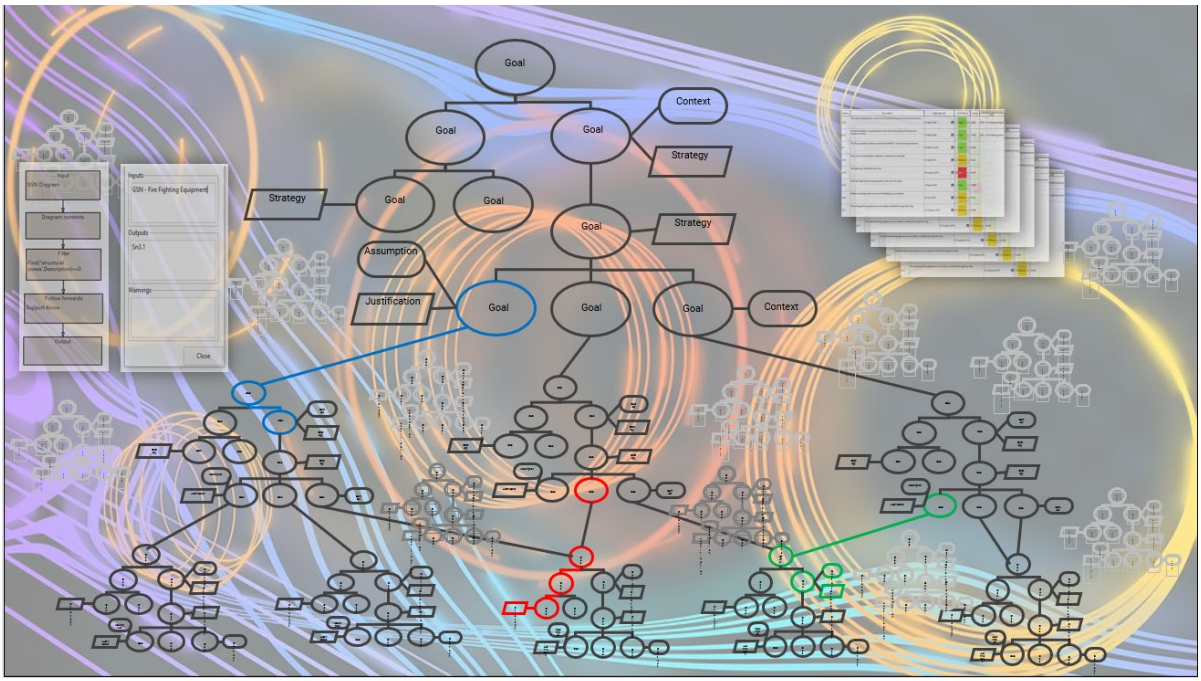
COMPLEX SAFETY CASES – ENHANCING THE GOAL STRUCTURED NOTATION

By Andrew King – Diamatric Software (https://diametricsoftware.com)



This article discusses how the Goal Structured Notation (GSN), when encapsulated into a safety modelling tool, can enhance the ability of the GSN to manage large and complex safety cases. It will show how a software architecture can be built around GSN and how, using reference and data fields, that architecture can be used to manage modular safety cases. It will address how the GSN structure can be replicated in the safety modelling tool and how the model can then analyze the safety case to answer specific business and technical questions using queries and matrices. The article then goes on to look at how the software can enhance the GSN visually to make large and complex safety cases easier to manage.

GOAL STRUCTURED NOTATION

A safety argument is a representation of a number of safety claims and it comprises of goals, assumptions, justifications, strategies and solutions (evidence). The GSN captures these elements in a graphical notation and provides a clear representation of complex arguments with their supporting evidence. The GSN makes explicit the reasoning behind a safety case and thus makes it easier for stakeholders to understand. For complex arguments, the GSN breaks down the argument into manageable sections and shows how the safety argument has been constructed to meet the top-level claim. A large GSN can, however; consist of thousands of elements with complex interdependencies making tracking progress and managing changes a demanding and time-consuming task. When a challenge to a complex safety case is made, the owners must first identify all the areas which are affected by the challenge, assess if the challenge is valid and then make changes to rectify the problem and restore the validity of a safety case. These new changes must be readily apparent to the regulator if the safety case is to be reviewed and approved. When working with the Senior Engineering Officer at RAF HQ 22 Group some years ago, it quickly became apparent that the scope and depth of the Organisation's safety case was so extensive that it was very difficult to assess the GSN for progress visually – platforms, equipment and operating bases stretched the GSN structure into the distance – and the duty holder found it almost impossible to keep track of

developments and identify areas of weakness using the GSN. This has been an experience that I have seen duplicated in many organisations and has been one of the main tenets behind the development of a new safety modelling tool.

By building a safety modelling tool where elements of the GSN, including support and context arrows, are created as entities within that model and by adding reference and data fields to those entities, it becomes possible to rapidly search, analyze and report on large and complex safety cases.

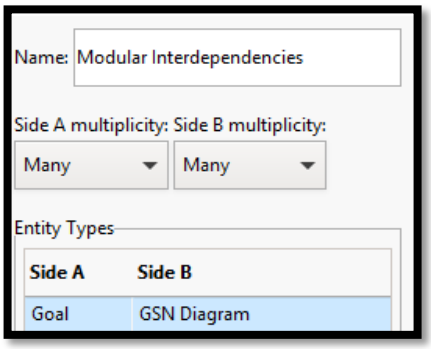
GSN MODEL ARCHITECTURE

Large and complex safety cases are easier to manage when they are broken down into sub-system safety cases or modules. This helps in the identification and isolation of areas where the change applies and also allows the development of the safety case by different teams. To break down a safety case into sections, it is necessary to build a safety case architecture. This now common term is defined as:

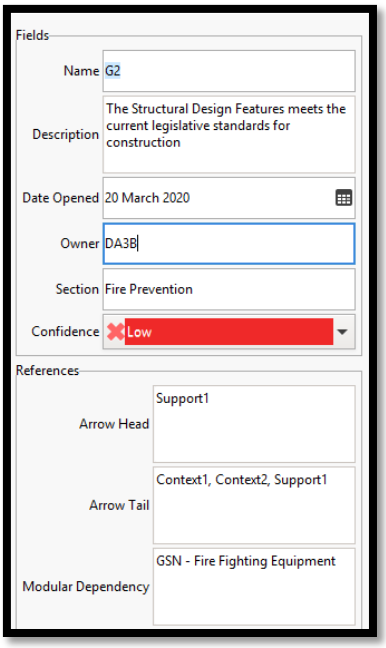
> *"the high-level organization of the safety case into components of argument and evidence, the externally visible properties of these components, and the interdependencies that exit between them*". (Kelly 03].

For example, a safety case covering the operation of a maritime oil tanker will be divided into separate safety cases for separate systems, such as the navigation equipment, ship construction, firefighting, cargo handling etc, with a high level safety case that covers the general operation of the vessel. The individual safety case modules will have their own clear boundaries but will also have interdependencies, such as ship construction and the ability to fight fires (thermal insulation between accommodation and cargo). In the architecture definition, equal weight is placed on the dependencies between safety case modules as on the safety components themselves. So dependencies must also be recorded as part of any interface definition including arguments requiring support from other modules and reliance on objectives, evidence, context presented elsewhere.

The need to identify objectives, evidence and context for each module or component and the interdependencies between them is crucial to a successful modular safety case. Kelly outlines extensions to the GSN to support the concept of modular safety case construction. In a safety modelling tool, this can be achieved through the use of a reference field sitting behind the 'Goal' entity. If a goal is supported by a GSN diagram elsewhere in the safety case, this interdependency can be imbedded in the reference field for that goal and subsequently can be shown to exist through analysis of the safety case (see analysing the GSN structure). In a safety modelling tool, if a goal is used to support an argument in several GSN structures, it is simply dragged onto the GSN diagram with the knowledge that if a change is made to that goal in one section, it will automatically be reflected whereever else that goal is used.



Data fields can be added to a GSN element to provide information to the user (see the diagram to the right). Project management information such as owner, status, confidence, date created, date amended can also be added to provide further depth of understanding through analysis.



In a safety Modelling tool, sections of the safety case can be exported as multiple files and assigned to different teams and imported back into the Model once the work has been completed. A specific area of a single file model can also be assigned to a team with permissions giving access only to the assigned area. However modules are handled, the underlying principle must be that every fact and every relationship is stored exactly once. If a goal is used many times in a structure, updating it will automatically update the goal everywhere it is used in the model. In comparison to a paper-based modular safety case argument, a safety modelling tool will considerably reduce the time needed for review, identification of areas for change and amendment.

ANALYZING THE GSN STRUCTURE

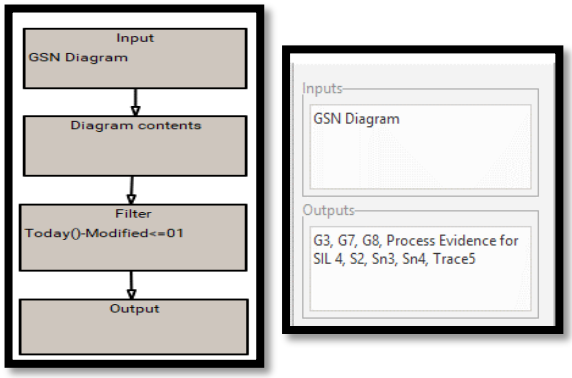
To effectively analyse a GSN Structure it is necessary to identify not only the goals, strategies, assumptions, justifications and solutions but also the links (support and context arrows) down through sub-goals to solutions and the evidence. Thus GSN elements and GSN arrows need to be created as entities in the software model. Each entity can then have its own set of properties, either inherent or added by the user and which contain key data for analysis. References will hold the links to other entities and will appear in the entity and the entity being referenced; an important factor when tracing up the GSN from evidence or down from goals.

In order to analyze a GSN structure effectively, you need to be able to examine each element in the GSN and follow the links up from a piece of evidence or down from a high-level goal. A query can achieve this and other analytical functions by identifying a start point (input) and through a number of steps arrive at an analytical result (Output). The following functions are required to analyse a GSN safety argument:

- Identifying GSN structures that contain certain GSN entities – Where is the evidence?
- Identifying certain entities shown in a GSN structure- What are the strategies?
- Finding all the children of a GSN entity -Where are the GSN structures?
- Finding all the parents of a GSN entity – In what section is this GSN structure?
- Following arrows down from an entity - What are the sub-goals and solutions
- Following arrows up from a GSN entity – What are the high-level goals for this evidence?
- Filtering by GSN entity – Only show the contexts for this diagram.
- Filtering GSN entities by selected criteria – date, time, key word etc.
- Select the type of GSN entity – Only look at these entities.

With this capability the query can really start to address the business questions many owners of large safety cases will want answered:

- What areas of the safety case are affected by this challenge?
- What changes have been made over a certain period?
- Who is responsible for those changes?
- What other areas are affected by this change?
- What needs to be completed in the safety case?

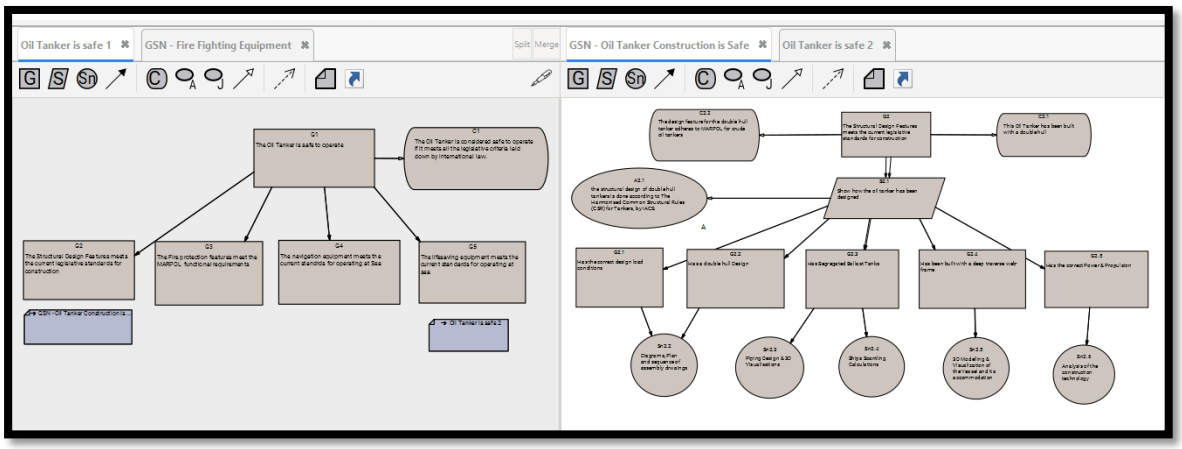


An example is given here. A safety case manager wants to know what has changed in the last 24 hrs. Using queries he can select the GSN diagram or diagrams he is interested in, highlight the contents and then set the period – in this case 1 day. The query output will then show the elements that have been changed during the last 24 hrs. The query could be targeted at key words if assessing a challenge to the safety case or at a status level or section owner. Queries are a very powerful tool for conducting GSN analysis of a safety case and they can be exported easily for use in other safety cases.

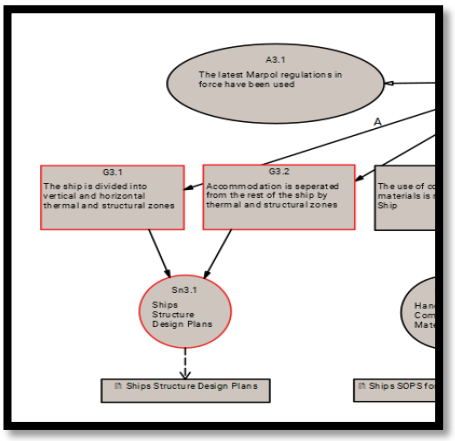
Presenting the information from analysis is equally imported for assessment and understanding. Matrices provide a tabular output for the analysis that can show references and data fields as columns in a table. A matrix uses the analysis queries to build the table can provide simple (single query) output or an in-depth (multiple queries)analysis.

ENHANCING THE GSN STRUCTURE VISUALLY

GSN is not just about making the reasoning behind safety cases explicit, it is also about a visual representation of the individual elements of the safety case. Assessing large and complex safety cases is challenging, even using GSN but this can be made simpler when the GSN structures are broken down into more manageable sections. The HQ 22 Group GSN structure is an example of a complex and extended safety case that proved difficult to navigate and manage. By breaking down the high-level goals into a number of smaller groups and with hyperlinks from one group to another, navigation and visual assessment becomes much easier. In addition, the ability to tab through a number of selected GSN structures and view 2 or more structures alongside each, provides more clarity and aids assessment.



Safety cases are no longer just an “into service” item. Throughout the life cycle of the system numerous challenges and changes will occur and when a challenge is made against a safety case, the applicable areas must be identified before rectification can take place. Where goals and evidence are used in a number of GSN structures, they must all be identified if the situation is to be resolved satisfactorily. Queries can also help in this area and can be used to first identify those areas that are affected by the challenge and then colour code them so they stand out from the rest of the Structure. This makes identification much easier and additional colour coding can be applied to changes that have been put in place to show what changes have been made to address the challenge



SUMMARY

Today’s safety cases are becoming ever larger and more complicated. The GSN captures safety case arguments in a graphical notation that provides a clear representation of complex arguments with their supporting evidence. A large GSN can, however; consist of thousands of GSN elements with many interdependencies that make tracking progress and managing change very difficult. Moreover, as safety cases embrace through life management, many organizations are finding it more and more difficult to keep track of the required changes. By building the GSN in a safety modelling tool where elements, are created as entities within that model and adding reference and data fields to those entities, it becomes possible to handle modular safety cases more easily and efficiently. Queries and matrices provide a powerful analytical function that can track development, identify change requirements and report on the actions taken to meet any challenge. By enhancing the visual representations of GSN structures through easier navigation and colour coding, managers and system engineers can quickly identify key elements without the need for lengthy and time-consuming reviews.

References:

[Kelly 03] Managing Complex Safety Cases – Dr T P Kelly 2003. Available from https://www.users.cs.york.ac.uk/tpk/sss03.pdf

Andrew King Pen Picture:

Andrew worked in the RAF as the Safety Manager Executive for Air Traffic Control and Air Surveillance & Control specialisations before becoming a client director for a leading information management & computer modelling company in the private sector. He now works as the Operations Director for Diametric Software.