Institution: University of York
Unit of Assessment: 11, Computer Science and Informatics
Title of case study: The Goal Structuring Notation (GSN)
1. Summary of the impact (indicative maximum 100 words)

The development, review and acceptance of an explicit 'safety case' forms a key component of the assurance and regulation of many safety critical systems, including those in the nuclear, defence, railway, automotive, medical device, and process industries. Industrial practice in safety case development prior to York's development of the Goal Structuring Notation (GSN) relied almost exclusively upon narrative text to communicate the safety argument within the safety case. This approach suffered from problems of lack of clarity, difficulty in comprehension, poor structure, and limited formalised development of 'case law' in safety argumentation. GSN was developed and matured by York to tackle these problems directly, and is now used internationally by safety critical industries in a large number of domains including defence, transport, nuclear and medical devices.

2. Underpinning research (indicative maximum 500 words)

The High Integrity Systems Engineering research group at York first developed and proposed the use of goal structures (initially termed 'goal hierarchies') to explicitly represent the argumentation component of safety cases as part of the EPSRC (then SERC) funded ASAM (A Safety Argument Manager) and ASAM-II projects. The ASAM project first attempted to directly apply Toulmin's work on logic and argumentation to industrial safety case development. However, early findings showed that the industry users needed instead an argumentation notation that allowed them to present their safety case reasoning at multiple levels of abstraction. This led to the development of GSN, through combining concepts from Toulmin argumentation with those that were emerging from the field of (hierarchical) goal-based requirements engineering (such as van Lamsweerde's KAOS). Early industrial use of York's goal structuring approach was limited to trials and pilot projects by the industrial partners on the ASAM-II project – Rolls-Royce, British Aerospace, Lloyd's Register, Logica and York Software Engineering).

Early papers by York, such as the paper by Professor McDermid in 1994 [1] and Professor Kelly in 1995 and Wilson [2], clearly established and illustrated the concepts of goal structuring, but lacked a canonical definition of the notation. Initial application by industrial users (e.g. Rolls-Royce), whilst providing promising results, lacked consistency and it was identified that further work was necessary to clearly define and support the application of the approach. This resulted in the development and definition of a method for the construction of arguments using GSN, published by Kelly in 1998 [3]. For users, [3] provided a clear semantics of the notation, reduced ambiguity in the purpose and meaning of the notation, and provided step-by-step guidance in the development of GSN arguments. The method became an essential component in the training and education of end-users in GSN. Based upon an adaption of concepts from the body of work on 'Design Patterns' GSN was extended in 1997 to support the expression and documentation of reusable Safety Case (Argument) Patterns [4]. GSN has underpinned much of York's research on system and software safety case development (such as work on safety case maintenance published in 1999, and work on software safety case patterns for the UK Ministry of Defence, published in 2011). In order to support the cost-effective certification of Integrated Modular Avionics systems, industry (QinetiQ and BAE Systems) requested in 2000 that York extend GSN to support the management of 'modular' and compositional safety cases (safety cases established through contract-based composition of component 'modules' of argument and evidence with well-defined interfaces) [6]. Modular GSN has formed the technical basis of the UK's Industrial Avionics Working Group (IAWG) UK MoD funded programme of work on modular certification for the last 8 years and the associated BAE Systems Chairman's Award in 2007.

McDermid was and remains Professor of Software Engineering, Kelly joined York as a research student in 1994, then went on to be Research Fellow, Lecturer, Senior Lecturer, and is now Professor, and Bate was Lecturer and is now Senior Lecturer (all at York). Wilson was a Research Associate (at York from 1993-1997).

3. References to the research (indicative maximum of six references)

[1] John A. McDermid, Support for safety cases and safety arguments using SAM, Reliability Engineering & System Safety, Volume 43, Issue 2, 1994, Pages 111-127, ISSN 0951-8320, doi: 10.1016/0951-8320(94)90057-4. (Google Scholar Citations: 49, Scopus Citations: 14),

[2] Wilson, S. P., T. P. Kelly, and J. A. McDermid. "Safety Case Development: Current Practice, Future Prospects." Safety and reliability of software based systems: twelfth annual CSR workshop (Bruges 12-15 September 1995). Vol. 12. Springer Verlag, 1996, doi: 10.1007/978-1-4471-0921-1_6 (Google Scholar Citations: 54, Scopus Citations: Not indexed)

[3] Kelly, T. "Arguing Safety – A Systematic Approach to Safety Case Development", DPhil Thesis, Department of Computer Science, University of York, 1999 (Google Scholar Citations: 325 Scopus Citations: Not Indexed) Available on request

[4] Kelly, Tim P., and John A. McDermid, "Safety case construction and reuse using patterns." In 16th International Conference on Computer Safety, Reliability and Security (SAFECOMP 1997), pp. 55-69. Springer, 1997, doi: 10.1007/978-1-4471-0997-6_5 (Google Scholar Citations: 74, Scopus: Not indexed)

[5] Kelly, T. P., and J. A. McDermid. "A systematic approach to safety case maintenance." Reliability Engineering & System Safety 71, no. 3 (2001): 271-284, doi: 10.1007/3-540-48249-0_2 (Google Scholar Citations: 34, Scopus Citations: 20)

[6] Bate, Iain, and Tim Kelly. "Architectural considerations in the certification of modular systems." Reliability Engineering & System Safety 81, no. 3 (2003): 303-324, doi: 10.1007/3-540-45732-1_31 (Google Scholar Citations: 21 Scopus Citations: 16)

We highlight [1], [3], and [5] as particularly indicative of research quality. We have provided both Google Scholar and Scopus citation counts where possible (counts taken 13.09.2013). For [3], a PhD thesis, not indexed by Scopus, we can only provide a Google Scholar count. This count clearly highlights that [3] is the most influential and commonly cited source when referring to GSN. (It is, for example, the source cited by the 2012 International automotive safety standard ISO 26262 and the 2010 US Federal FDA 510(k) guidance for Infusion Pump Safety.) *Reliability Engineering and System Safety* is one of principal journals in system safety engineering. It has a 5-year impact factor of 2.170. SAFECOMP was ranked 'B' by ERA and is a primary conference for the discipline of computer system safety and dependability.

4. Details of the impact (indicative maximum 750 words)

York's work on GSN through the research and outputs described in the previous section has provided industry with a new approach and method to presenting safety arguments that improves the rigour and clarity of their safety cases (e.g. [7] presents a discussion of the experienced benefits). Since its inception, the adoption and use of GSN has grown year-on-year as a result of the publications on GSN, and the GSN training and education provided by York since 1995 through its MSc in Safety Critical Systems Engineering, and associated Continuing Professional Development courses for industry. In many settings (e.g. European Air Traffic Management - ATM - [8]) GSN has become the de facto standard for representing safety arguments within safety cases. It is cited by international safety standards (e.g. the new automotive safety standard ISO 26262 [9] published in 2012) and is commonly referenced in safety practitioner textbooks - e.g. [10]. It is the subject of its own book authored by a engineer in the ATM domain [11] (published in 2012) and is taught widely on safety education and training courses external to York. In addition, application of the technique is now a widely and commonly offered service by safety consultancies and forms a common skill requirement of many job vacancy descriptions in the safety domain (e.g. [12]). GSN has become an embedded and established international[1] approach to safety case development, and has changed the culture of safety case development such that the use of graphical argument structures is now commonplace. There is wide adoption and use in industrial safety cases – GSN is being used in large numbers of industrial safety cases in a huge variety of settings. Early adoption (e.g. from the mid 1990s onwards) was predominantly in the domains of ATM, military aerospace and defence. Notably over recent years (2008 onwards), in addition to these domains there has been a significant increase in the number of industrial sectors using GSN

[1] *See examples of countries using GSN at testimonial references [20] to [24] in Section 5*

for their safety assurance cases, notably Off-shore Oil and Gas [13] (2009), Space Systems [14] (2012), Medical Systems (2009 onwards), Railways [15], and Automotive [16] (2013). GSN has been used to construct a diverse range of safety cases, with applications ranging from the Battle of Britain Memorial Flight, through medical device safety, to the new autonomous personal rapid transit system in Heathrow Terminal 5. Over the last five years there has also been a notable increase in the number of safety case tools that support users (safety engineers, safety case authors and safety assessors) in the development, presentation and analysis of GSN arguments including: Adelard's ASCE Tool [17] (publicly available and supporting GSN since the late 1990s and now in it's 4th version, the 2012 tool now supporting York's modular extensions to GSN [6] in addition to it's longstanding support for the core notation); Japan's D-Case Tool (publically available from 2011); NASA's AdvoCATE Toolset [14] (2011-onwards); Atego's GSN Modeler (2008 onwards); USA-based Kestrel Technology's CertWare tool (2011-onwards); Dependable Computing's GSN Editor (2012-onwards); and the USA GessNet Tool (2011 onwards) that helps users construct GSN arguments specifically for medical devices. The Adelard ASCE tool alone has been licensed to 3000 users worldwide, with the majority of these using the tool for GSN argument development. Adelard's biggest user-base for the ASCE tool is in defence, where they have reported that 75% of all UK military aircraft have a GSN-based safety case.

In recent years, an industry group - supported by York - was formed to establish a GSN standard to support the now widespread industrial use of the approach. This industry group was formed of representatives from companies including: AACE Ltd, Altran Praxis Ltd, ERA Technology Ltd, Lloyds Register Rail Ltd, RPS Group Ltd, Selex-Galileo Ltd, UK Ministry of Defence, Adelard LLP, BAE Systems Ltd, CSE International Ltd, General Dynamics UK Ltd, Thales Ltd. Issue 1 of the GSN 'Community' standard was published in November 2011 [18].

As a result of growing international interest in assurance cases (for both security and safety), York was invited by the international OMG (Object Management Group) Systems Assurance Task Force to use its experience with GSN to be a lead author (alongside industrial partners that included from the US Lockheed Martin, MITRE and NIST) a new international standard on assurance cases. This work has resulted in the definition of the publicly available OMG ARM (Argumentation Metamodel) (2010) and SACM (Structured Assurance Case Metamodel) (2013) standards that both explicitly include examples of GSN and mappings to GSN.

In 2006 York staff established the GSN User Club (now the Assurance Case Forum) to support the GSN user base and promote sharing of best practice amongst users. Since 2006, there have been 18 physical meetings of the forum, with over 117 unique attendees, representing 52 companies with end users in rail, aerospace, ATM, marine (surface and sub), telecoms, automotive, weapons, power generation, together with consultancies, lawyers, academics and tool developers.
In the 2009 UK government-funded public enquiry into the explosion of a RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006 it was stated that, "GSN provides a useful structured way of presenting a complex safety argument" [19].

The benefits gained from the use of GSN are accrued firstly by safety engineers (enabling them to better manage the development of safety arguments for complex systems [7] and – through more explicit treatment – create compelling safety arguments) and regulators (through enabling greater comprehension and review of safety case arguments). However, ultimately the benefits gained from using GSN are reaped by operators and the general public through safer systems (arising from developers and regulators having used a more rigorous and systematic approach to safety argument construction).

5. Sources to corroborate the impact (indicative maximum of 10 references)

[7] Chinneck, Paul, D. J. Pumfrey, and T. P. Kelly. "Turning up the HEAT on safety case construction." In Practical Elements of Safety: Proceedings of the Twelfth Safety-critical Systems Symposium, pp. 223-240. 2004, doi: 10.1007/978-0-85729-408-1_14, Primarily authored by Paul Chinneck from Agusta Westland (now at Altran) - *Confirms GSN application in the defence / military aerospace domain and describes benefits.*

[8] Eurocontrol Safety Case Development Manual, 2006, available from http://publish.eurocontrol.int/sites/default/files/content/documents/nm/link2000/safety-case-

development-manual-v2.2-ri-13nov06.pdf, last accessed 12/9/2013 - *This standard defines European Air Traffic Management safety case development practice. The standard requires documented GSN arguments as part of any safety case report. Confirms GSN application in the ATM domain.*

[9] ISO/DIS 26262 (2012) Road vehicles - Functional safety - Part 1-10, available from http://www.iso.org - *Automotive safety standard includes the requirement for automotive system providers to provide a safety case. Part 10 cites Kelly's thesis [3] and references GSN and as a suitable technique*.

[10] Kritzinger, D., "Aircraft system safety: Military and civil aeronautical applications", CRC Press, 2006, ISBN-10: 0849390125 - *GSN is described in the section on safety case development. See also Appendix C for an example GSN argument.*

[11] Spriggs, J., "GSN – The Goal Structuring Notation", Springer, 2012, ISBN-10: 1447123115 - *This is a (non-academic) textbook on GSN produced by a practitioner from the Air Traffic Management domain. The University of York is clearly attributed as the developer of the technique in the Preface (page viii).*

[12] Safety Engineers and Safety Consultants, rtmjobs.com http://www.rtmjobs.com/rail-job-vacancies/12565-lhrtm10-safety-engineers-and-safety-consultants-various-location/, Last accessed 12/9/2013 - *Example of the citation of GSN as a desired skill for safety engineering jobs.*

[13] Aas, A. L., Andersen, H. S., "A Retrospective Safety Case for an Advanced Driller's Cabin", in Proc. of the 2009 International Petroleum Technology Conference, Qatar, doi: 10.2523/13755-MS - *Confirms GSN application in the oil and gas domain.*

[14] Denney, E., Pai, G., and Pohl, J.. "AdvoCATE: An Assurance Case Automation Toolset." Computer Safety, Reliability, and Security (2012): 8-21, doi: 10.1007/978-3-642-33675-1_2 - *Confirms GSN application in the space domain and NASA's development of tools to support GSN.*

[15] International Rail Industry's Engineering Safety Management Handbook, Volume 2, published on behalf of the International Rail Industry by Technical Programme Delivery Ltd., Issue 1, April 2013, available from http://www.intesm.org, last accessed 12/9/13 - *This international rail industry handbook sets out best practice for the rail industry and cites GSN as a "useful technique" for structuring and illustrating safety cases.*

[16] Birch, J., Rivett, R., Habli, I., Botham, J., Higham, D., Jesty, P., Monkhouse, H., Palin, R., Safety Cases and Their Role in ISO 26262 Functional Safety Assessment, in 32nd International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2013), pp154-165, Springer, 2013, doi: 10.1007/978-3-642-40793-2_15 - *Authored by members of the MISRA (Motor Industry Software Reliability Association) working group on safety cases. Shows the use of GSN in automotive safety arguments in compliance with ISO 26262 [9]. This group is currently preparing new guidance for the automotive industry on safety case construction that uses GSN.*

[17] Adelard ASCE Tool, download available from http://www.adelard.com/asce/choosing-asce/gsn.html, last accessed 12/9/13 - *Confirms industrial third-party tool support for GSN. One of the increasing number of such tools.*

[18] GSN Community Standard, Version 1, available from www.goalstructuringnotation.info, last accessed 12/9/13 - *This community standard demonstrates the level of industry support for GSN (see large number of contributing authors).*

[19] C. Haddon-Cave, The Nimrod Review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006 report, Report No. No 1025 2008–09, 28th October 2009, Published by the Stationery Office (TSO) - *Cites GSN as a "useful technique" for safety case development.*

[20] ECOS UK Programme Manager, BAE Systems

[21] Head of the RAMSS Competence Centre, Siemens Transportation Systems - Rail Automation, Germany

[22] Chief, General Hospital Devices Branch, US Food & Drug Administration

[23] Professional Head of Systems Safety, London Underground, Transport for London

[24] Senior Computer Scientist - Robust Software Engineering Group, NASA Ames Research Center - Computational Sciences Division