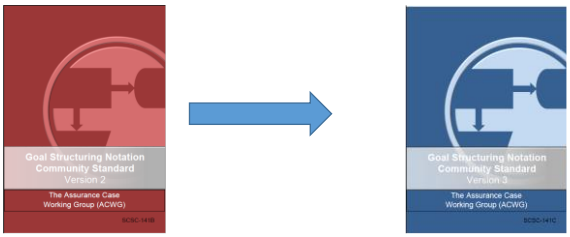
ACWG [GSN_SWG]

Goal Structuring Notation Standard

Changes from Version 2 to Version 3



1

ACWG [GSN_SWG]

Role of SCSC ACWG

- GSN Community Standard is now maintained by the Safety Critical Systems Club Assurance Case Working Group [GSN_SWG]
- Volunteer group with peer-reviewed output
- Standard and related material available (FREE) at scsc.uk/gsn

2

ACWG [GSN_SWG]

Change Categories

- Administrative/Typographical
- Patterns – including introduction of 'Templates'
- Modular notation
- Confidence Argument
- Dialectic
- Other

3

ACWG [GSN_SWG]

Administrative/Typographical

- Contextual updates to Foreword, Document History, Contributors & Introduction
- Re-structure of document
  - 'Extension' notations are now part of the main definition section of the document, as both notations and guidance to aid readability
- Review for language consistency and clarity resulting in minor re-work
- Recognition that guidance on interaction of extensions need to be addressed
- Updated Glossary and References
  - Addition of reference to broader assurance case guidance

4

ACWG [GSN_SWG]

Patterns

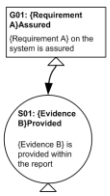
- Introduction of ‘Pattern Definition’
  - Minimum attributed to be declared alongside graphical pattern
  - See Section 1:3.4
- Introduction of ‘Template’
  - Special type of pattern to avoid graphical repetition
  - See Section 1:3.5
- Optionality, Multiplicity & Choice
  - Clarification of use & explicit definition of choice
  - See Table 1: 3-1

5

ACWG [GSN_SWG]

Patterns: Templates (general)

- For arguments where a single fragment of GSN would be repeated multiple times for a number of instantiations
- created using pattern notation
  - without ‘undeveloped’ elements
  - instantiation data e.g. in a table



Instantiation Number	(Requirement A)	(Evidence B)
1	Displayed information is red	Section 3.2
2	Font is Times New Roman	Section 4.7
3		
4		

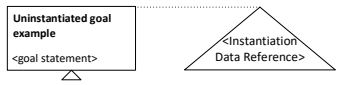
- New symbol : reference to instantiation data
  - See next slide

6

ACWG [GSN_SWG]

Patterns: Templates (symbol)

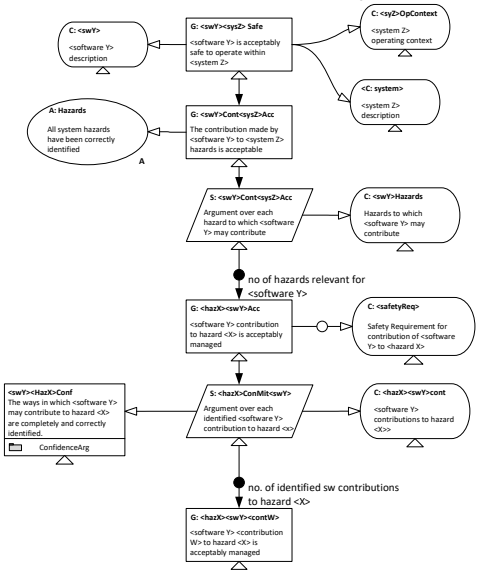
- New Symbol (Table 1:3-3):

GSN Symbol Rendering	Definition
	**Instantiation Data Reference**. This symbol indicates that the GSN argument below the attached element is to be instantiated as a template argument. It provides a reference to the information used to instantiate the template argument. The symbol is not considered a GSN element as it does not form part of the argument. It is attached to the top element of the template argument by a dotted line between the top edges of that element and the symbol (as shown below).
	Example use of an instantiation data reference.

7

ACWG [GSN_SWG]

Patterns: Templates (example)



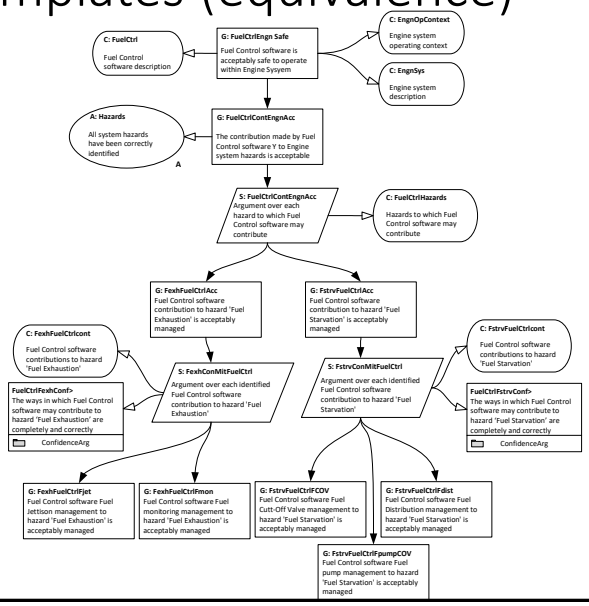
<system Z> [<sysZ>]	<software Y> [swY]	<X> (hazard) [hazX]	<contribution W> [<contW>]
Braking System [Brk]	Brake control Software [BrkCtrl]	Runway Excursion [RwEx]	TBD
		Runway Overrun [RwOR]	TBD
		Fire due to overheated brakes [OhtBrk]	TBD
Engine System [Engn]	Fuel Control Software [FuelCtrl]	Fuel starvation [Fstrv]	Fuel Distribution management [Fdist]
			Fuel Pump management [Fpump]
			Fuel Cut-Off Valve management [FCOV]
		Fuel Exhaustion [Fexh]	Fuel Monitoring management [Fmon]
			Fuel Jettison management [Fjet]

8

ACWG [GSN_SWG]

Patterns: Templates (equivalence)

- Potential for automated population of instantiated data into full GSN
- For this example….
- *(NB this is an incomplete, instantiation, but is to illustrate the concept)*
- Ideally, tools would either show the template and table, or would automatically instantiate the GSN elements, based on data from the table, as alternative views

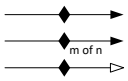


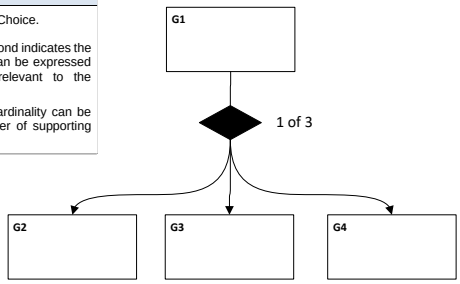
9

ACWG [GSN_SWG]

Pattern: Choice

- ‘Choice’ was confused with ‘option’ in previous versions, but now made explicit

GSN Relationship Rendering	Definition
	A solid diamond is the symbol for Choice. The optional label next to the diamond indicates the cardinality of the relationship. It can be expressed as an instantiable parameter relevant to the argument. If no label is included then the cardinality can be any value from one to the number of supporting elements.



10

ACWG [GSN_SWG]

Modular GSN

- Re-definition of view names to reduce over-loading of term ‘module’
- New/Changed Symbols
- Clarified module containment in other modules (See 1:4.1)
- Clarification of context assertion with away_goals (See 1:4.3)
- Added explicit definition of module interfaces (See 1:4.6)
- Clarified concept of inter-module contracts (See 1:4.7)
- Updated associated guidance (See 2:9)

11

ACWG [GSN_SWG]

Modular: Views

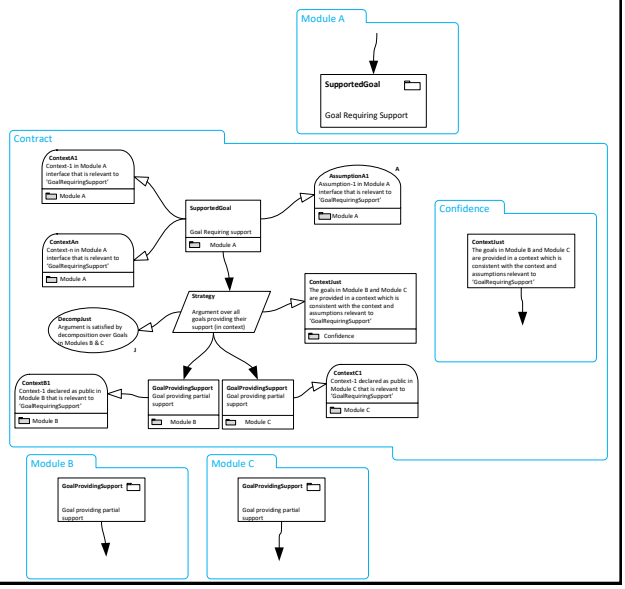
- Re-definition of view names to reduce over-loading of term ‘module’
  - ‘Architecture View’
    - Safety Case Architecture
    - Replaces ‘module view’ and ‘inter-module’ terminology
  - ‘Argument View’
    - for the argument within the module
    - Replaces ‘intra-module’ terminology
  - ‘Extended Views’
    - Accepted the common usage but not normalised by the standard

12

ACWG [GSN_SWG]

Modular: Views (Extended Example1)

- Informative (not normatively defined)
- Extended View Example –
  Contract Argument and Related Modules

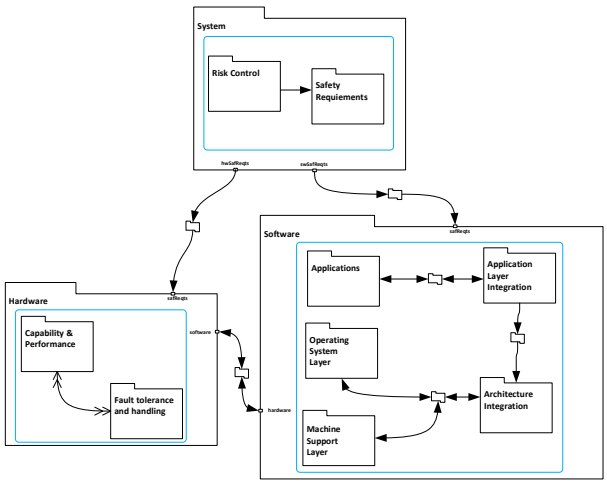


13

ACWG [GSN_SWG]

Modular: Views (Extended Example2)

- Informative (not normatively defined)
- Extended View Example –
  Modules Contained Within Modules



14

ACWG [GSN_SWG]

Modular: New/Changed Symbols

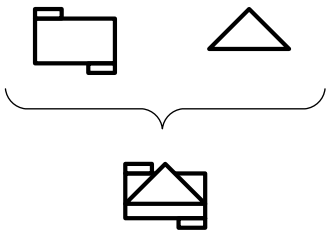
- Clarified terminology within the definition of existing symbols
- Argument View
  - Added notation for combined decorator
    - 'solved by contract' AND 'to be instantiated'
  - new away_justification and away_assumption;
  - illustration of public decorator for justification and assumption
- Architecture view
  - New Module, Contract, Interface decorator & Relationship Symbols for
  - Use of away_goal as top goal in contract module

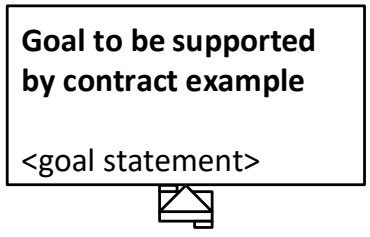
15

ACWG [GSN_SWG]

Modular: Symbols (1)

- New combined decorator for 'to be instantiated' and 'to be solved by contract'



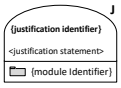


16

ACWG [GSN_SWG]

Modular: Symbols (2)

- New away justification and justification annotated to show it is public



An **away justification**, rendered as a semi-ellipse sitting on top of a rectangle with the letter 'J' at the top-right (the semi-ellipse may be raised above the rectangle by extending its vertical extremes in a straight line).

An away justification repeats a justification presented in another argument module and is typically used only in Contract Modules.

- New away assumption and assumption annotated to show it is public

An **away assumption**, rendered as a semi-ellipse sitting on top of a rectangle with the letter 'A' at the top-right (the semi-ellipse may be raised above the rectangle by extending its vertical extremes in a straight line).

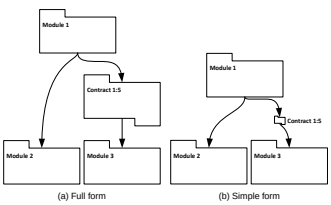
An away assumption repeats an assumption presented in another argument module and is typically used only in Contract Modules.

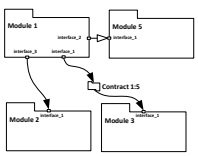
17

ACWG [GSN_SWG]

Modular: Symbols (3)

- New Module and Contract symbols for Architecture view
- …and examples of use





GSN Element Rendering	Definition
{module Identifier} <module description>	**Module** symbol view to repre The module i to the symbo below the sy Inclusion of t
{contract Identifier} <contract description> {contract Identifier}	**Contract** sym view to repre defines the re module interf supports the Alternative co available to s of the archite The contract to the symbo below the sy symbol is use the side of th Inclusion of t optional.
{interface identifier} {module Identifier} {interface identifier} {interface identifier} <module description> {interface identifier}	A **Module Int** a small squa symbol, can of the specifi {interface ide relationship. Where no int interface is a See section **I** **found.** for fu

18

ACWG [GSN_SWG]

Modular: Symbols (4)

- Clarified/additional relationships in Architecture View
- Arrow heads can be:

- 'InContextOf' (for exclusively context relationship in the interface),

- 'SupportedBy' (for exclusively supported relationships [includes in scope context but not contextual relationships])

- Composite (mixture of 'InContextOf' and 'SupportedBy' relationships)

- Arrow heads can be at either or both ends (i.e. relationships can go both ways simultaneously as long as no 'loops' are created)

- Optionally, the relationship line can be decorated with a number indicating the number of relationships represented.

19

ACWG [GSN_SWG]

Modular: Interfaces

- Added explicit definition of module interfaces
  - interfaces used to support abstraction and information hiding,
    - E.g. to protect IP when integrating 3rd party products
  - may publish more than one interface;
    - interfaces with difference scopes published to different collaborating parties

20

ACWG [GSN_SWG]

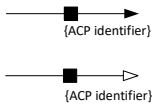
Confidence Arguments

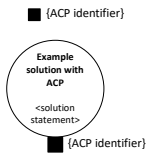
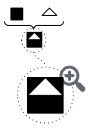
- New notation
  - can be added to any 'SupportedBy' or 'InContextOf' relationships
  - can be added to elements that make a reference (e.g. solution, context)
- Allows a separate argument to be made about the confidence in the inference
- Guidance on use added

21

ACWG [GSN_SWG]

Confidence: Symbols (1)

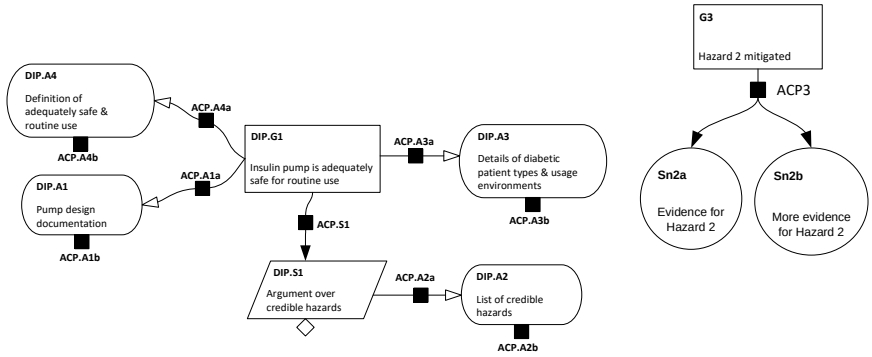
GSN Relationship Rendering	Definition
	A solid square is the symbol for ACP. The label next to the square indicates the ACP identifier. It can be applied to 'SupportedBy' and 'InContextOf' relationships.

GSN Element Rendering	Definition
	A solid square is the symbol for ACP used as a decorator for an element. The label next to the square indicates the ACP identifier. It can be applied as a decorator to solution, context, assumption and justification elements.
	The ACP decorator can be combined with the 'uninstantiated' decorator. 

22

ACWG [GSN_SWG]

Confidence: Symbols (examples)



23

ACWG [GSN_SWG]

New notation for Dialectics

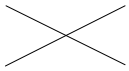
- Allows Challenges to the argument to be recorded and managed
  - cf. Haddon-Cave criticisms about bias in safety cases
  - Way of representing/recording counter-argument and counter-evidence within the GSN structure and how it has been addressed
  - Based on a GSN mark-up notation
- Guidance provided

24

ACWG [GSN_SWG]

Dialectics: Symbology (1)

- New notation

GSN Element Rendering	Definition
 Defeated Element Decorator Symbol	***Defeated Element*** decorator symbol, rendered as a cross ('**X**') superimposed on a GSN element. This indicates that the element is defeated The *Defeated* decorator can be applied to any of the GSN elements.
	A ***defeated element,*** *Example:* *(here applied to a Goal)*, rendered with the cross ('X') decorator, presents a claim that is defeated.

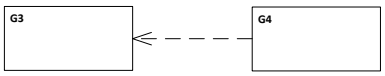
GSN Relationship Rendering	Definition
	***Challenges***, rend open arrowhead, GSN entity to be Permitted connec element, solution- relationship, soluti
 Defeated Relationship Decorator Symbol	***Defeated Relatio*** rendered as a cro GSN relationship. relationship is *defi* The *Defeated* dec of the GSN relatio
Example of use (SupportedBy relationship) 	A ***defeated relati*** (here applied to *S* rendered with the presents a Suppo defeated.

25

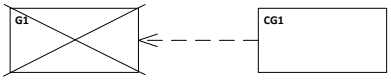
ACWG [GSN_SWG]

Dialectics – Example Usage

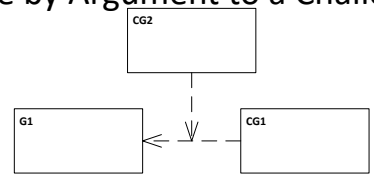
- Unresolved Challenge by Argument to a Goal



- Successful Challenge by Argument to a Goal



- Challenge by Argument to a Challenge



26

ACWG [GSN_SWG]

Other

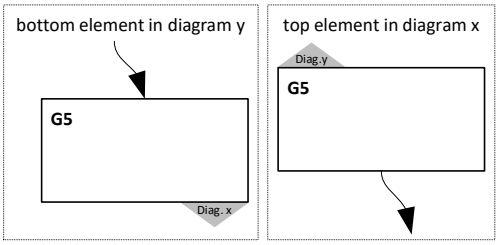
- Part 0 Section 0:4
  - Emphasis that use of GSN alone does not create a good argument – needs process including review and challenge
- Part 1
  - Clarification of 'core' GSN and relationship to 'Module'
  - Element Identifier – was optional, now mandatory
  - Assumption/Justifier labels (A/J) can now be top or bottom right
  - Emphasised that inferential/evidential links are indivisible when multiple SupportedBy relationships used
  - Introduction of 'off diagram' notation to link separate diagrams that illustrates fragments of a goal structure

27

ACWG [GSN_SWG]

Additional: Off-diagram decorator

- Section 1:2.2.20
  - Added normative part of the standard saying that off-diagram decorator need to be distinct from the GSN elements
  - Recommends a preferred off-diagram symbol



28