- Standards are moving from prescriptive approaches to goal based
  - That is, it says what you must achieve, not how you must go about it
- Assurance requirements flow from legislation, regulations, standards and policy
- Assurance should be considered from the earliest stage in a program and used to influence all activities, products and systems
- Culture of Assurance:
  - Competency, SMS, systems engineering approach, systems and organizational interfaces
- Hazard/mishap management
  - Hazard ID/analysis, risk identification/minimisation, risk acceptance, defect/mishap identification and feedback
What is an Assurance Case?

… 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 environment.

- The Safety Case contains a structured argument (rationale) demonstrating that the evidence contained therein is sufficient to show that the system is safe.
- The argument should commensurate with the potential risk, the system’s complexity, the novelty of approach or technology, the uncertainty of the context of use...
- To be compelling and comprehensible an Assurance Case and its derived reports must ‘tell a story’.
Viewpoints

Stakeholder viewpoint - a key issue.

Stakeholders include:

- Supplier
  - safety manager
  - safety specialists
  - project manager
  - design team
- Customer
  - Duty Holder
  - Safety Manager
  - Safety specialists
- Sub-contractors
- Users, operators and managers
- Passengers, public
- ISA/Regulator
- and if things go wrong ... Lawyers
Assurance Case Context

- Assurance Cases
  - Complex bodies of interdependent and evolving information
  - Combination of many documents
    - Test reports, requirements, design documents, analysis, simulations, competency records, risk registers, hazard logs...
  - Heterogeneous document formats
    - PDF, MS Word, Excel, Access, DOORS...
  - Probably not under completely coherent configuration control
    - Perhaps several parties contributing
    - Hierarchies of Assurance Cases with dependencies
      - Service, platform, equipment, system, component...
  - May not be easily auditable or reviewable as a whole

- Assurance Case Reports
  - A ‘projection’ of the rationale and content of a Assurance Case at an appropriate milestone
  - Reviewable against the project expectation at the milestone
  - May need several reports for various stakeholders
A conceptual framework and graphical notation for representing the structure of an argument can be traced back to Toulmin*.

Toulmin makes a distinction between "claim or conclusion whose merits we are seeking to establish" and "the facts we appeal to as a foundation for the claim".

*Toulmin, Stephen. The Uses of Argument (Cambridge University Press, 1958)
Structured Assurance Cases

This approach underpins both Claims-Argument-Evidence and GSN Assurance Case notations

Claim

- functional correctness, reliability, availability, inherent safety, security, fail-safety, competence, supportability, etc.

Sub-claim

- standards compliance, analytical, process, experience

Evidence

- direct evidence, underpinning or backing evidence

Argument Structure
Assurance Case “story”

To tell the story we need to:

- make an explicit set of *claims* about the system
- identify the supporting *evidence*
- provide a set of safety *arguments* that link the claims to the evidence

The Assurance Case should be initiated at the earliest possible stage in the safety programme so that hazards are dealt with while their opportunity for exclusion exists.

- make clear the assumptions and judgments underlying the arguments
- allow different viewpoints and levels of detail

DefStan 00-56
Claims - Argument - Evidence

- **Node types:**
  - **Claim** Blue Ellipse
    - and sub-claims ‘is sub-claim of’
  - **Argument** Green Rounded Rectangle
    - ‘supports’ claims
  - **Evidence** Pink Rectangle
    - ‘is evidence for’ arguments and claims
  - **Other** Grey Hexagon
    - used for context, disconnected components, etc
  - **Caption** Transparent
    - used to provide annotation over the graph
Representation in ASCE
## Goal Structuring Notation

### Node Types:

<table>
<thead>
<tr>
<th>'Spinal’ Nodes</th>
<th>'Contextual’ Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Goal</td>
<td>Assumption</td>
</tr>
<tr>
<td>Strategy</td>
<td>Justification</td>
</tr>
<tr>
<td>Solution</td>
<td>Context</td>
</tr>
</tbody>
</table>

- Goal: Rectangle
- Strategy: Parallelogram
- Solution: Circle
- Assumption: Ellipse (A)
- Justification: Ellipse (J)
- Context: Rounded Rectangle

*Not formally part of GSN, but included in ASCE:*

- Model: Diamond
- Note: Part Rectangle

© Adelard 2008
The links are typed:
- Spinal nodes with solid arrows
- Contextual nodes with open arrows

The ‘A’ and ‘J’ are part of the node shapes
A ‘Note node is not usually linked into the structure, but is commonly used for overall project context (e.g. references, glossary, ReadMe etc.)
GSN Standard

- Available as draft version:
  - [http://www.goalstructuringnotation.info](http://www.goalstructuringnotation.info)
- Issued for comment in May
- Comment period closed end August
  - but...
- Final committee meeting early November
- Expect publication by the end of the year

- Covers both the core language
  - already described
- but also extensions
  - Pattern Language
  - Modular GSN
  - will (briefly) cover these tomorrow
A conceptual framework and graphical notation for representing the structure of an argument can be traced back to Stephen Toulmin*.

Toulmin makes a distinction between “the claim or conclusion whose merits we are seeking to establish” and "the facts we appeal to as a foundation for the claim".

(*)& Toulmin, Stephen. The Uses of Argument (Cambridge University Press, 1958)
The Assurance and Safety Case Environment
  
  - a sophisticated information management system

Supports numerous graphical presentation styles (schemas)
  
  - Goal Structuring Notation (GSN)
    - (+ Modular GSN)
  - Claims-Argument-Evidence (CAE)
  - Fault trees
  - Why-Because
  - Project management
  - Hierarchical task analysis
  - ...

Powerful and flexible reporting system
  
  - to HTML for interactive reports
  - to MS Word or PDFs for more conventional reports

Integrates with other information sources

Plugins
  
  - DNR plugins
    - Dynamic Narrative Regions – map information from diverse sources into ASCE
      - e.g. regions from spreadsheets, queries from databases, pages from PDFs
  - Macro plugins
    - Programs that can process information in ASCE documents
    - or link to and interact with other programs

...
Information integration

- ASCE’s DNR Plugins support
  - Mapping of information from other common sources
    - tracking change in the mapped information
    - automatic re-mapping of imported information
      - individually and globally

- ASCE has plugins for importing
  - paragraphs from MS Word documents
    - and linking out to bookmarks in Word documents
  - pages and highlighting lines from a PDF file
    - and linking out to specific pages in PDF documents
  - regions from an Excel spreadsheet
  - SQL queries from databases
  - DOORS objects and components
This allows engineers to continue to use existing processes and tools, but assemble the assurance argument structure in ASCE.

- Links in key evidence from a range of supporting file formats

- Create Assurance Case Reports in
  - HTML for viewing interactively and mounting on intranets
  - MS Word and PDF
    - including export to corporate templates
    - production quality docs
    - without touching Word
Assurance Case and Hazard Management

- Assurance Cases
  - required for systems, processes, services in many domains
    - A structured argument supported by a body of evidence...
    - Governed by Def Stan 00-56, CAP 670, ROGS...
  - The Assurance Case must demonstrate *inter alia* that
    - risks are identified, managed, and reduced to an acceptable level
      - (ALARP)
    - all legislative requirements met
- The Hazard Log (or Risk Register, or ...)
  - An important source of evidence that risks are managed and controlled
  - Typically involves identification of
    - Hazards, Accidents and Controls
    - and relations between these
- The Assurance Case needs to refer to and use information held in the Hazard Log
  - To report overall Hazard log status
  - To monitor for changes
  - To summarise status of specific items of interest
Resources

- ASCE ‘Goodies’ CD
  - See the ‘ReadMe’ file for contents
  - ASCE 3.5 evaluation version
  - Lots of examples
    - POSMS
    - JSP520
    - ‘Kettle’ Safety Case
    - Report examples
    - Adelard Safety Case Development Manual
- Free!
Simple example C-A-E

- Safety case for a simple control system
- Simple, but realistic
- ~25 nodes

Top Claim

[ATC] is adequately safe to use, in the environment defined by the assumptions, for air traffic services
User Views

- User view of top claims
  - View on to subset of main argument
  - Used to manage comprehension of large-scale networks
  - Semantics identical to main view
  - Layout and geometry variable
  - Unlimited number of user views
  - Once-only definition - persistent thereafter
  - Navigation between views and main view
  - Editing supported at view level
  - Powerful tool in ASCE reporting features
User View of top level decomposition

[ATC] is adequately safe to use in the environment defined by the assumptions, for air traffic services

If it meets appropriate safety targets and is used within a suitable environment:
- Restricted

Appropriate safety target for [ATC]

[ATC] meets safety target

Appropriate safety management system and culture of safe working are in place for [ATC]

Occupational safety standards are met
**Structural assurance backed by detailed narrative**

Each 'Node' in ASCE has private HTML narrative:
- Standard HTML, so simple copy/paste from other applications
- Supported by powerful hyperlink capability
- Within the assurance case
- To external resources
- Underlying format XML

Sub claim: Equipment failure targets met

**Argument:** because 'Software and hardware both adequately reliable'

**Evidence:** 'Hardware reliability assessment'

Double click a node to open...
Global link checking

- Checks that all internal links terminate sensibly,
- file links terminate on an existing file and that the file has not changed since the link was last updated.
The Platform Safety Case demonstrates that for each Nonsuch Class submarine, the platform systems and equipment meet the defined Safety Objectives by presenting a number of Safety Arguments based upon a body of Evidence.

**Safety Objectives**

Safety Objectives are the high level propositions that the safety case must prove to demonstrate that the safety policy has been implemented. The Safety Objectives are defined in the Whole Submarine Safety Case Safety Policy, Principles and Criteria paper, **01 - Platform Safety Case References, MP1**. The key objectives are summarised below.

**Primary Safety Objective**

The primary safety objective for in-service submarines is to ensure that levels of risk are kept as low as realistically practicable (ALARP). That is, that the risks associated with the submarine platform, its systems and equipment are managed through the Platform Major System Safety Case to ensure that the primary safety objective is met.

**Support to this Claim**

This claim is supported by 4 principal claims, arguments and items of evidence as follows:

The Current Status of Key Hazard Certification for Nonsuch Class
Birds-eye View

- Floating window gives overview of network
- Improves navigation
- Active region highlighted
- Wheel mouse zoom
- Drag the focus area to scroll the main view
Bird’s Eye View
Table View

- ‘Excel’-like view of all nodes
- Each row has all properties of a node:
  - ID, Title, Type, Status fields
  - Status fields:
    - Structured data elements (cf free format narrative)
      - Numeric
      - Boolean
      - Text
      - Enumerated list
  - Difference for each schema
- Filter on node type
  - e.g. may want a list of only evidence elements
- Navigate from the list to
  - edit node content
  - see node in context on the main graph
- Export to Excel, Access
  - Can help with management of large ASCE documents
<table>
<thead>
<tr>
<th>Id</th>
<th>T No</th>
<th>Twc Node type</th>
<th>Annotation</th>
<th>Audited</th>
<th>Completed</th>
<th>Has External Evidence</th>
<th>Confidence</th>
<th>Spectrum 1</th>
<th>Spectrum 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Hazard managed through hazard log</td>
<td>Argument</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE to be employed in standalone and integrated water heating system</td>
<td>Argument</td>
<td>True</td>
<td>True</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Follows from correct handling of water</td>
<td>Argument</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If all relevant safety requirements have been identified, KETTLE meets them and, additionally, KETTLE is safely operated</td>
<td>Argument</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE meets its safety requirements</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE correctly heats water</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE is operated within an adequate safety management system</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Safety requirements for KETTLE were correctly captured and validated</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hazards are managed and ALARP</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE meets HO work device requirements</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE does not impede the provision of HO water</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE meets its physical safety requirements</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE meets its functional safety requirements</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functional safety requirements captured and validated</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE correctly interfaces with other HWGs</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Physical safety requirements correctly captured and validated</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>KETTLE is adequately safe to use, in the environment defined by the assumptions and if the prerequisites are met, to provide water heating and delivery services, both in standalone and integrated configurations</td>
<td>Claim</td>
<td>True</td>
<td>False</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Functional safety requirements</td>
<td>Evidence</td>
<td>True</td>
<td>False</td>
<td>High</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HWGs testing</td>
<td>Evidence</td>
<td>True</td>
<td>False</td>
<td>Low</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Description of the SMS</td>
<td>Evidence</td>
<td>True</td>
<td>False</td>
<td>Medium</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>
Basic Traceability
The ASCE Difference tool

- Compares two ASCE networks
- Reports structural changes
  - deleted/new nodes
  - delete/new links
  - etc
- Displays node content differences
- Supports traceability and reviewing throughout the Assurance Case lifecycle
Assurance Case Report Templates

- Examples
  - JSP 520 - OME
  - Yellow Book
- Standards encoded as ASCE template
- Guidance from standard included
- Replace guidance with content to create report
- ASCE DNR Plugins provide change tracking and dynamic re-mapping of content
- ASCE Export Functions support ‘instant’ publication into Word
Risk Assessment

The Risk Assessment process can be considered as four distinct phases. The process is summarised below (AOP-15, Defence Standard 00-55 and Mil-Std-882 all provide detailed guidance on the procedures and techniques that should be followed):

Hazard Identification - Identify all potential hazards, firstly at system level (Preliminary Hazard Analysis), and subsequently at subsystem and component level. This is the most critical stage of the process, as any missed hazards may cause the overall safety risk associated with a system to be incorrectly estimated. Historical accident/incident data and any previous risk assessments can provide useful inputs to this process.

Hazard Severity Category - All identified hazards must be categorised according to the severity of the worst credible repercussion to personnel, capability and the...
Exporting Electronic Assurance Cases

- HTML export
  - Can be viewed using any Web Browser

Also available:

- The ASCE Browser
  - Download free from www.adelard.com
  - Freely distributable with HTML export
  - Intuitive in use
  - For distribution of structural cases for reviewers/managers
  - Auto-start CD
Relevant standards applied

Completed: True
Annotation:
Parent nodes:
- Supports: Workplace H&S adequate
Child nodes:
- Has evidence: PHA
- Has evidence: PHI

Applicable standards


Adequately safe, Top level Claim

All the relevant activities that are required by IOF 476 for systems in Risk Category 4 have been carried out, namely:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preliminary Hazard Identification</td>
<td>PHI, Methodology</td>
</tr>
<tr>
<td>Preliminary Hazard Analysis (PHA)</td>
<td>PHA, Preliminary hazard analysis</td>
</tr>
<tr>
<td>Hazard Log establishment</td>
<td>Hazard Log, Appendix A Hazard Log</td>
</tr>
<tr>
<td>Safety Review</td>
<td>Safety Review, Safety Review</td>
</tr>
</tbody>
</table>
Creating formal Assurance Case reports

- Tools for export to Word version, including
  - ‘One click’ export
  - dynamic section ordering and numbering
  - cross reference resolution
  - style sheets
  - export filter to control layout

- Powerful, but transparent support for house styles/layout
  - source provided
Managing safety document hierarchies

- Assurance Case is a key document in the assurance of equipment throughout its operational life
- Does not stand alone though
- Inputs:
  - Analysis, testing, process documentation etc
  - Subsidiary Assurance Cases, Hazard Logs
- Outputs:
  - Assurance Case reports
  - Executive summary
  - Statement of operational limitations/instructions
- Sets of interlinked documents with crucial dependencies
Managing safety document hierarchies

- Platform Safety Case
- Equipment Safety Cases
- Hazard Management Systems
- ISA/Regulator
- Customer/Duty Holder
- Safety Case Summary Report
- Statement of Operational Limitation
- Safety Case Detailed Report
- Other evidence e.g. FTA, testing
  - Validate
  - Informs safe operation
Custom notations in ASCE

- Flexible schema (notation) definition
  - Extensions of existing schemas (e.g. to support process extension)
  - Definition of new schemas
  - Definition of new check rules and status display (e.g. traffic lights)
  - User driven option in ASCE 3.5
  - Is being used to implement other notations
    - Causal analysis
    - Project management
    - Assurance Case Review
    - Navigating complex document sets
    - Fault trees
    - Task analysis
    - Problem Frames
    - ....
Schemas

- Components:
  - Nodes (types, shapes, colour, <compound>)
  - Links (annotation, arrow type/direction, colour)
  - Status fields
    - Narrative, Boolean, dropdown lists
  - Display rules
    - Drive various display features (e.g. whole node shading)
    - driven by status fields (traffic lights, GSN TBDvpt)
    - toggle on or off (Options)
  - Checkrules
    - 4 levels of severity
    - XPATH
    - Circularity checker built in
Exporting

- Export to HTML
  - Can be viewed with a normal web browser
  - However
    - can get lost easily
    - main graph does not zoom
    - platform issues (graphic formats)
- ASCE Browser
  - free and intuitive
  - zoomable map, tooltips
  - configurable as autostart
  - convenient way to ship case and supporting docs
  - need to think of configuration control though
Export to Word

- Usually a fundamental requirement to produce a production quality narrative document
- ASCE reporting: Export to Word:
  - Two paths
    - 1-click export
      - all-in-1
      - plugin, so easily improved and customised
      - Simpler
      - Supports export to corporate templates, paragraph numbering
    - built in: three phase
      - export to temporary folder
      - open up in Word
      - apply Word macro and style file
Customisation of exports

- **Standard export:**
  - Create export (3 stage)
  - Copy into a corporate template
  - Apply update macro (if it has one)

- **One-click:**
  - Select a template
  - Run the export
  - Err, that’s it.
One click export - 0.1.41

- Content now inserted *into* house template
  - Based on optional Bookmark in template `InsertASCEContentHere`
  - Otherwise inserted at end of document (graceful degradation)

- Post processing supported
  - `ASCEPostProcessingMacro` if defined in template
  - Typically to convert styles, and to run any corporate update macros

- Note: 3.5.30 delivers 0.1.14, need to download 0.1.41 from www.adelard.com
Additional export features

- Export template:
  - HTML comment fields
  - controls exactly what is exported e.g.
    - Narrative, author, logo, status field, links to parent/child nodes
  - example

- Style sheet
  - example
ASCE plugins

- What are ASCE Plugins?
  - A user extensible capability
  - Scope
    - VBScript + COM
    - e.g. interface with other applications, interrogate data sources
  - XML container: vbscript + HTML
  - Plugins can:
    - Integrate Assurance Case content from external data sources
    - Query the underlying Assurance Case
    - Run a report (e.g. 1-click export)
    - Propagate information across a case (e.g. fault trees)
ASCE 3.5 DNR plugins

- ASCE node content
- ASCE traceable statement
- Excel region
- Access SQL query
- BMT HARMS
- Cassandra (3.1 and later) Excel export
- Windows folder listing
Additional available DNR plugins

- DOORS object import
- Word bookmark navigation
- Evidence summary (GSN)
- Code input/format
- HVR Cassandra (3.2)*
  - Risk matrix
  - Accident/hazard/control tables
  - Individual accident/hazard/control
- PDF navigation
- Issues mapping*
- Word import (beta)
Examples

- ASCE node mapping
- Excel region mapping
- PDF
- Issues mapping
- Cassandra 3.2
Issues mapping plugin

- During the Assurance Case management lifecycle a number of issues will often arise requiring further management:
  - Assumptions to be confirmed, Actions for other parties and stakeholders, Issues to be resolved, Operating limitations
  - ...;
- These issues usually arise in a specific context of the argument structure, e.g.:
  - Limitations arising as a result of test case failure
  - Issues reflecting incomplete knowledge at the time
    - Obviously requiring resolution later
- From a management point of view we want to
  - look after them and summarise them
  - understand them in context
Use is simple

- As the analysis proceeds, drop any number of embedded issues within the narrative of the nodes
  - Basic fields: titles, text, keywords
  - Different types available
    - Issue, Action, Requirement, Limitation, Assumption, Risk
    - ... (the list could be extended if desired)
- At a high level in the case insert a Issues summary DNR
  - This collates all issues of a certain type into a table
  - Shows context where the issue is
- Summary can be of the current network or an external network
  - Can be used to manage issues and limitations across a collection of related cases (system/subsystem/component)
This screenshot shows:
- Embedded issue DNR in an individual node
- Summary DNR of all issues in the current network
Modular Assurance Cases

- GSN ‘Modular cases’
- IEC 61508 ‘safety manuals’
Modular GSN

Sources:
- Tim Kelly - 2001 MoD report
- Bates et al - 2003 ISSC Conference paper
- Tim Kelly - Visio plugin for GSN
Modular GSN representation in ASCE

- Publicly visible goal
- Publicly visible context
- Strategy
- Normal goal
- Q
- Normal goal
- Normal goal
- Normal goal
- Away context
- Solution
- Contract reference
- Module reference
- Goal solved by unspecified contract
- Away goal
- D:/path/file.axml#N1234
- D:/foo/path.axml
Assurance Case Review

- Markup
  - Review Nodes

- Adelard Assurance Case Review Template
  - Extend CAE with ‘Review’ nodes
  - Make SC Review criteria explicit
  - Assess against criteria and document in review nodes
  - Export path to create SC Review report
<table>
<thead>
<tr>
<th>Part 1 Introduction</th>
<th>Part 2 Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>Overview of approach</td>
</tr>
<tr>
<td>The importance of a good safety case</td>
<td>Safety case development</td>
</tr>
<tr>
<td>Basis of the ASCAD methodology</td>
<td>Developing safety case elements</td>
</tr>
<tr>
<td>How to use the manual</td>
<td>Safety case project structure</td>
</tr>
<tr>
<td>Feedback</td>
<td>Independent assessment and acceptance</td>
</tr>
<tr>
<td>Acknowledgements</td>
<td>Long-term maintenance</td>
</tr>
<tr>
<td></td>
<td>Contents of a safety case report</td>
</tr>
</tbody>
</table>
ASCAD - Appendices

A. System safety context
B. Design options to limit dangerous failures
C. Checklist of safety documents
D. Attribute-claim-evidence tables
E. Review of changes affecting the safety case
F. Safety case review checklist
G. Use of field evidence for reliability claim
H. Long term issues
I. Maintenance and human factors
J. Checklist of long term issues
K. Example safety case
The end