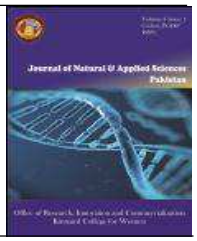
Contents lists available http://www.kinnaird.edu.pk/

Journal of Natural & Applied Sciences Pakistan

Journal homepage: http://jnasp.kinnaird.edu.pk/



ENGINEERING SAFETY CASE ARGUMENTS USING GSN STANDARDS

Maidah Mumtaz [1]*, Sidra Anwar [2], Nahal Mumtaz 3, Tabassum Kausar [4]
[1]Department of Computer Science, Govt. College Women University, Sialkot, Pakistan
[2]Department of Computer Science, Govt. College Women University, Sialkot, Pakistan
[3]Department of Computer Science, Govt. College Women University, Sialkot, Pakistan
[4]Department of Computer Science, Govt. College Women University, Sialkot, Pakistan

Article Info

* Maidah Mumtaz
maidahmumtaz6@gmail.com

Abstract

In Europe, over ongoing years, the obligation regarding guaranteeing the system safety has moved onto the developers and engineers to build and present well-reasoned arguments underlying the structure and presentation of obtuse document. These arguments together with supporting solutions and constraints are typically referred to as a "safety case". This study aims to benefit the risk-based Safety domain by demonstrating or clarifying how the set of evidence items may be combined together and argued to present the structure of engineering arguments. Therefore, an algorithm is proposed to serve the purpose following GSN standards while engineering the cases. The system would explicitly represent the individual elements of any safety argument i.e. requirements, claims, evidence and context; and relationships that exist between these elements. It will reduce the complications and misunderstandings due to poor communication between Safety arguments in safety cases and would strengthen the safety-critical industries in result.

Keywords

Goal Structuring Notation; Safety cases; Engineering arguments; risk-based Safety domain, Structuring Notations

1. Introduction

An argument or logic-based methodology is Goal Structuring Notation (GSN) that symbolizes all aspects of a safety argument to expand clarity and enhance structure under study in any industry or engineering phase i.e. (requirements, claims, evidence and context etc.) in an elegant and logical diagram. In recent years it has been used within the risk-based Safety domain to depict Safety Case structure. It assists with the demonstration or clarification of how the set of evidence items may be combined together and argued to demonstrate the top claim. Goal structuring notation is presented to support a user to draw a structure of engineering arguments and Data flow while taking technical arguments and following standards.

A solid relationship exists between its fundamental components, for instance how single necessities are upheld by explicit objectives, how objectives/Claims are supported by proof and the accepted setting that is characterized for the contention [1]. At the point when all these components of the GSN are associated together in a system they are depicted as an 'objective structure' [2]. The primary motivation behind any objective/goal structure is to indicate how objectives guarantees about the framework and are progressively separated into sub-objectives until a point is achieved where cases can be supported by direct reference to accessible proof.

Moreover, safety cases have been increased in size and difficulty with time to sustain [3]. There have been proposed Standard certifications that affect the safety cases and add into systems' complexity. For large systems, evidences can harm the high level argument clarity. Safety cases, its analysis and its structure should be clear and needed to avoid the errors to eventually overcome the cost that occurs due the increase in size of cases. Furthermore, the Objective Structuring Notation has become possibly the most important factor in mid-1990 at the University of York and became popular in 2012 [4] and has been utilized for various purposes. Also, GSN has been received by a developing number of organizations inside security basic enterprises, for instance, aviation, railroads and protection for the introduction of safety arguments inside safety cases [5].

While examining early researches, firstly by York and Professor McDermid in 1994 and Professor Kelly in 1995 and Wilson, were found to be unmistakably settled and outlined the ideas of goal structuring, however needed an authoritative meaning of the documentation [7]. While giving promising outcomes, needed consistency and it was recognized that further work was important to plainly characterize the use of the methodology. This brought about the improvement and meaning of a strategy for the development of contentions utilizing GSN, distributed by Kelly in 1998. For clients, gave a reasonable semantics approach of the documentation, and gave the improvement of GSN arguments. The technique turned into a fundamental segment in the preparation and training of end-clients in GSN. In 1996, Wilson, S.P.; McDermid, J.A.; Pygott, C. H.; Tombs, D. J, Assessed Complex Computer Based Systems using the Goal Structuring Notation [4]. External contractors provide the suitability of implementations that are assessed by the procurer of complex computer based systems. Assessor's requirements are clear, defensible and understandable argument that is supported with evidence that the system will perform reasonably and acceptably. Here, we describe the use of GSN to confine suitability argument with attached argument in the shape of design models, audit reports, test results etc. The Safe argument manager tool support work performed by University of York and the Defense Research Agency are also described in this paper.

Whereas, GSN was reached out in 1997 to help the articulation and documentation of reusable safety Case (Argument) Patterns [8]. In 1997, T P Kelly, S K Dawkins, Commercial-Off-The-Shelf used GSN in safety critical applications in development [9]; it eliminates the possibility of component mismatch. The GSN [15] has been developed to support the depiction of safety arguments. By Utilizing GSN, it is possible to present claims concerning a part and to indicate obviously on what premise those cases are

made. While by 1999, GSN dealt with programming safety case designs for the UK Ministry of Defense, distributed in 2011. So as to help the practical affirmation of Integrated Modular Avionics frameworks, industry (QinetiQ and BAE Systems) asked for in 2000 that York stretch out GSN to help the board of 'measured' and compositional safety cases.

Reaching 2006, Bateman, B.; Hatton, S.W., introduced the Increasing Role of Structured Methods in Arguing Safety [10]. The author reported succeeding practical application of proper methods, including GSN and Bayesian Networks, in development of safety arguments .Particular GSN has framed the specialized premise of the UK's Industrial Avionics Working Group (IAWG) UK MoD supported program of work on measured confirmation throughout the previous 8 years and the related BAE Systems Chairman's Award in 2007 [11].

By 2007, Grundy, John; Hosking, J., discussed Supporting generic sketching-based input of diagrams in a domain-specific visual language meta-tool [12]. Most of time, Software engineers used hand-made diagrams as beginning design artifacts and as comments or remarks during reviews [13]. In addition, sketching helped in enabling a wide range of diagram-based design tools to leverage this human-centric interaction support [14]. Visual plan devices produced from abnormal state particulars were in the way to deal with a scope of outlining based usefulness with quick and moderate acknowledgment, moving from draw to formalized substance and again at begin, in addition to utilizing portrays for optional explanation and community configuration survey.

In 2011, Matsuno, Y.; Taguchi, K, introduced Parameterized Argument Structure for GSN Patterns [15]. Goal Structuring Notation was proposed to use in safety critical system for the system assurance, a graphical notation broadly used to create assurance cases [16]. GSN included parameterized notations to make ease of reuse of existing assurance cases by prototypes and constructs projected in it. As the facility of parameterized notations is not provided by current GSN so it's inflexible to automate the regularity checks. Proposing an idea towards parameterization and its background in GSN was the aim of the paper. Types, scoping rules and type checking mechanism of a new parameterized notation providing protection to misuses of patterns and to type consistency checks were the limitations for near future.

Matsuno, Y.; Yamamoto, S., in 2013, discussed that GSN (Goal Structuring Notation) is a graphical documentation generally utilized, required for the framework confirmation of safety basic frameworks explicitly in Europe [17], and now everywhere throughout the world has been expanding [9]. In GSN Community Standard the sentence structure and augmentations for module and examples have been characterized. On D-Case Editor the model execution has been done, an Eclipse based GSN proofreader. Between sentence structure characterized in the standard, "objective away" and "module hub" as the reason for the module framework was actualized [12], joined with parameters with degree and example instantiation work, expansions of our last works. In light of to a few guided judgments in the GSN people group standard further safety issues for actualizing the full language structure of the GSN people group standard are likewise detailed.

B.Gallina, also proposed Model-driven safety certification method by 2014 [18]. The creation of a safety case is an extremely time consuming and costly activity needed for certification purposes. To lessen time and cost, it focused on safety standards and identified process-related structures from which process-based arguments those aimed at showing that a required development process has been applied according to the standard can be generated and more easily reused [19],. Then, a model-driven safety certification method was also proposed to determine those arguments as goal structures given in GSN from process models given in compliance with Software Process Engineering Meta model 2.0 [20]. The method was outlined

by creating process based arguments with regards to ISO 26262. To lessen cost and time, a novel model-driven technique called MDSafeCer was introduced, which allowed the clients to produce process-based contentions from process models

Finally, T P Kelly, discussed the Structuring Notation (GSN) standard in 2015 that were used in the railroad, air traffic the executives and atomic enterprises, medical community. On a basic level, it can be utilized to present and test any argument [13-16].

However, the most commonly observed fact based on evidences related to the failing of a safety cases is observed to neglect the main role of a safety cases which primarily communicate between objectives and evidences. In such cases number of supporting evidences is often presented like hundreds of fault tree's pages, effect analysis tables, and failure modes. However, the main responsibility still remains to a system to ensure its safety all in all and for this purpose, well-reasoned arguments are used to ensure or achieve the acceptable level of concern. Various industries including Medical, railway, robotics [6], automotive etc. use "safety cases" in regulation and certification. Therefore, an engineering platform is required to build and structure such safety arguments which can smoothly communicate between objectives and evidences also, the connection among goals and proof are well conveyed.

Conclusively, the Goal Structuring Notation is both for the individuals who wish to get ready and present convincing arguments utilizing the documentation, and for the individuals who wish to audit such arguments adequately. The Goal Structuring Notation presents models from differing branches of knowledge, including business the board, show, building, and legislative issues. Hence, in the present work, GSN device gives the present safety status of a venture on the punch of a catch, i.e., for task the executives, show a hued safety argument, with green and red demonstrating the safety status of framework parts, and, in the end, incorporate the safety reports for the investigation office.

2. Methodology

2.1 Principal Elements of GSN

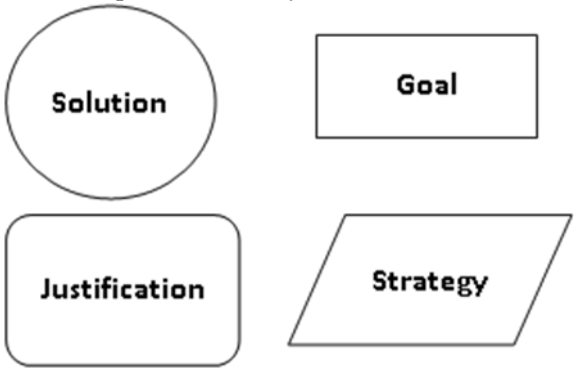


Fig: 1 principal elements of GSN

2.2 Restrictions:

Strong safety arguments are very vital to build in GSN for safety critical systems [15]. In GSN, goals can be decomposed into further goals and can be supported by solutions.

2.2.1 Safety requirements of the system:

Goal must be completed and unambiguous i.e. incomplete goals have undeveloped sub-goals. Each child must be complete and valid, dependent, and must relevant to the parent goal.

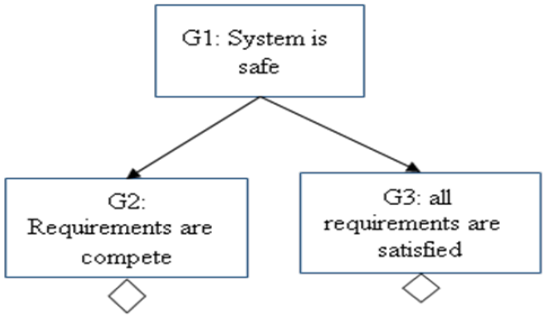


Fig: 2 Goals

2.2.2 SAL Apportionment across Linked Support (Loss of relevance) / SAL Apportionment across Convergent Support:

With respect to the parent goal, if the relevance/dependability of the child goals is not valid then another child goal is made, that is relevant to the parent goal to provide assurance and maintainability to the parent goal.

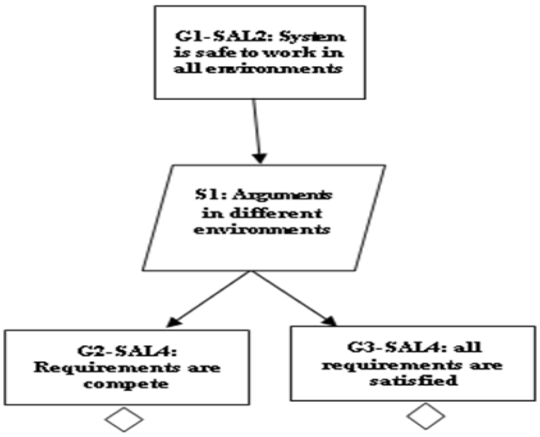


Fig: 3 SAL Appointment across linked/ convergent support

2.2.3 Justification:

It gives support to claim. Must be stated once, no repetition elsewhere. Information should being the form of complete sentences. Assumptions should be atomic.

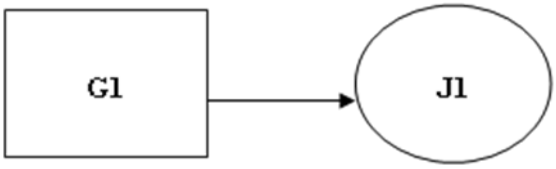


Fig: 4 Justification

2.2.4 Solution:

Each goal must have solution. Evidence or solution, ensures that the correct balance can be achieved.

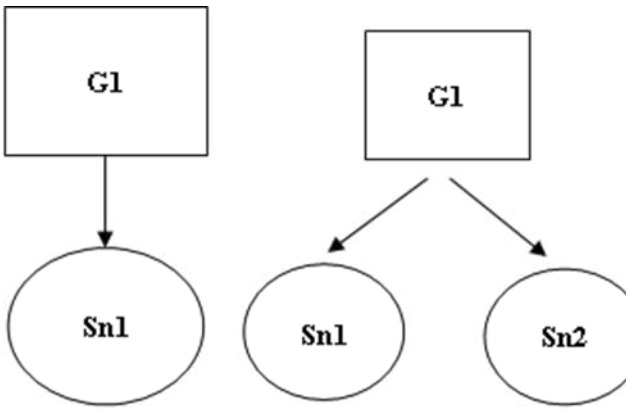


Fig: 5 solution

2.2.5 Strategy:

Strategies depend on goals. If at a point strategy changes, goal changes OR if goal change then new strategy must be made according to new goal. Strategy S1 is a description which is asserted between the goals to its sub-goals.

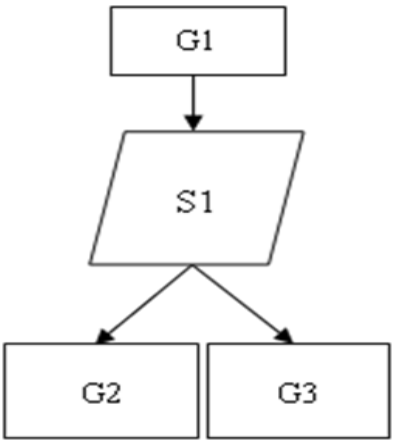


Fig: 6 Strategy

2.2.6 Other:

•The wording will be limited to single unambiguous statements consisting of a noun phase (subject) followed by a verb phase (a statement which is either true of false).

•Must give unique IDs, Numerical sequential IDs, Hierarchical to all elements in a GSN.

•Must provide pre-requisite shape/information.

•It is optional to fill each shape with color.

•Contextual relationship – Goal-to-context, goal-to-assumption, goal-to-justification, strategy-to-context, strategy-to-assumption and strategy-to-justification.

Fig: 7 Contextual Relationship

•Evidential relationships– Goal-to-goal, goal-to-strategy, goal-to solution, strategy to goal.

Fig: 8 Evidential Relationship

•All these shapes can be interrelated to each other and all dependability attributes can result in competing objectives.

2.3 Algorithm

The six steps involved in the engineering of a goal structure are:

1) START
2) Identify goals.
3) Identify sub-goals, if more than one goal.
4) Identify strategies, if more than one then repeat this step until completed.
5) Identify solutions, if more than one solution then repeat this step until completed.
6) Check goal is achieved.
7) Go to step 3 for remaining goals.
8) END.

3.4 Flowchart

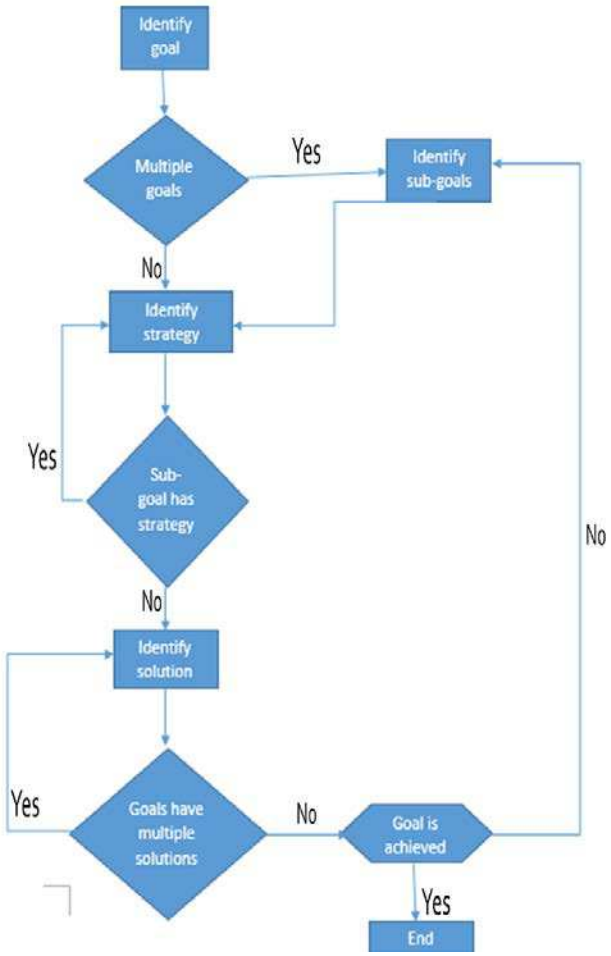


Fig: 9 Algorithm of GSN

3. Discussion

The use of GSN has arisen in response to poorly written Case documents. The upcoming automotive industry introduces the safety standard ISO/WD 26262 which imparts a reasonable, thorough and solid arguments that make a framework is acceptably protected [20]. Safety case will automatically resolve all safety related issues have been tended to in a security basic framework in the automatic space. GSN elements are also discussed in terms of goal, strategy, justification and solution. GSN describes the relationship between evidences and conclusions. The main purpose of safety arguments in GSN is basically to provide automatic safety generator associated goals with solutions [14]. Assurance can be provided by multiple forms of evidence or elements of argument may not be so convincing if they are not truly independent [18]. GSN is examined to reduce the complications and misunderstandings due to poor communication between safety arguments in safety cases and would strengthen the safety-critical industries in result. Regular structures in safety case arguments can be reused through their documentation as Safety Case Pattern. GSN safety approach, however, can maintain a strategic distance from a portion of the issues with the current, casual and unplanned methodologies with security case material reuse. Through the unambiguous catching and documentation of reusable safety case components, structure design can be made increasingly composed, legitimate and less mistake inclined.

An engineering goal structure based algorithm is also proposed identifying supporting goals, its basis, supportive strategies, its definitions, and eventually the final solution. Utilizing safety case platform including a beginning stage to new building arguments which help in arrangements and checking authenticity, help enhance arguments accuracy and culmination and finally provide a standard while investigating a safety argument.

4. Conclusion

It is depicted how a safety case can be developed and dependent on the objective organizing documentation that proposes to make a solid and safe arguments out of objectives that are broken recursively into sub-objectives or sub-goals until a sub-objective can be demonstrated by evidence. The evidence or proof is given by reports tending to the safety issues. The standards are illustrated on piece of the safety cases showing the beginning acknowledgment and verification for each prerequisite which were plainly reported earlier. Moreover, all necessities ought to be perceptible to their particular executions forward and in reverse are accommodated. Conclusively, the accomplishment of GSN with the safety case area is observed to be driven its more extensive use in different spaces where assurance cases or safety cases are required. Also, the selection of GSN as an organized argumentation strategy is examined to enable users to consider boosted ideas, of upkeep and overseeing dimensions of arguments affirmation.

References

"Introducing Goal Structuring Notation to explain decisions in clinical practice". 2006. The 1st Institution of Engineering and Technology

2011

A. Groza and N. Marc, "Consistency checking of safety arguments in the Goal Structuring Notation".

Argument Structure for GSN Patterns", (2011) Visual

B. Gallina, "A Model-Driven Safety Certification Method for Process Compliance," November 2014.

Bateman, B., Hatton, S.W., "The Increasing Role of

Bloomfield, R., & Bishop, P. (2010). Safety and assurance cases: Past, present and possible future–an Adelard perspective. In Making Systems Safer (pp. 51-67). Springer, London.

C. Gonzaga-Lopez, "The impact of COTS software on the public procurement of mission-critical systems," pp. 1-39, Jan 2015.

I. Habli, "GSN STANDARD VERSION 1.0," no. Review Committee, pp. 1-30, May 19th to August 27th 2010.

International Conference on, vol., no., pp.158, 163, 6-8 June 2006.

Kelly, T. (1998). A six-step method for developing arguments in the goal structuring notation (GSN). Technical report. York Software Engineering.

Kelly, T., & Weaver, R. (2004, July). The goal structuring notation–a safety argument notation. In Proceedings of the dependable systems and networks 2004 workshop on assurance cases (p. 6). Citeseer.

Languages, 2011. Proceedings. 2011 IEEE International

Matsuno, Y., Yamamoto, S., "An implementation of GSN community standard," Assurance Cases for Software Intensive Systems (ASSURE), 2013 1st International

Mueller, W. , Meyer, A. , Zabel, H. "Parameterized

R. A. Weaver, "The Safety of Software – Constructing and Assuring Arguments," pp. 1-298, Sep, 2013.

R. Hawkins1, T. Kelly1, J. Knight and P. Graydons2, "A new approach to creating clear safety arguments".

R. Weaver, G. Despotou, T. Kelly and J. McDermid, "Combining Software Evidence – Arguments and Assurance," pp. 1-7.

S. B. Dagstuhl, "Safety Cases: Arguing the safety of autonomous systems," 2017.

S. P. Wilson, J. A. McDermid, C. H. Pygott and D. J. Tombs, "Assessing complex computer based systems using the Goal Structuring Notation," Nov 1996.

Spriggs, J. "GSN-The Goal Structuring Notation: A Structured Approach to

Presenting Arguments. Springer Science & Business Media". (2012).

Structured Methods in Arguing Safety," System Safety,

Symposium on, vol., no., pp. 77 – 78, 0 Sep 2011-13 Sep

T. Kelly and J. McDermid, "A systematic approach to safety case maintenance," pp. 3-10, 2001.

T. Kelly and R. Weaver, "The Goal Structuring Notation- A safety argument notation".

T. P. Kelly and J. A. McDermid, "Safety Case Construction and Reuse Using Patterns," pp. 55-69, 1997.

Workshop on, vol., no., pp.24, 28, 19-19 May 2013.