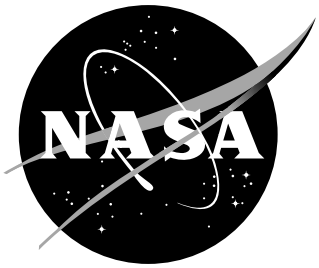
NASA/TM–2017–219650



Assurance Arguments for the Non-graphically-inclined: Two Approaches

Emily Heavner
Intern, Langley Research Center, Hampton VA

C. Michael Holloway
Langley Research Center, Hampton VA

July 2017

NASA STI Program . . . in Profile

Since its founding, NASA has been dedicated to the advancement of aeronautics and space science. The NASA scientific and technical information (STI) program plays a key part in helping NASA maintain this important role.

The NASA STI Program operates under the auspices of the Agency Chief Information Officer. It collects, organizes, provides for archiving, and disseminates NASA's STI. The NASA STI Program provides access to the NTRS Registered and its public interface, the NASA Technical Reports Server, thus providing one of the largest collections of aeronautical and space science STI in the world. Results are published in both non-NASA channels and by NASA in the NASA STI Report Series, which includes the following report types:

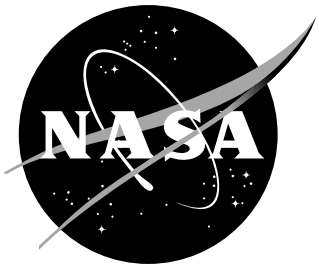
- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA counterpart of peer-reviewed formal professional papers, but having less stringent limitations on manuscript length and extent of graphic presentations.
- TECHNICAL MEMORANDUM. Scientific and technical findings that are preliminary or of specialized interest, e.g., quick release reports, working papers, and bibliographies that contain minimal annotation. Does not contain extensive analysis.
- CONTRACTOR REPORT. Scientific and technical findings by NASA-sponsored contractors and grantees.
- CONFERENCE PUBLICATION. Collected papers from scientific and technical conferences, symposia, seminars, or other meetings sponsored or co-sponsored by NASA.
- SPECIAL PUBLICATION. Scientific, technical, or historical information from NASA programs, projects, and missions, often concerned with subjects having substantial public interest.
- TECHNICAL TRANSLATION. English-language translations of foreign scientific and technical material pertinent to NASA's mission.

Specialized services also include organizing and publishing research results, distributing specialized research announcements and feeds, providing information desk and personal search support, and enabling data exchange services.

For more information about the NASA STI Program, see the following:

- Access the NASA STI program home page at http://www.sti.nasa.gov
- E-mail your question to help@sti.nasa.gov
- Phone the NASA STI Information Desk at 757-864-9658
- Write to:
  NASA STI Information Desk
  Mail Stop 148
  NASA Langley Research Center
  Hampton, VA 23681-2199

NASA/TM–2017–219650



Assurance Arguments for the Non-graphically-inclined: Two Approaches

Emily Heavner
Intern, Langley Research Center, Hampton VA

C. Michael Holloway
Langley Research Center, Hampton VA

National Aeronautics and
Space Administration

Langley Research Center
Hampton, Virginia 23681-2199

July 2017

Acknowledgments

We thank Patrick J. Graydon and Kelly Hayhurst for their feedback on this work. We also thank Universities Space Research Association for administering the intern program.

Available from:

NASA STI Program / Mail Stop 148
NASA Langley Research Center
Hampton, VA 23681-2199
Fax: 757-864-6500

Abstract

We introduce and discuss two approaches to presenting assurance arguments. One approach is based on a monograph structure, while the other is based on a tabular structure. In today's research and academic setting, assurance cases often use a graphical notation; however for people who are not graphically inclined, these notations can be difficult to read. This document proposes, outlines, explains, and presents examples of two non-graphical assurance argument notations that may be appropriate for non-graphically-inclined readers and also provide argument writers with freedom to add details and manipulate an argument in multiple ways.

1 Introduction

An assurance argument is an argument "that a system, service, or organization will operate as intended for a defined application in a defined environment" [1]. The purpose of a safety case is to combine evidence and an assurance argument to convince assessors that a system is safe [1]. Safety cases are a specific instance of assurance cases and allow writers to argue for the safety of a produced system.

The concept of safety cases was born in the United Kingdom between the 1950s and 1980s as a result of multiple incidents, including a fire at a nuclear reactor [2]. Today safety cases have evolved and are used in multiple fields, including medical and automotive industries, to argue for the safety of a product or application [1]. It is common to find research on safety arguments presented in a graphical notation like the Goal Structuring Notation (GSN); however, this approach is not ideal for everyone. When first looking at a graphical notation, readers must know how to read it, i.e., what every symbol means and where to start, before understanding the actual argument. For readers who are not graphically inclined this can pose a challenge, which may be greater than they are willing to undertake.

In this document we present two new approaches to writing assurance arguments. The first is a monograph structure; the second is a tabular structure. These structures are intended to be helpful for safety case assessors and writers who prefer not to use a graphical notation, or want more detail and freedom when constructing an argument. This paper does not discuss properties of GSN or other graphical notations. To see more information on GSN refer to the *GSN Community Standard* [3]. We also do not discuss which approach may be superior but instead simply introduce two ways to structure assurance arguments. Although we translated elements from GSN (e.g., goals and strategies) into the new structures, we will refrain from using *GSN Community Standard* vocabulary for those who are unfamiliar with it. We hope those who are familiar with GSN will see the similarities.

After researching psychological studies on how people perceive arguments, we found common unbiased characteristics and attributes that enhance prob-

lem solving skills. The two structures we introduce possess some of these characteristics. The monograph structure is great for argument assessors that have little prior knowledge of a produced system or the field the system is in because the monograph structure leans toward a more, "coherent and explicit [form] to facilitate learning" [4]. Unlike some graphical notations, the monograph structure does not impose restrictions on how additional details may be included or elaborated. Therefore, this structure is designed to include complete thoughts, ideas, and sentences. Recent studies show that, "revisions that increased the structural and explanatory coherence of texts resulted in substantial increases in recall" [5]. However, if assessors already have sufficient prior knowledge the tabular structure may be better because it can contain unspecified steps between one conclusion and the next, which requires readers to fill in the gaps. This action helps "stimulate constructive activities [that are] better for learning" [4].

Before introducing the new approaches, we will explain certain aspects and vocabulary used in this document. We focus on five elements that make up an argument: *conclusions*, *premises* (some of which are called *evidence*), *warrants*, *contextual information*, and *assumptions*. An argument is not complete without some combination of these five elements found at any given level.

A *conclusion* might be either a top level conclusion or a sub-conclusion. A top level conclusion is the main statement the writer is arguing for. Its *premises* are the statements that are claimed to provide support for the truth of the top level conclusion. A sub-conclusion serves hierarchically as a premise for one argument step, and as the conclusion of another. Main sub-conclusions refer to all the sub-conclusions that fall directly below the top level conclusion; that is, they serve as premises for the top level conclusion. For example, if an argument has three levels then the reader may think of the top level conclusion as the grandparent, the main sub-conclusions as the parents, and the sub-sub-conclusions, or remaining sub-conclusions, as the grandchildren.

Another important word used in this document is *warrant*. A warrant explains the reasoning for why the truth of the premises (which may be either sub-conclusions or evidence) should lead the reader to hold the conclusion true. Although there are other synonymous words and views of evidence, in this paper we define *evidence* as a known fact, artifact, or support that relates to and provides support for a sub-conclusion [6]. For more information on the history and different views of evidence see [7].

We use *contextual information* and *assumptions* for support throughout arguments. In these assurance arguments, contextual information informs readers of details, descriptions, or constraints needed to better understand an argument. Contextual information also explains how certain elements in an argument should be interpreted. Assumptions are statements that the conclusions and warrants, "rely [on], but which are not elaborated or shown to be true" [6]. These two forms of statements can boost arguments, clarify ideas, explain background information, or give reasons behind why the argument writer is doing something.

The important thing to note for the two structures in this paper, is that each

contextual information or assumption should only be mentioned once, preferably at the highest conclusion to which they apply. We recommend this because repeating contextual information or assumptions may "influence the reception of an argument" [8]. An argument should neither convince an assessor that a system is safe when it is not, nor make them doubt the system is safe when it is. Repeating information may cause an assessor to place more confidence in the strength of the argument than is justified by the strength of the system [8]. That being said, if an assumption applies to the whole argument, the assumption will be mentioned and discussed in the top level conclusion section (first section) only. If the assumption applies to one sub-conclusion or a specific part of an argument instead of the entire thing, the assumption will be brought up in the argument for that sub-conclusion. This approach will be elaborated on later.

In this paper we introduce and discuss both monograph and tabular structures that are used to present the safety of a system by introducing an outline, analyzing uncommon concepts in arguments, and working through real world examples. We will introduce the monograph structure first and then the tabular structure. Afterwards, we will show examples for the two approaches. The examples will be the same to allow for an easy comparison between both structures. Then we will explain how to handle a few complex argument concepts using these structure. In the examples, words appearing within angle brackets (for example, <foo>) serve as placeholders where the argument writer can insert one of the five specified elements of an argument. We suggest thinking of it like a fill-in-the-blank, where the category is an argument element.

2 Monograph Structure

Section 2 discusses the monograph structure. Every argument made in this form should look and feel like the outline of a paper, allowing the structure to have more details and elaborations than graphical notations. Multiple studies have found that readers who have little prior knowledge of a produced system or its domain tend to benefit from a seeing a "fully explicit [and] totally coherent" argument [4, 5]. Studies also show that other problem solving skills improve when arguments are complex and less explicit, suggesting that the monograph structure may not be as beneficial to assessors who have prior experience as it is to those just starting out [9].

For an assurance case to benefit from using this structure all five elements of an argument should be present. The monograph structure breaks up the overall argument into four sections and each section will have at least one of the five elements of an argument inside it.

2.1 Four Sections of an Argument

As mentioned, the monograph structure divides the overall argument into four sections. These sections help organize the argument. Just like people may put certain items into a particular drawer, certain elements and concepts of an argument are placed in a specified section. For example, a stapler may always

go in the top desk drawer while the top level conclusion, or the conclusion the writer is claiming to be true (analogous to a thesis statement in a paper), will always be stated in the first section of an argument. Putting the conclusion first allows a reader to know how each premise matters, and have an initial intuition about how strong each must be at the beginning. Section two lays out every premise, or sub-conclusion under the top level conclusion in a hierarchal order (similar to a table of contents). Following that section, is the main argument which should have the most detail and be the reasoning behind why the top level conclusion is true (like the body of a paper). The last section has a glossary, which also includes any information that was referred in the paper earlier and which needs elaboration (similar to an appendix). Any words found in the glossary should be italicized, highlighted, or underlined throughout the argument to indicate that an argument-specific meaning is intended.

2.1.1 Top Level Conclusion Section

The top level conclusion—the statement the writer wants the reader to believe is true—begins the monograph. The argument writer states the top level conclusion first and spends the rest of the document arguing why it is true through support of premises, or sub-conclusions. Besides the top level conclusion, this section also includes information used throughout the entire argument. As mentioned in the introduction, any contextual information or statements used to support the entire argument can be noted or explained using phrases like "seen in", "found in", "we note", or "given that". If there are other arguments that support the whole of this one, the writer should reference where to find the other arguments in this section. Any assumptions that are intended to be accepted throughout the entirety of the argument will be explained in this section using phrases that have the word assume in it (for example, "we assume" or "assuming that"). The monograph structure is intended to allow argument writers flexibility in their expression. Although we have listed a few phrases recommended phrases, the writer is not bound to use those exact phrases, rather the writer is free to choose words that seem best to them for the specific argument being written. Inside this section we also recommend explaining the purpose for this argument, specifically why the writer is arguing for and using certain argument concepts for this specific top level conclusion.

As to general structure, we recommend that this section have a framework similar to one of two forms. The first form employs an explicit warrant:

> We argue <top level conclusion> is justified by applying <warrant> to <main sub-conclusions>. We note <contextual-information> and <references> and we assume <assumptions>.

The second form omits the warrant:

> We argue <top level conclusion> because <main sub-conclusions>. We note <contextual-information> and <references> and we assume <assumptions>.

Even though we recommend putting contextual information and assumptions toward the end of the section, the writer has the freedom to choose their own style. Also, depending on the argument size, the writer may want to separate the top level conclusion and the other information into multiple paragraphs. A generic, single paragraph, example is shown below. This example will be expanded as we continue introducing the monograph structure.

Example One

We argue <top level conclusion> is justified by applying <warrant> to sub-conclusion A and sub-conclusion B. We note the explanation of <contextual-information> and reference an external argument in <document>.

2.1.2 Premises Section

This next section lists all premises, or sub-conclusions, in a hierarchical manner. The point of this section is to help argument readers understand which premises support each (sub-)conclusion, and get an initial sense of the argument that will follow in later sections.

While the argument will later be given in bottom-up order, the sub-conclusions are listed in this section in top-down order. Studies suggest that this difference in order will help the reader perceive an argument [10]. This is because when sub-conclusions are presented in a different order than they are explained, the reader "participates more actively in the comprehension process", which helps with memory and learning [4].

Starting with the main sub-conclusions (least indented), the argument writer works their way down and to the right until they get to the bottom level conclusion (most indented). We suggest that if this section breaks across more than one page, the break should be at a main sub-conclusion (least indented). Not every argument is symmetric and certain conclusions may not have as many supporting sub-conclusions as others. We note the entire premises section is indented underneath the top level conclusion section because all sub-conclusions, even the main sub-conclusions, fall underneath the top level conclusion. A continuation of the generic Example One is below.

Example One

- Sub-conclusion A (Ex1.5)
  - Sub-sub-conclusion A (Ex1.3)
    - Bottom Level Conclusion A (Ex1.1)
    - Bottom Level Conclusion B (Ex1.2)
  - Sub-sub-conclusion B (Ex1.4)
- Sub-conclusion B (Ex1.8)
  - Sub-sub-conclusion C (Ex1.6)
  - Sub-sub-conclusion D (Ex1.7)

2.1.3 Argument Section

This section holds the actual argument for the monograph structure. Each of the premises will be argued for in this area, although, not in the same order as presented in the previous sections. Studies have shown that when the outline is not identical to the text, "readers perform better on problem solving tasks" [9, 11]. Because assessors are engaging in problem solving activities when they declare a system safe or unsafe, it makes sense to have a structure that encourages these decision making skills.

The writer starts the argument from the bottom level and works their way up to each sub-conclusion individually. This way a reader does not have to assume the truth of any premises until after seeing the explicit support for them. Explaining the suggested process abstractly is likely to be more confusing than helpful. So we will explain it by referencing Example One, which was just shown.

To expand Example One, the writer will start by arguing both Bottom Level Conclusion *A* and *B* hold true, then arguing that Sub-sub-conclusion *A* and *B* are true. Finally, with all conclusions under Sub-conclusion *A* discussed, the writer will argue that Sub-conclusion *A* is true. Once the writer has made it to a main sub-conclusion (Sub-conclusion *A*), they will start working on the next main sub-conclusion (Sub-conclusion *B*). Starting from the lowest level again, the writer will argue for Sub-sub-conclusion *C* and *D* and then Sub-conclusion *B*. Lastly, the writer will conclude by bringing everything together and arguing for the top level conclusion using Sub-conclusion *A* and *B* as evidence (premises whose truth is accepted).

As previously mentioned in the introduction, the writer may have contextual information, references to other arguments, or assumptions that need to be stated. However, unlike in the top level conclusion section, these items may only deal with certain aspects of the argument as opposed to the whole argument. For these cases, we recommend the argument writer only state the contextual information once, preferably at the highest level conclusion to which the information applies. To illustrate, suppose there is a four-level argument (great-grandparent, grandparent, parent, grandchild). If we are discussing an assumption at level-two (parent) and it applies to every premise underneath (grandchild) but nothing above it (great-grandparent and grandparent), we include the assumption at the current level (parent) but no where else above or below that level, unless necessary to enhance overall understanding. We note the argument reader should understand contextual information and assumptions at one level (parent) apply to every level underneath it (child), unless the argument writer states otherwise.

Similar to the top level conclusion section, we recommend every argument for a sub-conclusion have one of two forms, but do not intend for these forms to be adhered to exactly, if tweaking them results in a clearer explanation of the argument. The first form applies when an explicit warrant exists:

> For the purposes of this argument, we note <contextual-information>. By applying <warrant> to the <evidence>, we

conclude <conclusion>.

The second form applies when there is no explicit warrant:

> For the purposes of this argument, we note <contextual-information>. Based on examination of <evidence>, we conclude <conclusion>.

Unlike in the top level conclusion section, we suggest listing the contextual information first in the arguments for each sub-conclusion. This is done so the argument reader knows everything up front before conclusions are made. For example, suppose there is evidence that 50 percent of the people on this planet are male and the writer concludes that at least four out of five students in a room are male. Considering the evidence, the conclusion of four out of five, or 80 percent, might be too high. However, if the writer had stated they are assuming this room of students is found in an all boys school at the beginning, the reader may be more likely to hold the conclusion true. This is just one example of why it is important that the reader know all information before making a conclusion.

A further expansion of Example One illustrates the ideas just presented.

Example One

Below is a bottom level conclusion that has an assumption that only applies to it.

Bottom Level Conclusion *A* **(EX1.1)**

Assuming <assumption> and by examining <evidence> provided, we conclude Bottom Level Conclusion *A*.

This is an argument for a bottom level conclusion that has contextual information that only applies to it.

Bottom Level Conclusion *B* **(EX1.2)**

For the purposes of this argument, we note <contextual-information>. By examining <evidence> provided, we conclude Bottom Level Conclusion *B*.

The writer worked their way up to the next indentation, but this argument does not have any extra information besides the evidence. Notice when a main argument starts to build, the evidence is provided by the conclusions of previous lower level arguments, which is why it is important to work from the bottom up.

Sub-sub-conclusion *A* **(EX1.3)**

Based on the arguments above in EX1.1 and EX1.2, we conclude Sub-sub-conclusion *A*.

The argument below has a warrant along with evidence.

Sub-sub-conclusion *B* **(EX1.4)**

By applying <warrant> and examining <evidence> provided, we conclude Sub-sub-conclusion *B*.

This is one of the main sub-conclusions and will use evidence from the lower level arguments seen above. This argument has a warrant and contextual information.

Sub-conclusion *A* **(EX1.5)**

We note <contextual-information>. By applying <warrant> to the results of the arguments EX1.3 and EX1.4, we conclude Sub-conclusion *A*.

This argument is for a low level conclusion that only has evidence.

Sub-sub-conclusion *C* **(EX1.6)**

Based on <evidence>, we conclude Sub-sub-conclusion *C*.

This argument is also for a low level conclusion that only has evidence.

Sub-sub-conclusion *D* **(EX1.7)**

From <evidence>, we conclude Sub-sub-conclusion *D*.

The argument below is for a main sub-conclusion and uses earlier arguments' results as evidence and contextual information that refers the reader to another document.

Sub-conclusion *B* **(EX1.8)**

We note <contextual-information> found in <document>. Based on the conclusions of the arguments given in EX1.6 and EX1.7, we conclude Sub-conclusion *B*.

Here is an example of breaking the page at an appropriate place.

Here the writer repeats the top level conclusion to bring the argument full circle, similar to a conclusion paragraph. Unlike when it was first mentioned, the writer now argues that the top level conclusion is true instead of just stating it. Also unlike before, we recommend not including any contextual information or assumptions, unless needed because they are used throughout the argument and should still be in the reader's mind.

Top Level Conclusion (Ex1.9)

Applying <warrant> to the conclusions of the arguments in Ex1.5 and Ex1.8, we conclude the <top level conclusion>.

2.1.4 Glossary Section

The last section of the argument presents definitions of words italicized throughout the argument, and also references to external documents made earlier in the argument. This section may look like an appendix and can be labeled as one if preferred. Depending on the argument and necessary information this may be lengthy or it may even not exist at all, because some simple arguments may not have any defined words or added information. The generic Example One does not have a glossary section; however, section 4 presents a longer example that does have the section.

3 Tabular Structure

So far, we have gone into detail about the monograph structure. In this section we present a different approach, which is also not based on graphics. The tabular structure has a few similar properties to the monograph structure, with all four sections of an argument alike except for the main argument section. The tabular based structure should look familiar to readers who have worked with geometrical proofs. One of the nice things about this structure is the body of the argument can sometimes be more compressed than the monograph structure. This makes it easier for the reader to see the whole argument or a branch of the argument at once. Although it looks involved at a first glance, the vertical and horizontal lines are only there to help organize and separate each argument and its evidence. This layout causes the reader to become more focused and active in the argument, which is beneficial for learning and making inferences [9]. The same recommended keywords previously discussed for elements like contextual information or assumptions will still apply in this approach, (such as "given that", "we note", "assuming that"). After discussing all four sections of an argument, we present a few complete arguments that use both structures and examine how to handle other argument concepts.

Just like in the previous textual structure, the tabular structure has a top level conclusion section, a premises section, an argument section, and a glossary section. The top level conclusion, premises, and glossary sections are all identical to the monograph structure, with the same ideas, properties, keywords,

and forms. Therefore, we will only focus on the body of the argument rather than the other sections.

3.1 Argument Section

The argument section for the tabular structure is the only difference between the two approaches discussed in this document. This section should be the most detailed part of the entire argument. We recommend keeping the same properties as the previous approach, i.e., sub-conclusions are argued from the bottom level up until the writer reaches a main sub-conclusion and starts again. The body of the argument for the tabular structure will look like a table, specifically a three column table, with a row for each sub-conclusion's argument. The columns and rows help organize each conclusion and its supporting argument. One column will have a reference to each sub-conclusion, another will have all conclusions listed in it, and the third will have warrants, contextual information, assumptions, and evidence in it. Although the third column can have four different elements inside it, we have labeled it as just "Argument" for simplicity and to save space. However, the monograph and tabular structures allow the writer to make their own changes, therefore the column can be renamed. Just like the top level conclusion section, this approach has the sub-conclusion the writer is arguing for stated first, followed by the support. This is a different order than the argument section for the monograph structure. The tabular structure is helpful for argument readers who already know or believe a sub-conclusion is true because they can easily skip the supporting material. We recommend every argument have one of the below two forms, depending on if a warrant exists for the argument or not.

Label	**Conclusion**	**Argument**
1.	<Conclusion>	Noting <contextual-information> and applying <warrant> to <evidence>.
2.	<Conclusion>	Noting <contextual-information> and examining <evidence>.

There are a few things to note before introducing an example. In this approach, the writer argues for the top level conclusion after arguing for all main sub-conclusions. If an argument, or the columns or rows, are getting too large for the writer's liking, the writer can choose to break up the argument at whatever level is desired. For example, the writer could argue for each main sub-conclusion separately and then put everything together at the end when arguing for the top level conclusion. If a writer decides to break up an argument, we recommend stating the end sub-conclusion for that specific break off point above the divided argument. This way the reader understands the focus of each specific part of the argument. For example, when breaking up the argument at each main sub-conclusion, the recommended approach would result in each main sub-conclusion being stated right before the argument for it, just like the

top level conclusion is stated right before the entire argument for it. An example of breaking up an argument is seen in section 6. Example One has the same exact material as the earlier approach's Example One, but is presented using the tabular structure.

Example One

Top Level Conclusion (EX1.9).

Label	Conclusion	Argument
EX1.1	Bottom Level Conclusion *A*	Based on <assumption> and examining <evidence>.
EX1.2	Bottom Level Conclusion *B*	Noting <contextual-information> and examining <evidence>.
EX1.3	Sub-sub-conclusion *A*	Follows from the arguments in EX1.1 and EX1.2.
EX1.4	Sub-sub-conclusion *B*	By applying <warrant> to <evidence>.
EX1.5	Sub-conclusion *A*	Noting <contextual-information> and applying <warrant> to EX1.3 and EX1.4.
EX1.6	Sub-sub-conclusion *C*	Based on <evidence>.
EX1.7	Sub-sub-conclusion *D*	Based on <evidence>.
EX1.8	Sub-conclusion *B*	Noting <contextual-information> found in <document> and following from the arguments seen in EX1.6 and EX1.7.
EX1.9	Top Level Conclusion	Applying <warrant> to EX1.5 and EX1.8.

4 Simple Example

4.1 Monograph Structure Example

In section 2 and 3, we presented a very generic example, in chunks. Although that may be helpful when learning about each section it can get confusing. This basic example is based off a GSN model and all main elements are taken from the *GSN Standard* [3]. The graphical version of this example is shown in Figure 1 [3]. For people familiar with GSN, looking at the graphical notation and the monograph structure version of the same argument allows for a visual comparison between the two approaches. Certain contextual information and assumptions may not be very clear; however, the point of all examples in this document is for assistance in understanding the structure, not the content. For more information about the actual argument and what an evidence scheme is, as this argument uses them, see [3, 7].

Top Level Conclusion:
For this argument, there is not a warrant but there is a top level conclusion and main sub-conclusions. Therefore the argument has the form, 'we argue <top

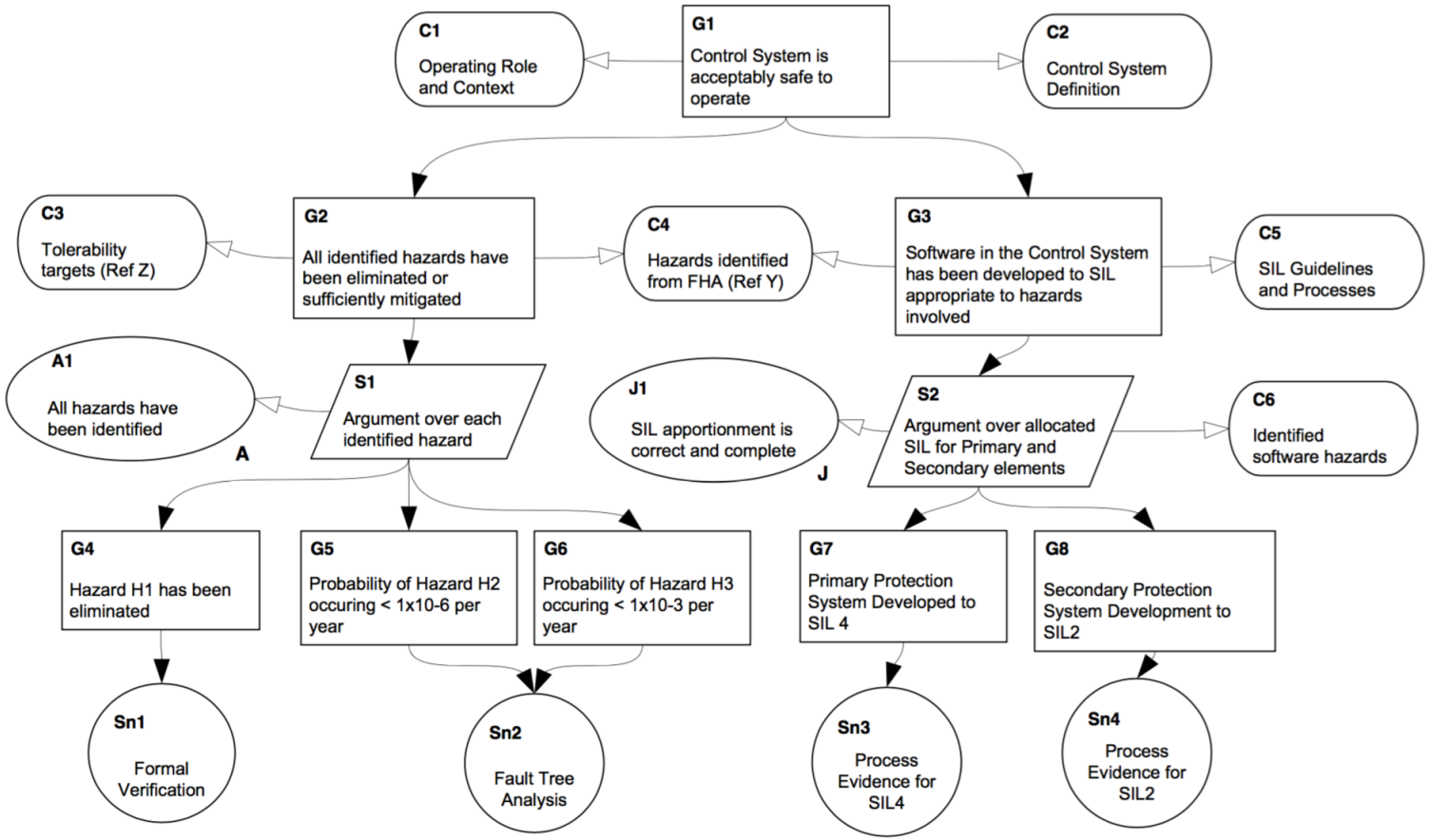


Figure 1: *A simple example of a GSN argument from the GSN Standard [3]*

level conclusion> because of <main sub-conclusions>'. Also note the italicized words that are found in the glossary section.

We argue that the *Control System* is *acceptably safe* to operate because all identified hazards have been *eliminated* or sufficiently mitigated and software in the *Control System* has been developed to SIL appropriate to hazards involved.

In a separate paragraph, we list all contextual information and assumptions that support the whole argument.

We assume that all software hazards have been identified. The SIL guidelines can be found in the <referenced document>, the hazards that were identified from FHA can be seen in <referenced document>, and the tolerability targets can be seen in Ex2.10. The operating role and context of the *Control System* is listed here.

Premises:

- *Control System* software developed to appropriate SIL (Ex2.3)
  - *Secondary Protection System* developed to SIL2 (Ex2.1)
  - *Primary Protection System* developed to SIL4 (Ex2.2)
- All identified hazards have been *eliminated* (Ex2.7)
  - Hazard H1 has been *eliminated* (Ex2.4)
  - Probability of Hazard H2 occurring (Ex2.5)
  - Probability of Hazard H3 occurring (Ex2.6)

Below is a bottom level conclusion that only has evidence.

***Secondary Protection System* development to SIL2 (Ex2.1)**

By examining evidence for SIL2, we conclude that the *Secondary Protection System* has been developed for SIL2.

This is a bottom level conclusion that only has evidence.

Primary Protection System developed to SIL4 (Ex2.2)

By examining evidence for SIL4, we conclude that the *Primary Protection System* has been developed for SIL4.

The argument below is a main sub-conclusion that has contextual information and earlier arguments as evidence.

Software in the _Control System_ developed to appropriate SIL (Ex2.3)

Given that SIL apportionment is correct and complete and by arguing over allocated SIL for Primary and Secondary elements, seen in Ex2.1 and Ex2.2, we conclude the software in the *Control System* has been developed to SIL appropriate to hazards involved.

Below is a bottom level conclusion that only has evidence.

Hazard H1 has been _eliminated_ (Ex2.4)

Using formal verification, we conclude that hazard H1 has been *eliminated*.

This is a bottom level conclusion that has contextual information referring to information found elsewhere in the document. Based on grammar rules and ease of readability we put the context at the end of the argument.

Probability of Hazard H2 occurring (Ex2.5)

We use a Fault Tree Analysis to conclude the probability of Hazard H2 occurring is less than 1 x 10^{-6} per year, which meets our tolerability targets, seen in Ex2.10.

Below is a bottom level conclusion that has contextual information referring to information found elsewhere in the document. Based on grammar rules and ease of readability we put the context at the end of the argument.

Probability of Hazard H3 occurring (Ex2.6)

We use a Fault Tree Analysis to show the probability of Hazard H3 occurring is less than 1 x 10^{-3} per year, which meets our tolerability targets, seen in Ex2.10.

The main sub-conclusion below has a warrant and three lower level sub-conclusions as evidence.

All identified hazards have been _eliminated_ (Ex2.7)

By arguing over each identified hazard seen in Ex2.4, Ex2.5, and Ex2.6, we conclude that all identified hazards have been *eliminated* or sufficiently mitigated by meeting our tolerability target, seen in Ex2.10.

Here we repeat the top level conclusion but no contextual information, references, or assumptions. There is no warrant in this argument but we do use the main sub-conclusions as evidence.

The *Control System* is *acceptably safe* to operate (EX2.8)

Based on the arguments in EX2.3 and EX2.7, we conclude the *Control System* is *acceptably safe* to operate.

Glossary:

The below section includes definitions used in the argument (note: we have not provided definitions in this example) and the information referenced for tolerability targets.

Glossary (EX2.9)

Acceptably Safe: a definition of "acceptably safe" goes here

Eliminated: definition goes here

Control System: definition goes here

Primary Protection System: definition goes here

Secondary Protection System: definition goes here

Tolerability Targets (EX2.10)

In here the reader will find information on tolerability targets

4.2 Tabular Structure Example

A complete example using the tabular structure is on the top of page 16. Because three argument sections are identical to the previous textual based example, we only show the main argument section. This example helps compare the two structures in this paper and the GSN model on which they based.

5 Additional Argument Concepts

The arguments already presented have been fairly straight forward; however, arguments can have a number of concepts that we may not have discussed yet. In section 5, we describe certain concepts that may appear in an argument and how to handle them with these non-graphical structures. Like before, people with a GSN background should be able to see a connection, although we will refrain from labeling elements with the standard GSN vocabulary.

Example Two

We argue the *Control System* is *acceptably safe* to operate (Ex2.8).

Label	Conclusion	Argument
Ex2.1	The *Secondary Protection System* has been developed for SIL2	By examining evidence for SIL2.
Ex2.2	The *Primary Protection System* has been developed for SIL4	By examining evidence for SIL4.
Ex2.3	The software in the *Control System* has been developed to SIL appropriate to hazards involved	Given that SIL apportionment is correct and complete and by arguing over allocated SIL for Primary and Secondary elements (seen in Ex2.1 and Ex2.2).
Ex2.4	Hazard H1 has been *eliminated*	Using formal verification.
Ex2.5	The probability of Hazard H2 occurring is less than 1 x 10^{-6} per year	Based on tolerability targets (seen in Ex2.10) and by conducting a Fault Tree Analysis.
Ex2.6	The probability of Hazard H3 occurring is less than 1 x 10^{-3} per year	Based on tolerability targets (seen in Ex2.10) and by conducting a Fault Tree Analysis.
Ex2.7	All identified hazards have been *eliminated* or sufficiently mitigated	By meeting our tolerability target (found in Ex2.10), assuming that all hazards have been identified, and by arguing over each hazard seen in Ex2.4, Ex2.5, and Ex2.6.
Ex2.8	The *Control System* is *acceptably safe* to operate	Based on the arguments in Ex2.3 and Ex2.7.

5.1 Referencing

Depending on the size of the safety case or the system itself, two arguments may relate to each other in a multitude of ways including but not limited to, repeated evidence, supporting arguments, or repeated sub-conclusions. Suppose that an element within an argument A refers to another argument B that supports the original argument A, the argument writer should note or reference where to find the other argument B. If an element within an argument refers to a sub-conclusion, premise, contextual information, or even a piece of evidence from another argument, the writer should reference the information and where

to find it. We recommend doing this so that all information is clear and known to the reader. Occasionally, there are two arguments that may not seem similar but do have an association with each other explicitly stated somewhere [3]. Whether it be in another document or later in the same document, a quick way for the reader to find the explicitly stated association would be to reference the section or document. Essentially, if there is any relationship between an element from one argument and an element of another argument, the writer should always reference the elements. When the argument writer references anything, they should handle it similarly to how we introduce contextual information. This means, the element referenced will be stated in the argument at the highest conclusion to which it applies. In the tabular structure, references will be found in the Arguments column. Examples of referencing one argument inside another is found in section 6.

5.2 Incomplete Arguments

Much like writing a paper, creating a compelling argument may take multiple tries as the writer learns from previous versions of the document. In the beginning, the argument may not be as detailed or complete as the final product. That being said, there may be a time when the argument writer has a conclusion that may not be as elaborated or expanded on as they would like. While arguing for that conclusion, they should be sure to note that the argument still needs to grow using their own words. Doing this makes the writer and reader understand that although the argument for the conclusion is not complete, it will be fixed later. For example, the writer could state, 'we claim <conclusion> to be true' or even, 'we show <conclusion> to be true based on evidence provided at a later time/date'. This allows writers to have a quick solution and placeholder when needed as well as note what to work on later down the road. For the Tabular Structure, the writer notes the incomplete argument inside the Argument column. A basic generic example is seen below.

Label	**Conclusion**	**Argument**
1.	<Conclusion>	Based on evidence provided at a later date.

5.3 Confidence Arguments

Another situation to keep in mind when writing an argument, especially with real world systems, is that writers may want to explain how confident they are in the argument, or more specifically, they may want to write a separate confidence argument. When discussing a certain section or branch of the argument the writer wants to argue confidence for, it makes sense to reference the confidence argument in that specific area. Much like the contextual and reference information mentioned throughout this document, we recommend these confidence arguments are referenced once, at the highest level to which they apply. Meaning, if the confidence argument gives confidence to the top level conclusion, the reference will be in the first section of the argument along with

assumptions and contextual information. If the confidence argument gives confidence to a particular sub-conclusion, the reference will be noted when arguing for that specific sub-conclusion. For the Tabular Structure, the confidence argument reference should be in the Argument column at the highest sub-conclusion to which it applies. Besides referencing arguments, both structures allow the writer to use multiple options when arguing for sub-conclusions.

5.4 Choices

There are many different ways to express an argument that connects conclusions together. Sometimes argument writers may want to discuss or point out the various ways to complete an argument. A conclusion may state that only 1−of−n or m−of−n cases needs to be shown true for the conclusion to be true [3]. As the writer works from the bottom up, no matter the path the reader decides to take, all sub-conclusions will already be argued for, regardless of the n multiple cases. When the writer comes across the multiple options, they should argue all n cases and write an OR in between each of them. Each of these arguments should have a unique technique or approach to them or else this method would not be used. Below is a generic example of the choices concept using the monograph structure [1].

Example I

Only two of these three arguments needs to be shown true for the conclusion to hold true.

Argument One:
We note <contextual-information>. Applying <warrant> to <evidence>, we conclude <conclusion>.

OR Argument Two:
We assume <assumption>. Based on <evidence>, we conclude <conclusion>.

OR Argument Three:
Examining <evidence> and arguments seen earlier, we conclude <conclusion>.

For the tabular structure, we recommend breaking each case into its own separate argument because it allows the reader to easily identify where the cases are as well as follow everything clearly. A generic example is seen below and a complete example of an argument using choices is seen in section 6.

Example II

Only two of these three arguments needs to be shown true for the conclusion to hold true.

Argument One:

Label	Conclusion	Argument
1.	<Conclusion>	Noting <contextual-information>, and applying <warrant> to <evidence>.

Argument Two:

Label	Conclusion	Argument
2.	<Conclusion>	Based on <assumption> and <evidence> provided.

Argument Three:

Label	Conclusion	Argument
3.	<Conclusion>	By examining <evidence> provided and <referenced-arguments>.

5.5 Multiplicity

5.5.1 Monograph Structure

At certain times, when talking about evidence or sub-conclusions, an argument may have a similar pattern or element repeat itself. Here we discuss multiplicity or, the number of "instances of one element-type relat[ing] to another" [3]. We note the GSN version of multiplicity is slightly different from this approach because identical elements with a pattern can be considered as multiplicity using these structures. Sometimes the order in which these similar elements are presented and related to each other matters. For example, when one sub-conclusion is chained to another. However, other times the order does not matter but the consistent relationship is still present. Either way, the argument writer can handle both methods in a similar way and treat the elements in a hierarchical manner, whether they are evidence or sub-conclusions.

If the elements are sub-conclusions and the order does not matter, we recommend the elements all be listed on the same level (same indentation) in the premises section and each sub-conclusion argued for separately. Supposing that the elements are evidence and not conclusions, then we suggest all evidence be presented and discussed in any order the writer would like within the sub-conclusion that the evidence applies to. Note the similar forms between the three sub-conclusions in example *A*, which shows a generic string of sub-conclusions that relate to each other but do not depend on each other, allowing the order not to matter [1].

For the case in which the order does matter or, one element depends on another, we recommend handling the elements much like above. If the elements are sub-conclusions, then each element should be listed in the premises section in a ranked order (grandparent, parent, grandchild) and should be argued

for individually, making sure to start from the bottom and relate each sub-conclusion as the writer works their way up. Supposing that the order matters and the writer is dealing with evidence and not sub-conclusions, then all the evidence should be inside the sub-conclusion to which it applies. The writer argues working from the bottom up, making sure to relate each evidence to the previous one stated. Example *B*, shows a generic string of sub-conclusions that depend on each other, which is why the order in which they are presented matters [6]. Like before, we note the similar form each sub-conclusion has.

In academic and research uses of assurance arguments, examples may be based on real arguments and systems but may not always be complete. Occasionally, a researcher may want to represent multiplicity but may not know the specific number of elements, have the time, or have the space to include every element. When this occurs, the argument writer should include only one sub-conclusion that involves *X*, or the number of times the pattern occurs. An example of this is seen in section 6. The reader should understand if one element depends on another, either by the set up of the argument or the writer explicitly stating it.

Example *A*

These arguments have a similar form and have to do with user defined factor claims.

High confidence in user defined factor claim *A* (EXA.1)

We note <contextual-information>. By examining <evidence>, we conclude there is high confidence in user defined factor claim *A*.

High confidence in user defined factor claim *B* (EXA.2)

We note <contextual-information>. By examining <evidence>, we conclude there is high confidence in user defined factor claim *B*.

High confidence in user defined factor claim *C* (EXA.3)

We note <contextual-information>. By examining <evidence>, we conclude there is high confidence in user defined factor claim *C*.

Example *B*

These arguments are based on a chain. The writer references previous arguments to provide support for the next argument.

The low-low level requirements satisfy the low level requirements (EXB.1)

By examining <evidence>, we conclude the low-low level requirements satisfy the low level requirements.

The low level requirements satisfy the high level requirements (ExB.2)

By examining <evidence> and the argument seen in ExB.1, we conclude the low level requirements satisfy the high level requirements.

The high level requirements satisfy <sub-conclusion> (ExB.3)

By examining <evidence> and the argument seen in ExB.2, we conclude the high level requirements satisfy <sub-conclusion>.

5.5.2 Tabular Structure

Multiplicity using the tabular structure has the same properties as above. Example *C* shows a generic string of sub-conclusions that relate to each other but do depend on each other, allowing for the order to not matter. Example *D* is a generic example where the order matters because the elements relate and depend on each other.

Example *C*

There is high confidence in all defined factor claims.

Label	Conclusion	Argument
ExC.1	There is high confidence in user defined factor claim *A*	We note <contextual-information> and examine <evidence>.
ExC.2	There is high confidence in user defined factor claim *B*	We note <contextual-information> and examine <evidence>.
ExC.3	There is high confidence in user defined factor claim *C*	We note <contextual-information> and examine <evidence>.

Example *D*

The bottom level requirements satisfy the highest level requirements.

Label	Conclusion	Argument
ExD.1	The low-low level requirements satisfy the low level requirements	By examining <evidence>.
ExD.2	The low level requirements satisfy the high level requirements	By examining <evidence> and the argument seen in ExD.1.
ExD.3	The high level requirements satisfy the sub-conclusion	By examining <evidence> and the argument seen in ExD.2.

6 Complex Example

6.1 Monograph Example

The argument below is a complete example that uses multiple concepts introduced in section 5. These concepts include multiplicity, options, referenced arguments, and incomplete arguments. For the options concept, we introduce a main sub-conclusion that has three possibilities that will complete the argument; however, only one needs to be shown true for the main sub-conclusion to be true. The multiplicity concept represents a pattern in the argument that we invoke X number of times. This complete argument is based off a GSN diagram originally developed for educational purposes [2] and expanded for this paper. The GSN diagram is shown in Figure 2 . This argument revolves around a son, Jon, creating a safety case convincing his father to allow Tim, Jon's friend, to drive Jon to a football game.

Top Level Conclusion:

We argue Tim is a *safe enough* driver to take Jon to a football game by showing five independent sources of support for Tim's ability to drive safely. These sources are (i) Tim has satisfied all legal requirements for driving; (ii) Tim has not been in an accident; (iii) nothing untoward is going on in Tim's life that might cause him to drive less well than usual; (iv) Tim has a good reputation for driving; and (v) Tim's car does not pose any *special danger*. We assume that Tim will be the driver and Jon the only passenger.

Premises:

- Tim has a good reputation for driving (Ex3.2)
  - Safe Driver X believes Tim is a safe driver (Ex3.1)
- Tim's car does not pose any *special danger* (Ex3.3)
- Tim has not been in an accident (Ex3.4)
- Tim has satisfied all legal requirements for driving (Ex3.5)
- Nothing untoward is going on in Tim's life (Ex3.10)
  - Tim is not currently in any fights (Ex3.8)
  - Tim's academic life will not affect his driving (Ex3.7)
    - Tim consistently gets *good grades* (Ex3.6)
  - Tim has no big life decision that may distract him (Ex3.9)

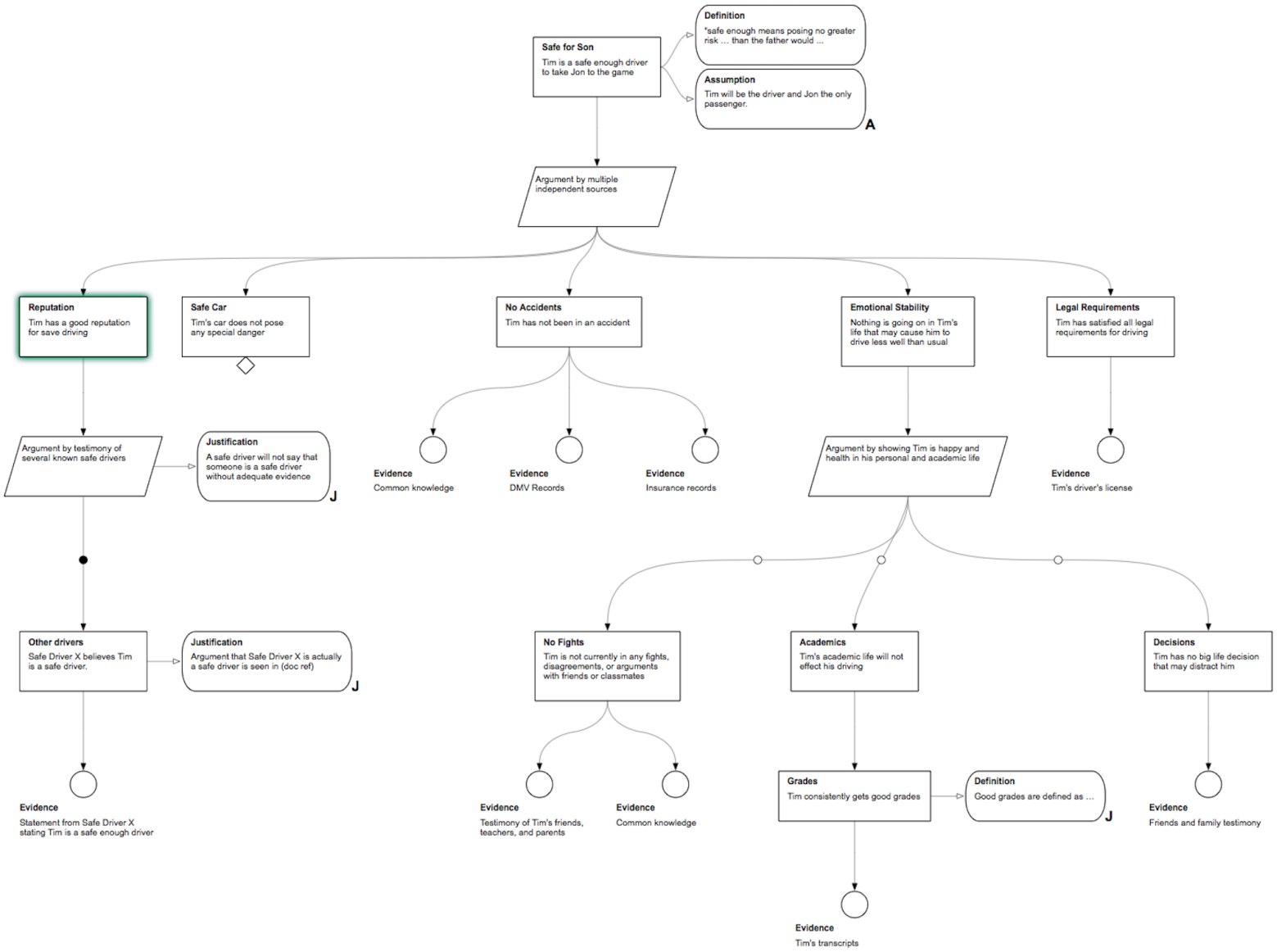


Figure 2: *GSN argument for Tim driving Jon to a football game [2]*

The argument illustrates multiplicity where X represents the certain number of safe drivers. We would repeat the pattern X times, if X is known. This is an example where the order does not matter, or where each safe driver's argument does not depend on another safe driver's argument.

Safe Driver *X* believes Tim is a safe driver (Ex3.1)

We note that the argument for Safe Driver *X* actually being a safe driver is found in <referenced document>. Through the statement provided by Safe Driver *X* regarding Tim's driving, we conclude Safe Driver *X* believes Tim is a safe driver.

The argument below uses the previous argument as evidence. The assumption stated in this argument applies to a lower level sub-conclusion but no sub-conclusions at a higher level so the assumption is stated here.

Tim has a good reputation for safe driving (Ex3.2)

We assume a safe driver will not say that someone is a safe driver without adequate evidence. By the testimony of several known safe drivers seen in Ex3.1, we conclude Tim has a good reputation for safe driving.

The below argument informs the reader and writer that it is not complete and will be elaborated on at a later date.

Tim's car does not pose any *special danger* (Ex3.3)

Based on evidence to be provided at a later date, we conclude Tim's car does not pose any *special danger*.

Tim has not been in an accident (Ex3.4)

Based on common knowledge, DMV records, and insurance records, we conclude Tim has not been in an accident.

Tim has satisfied all legal requirements for driving (Ex3.5)

Given that Tim has a driver's license, we conclude Tim has satisfied all legal requirements for driving.

Tim consistently gets *good grades* (Ex3.6)

Based on Tim's transcript, we conclude Tim consistently gets *good grades*.

The argument below uses information based on a previous argument as evidence.

Tim's academic life will not affect his driving (Ex3.7)

By the argument seen in section Ex3.6, we conclude Tim's academic life will not affect his driving.

Tim is not currently in any fights (Ex3.8)

Based on common knowledge and testimony of friends and family, we conclude Tim is not currently in any fights, disagreements, or arguments with friends or classmates.

Tim has no big life decision that may distract him (Ex3.9)

Based on testimony from friends and family, we conclude Tim has no big life decisions that may distract him.

The argument below illustrates options: the writer asserts that two of the three sub-conclusions must be shown true for the argument to hold. An assessor of this argument may question whether all three ought to be required.

Nothing untoward is going on in Tim's life (Ex3.10)

Only two of these three arguments need to be shown true for the sub-conclusion, nothing is going on in Tim's life, to be true.

Argument One:
By showing Tim is happy and healthy in his personal life based on the argument in Ex3.7, we conclude nothing is going on in Tim's life that may cause him to drive less well than usual.
OR Argument Two:
By showing Tim is happy and healthy in his personal life based on the argument in Ex3.8, we conclude nothing is going on in Tim's life that may cause him to drive less well than usual.
OR Argument Three:
By showing Tim is happy and healthy in his personal life based on the argument in Ex3.9, we conclude nothing is going on in Tim's life that may cause him to drive less well than usual.

Tim is a *safe enough* driver (Ex3.11)

Using multiple independent sources of support justified by arguments Ex3.2, Ex3.3, Ex3.4, Ex3.5, and Ex3.10, we conclude Tim is a *safe enough* driver.

Here the writer includes short definitions.

Glossary (Ex3.12)

Safe enough: at least as safe as Jon's dad

Special danger: a problem safe driving cannot overcome

Good grades: at least a B average

6.2 Tabular Example

Below is the same complex argument using the tabular structure. Because of the complexity, we will repeat the entire argument. We note that the options sub-conclusion is broken up to better differentiate between the choices.

Top Level Conclusion:

We argue Tim is a *safe enough* driver to take Jon to a football game by showing five independent sources. of support for Tim's ability to drive safely. These sources are (i) Tim has satisfied all legal requirements for driving, (ii) Tim has not been in an accident, (iii) nothing is going on in Tim's life that might cause him to drive less well than usual, (iv) Tim has a good reputation for driving, and (v) Tim's car does not pose any *special danger*. We assume that Tim will be the driver and Jon the only passenger.

Premises:

- Tim has a good reputation for driving (Ex3.2)
  - Safe Driver X believes Tim is a safe driver (Ex3.1)
- Tim's car does not pose any *special danger* (Ex3.3)
- Tim has not been in an accident (Ex3.4)
- Tim has satisfied all legal requirements for driving (Ex3.5)
- Nothing untoward is going on in Tim's life (Ex3.10)
  - Tim is not currently in any fights (Ex3.8)
  - Tim's academic life will not affect his driving (Ex3.7)
    - Tim consistently gets *good grades* (Ex3.6)
  - Tim has no big life decision that may distract him (Ex3.9)

(intentional page break)

Tim is a *safe enough* driver to take Jon to a football game (Ex3.11).

Label	Conclusion	Argument
Ex3.1	Safe Driver X believes Tim is a safe driver	The argument that Safe Driver X is actually a safe driver is found in <referenced document> and through the statement provided by each Safe Driver X regarding Tim's driving.
Ex3.2	Tim has a good reputation for safe driving	By assuming a safe driver will not say that someone is a safe driver without adequate evidence and by testimonies of several known safe drives seen in Ex3.1.
Ex3.3	Tim's car does not pose any *special danger*	By evidence provided by a later date.
Ex3.4	Tim has not been in an accident	Based on common knowledge, DMV records, and insurance records.
Ex3.5	Tim has satisfied all legal requirements for driving	Based on Tim's drivers license.

Nothing untoward is going on in Tim's life that may cause him to drive less well than usual (Ex3.10).

Only two of these three arguments need to be shown true for the conclusion to hold true.

Argument One

Label	Conclusion	Argument
Ex3.6	Tim consistently gets *good grades*	Based on Tim's transcript.
Ex3.7	Tim's academic life will not affect his driving	Seen through argument Ex3.6.
Ex3.10	Nothing is going on in Tim's life that may cause him to drive less well than usual	By showing Tim is happy and healthy in his personal life and by argument Ex3.7.

OR Argument Two

Label	Conclusion	Argument
Ex3.8	Tim is currently not in any fights, disagreements, or arguments with friends or classmates	Based on common knowledge and testimony from friends and family.
Ex3.10	Nothing is going on in Tim's life that may cause him to drive less well than usual	By showing Tim is happy and healthy in his personal life and by argument Ex3.8.

OR Argument Three

Label	Conclusion	Argument
Ex3.9	Tim has no big life decisions that may distract him	Based on testimony from friends and family.
Ex3.10	Nothing is going on in Tim's life that may cause him to drive less well than usual	By showing Tim is happy and healthy in his personal life and by argument Ex3.9.

Tim is a *safe enough* driver to take Jon to a football game (Ex3.11).

Label	Conclusion	Argument
Ex3.11	Tim is a *safe enough* driver to take Jon to a football game	Using multiple independent sources seen in arguments Ex3.2, Ex3.3, Ex3.4, Ex3.5, and Ex3.10.

7 Conclusion and Future Work

We presented and described two techniques to write an assurance argument that avoids using graphical notations. Overall we explained the importance of four sections in both techniques: top level conclusion, premises, main argument, and glossary. Also, we gave realistic examples using these approaches. The intent of these two methods is to allow for more freedom, more detail, and better readability of assurance arguments for people who are not graphically-inclined. Although we illustrated several different ways to use both proposed techniques, the approaches can always be tweaked for the sake of the argument, the reader, or the writer.

One potential advantage about these two proposed approaches is their similar characteristics. If an argument is written in the monograph structure but a certain branch or area of the argument is suited better for the tabular structure, as it may need less explanation, the writer can easily make the change. The only difference between the two structures is the argument section so the writer can interweave the two structures if they would like. We suggest the writer should

state this structure change will happen in the top level conclusion so the reader is prepared.

Although we discussed two non-graphical ways to present assurance arguments, we do not know if one approach is easier to understand, to write, or to assess. Nor do we know whether an approach tends to encourage any type of biases in argument assessment. For future work, we suggest creating a study to look at the relative effectiveness and unbiasedness of our suggested structures. Such a study would provide real data upon which to evaluate the relative efficacy of the approaches. Such a study should also provide insight into specific benefits and drawbacks of each approach. Below is a sketch of one way to design an initial comprehensive, but possibly feasible study.

In this proposed study, the following attributes are relevant:

- Quality of the system for which arguments are developed, which may be either strong (the system is known to be sufficiently safe for its intended purpose), or weak (the system is known to be unsafe).
- Quality of the argument, which may be either compelling (it justifies its top level conclusion), or unconvincing (it fails to justify its conclusion).
- Notation of the argument: graphical, monograph, or tabular.
- Skill level of the assessor: beginner, mid-level, or experienced.

Note the combination of the two quality attributes, which we'll denote simply as quality, has four possibilities: strong system + compelling argument, strong + unconvincing, weak + compelling, and weak + unconvincing. The first and last of these four are desirable; the second and third are not.

Each assessor participating in the study will be given an argument written in one of the three notations. The assessor will be asked to evaluate the quality of the argument, and answer questions. The assessor will then be given an argument written in another notation, and asked to evaluate the argument, and answer questions. Finally, the assessor will be asked to answer questions comparing the two notations to each other.

To help mitigate against the threat to validity of an assessor's second evaluation being effected by their first evaluation, the underlying systems for which the two evaluation attempts should be different. To help provide some evidence about whether a particular notation encourages a bias in evaluation, the quality should be the same for both attempts by a single assessor.

Conducting a study satisfying the requirements established so far requires a minimum of four underlying systems: two strong (S_1, S_2) and two weak (W_1, W_2). For each of these four systems, a compelling argument (C) and an unconvincing argument (U) must be written. Finally, each of the resulting eight arguments must be presented in all three notations (G, M, T). Thus, the total number of distinct arguments will be 24: S_1CG, S_1UG, S_2CG, S_2UG, W_1CG, W_1UG, W_2CG, W_2UG, S_1CM,S_1UM, S_2CM, S_2UM, W_1CM, W_1UM, W_2CM, W_2UM, S_1CT, S_1UT, S_2CT, S_2UT, W_1CT, W_1UT, W_2CT, and W_2UT. Given the requirement that the quality presented to a single assessor for both

evaluation attempts such remain the same, then once the assessor is given a particular notation and quality combination, only two options exist for what they will be given for their second attempt (for example, S_1CG may be followed by only S_2CM or S_2CT), yielding 48 possibilities. If we chose to include three different levels of assessor experience (beginner, mid-level, and experienced), then the study will have a total of 144 possible variations.

Suppose conducting an experiment involving 144 variations is infeasible. The study options could be cut in half by considering only compelling arguments. A compelling argument for a strong system is desirable; a compelling argument for a weak system is the worst possible combination. Studying whether there is a difference among the three notations in how well they allow assessors to accept the former and (even more importantly) reject the latter is important.

Another variation on the study would including timing how long assessors take, and seeing whether there appears to be a difference among notations. Such a variation seems unlikely to be useful, however, because any differences that might be attributable to notations are likely to be minimal compared to differences that are attributable to differences in reading and thinking speeds among individuals.

Our suggested study approach is only one of many that could be designed. We hope readers of this document will think of others themselves. We also hope that conducting empirical assessments of proposed new approaches to argumentation presentation will one day become a normal part of excepted practice.

References

1. Graydon, P. J.; and Holloway, C. M.: An Investigation of Proposed Techniques for Quantifying Confidence in Assurance Arguments. Technical Memorandum NASA/TM-2016-219195, National Aeronautics and Space Administration, Hampton, VA, USA, May 2016.

2. Holloway, C. M.: Understanding Assurance Cases: Module 2 —Application, September 2015. Developed for the FAA under Annex 2 of IAI-1073.

3. *GSN Community Standard Version 1*. 2011.

4. Kintsch, W.: Text Comprehension, Memory, and Learning. *American Psychologist*, vol. 49, no. 4, April 1994, pp. 249–303.

5. McNamara, D. S.; Kintsch, E.; Songer, N. B.; and Kintsch, W.: Are Good Texts Always Better? Interactions of Text Coherence, Background Knowledge, and Levels of Understanding in Learning From Text. *Cognition and Instruction*, vol. 14, no. 1, 1996, pp. 1–43.

6. Holloway, C. M.: Explicate '78: Uncovering the Implicit Assurance Case in DO-178C. *Engineering Systems for Safety. Proceedings of the 23rd*

Safety-critical Systems Symposium, M. Parsons and T. Anderson, eds., Safety Critical Systems Club, Bristol, UK, February 2-5 2015, pp. 205–225.

7. Graydon, P. J.; and Holloway, C. M.: "Evidence" Under a Magnifying Glass: Thoughts on Safety Argument Epistemology. *Proceedings of the IET System Safety and Cyber Security Conference*, Bristol, UK, October 2015.

8. Reed, C.: Representing and Applying Knowledge for Argumentation in a Social Context. *AI & Society: Knowledge, Culture, and Communitcation*, vol. 11, 1997, pp. 138–154.

9. Wiley, J.; and Voss, J. F.: Constructing Arguments From Multiple Sources: Tasks That Promote Understanding and Not Just Memory for Text. *Journal of Educational Psychology*, vol. 91, no. 2, 1999, pp. 301–311.

10. Reed, C.; and Long, D.: Content Ordering in the Generation of Persuasive Discourse. *Fifteenth International Joint Conference on Artificial Intelligence*, M. E. Pollack, ed., Japanese Society for Artificial Intelligence, Morgan Kaufmann Publishers, 340 Pine Street, 6th Floor San Francisco, CA 94194, vol. 1, 1997, pp. 1022–1027.

11. Mannes, S. M.; and Kintsch, W.: Knowledge Organization and Text Organization. *Cognition and Instruction*, vol. 4, no. 2, 1987, pp. 91–115.

12. RTCA: DO-178C: Software Considerations in Airborne Systems and Equipment Certification. RTCA, Inc., Washington DC, USA (Also published as EUROCAE ED-12C), 2011.

13. RTCA: DO-248C: Supporting Information for DO-178C and DO-278A. RTCA, Inc., Washington DC, USA (Also published as EUROCAE ED-94C), 2011.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01-07-2017	Technical Memorandum	January 2017–May 2017

4. TITLE AND SUBTITLE
Assurance Arguments for the Non-graphically-inclined: Two Approaches

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Emily Heavner and C. Michael Holloway

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
999182.02.85.07.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, Virginia 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER
L–20822

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)
NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
NASA/TM–2017–219650

12. DISTRIBUTION/AVAILABILITY STATEMENT
Unclassified-Unlimited
Subject Category 03
Availability: NASA CASI (443) 757-5802

13. SUPPLEMENTARY NOTES
An electronic version can be found at http://ntrs.nasa.gov.

14. ABSTRACT

We introduce and discuss two approaches to presenting assurance arguments. One approach is based on a monograph structure, while the other is based on a tabular structure. In today's research and academic setting, assurance cases often use a graphical notation; however for people who are not graphically inclined, these notations can be difficult to read. This document proposes, outlines, explains, and presents examples of two non-graphical assurance argument notations that may be appropriate for non-graphically-inclined readers and also provide argument writers with freedom to add details and manipulate an argument in multiple ways.

15. SUBJECT TERMS
assurance case, assurance argument, argument structure, notations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	36	19b. TELEPHONE NUMBER *(Include area code)* (443) 757-5802