2012 Developments in Modular (Software) Safety Cases and Modular GSN

John Carter
General Dynamics on behalf of IAWG
Agenda

• **What** is IAWG MSSC?
  – System Wide Arguments
  – Applicability
• Status of IAWG MSSC work
• MSSC and Standard Modular GSN
  – Away References to Consumer Goals
  – Contract and Integration SC Modules
  – Patterns and Templates
  – Context
  – Containment
• Future Developments?
  – Strength of Assurance
IAWG MSSC

The modular construction of a Safety Case seems like common sense, but in practice, over a real supply chain, it is challenging.

MSSC describes \textit{practically} how to;

- Make the best choice of SC modules
  - Hazard Mitigation
  - Requirements
  - Component Related
  - Integration
- Fit them all together
- Populate them with argument (from GSN patterns)
- Alter an approved SC upon System change
IAWG MSSC: Applicability

**MSSC principles are applicable at System Level**

- It was developed originally for Software
- It has been applied
  - to SC with both HW and SW elements.
    - Integrating to a traditional HW safety case in a SC Module “wrapper”
    - Where Hazards are the starting point, rather than (Software) Safety Related Requirements.
- Potentially larger benefits than for SW alone
IAWG MSSC: System Wide Arguments

**MSSC modularises the argument and evidence only where it is beneficial to do so**

- Some evidence may not be efficiently modularised.
  - Resource consumption
  - Latency
- Generate this evidence later in the integration process… and…
- Introduce it higher up the safety argument
IAWG MSSC

• The research strand started in 2005.
• Programme completed on 20\textsuperscript{th} Nov 2012
• Trialled on real programmes, Hawk & Wildcat
• Process documents now public domain
  – Overview (0101)
  – Core Process (0201)
  – Glossary (0202)
  – GSN (0203)
  – Artefacts (0204)

Available at
www.capability-agility.co.uk

Leaflet & White Paper available today
Away References to Consumer Goals

• The final argument must be navigable top-down
  – but modular argument construction order varies
• SC Modules that change independently cannot refer to each other
  – instead the integrator will refer to them both in a SC Contract.

The integrator’s view needs clarification by distinguishing away references to goals that **require** support from those to goals that **provide** support.
Contract and Integration SC Modules

**MSSC users need to be allowed to develop away goals in integration arguments that are not constrained to a SC contract pattern.**

- Necessary in
  - No Unwanted Interactions (NUI) pattern
  - Initialisation
  - Possibly elsewhere in future.

---

**New1**

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To be solved by contract argument integration SC module.</td>
</tr>
</tbody>
</table>
Patterns and Templates

• It is necessary to distinguish:
  – (MSSC) Patterns
    Incomplete GSN arguments that guide SC authors
  – (MSSC) Templates
    A concise presentation of multiple similarly formed arguments in the final SC.

• Templates have particularly been used for:
  – contract arguments for many communication channels between applications.
  – Similar arguments for many guaranteed behaviours of a part of the system.
Treatment of Context

MSSC takes positive steps to de-mystify and address treatment of the vague term “context”.

- Must be **Captured** completely and then **Compared** for incompatibilities during integration.
- Limited to information that constrains a claim’s validity
- Relies upon Problem Domain and Argument experts
  – But provides aid-memoires by argument subject
- High Level - e.g. Sub-system Integrity Level, authoring organisation
- Low Level - e.g. units, precision and accuracy of exchanged data.

MSSC needs a concise diagrammatic symbol behind which all captured context inherited by an away reference to a goal may be documented.
Containment

MSSC found value in the use of Containment

• To allow suppliers to both
  – hide their SC Module structure
  – make their argument available to independent scrutiny
• Simplifies Integration
• Protects IPR
• (Along with Public I/F Private Argument)
Strength of Assurance

The problem of capturing the strength of a claim or argument is unchanged by the use of MSSC

Compatibility with any particular scheme;
- Stakeholder satisfaction
- Providing assurance measures as context
- Assurance meta-argument
- Also with a parallel meta-argument (although this work has not been done)
  - Presumably this would also need to be modular
MSSC Process Steps

1. Analyse the Product Lifecycle
2. Optimise Design & Safety Case Architecture
3. Construct Safety Case Modules
4. Integrate Safety Case Modules
5. Assess/Improve Change Impact
6. Reconstruct SC Modules
7. Reintegrate SC Modules
8. Appraise the Safety Case
End of Presentation