

NASA/CR-2015-218678



# Current Practices in Constructing and Evaluating Assurance Cases With Applications to Aviation

*David J. Rinehart*  
*Saab Sensis Corporation, East Syracuse, New York*

*John C. Knight and Jonathan Rowanhill*  
*Dependable Computing, Charlottesville, Virginia*

---

January 2015

## 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 counter-part of peer-reviewed formal professional papers but has 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](mailto: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/CR-2014-218678



# Current Practices in Constructing and Evaluating Assurance Cases With Applications to Aviation

*David J. Rinehart*  
*Saab Sensis Corporation, East Syracuse, New York*

*John C. Knight and Jonathan Rowanhill*  
*Dependable Computing, Charlottesville, Virginia*

National Aeronautics and  
Space Administration

Langley Research Center  
Hampton, Virginia 23681-2199

Prepared for Langley Research Center  
under Contract NNL13AC56T

January 2015

## Acknowledgments

The authors thank C. Michael Holloway for his oversight and guidance of this project and NASA's Aviation Safety Program for its sponsorship. For special assistance with the Triton example, we thank M. Anthony Aiello from Dependable Computing. Our gratitude also goes out to reviewers and interested parties from the FAA, the aviation industry, and the system assurance domain for their feedback as we've crafted this report. Finally, we express our appreciation to colleagues and assurance case practitioners who helped us gather information on the many examples included here.

The use of trademarks or names of manufacturers in this report is for accurate reporting and does not constitute an official endorsement, either expressed or implied, of such products or manufacturers by the National Aeronautics and Space Administration.

Available from:

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

# Contents

1.	Executive Summary.....	1
2.	Scope, Motivation, and Objectives of this Report .....	3
3.	Assurance Cases Foundations.....	5
3.1	Role in System Development.....	6
3.2	Paradigm.....	7
3.3	Brief History.....	9
3.4	Assurance Case Properties .....	10
3.5	Assurance Case Stakeholders.....	11
3.6	Terminology .....	11
3.6.1	Argument.....	11
3.6.2	Claim.....	12
3.6.3	Evidence.....	12
3.6.4	Goals .....	13
3.6.5	Risk Management.....	13
3.6.6	Levels of Rigor.....	13
3.6.7	Evaluation.....	14
3.7	Notations.....	14
3.7.1	Goal Structured Notation (GSN).....	14
3.7.2	Claims, Arguments, and Evidence (CAE) Format .....	16
3.7.3	OMG Structured Assurance Case Metamodel (SACM) .....	18
3.7.4	Textual Forms .....	18
3.8	Standards and Assurance Cases.....	19
3.9	A Classification Scheme for Assurance Cases.....	21
4.	Example Uses of Assurance Cases.....	23
4.1	Energy Sector.....	24
4.1.1	Offshore Oil and Gas.....	24
4.1.2	Generic Design Assessment (GDA) of Nuclear Plants .....	30
4.2	Aviation Infrastructure.....	34
4.2.1	U.K. Civil Aviation Authority CAP 670 & 760.....	34
4.2.2	Eurocontrol Wide-Area Multilateralation (WAM) Preliminary Safety Case.....	38
4.3	Aerospace Vehicles.....	41
4.3.1	NASA Risk-Informed Safety Case (RISC).....	42
4.3.2	Navy Triton UAS.....	45
4.3.3	RAF Aircraft Nimrod and Related.....	46
4.4	Rail (Infrastructure and Vehicles).....	50
4.4.1	European Rail Safety Management Systems.....	51
4.4.2	U.K. Rail Safety Cases: 1994 - 2006 .....	53
4.5	Automobiles .....	55
4.5.1	ISO 26262.....	55
4.6	Medical Devices.....	57
4.6.1	Infusion Pumps (Food and Drug Administration).....	58
4.6.2	Generic Pacemaker Assurance Case .....	61
5.	Assurance Case Evaluation.....	63
5.1	Evaluation Stakeholder Roles .....	63
5.2	Properties of Interest.....	64
5.3	Conformance with Standards .....	66
5.4	Assurance Case Standards and Guidance Documents.....	67
5.5	ISO/IEC 15026-2.....	69
5.6	Documentation Review .....	70
5.7	Assurance Argument Evaluation Theory .....	70
5.7.1	Baconian Probability .....	71

5.7.2	Bayesian Belief Networks .....	71
5.7.3	Argumentation Theory .....	72
5.7.4	Operational Definition .....	72
5.8	Argument Structural Analysis .....	72
6.	Conclusion .....	74
7.	References .....	75

# 1. Executive Summary

This report introduces and provides an overview of *assurance cases* including theory, practice, and evaluation. We present and discuss a concise definition of an assurance case as “an organized argument that a system is acceptable for its intended use with respect to specified concerns (such as safety, security, correctness).” Assurance cases share an extensive lineage with safety cases, but broaden the content to all necessary subjects of assurance, which are often related. For example, common evidence and argument can be used to show that a system is both safe and secure.

Our interest in assurance cases is motivated by potential application to aviation, specifically in the U.S. National Airspace System (NAS). Modern aviation is characterized by high levels of safety criticality, technical complexity, and operational complexity. Moreover, these are trends which are increasing with the development and deployment of “NextGen.” The aviation system is, therefore, a likely candidate for advanced assurance methods. The project producing this report brought together cross-domain expertise on assurance cases and conducted an extensive literature review for the purpose of relating assurance cases to aviation.

Beginning with fundamentals, this report explains the role of assurance cases in system development and the paradigm they represent. Assurance cases are best deployed as a parallel, ongoing process during system development so that weaknesses can be identified and addressed as early as possible. *Argumentation* plays a central role in assurance cases; it is the organizing principle that connects what is done and recorded with system assurance goals. Our brief history, paradigm discussion, and examples show how good assurance cases unite many existing practices already aimed at assurance and organize them into a cohesive whole, facilitating the identification of gaps and overlaps. Assurance cases represent a shift toward broader scope and greater flexibility relative to prior methods of ensuring system acceptability. We present desirable properties of assurance cases (such as compelling, valid, and complete) and key stakeholders (such as developers, regulators, and operators).

This report introduces the principles and terminology of assurance cases. Consistent with the theme of argumentation, predominant terms include *claim* and *evidence*. We also define goals in the context of assurance cases, discuss associated risk management, and present the concept of levels of rigor. We provide an overview of specific notations often featured in assurance cases.

Before surveying examples of assurance cases, we present a classification scheme to be used. There are three axes in this scheme: rigor in argument, rigor in evidence, and flexibility in process.

We then provide a lengthy exploration of examples of assurance cases. Some of our examples are called assurance cases, others are called safety cases (effectively a subset for our purposes), and others are called by some other term but are comparable in informative ways. Walking through these examples one by one, we examine for each: (1) the role of assurance cases, (2) a characterization of the content, and (3) the outcomes of their application. Though the majority of these examples are not from the aviation domain, we have selected them because in every case there are points of similarity. Table 1 lists the examples included in this report.

**Table 1: Assurance Case Examples Included in this Report**

Example	Domain
Offshore Oil and Gas	Energy
GDA of Nuclear Plants	Energy
CAA CAP 670 & 760	Aviation Infrastructure
Eurocontrol WAM PSC	Aviation Infrastructure
NASA Risk-Informed Safety Case	Aerospace Vehicles
Navy Triton UAS	Aerospace Vehicles
RAF Nimrod	Aerospace Vehicles
European Rail SMS	Railways
U.K. Rail Safety Cases	Railways
ISO 26262	Automobiles
Infusion Pumps	Medical Devices
Generic Pacemaker Assurance Case	Medical Devices

Our examples span a range of maturities. Given the relative newness of assurance case practices, no examples are more than a couple decades old; and in numerous instances, assurance cases are partway through the process of adoption. That is, in some cases we can look at guidance and regulations, but application to specific systems with outcomes are difficult to find. Furthermore, given the nature of assurance cases, many details are kept out of the public domain. Within these limits, our survey gathers the best information available to illustrate the current state of assurance cases.

We also include a section dedicated to the subject of evaluating assurance cases. In order for any assurance case regime to be consistently effective, there must be adequate provision for evaluation and improvement (as needed). We will see that there are a number of approaches to evaluating assurance cases. There are assurance case standards and guidance documents available, some fairly recent on the scene. There are also some promising evaluation approaches that take advantage of argumentation structure and theory, including Baconian probabilities and Bayesian Belief Networks. We do not cover these in detail but simply provide a brief introduction. While technical analyses may play an important role, assurance case evaluation is likely to rely for a long time on human insight and judgment. Generally, this can be incorporated in straightforward ways; for example, with appropriate documentation review processes and training. Assurance cases are efficient and organized in how they manage a complex task: demonstrating acceptability. With appropriate resourcing and preparation, evaluation is an achievable task.

In summary, this report provides a comprehensive introduction to the state of the art of assurance cases in theory and practice. We present and characterize many informative, real-world examples drawn from multiple domains. We believe that these precedents – and the argument-based assurance case concepts they illuminate – have important relevance for the future of U.S. aviation and complex, safety-critical systems development in general.

## 2. Scope, Motivation, and Objectives of this Report

The objective of this report is to provide a comprehensive introduction to assurance cases. To that end, we have broken down the report into Section 3 - Foundations), Section 4 - Examples, and Section 5 - Evaluation.

The first major section presents fundamental assurance case concepts. Assurance case development is best integrated with system development, not conducted as a *post facto* exercise. Many related assurance paradigms are incorporated into assurance cases, such as standardization, risk management, and auditing. The innovative element of modern assurance cases (as in safety cases) is the construction of an explicit *argument* for the desired assurance property. In this foundations section, we provide a brief history of assurance cases. We also introduce basic terms such as claims, arguments, evidence, and goals. In closing Section 3, we look at notations and standards for expressing assurance cases.

The centerpiece of this report is a collection of examples of assurance cases drawn from many domains. We present these examples in Section 4. Many examples are known as safety cases, but they suffice as examples of assurance cases as well (with a specific focus on safety). Our examples include:

- Energy (oil and gas, nuclear),
- Aviation Infrastructure (ground systems),
- Aerospace Vehicles (aircraft, space vehicles),
- Rail (both infrastructure and vehicles),
- Automobiles, and
- Medical Devices (infusion pumps, pacemakers).

As we present these examples, we classify and discuss them in terms of three characteristic properties that we have developed: *rigor in argument*, *rigor in evidence*, and *flexibility in process*.

The final major section is dedicated to the subject of evaluating assurance cases. Here we discuss assurance cases properties, stakeholders, and standards (and other published guidance). We also present a range of evaluation techniques ranging from basic to advanced. Basic techniques include review of documentation and such practices; even simple methods like these bring the essential ingredient of expert judgment into assurance case evaluation. We also discuss several more advanced techniques such as Baconian probabilities, Bayesian belief networks, and argument structural analysis.

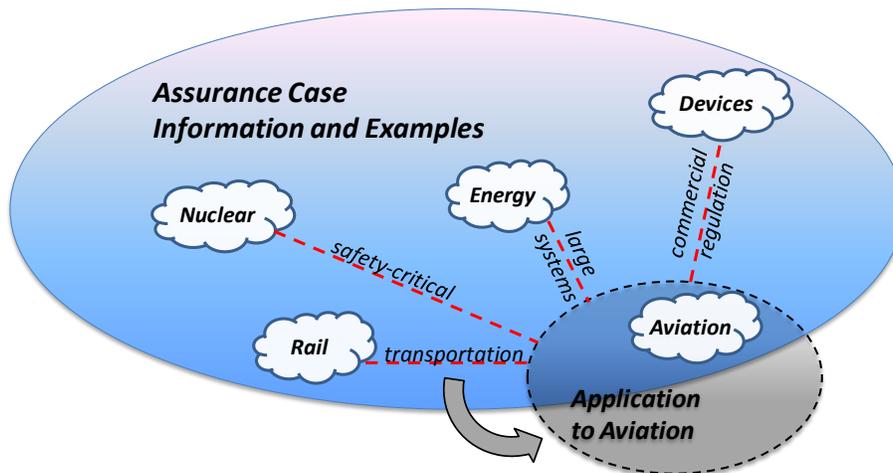
While the report structure described above serves as a general-purpose introduction to assurance cases, our specific interest is from the perspective of aviation and, specifically, U.S. aviation. There is a certain timeliness associated with this point of view: while assurance cases are becoming established in some areas of the world (especially the U.K., and Europe more broadly), they are not yet common in the U.S. Furthermore, aviation has historically been a leader in U.S. technology development and system assurance practices such as those which improve safety. Hence, there is a natural interest at this time in applying assurance case methods to U.S. aviation.

Furthermore, certain trends are placing greater pressure on the aviation system. Legacy systems have been quite effective in terms of safety, but at some expense of limited efficiency and manual effort. On the infrastructure side, modernization seeks to improve efficiency by greater automation and coordination – factors which increase complexity and introduce new risk

factors. On the vehicle side, innovation is producing a greater variety of aircraft that wish to operate in the NAS. These aircraft must be certified to operate; but as they include new and more complex design features (such as, cutting-edge propulsion and new levels of autonomy), there are few certification precedents on which to rely.

Our selection of examples is diverse by any measure. In part, this serves generality, but it also acknowledges the fact that the pedigree of assurance cases is by no means particular to aviation. On the contrary, though aviation has been involved in the history of assurance cases all along, in many instances it was other domains that pushed along the evolution of the methods.

Still, given our perspective, we note that all the examples bear some relevance to aviation. Figure 1 depicts the mappings of some of our examples to aviation.



**Figure 1: Assurance Case Domains and Aviation**

Through the following sections, we hope to provide an informative and beneficial introduction to assurance cases – both for the general audience, and specifically for the purposes of furthering their appropriate application within aviation.

### 3. Assurance Cases Foundations

In this section we lay out a foundation for understanding assurance cases that includes basic principles, terminology, and notations.

To start at the very beginning, what is an assurance case? Here is a standard definition of “assurance case,” which bears similarity to well-established definitions of “safety case” (GSN Committee 2011):

*“A reasoned and compelling argument, supported by a body of evidence, that a system, service or organisation will operate as intended for a defined application in a defined environment.”*

While this is accurate and provides a good official definition, it is a bit opaque. Furthermore, it gives no indication of the objectives that typically motivate assurance cases. For the purposes of this report, the following is a more concise and pointed (if less comprehensive) definition of “assurance case”:

*An organized argument that a system is acceptable for its intended use with respect to specified concerns (such as safety, security, correctness).*

There are several key elements in this abbreviated definition. An “organized argument” is the essential centerpiece of an assurance case. The fundamental strength that assurance cases bring to bear – which is absent in other practices – is that they apply disciplined argumentation to the domain of system assurance. An argument intrinsically includes *claims* and *evidence*. Another key element of our definition is “acceptable.” Precisely defining acceptability in any particular case is usually a thorny task. Assurance cases make it as straightforward as possible by placing acceptability on the table explicitly and consistently. The phrase “for its intended use” makes it clear that the operational scope and bounds must be established for any argument to have real validity. Finally, “specified concerns” are a key element of our definition. Traditionally, safety has been the most prominent concern, but there is also interest in others such as security and dependability (Alexander et al. 2011; Patu 2013; Weinstock et al. 2004). Note also that assurance concerns are often related. That is, a security weakness may also be a safety weakness, and evidence of a system’s correctness may also serve as evidence of its safety. In this manner, assurance cases take the sensible approach of collecting all related concerns into a comprehensive argument.

Other good, but longer, definitions of assurance cases expand on what is required from the argument, what is meant by *system*, and what bounds the assurance case. Many definitions specifically mention *evidence*, which we grant is essential; but again, we consider it intrinsic in *argument*.

At the root, an assurance case is designed to be a direct, specific, structured way to tackle the question, “Are we sufficiently certain that this system is acceptably [safe, secure, etc.]?” It is a collection of information that one would want to have when asked, “Have we thought of everything?” By which one means, everything that we should reasonably consider concerning this system and its application.

In some ways, assurance cases bear similarity to another common context for “cases” and “arguments”: the legal domain. In both contexts, the objective is to assemble convincing evidence concerning things about which 100% certainty is unattainable. In legal environments, lack of certainty comes from incomplete evidence. In the realm of assurance cases, perfect

certainty is less and less attainable as systems become more complex, independent, and integrated into daily life. Nonetheless, pragmatically speaking, both legal and system development processes must be decisive and move forward. In other words, sound judgment is required.

Legal and assurance case contexts differ most significantly in the *role of argumentation*. In legal contexts, argumentation is entirely after-the-fact, and skillful arguments are not expected to be completely objective. The legal system intentionally pits two competing arguments against each other concerning past events. Assurance cases follow a fundamentally different model in this regard. As mentioned above, assurance case development looks forward as well as backward, ideally being integrated with system development from its earliest stages. Furthermore, there are no competing arguments; the measure of an assurance case is its individual adequacy. Assurance cases must be clear and straightforward, characteristics that are enforced by practitioners, evaluators, and regulators.

As noted above, assurance cases are strongly intertwined with safety cases. We will see again and again in this report that many informative precedents relevant to assurance cases are safety cases in form and name. Therefore, to avoid confusion on the point, we are careful to state that for the purposes of this report we consider a safety case to be a subtype of an assurance case. A safety case that otherwise conforms to our definition of an assurance case is a valid assurance case, albeit one that is limited in concern to only safety; while in principle, an assurance case can be concerned with additional related objectives (such as security). The state of the practice is such that there are many more mature examples specific to safety assurance than to wider-ranging system assurance. Consequently, we will often find ourselves discussing safety case examples and resources.

### 3.1 Role in System Development

The act of writing of an assurance case does not, of course, in itself change the system or its acceptability. For it to be effective, it must be developed concurrently with the system. While it is theoretically possible that an assurance case will validly conclude that a system is acceptable as-is, that is rarely the case. More likely, the process of developing an assurance case efficiently directs attention to those areas that require more investigation or improvements. Therefore, the process of developing an assurance case should go hand-in-hand with system development and modification. Thinking that assurance cases are written after the fact (after system development) and simply argue, *post facto*, that what is already done is sufficient demonstrates a fundamental misunderstanding of assurance cases. The failure of the Nimrod safety case (see Section 4.3.3) is a cautionary example of this flawed approach. System developers need to be open to assurance cases calling for system changes; indeed, assurance cases are ineffective otherwise. While assurance cases can be developed late in the process, it is certainly less efficient than integrated development. Ideally, assurance case development occurs in parallel to the greatest extent possible, so that system development can adaptively strengthen the argument as needed – resulting in a legitimately strong argument for the desired property.

It is also important to note that practical regulation using assurance cases includes the specification of a domain-appropriate framework, structure, and process. That is, regulators not only *direct* providers and operators to submit an assurance case, they also *provide* further guidance and specific criteria. In virtually every example reviewed in this document, regulations provide detailed instructions on what constitutes an assurance case for their purposes and how it is to be managed. Where graphical argument forms are used, this often includes a high-level,

partially-completed argument structure. Examples of this include the Eurocontrol Preliminary Safety Cases (such as Eurocontrol 2012). NASA research is demonstrating how DO-178C (RTCA 2011) can be represented as an explicit assurance case with specified high-level argument structures (Holloway 2013). Examples that do not explicitly specify argument structures usually identify required sections, considerations, and processes (such as U.K. Statutory Instruments 2005). Accordingly, one might suggest that half the battle of successful implementation of assurance cases is properly identifying the domain-appropriate argument framework and elements – such as what standards to follow, risk mitigation areas, and aspects to review. A large part of the benefit of assurance cases is in providing a consistency and explicitness at the framework level (in place of a loose assortment of *ad hoc* elements).

### 3.2 Paradigm

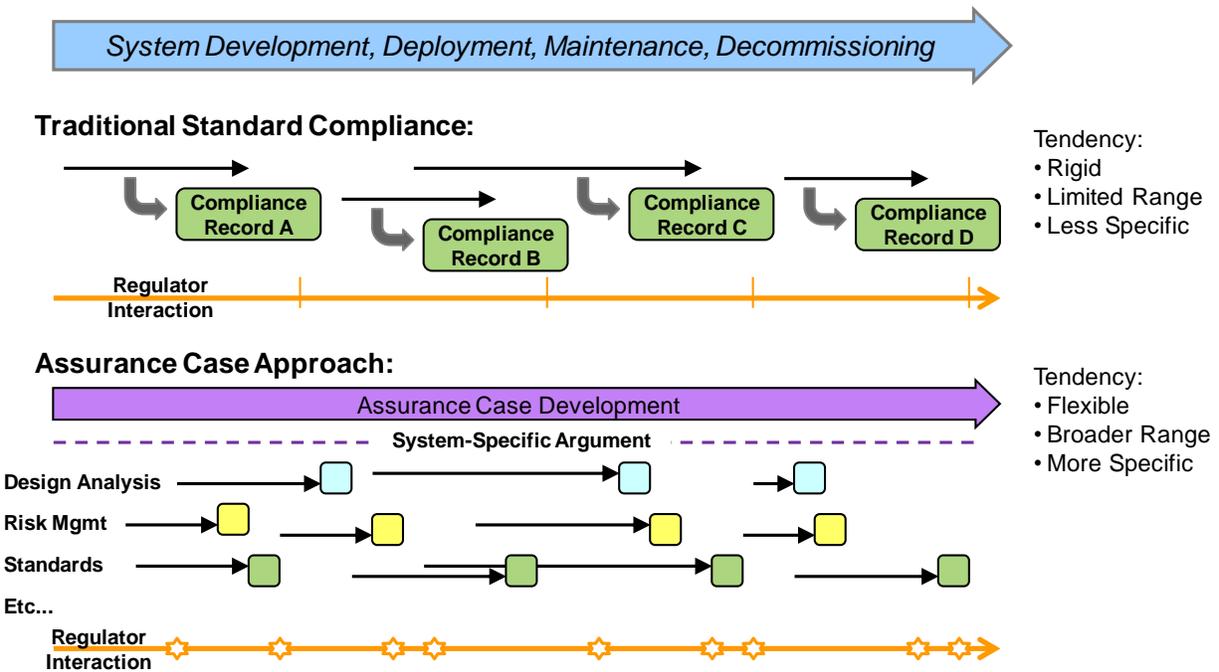
Assurance cases, as mentioned above, seek to answer the question, “Are we sufficiently certain that this system is acceptably [safe, secure, etc.]?” This is, of course, a very old question that systems and safety engineering have sought to answer in increasingly better ways over the history of safety engineering.

The assurance case paradigm can be thought of as the latest in a series of paradigms to be integrated into system development processes. A few other major paradigms are standardization, independent auditing, institutional regulation, and risk management. Synthesized into actual practices, these paradigms mix and merge. For example, standards are often used to encapsulate any and all concerns including those that emerge from other paradigms. There are standards for auditing practices, standards for risk management, standards for institutional processes, standards that require conformance with other standards, and so forth. Similar examples of paradigm mixing include regulators adopting auditing practices and audits of risk management evidence. This blending is to be expected of paradigm synthesis; but it can make it somewhat more complex to discuss, analyze, and improve assurance processes. We will see that assurance cases fit into this mix of paradigms at a range of touch points with standards, regulation, risk management, and so forth.

To provide some initial clarity to how assurance cases differ from other approaches, we will begin with a simple contrast between a purely standards-based approach and an assurance-case-based approach. This is in many ways an oversimplification; nonetheless, standards are perhaps the most pervasive single paradigm in system assurance to date. While conventional standards have indubitably had a beneficial effect on system quality, and they have a rightful place, they tend to be somewhat imprecise and often inefficient (standards and processes can be applied unnecessarily or inappropriately). One of conventional standards’ weaknesses is a “check the box” mentality. Another is that the incurred overhead can be high. Also, even the best general standards can miss something that is necessary in a specific situation.

Assurance cases take a more direct approach: system designers must construct a sufficient argument for desired properties. Note that building an argument inherently calls for relevance to the *particular* system in question. Assurance arguments encourage flexible, context-appropriate consideration of the system which provides a counter-balance to the one-size-fits-all approach of standardization. Adhering to standards may be a portion of the evidence used in an assurance argument, but it is not adequate by itself. Assurance cases push developers and evaluators to focus on and mitigate the weakest links specific to the system in question.

The distinctions between these two paradigms are captured in Figure 2.



**Figure 2: Standards-Only vs. Assurance Case Paradigms**

As shown in Figure 2, assurance cases do not *replace* standards compliance or rigorous processes. Rather, assurance cases organize these practices (and additional measures, as appropriate) into an *explicit* argument, whereas many times these have been used to *implicitly* result in system assurance. An assurance case is, in a sense, an umbrella under which evidence can be properly organized. It facilitates scrutiny. As formulated by one expert, an assurance case is an integration of a goal-based approach (desired system-level goals must be achieved), a rule-based approach (comply with standards), and a risk-informed approach (mitigate hazards) (Bloomfield 2012). The assurance case encompasses all these aspects.

Assurance cases are flexible enough to incorporate all existing assurance activities and artifacts in any particular case. Therefore, developing an assurance case does not necessarily require much additional effort, and doing so offers large potential value. The assurance case organizes and analyzes what is already being done to identify where there might be critical holes or activities that are irrelevant or unnecessary for the assurance argument

As noted earlier, the central feature of the assurance case is that it *presents an organized argument*. As we will see in our examples, the degree of rigor varies from application to application. On the less rigorous end of the spectrum, an assurance case may resemble documentation that has been required in the past using different terminology. System developers and regulators have long required organized documentation to support the belief that a system is ready to move forward. An assurance case of this variety could be nothing more than a template that outlines where to present performance goals, design information, risk mitigation, and so forth. On the more rigorous end of the spectrum, some domains require very structured arguments and artifacts. Developers may be required to explicitly state individual claims, arguments, evidence, assumptions, sub-claims, etc. Full graphical breakdowns, such as represented by Goal Structuring Notation (GSN), may be required. Semi-formal analytical processes may be applied to these artifacts. Though such an assurance case looks different from

traditional documentation, it deals with the same fundamental information and takes the core concept of assurance cases to a new level of rigor.

Why would the assurance case paradigm be a useful one? We submit that it provides an overall construct that allows all stakeholders to understand their necessary and reasonable roles in system assurance. Though the task may be complex and, in some cases, overwhelming in volume, the organizing principles of assurance cases are straightforward: there are system objectives and thresholds that are essential to meet, and each stakeholder must develop a reasonable level of certainty that they are met. This provides perhaps the best known way to connect individual behavior and contributions to critical system qualities in an efficient way. It helps engineers and managers take appropriate responsibility for the system.

The management of responsibility in safety-critical systems is a complex and difficult task because of the different system structures and associated management structures that can arise. Safety is an emergent property at the system level, but the system structure might map into a wide variety of different developers, integrators, and vendors. Any system component could affect the overall system safety, yet the management team associated with that component is unlikely to have the necessary materials to analyze the component unless either: (a) they are also responsible for the entire system, or (b) a very comprehensive and fully documented hazard management approach is employed.

There are real-world examples of how assurance-case-based approaches can manage system-wide safety from an organizational perspective. One example is in use at CGI, a global IT and business services company (Parsons & Hunter 2010). A set of patterns and an elicitation tool are used to document: (a) the types of system structures that can arise, (b) the types of risks associated with the elements of each system structure, and (c) the impact on CGI of the various types of risk and thus the types of engineering and management techniques that are needed. Final responsibility for both system and business risk is accepted by senior management by indicating acceptance of a Safety Briefing Memo. One of the benefits claimed for the approach by CGI is that it allows greater use of “template” safety arguments to assist with creating safety cases.

### 3.3 Brief History

Assurance cases trace their lineage to a series of assurance methods and techniques that are predominantly concerned with system safety. There are clear parallels between the development of system assurance methods and the increasing size and complexity of systems, the increasing impact of failures (including large-scale loss of life), and the development of effective national and global regulatory structures. System safety emerged as a distinct discipline in the 1940's, 1950's, and 1960's, starting with safety concerns in early aircraft manufacturing and culminating with the publication of MIL-STD-882 in 1969, which enshrined concepts such as hazards and risks that remain foundational (Ericson 2006).

A good example of the trends emerging in this time period is the case of the Windscale nuclear reactor in England, pictured in Figure 3. In 1957 a fire broke out and significant radiation was released, constituting a serious threat to public health (32 deaths, hundreds of cancer cases). As a result, regulation of nuclear facilities was instituted, which became one of the seminal instances of safety assurance: “The nuclear certification



**Figure 3: Windscale Reactor**  
("Storm Clouds over Sellafield" by Chris Eaton is licensed under [CC BY-SA 2.0](https://creativecommons.org/licenses/by-sa/2.0/))

process is widely cited as one of the first examples of a safety case regime, although the term safety case was not used at this time” (Kelly 1998).

Safety assurance methods continued to develop from the 1970’s forward, often motivated by disasters such as the Three Mile Island (1972) and Chernobyl (1986) nuclear reactor meltdowns, the Flixborough explosion in 1974, the Seveso chemical release in 1976, the Bhopal toxic gas leak in 1984, the Piper Alpha oil rig fire in 1988, and the Texas City refinery explosion in 2005. Standardization and regulation made great strides during this period, and techniques such as risk analysis and fault modeling matured.

Although the history of assurance is dominated by safety, it is not the only concern represented. For example, ISO/IEC 15408 “Common Criteria for Information Technology Security Evaluation” deals with assurance concerning security. ISO/IEC 15408 has roots going back to the 1990s and earlier.

The term “safety case” was well established by the 1990s, especially in Europe. The concept of *argumentation* in safety cases started gaining attention in that decade (McDermid 1994) and has steadily grown in influence. (Kelly 1998) includes a safety case definition that places argument at its core: “A safety case should communicate a clear, comprehensive and defensible argument that a system is acceptably safe to operate in a particular context.” This definition has proven durable and is echoed in the 2007 definition from the U.K. Ministry of Defence.

Finally, the term “assurance” has been used alongside objectives for safety, security, etc. for a long time, and the term “assurance case” as a generalization of a safety case has become familiar to many practitioners. Certainly, the term was in common use by the mid-2000s (Ankrum 2004, Emmet 2008), and standardized terms were established by ISO/IEC 15026 in 2011 (ISO 2011a).

### 3.4 Assurance Case Properties

Let us return to our simplified definition:

*An assurance case is an organized argument that a system is acceptable for its intended use with respect to specified concerns (such as safety, security, correctness).*

In order to achieve the desired purpose, it is important that an assurance case have certain properties. We introduce these briefly here and more exhaustively in Section 5 (on the subject of evaluation).

**Compelling:** The argument must reasonably convince an objective observer.

**Valid:** The argument must be a correct representation of the rationale for belief.

**Complete:** The assurance case must comprehensively document its argument and evidence.

**Transparent/Readable:** An assurance case must facilitate scrutiny by any stakeholder or interested party. Therefore, it must be readable and sufficiently transparent.

**Certifiable:** In many cases assurance cases must facilitate the mechanisms of approval.

**Facilitate System Development:** An assurance case and associated processes should be an asset to developers, not a burden.

**Modular:** Assurance cases are generally large, complex documents. Wherever possible, a “plug and socket” approach should be employed to make scope and management more tractable.

**Extensible:** Assurance cases need to be designed with future changes in mind (operating conditions, enhancements, and the like).

### 3.5 Assurance Case Stakeholders

Certain key roles have emerged in assurance case processes. These are summarized here and discussed in greater detail in Section 5.

**Developers:** Those responsible for designing and implementing the system in question.

**Regulators:** Those who have deployment authority based on the assurance case. Regulators often represent the public interest.

**Operators:** Those responsible for the installing and operating of the system in a manner consistent with the assurance case.

**General Public:** To some extent, the general public may be provided some access to an assurance case – especially to evaluate the implicit residual risk to them.

### 3.6 Terminology

The terms and definitions introduced in this section are used somewhat consistently by many sources in the assurance cases domain, including:

- regulatory bodies such as the U.K.’s Health and Safety Executive (HSE), Eurocontrol, and the U.K.’s Ministry of Defense (MoD);
- the GSN community;
- the Software Engineering Institute (SEI);
- the International Standards Organization (ISO); and
- the Object Management Group (OMG).

Where particular groups differ on their usage of terminology or introduce new terms that are not generally accepted, they are noted. One high-level resource that covers much of the generally-accepted terminology (with the caveat that it is not uniformly precise) is ISO/IEC 15026-2:2011, “Systems and software engineering – Systems and software assurance – Part 2: Assurance case” (International Organization for Standardization 2011a).

#### 3.6.1 Argument

The prominence of *argument* is important because it reflects the assurance case paradigm toward achieving safety, security, or some other desired property. An assurance case presents an argument to respond to the query, “Why should we believe this system is [safe, secure, etc.]?” By contrast, many alternative approaches seek to achieve safety, security, etc. by other means, such as adhering to certain best practices, adopting rigorous processes (reviews, documentation, etc.), or some other improvements to *how* the system is developed. Assurance cases augment and focus these approaches by fitting them into a specific argument concerning the desired property.

A valid *argument* must include specific *claims* and *evidence* (see following sections). On this point, however, we note that there is *de facto* double-usage of the term. The first usage of “argument” is in the sense we have used it thus far in this report; that is, the argument is what presents the whole case. The second usage associates “argument” with the logic that connects the claims and the evidence, which implies that claims, arguments, and evidence are all at the same semantic level. This implication is obvious, for example, in the Claims, Argument, Evidence (CAE) graphical format, which we will examine in Section 3.7.2. We do not hold this second

usage to be technically accurate; *argument* should be a higher-level term than *claims* and *evidence*. Better terms for the links between claims and evidence are *reasons* or *warrants*, as established by (Toulmin 1958) and described in section 3.7.4.) Still, as a practical matter, we note that the reader will encounter both variants in this document and in the field.

Some sources (UK Civil Aviation Authority 2014), introduce the concept of “primary arguments” and “secondary arguments.” When a sufficiently critical level of assurance is required, the primary argument represents the most straightforward way of establishing that a requirement is met. The secondary argument represents another *independent* way to establish that the requirement is met. This approach protects against possible weaknesses that are difficult to detect in the primary argument. The independence of the two arguments could be based on independent practitioners, independent evidence, or both. For example, concerning software safety requirements, the primary argument could be based on source code analysis; and the secondary argument could be based on stress testing in the field.

Example high-level arguments (from Adelard 1998) include:

*“Hardware reliability analysis (redundancy + monitor + self-tests) [and] No systematic faults (sub-claim C.NO-FLT) [limit hardware failures to less than  $10^{-3}$ ]”*

*“ $10^4$  reliability tests using representative trips without failure give more than 99% confidence in a PFD of  $10^{-3}$ ”*

*“Compiler, loader and processor flaws protected by the reversible computing technique”*

### 3.6.2 Claim

(UK Civil Aviation Authority 2014) gives this definition: “A claim is a simple statement typically used to indicate that a safety objective or requirement has been met as demonstrated by the associated argument and evidence.” Further, “A claim may be sub-divided into a number of smaller sub-claims which when combined meet the overall higher-level claim.”

Example claims include (GSN Committee 2011):

*“Control System is acceptably safe to operate”*

*“All identified hazards have been eliminated or sufficiently mitigated”*

*“System X can tolerate single component failures”*

### 3.6.3 Evidence

As an example of the role of evidence in an assurance framework, (UK Civil Aviation Authority 2014) specifies the following types of evidence for software safety assurance:

- Test evidence (activities that exercise the object code in a controlled environment),
- Field experience (documentation from operation, e.g. prototype or similar systems), and
- Analytic evidence (examination of the design, e.g. formal proofs).

(Object Management Group 2013) provides the following examples of evidence:

*“Fault tree analysis cutsets for event [x]”*

*“Black Box Test Results”*

(UK Civil Aviation Authority 2014) also defines the important concepts of “direct evidence” and “backing evidence.” Direct evidence consists of the records, data, or other artifacts that relate directly to supporting the argument. Backing evidence addresses the question, “Is the direct evidence trustworthy?” For example, the direct evidence of test records might be presented with backing evidence about audits, institutional processes (such as ISO 9001), and version control systems.

### 3.6.4 Goals

Assurance cases are often explicitly linked to goals, which are a form of high-level requirements. A goal in the context of an assurance case is often stated as a proposition (or *claim*) that has some relevance to the system of interest. Though goals and claims are often merged, there is a shade of distinction between them. One usually encounters goals in the context of system performance, whereas one usually encounters claims in the context of a documented argument.

Furthermore, assurance arguments are frequently organized using a goal structure. In a goal structure, belief in a goal is at least partly inferred from a set of lower-level goals, referred to as sub-goals, in which belief is already established. This decomposition is applied recursively until belief in sub-goals is inferred from evidence. This argument structure parallels the form of argument in deductive logic in which the truth of a conclusion is inferred using the rules of logic from a set of premises that are taken to be true.

Appropriate goals must be identified and established before arguments can be effectively constructed. As shown in Figure 4, goals are typically established at the highest level and flowed down to lower levels according to areas of concern.



**Figure 4: Goal Decomposition**

Goals tie in very naturally to existing practices that many systems developers already use. That is, requirement verification already typically links test information (a form of evidence) to requirements (a form of goal), and it is conceptually straightforward to take this process up to the next level in an explicit assurance argument.

### 3.6.5 Risk Management

Many assurance case instances explicitly incorporate risk management. This will be demonstrated by many examples in Section 4.

### 3.6.6 Levels of Rigor

In numerous examples, assurance case regimes describe and permit different levels of rigor depending on system criticality. This is common as a concept, though far from universal, with specific definitions varying to suit the example. The concept establishes that, in less critical systems, not only is it easier to meet the requirements, but it is not necessary to formulate as

extensive assurance cases. In highly critical systems, not only are the requirements more difficult to meet, but argumentation also must be commensurately more rigorous.

For example, DO-178B defines five “software levels” according to the effect of associated failures, and applies objectives more or less stringently depending on the level (Wlad 2006). Another example of this is “Assurance Evidence Levels” (AELs) as described in (UK Civil Aviation Authority 2014). All AELs call for the identification of hazardous failure modes in the requirements. AELs 2 and above require identification of hazardous failure modes in the internal design as well, and AELs 4 and above must also do the same in software source code.

### **3.6.7 Evaluation**

Inevitably, any assurance case is only as good as its evaluation. Can evaluation find the defects in an assurance case? A true answer is “yes and no.” “Yes” because, practically speaking, evaluation is very effective at finding the most important defects. “No” because, at the fundamental level, assurance cases, as currently formulated, are not fully deductive. There is no way to guarantee that every defect is found in the same manner as, for example, formal methods applied to a design may detect all of the logic defects in the design given a correct formal specification. Such an approach is currently impractical in nearly all cases.

We cover the evaluation topic extensively in Section 5. Here we introduce several evaluation terms and concepts.

It is impossible to remove expert judgment from the process of evaluating assurance cases. The complexity of modern systems and variability of critical factors means that, in all but trivial systems, assurance information that is objectively exhaustive is unattainable. Therefore, any evaluation processes must incorporate, at a foundational level, a reliance on sound judgment from qualified experts. Having said this, it is possible to incorporate structural analysis and even formal methods to suitable portions of the evaluation process. Again, we will cover this in detail in Section 5.

There are a few common terms in evaluation which we will introduce here:

- ALARP: As Low As Reasonably Practicable (usually referring to risk),
- ASARP: As Safe As Reasonably Practicable, and
- TLS: Target Level of Safety.

## **3.7 Notations**

### **3.7.1 Goal Structured Notation (GSN)**

GSN is a common graphical format used for safety cases; for example, a variant of it is used in Eurocontrol Preliminary Safety Cases (see example in Section 4). The primary graphical elements of GSN are (Kelly & Weaver 2004; GSN Committee 2011) listed in Table 2.

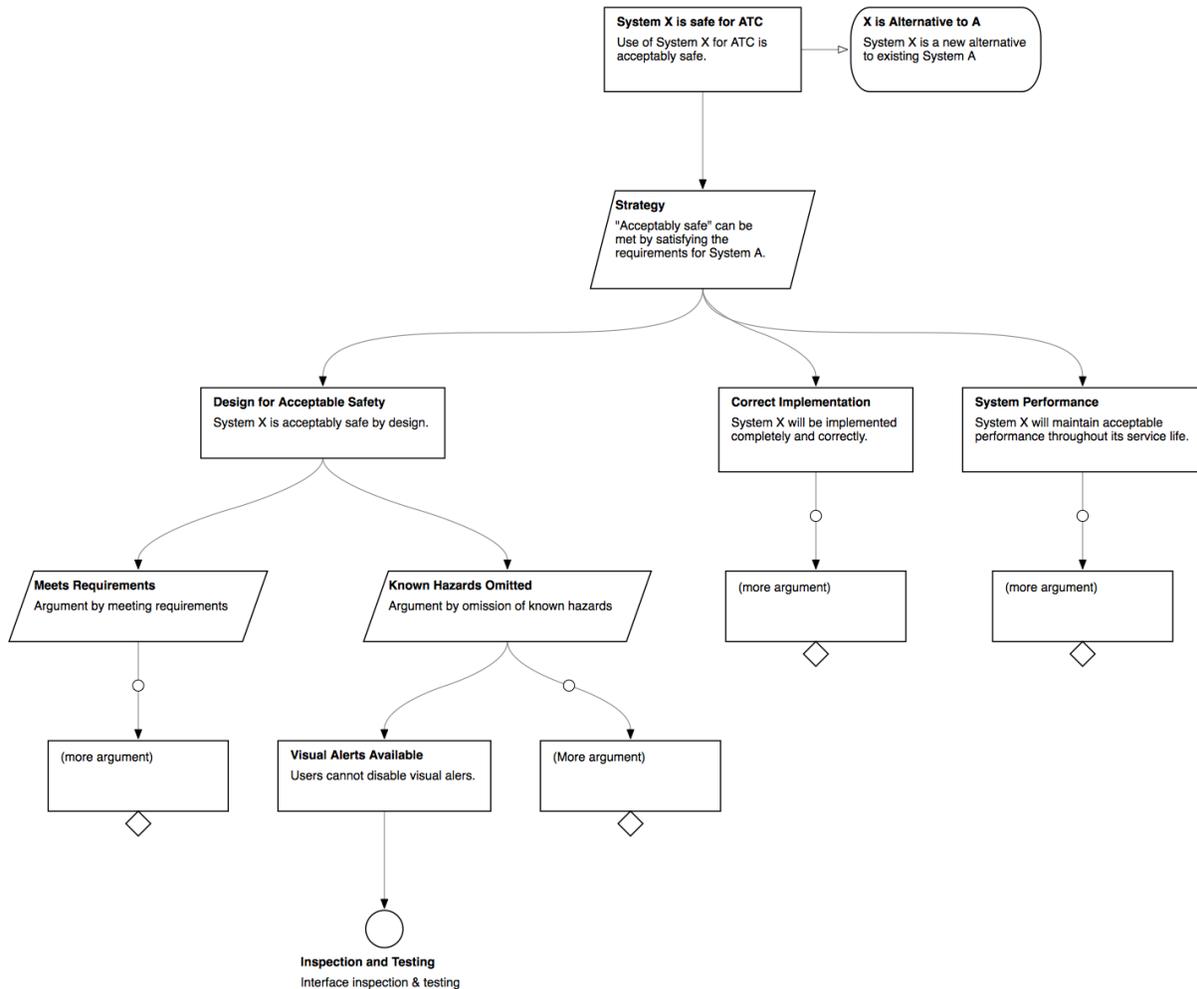
To the uninitiated, GSN’s fitness to represent arguments is not necessarily self-explanatory (for example, how does a “goal” relate to an “argument”?). However, the GSN Community Standard (GSN Committee 2011) provides a fairly thorough correlation, the major points of which are included in italics in Table 3. The primary concept behind GSN is *decomposition*: breaking the goals of the argument down into progressively more specific sub-goals until the sub-goals can be inferred from the indicated evidence. “Strategy,” “context,” “assumption,” and “justification” elements are used to provide further explanation and information.

**Table 2: GSN Graphical Elements**

	Goal ( <i>Claim</i> )
	Solution ( <i>Evidence</i> )
	Strategy ( <i>reasoning</i> )
	Context
	Assumption
	Justification
	"Supported by"
	"In Context of"
	Undeveloped (identified but not complete)

The argument embodied by a GSN diagram is intrinsic; that is, it is expressed by the structure and content of the entire diagram. The top-level goal is generally a fundamental claim to be argued. The argument itself is expressed by the structure below it. The satisfaction of any goal is shown by: (a) connecting it to evidence (solution) that clearly establishes it, or (b) satisfying its sub-goals. In this manner, a goal is decomposed to organize it into parts that are established by evidence. As new evidence becomes available, it is integrated into the diagram at the appropriate level of goal decomposition. If satisfying a goal proves unachievable, either the goals or solutions must be revised.

A simple example is provided in Figure 5 (loosely based on the 2012 Eurocontrol WAM-NRA Preliminary Safety Case).



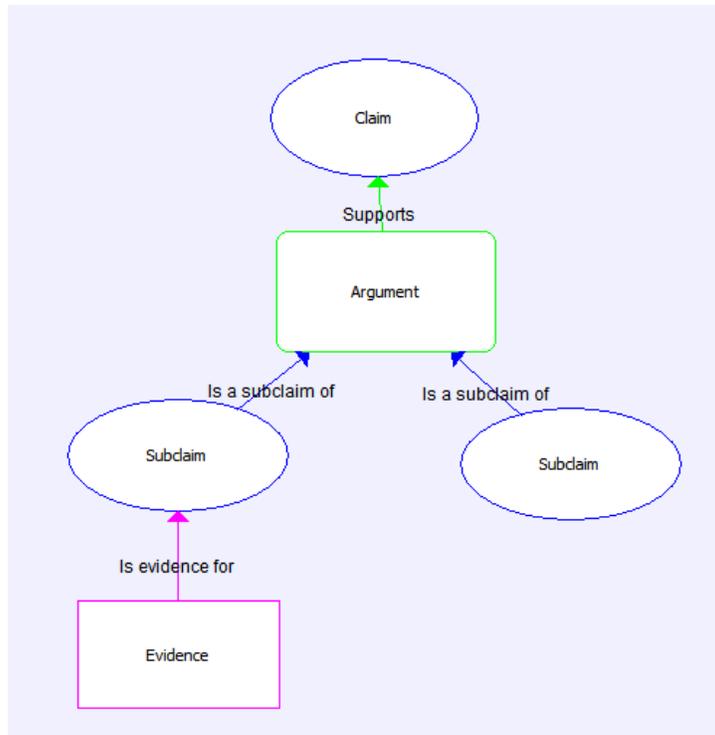
**Figure 5: Simple GSN Example (Partial)**

Many organizations use variations on GSN. For example, Eurocontrol’s preliminary safety cases:

- systematically call goals “arguments” (which somewhat confuses the GSN paradigm),
- add “criteria” entity (variation on goal), and
- add “constraint” entity (variation on context).

### 3.7.2 Claims, Arguments, and Evidence (CAE) Format

CAE was developed by Adelard, a U.K. company that is extensively involved in safety and assurance cases. It is a straightforward graphical format; the excerpts shown in Figures 6 and 7 from <http://www.adelard.com/asce/choosing-asce/cae.html> present the constituent elements.



**Figure 6: CAE Structure**

<p><b>Claim</b> - a statement asserted within the argument that can be assessed to be true or false, e.g.</p> <ul style="list-style-type: none"> <li>• "System X is adequately safe during the shut down phase of operation"</li> <li>• "Unit testing is complete"</li> <li>• "All identified hazards are adequately managed in the hazard log"</li> <li>• "Design personnel are suitably qualified"</li> <li>• "Training materials have been reviewed"</li> </ul>	<p>Each claim is supported by a number of sub claims, arguments or evidence.</p> <p>The claim may contain additional contextual material, for example explaining terms used and scope.</p> <p>ASCE contains tools for editing rich narrative at any node in the safety case</p>
<p><b>Argument</b> - a description of the argument approach presented in support of a claim. e.g.:</p> <ul style="list-style-type: none"> <li>• "argue by considering safety of subsystems"</li> <li>• "because wiring conforms to relevant electrical standards"</li> </ul>	<p>This element is optional, but often it is good practice to include to explain the approach to satisfying the parent claim</p> <p>If the approach to supporting a claim is straightforward or well understood by the intended audience, it is permissible to simply link directly from the supporting claim.</p>
<p><b>Evidence</b> - a reference to the evidence being presented in support of the claim or argument, e.g.</p> <ul style="list-style-type: none"> <li>• "the hardware reliability analysis report"</li> <li>• "interlock design documentation"</li> </ul>	<p>Usually the evidence node will summarise and link out to the relevant report containing the evidence</p> <p>ASCE contains a number of tools to support:</p> <ul style="list-style-type: none"> <li>• linking to, management and tracking of changes in the underlying evidence.</li> </ul>

**Figure 7: CAE Definitions**

Adelard has also been active in the development of the Argumentation Metamodel (ARM) and related standards (see section 3.7.3). CAE is compatible with these syntactic standards.

### 3.7.3 *OMG Structured Assurance Case Metamodel (SACM)*

The Object Management Group (OMG) is an organization that develops specifications in a number of areas. Particular specifications for which the OMG is well known include CORBA, UML, SysML, and XML.

Working with industry and academia, the OMG has developed the Structured Assurance Case Metamodel (Object Management Group 2013). The specification defines a metamodel for representing structured assurance cases. Conformance with the metamodel is designed to facilitate exchange of assurance case artifacts.

The metamodel includes several elements, but there are two major elements:

- 1) the Argumentation Metamodel, and
- 2) the Evidence Metamodel.

Each of these two elements of the specification defines a class hierarchy in UML for the various items in the associated element. The UML definition shows the inheritance and inclusion relationships between the various classes.

The terminology of evidence in an assurance case is defined in an annex of the SACM using the OMG's Semantics of Business Vocabularies and Business Rules (SBVR) Specification.

The SACM specification further defines XMI specifications for the various elements. The complete specification definition allows any tool designed to work with assurance cases to use the same structure and exchange assurance cases reliably.

### 3.7.4 *Textual Forms*

GSN and CAE are fairly recent developments in the field of safety analysis and documentation. SACM is recent as well, and technically it is a text form itself. However, its primary concern is ontology rather than the form in which an argument is expressed. Prior to these recent forms, textual forms were the *de facto* norm for assurance arguments.

Textual forms can vary in structure and rigor. There is a vast body of historical work in jurisprudence and philosophy that embodies critical arguments in text form, so this form is not to be discounted (Holloway 2008). One example of a loosely-structured safety case (at the textual level) is that of the Opalinus Clay radioactive waste storage facility. Upon analysis (Greenwell et al. 2006) describe this as “bulleted natural language with major safety claims enumerated as subsections accompanied by their corresponding arguments.” They further note that it is impressively compelling and apparently free of fallacies.

Stephen Toulmin famously created an argument model that imposes some structure on textual forms (Toulmin 1958). Translated to the terms we've introduced so far, Toulmin's model consists of the following parts:

- claims,
- evidence (or “data”),
- warrants (or “reasons”: logic connecting evidence and claims) with backing (further support),
- qualifiers, and
- rebuttals (or “counter-arguments”).

Although the Toulmin approach takes it for granted that arguments will be in textual forms, the above constituent parts can be deduced from the text in a well-structured argument. Toulmin's structure is shown in

Figure 8 (including a well-known example from Toulmin's seminal 1958 book).

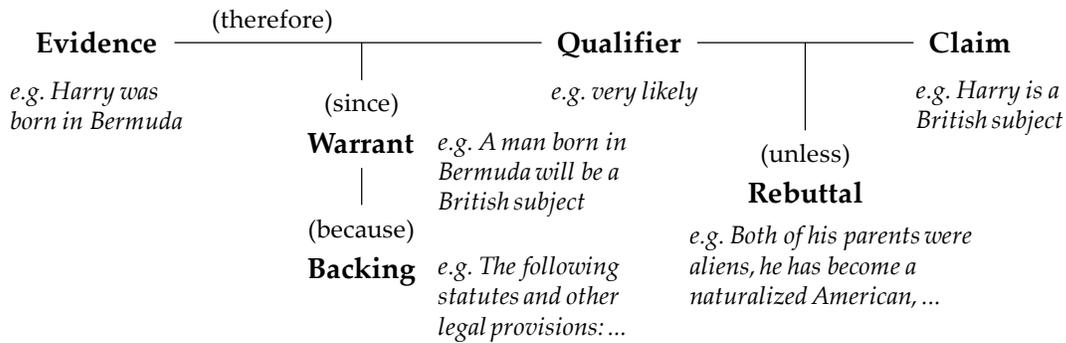


Figure 8: Example of Toulmin Argument

The majority of examples in Section 4 use textual forms of assurance cases. The U.K. safety case tradition does not emphasize graphical forms; consequently, cases in this tradition are typically expressed in various forms of structured text. It is also worth noting that graphical argument forms such as GSN are easily translated to textual forms such as structured outlines (Holloway 2008); so it could be said that assurance case structure is developing toward a consistent underlying model which can be viewed in a number of ways, including graphs and text. Here again we note SACM, which certainly aims to play an important role in such an underlying syntactic model.

### 3.8 Standards and Assurance Cases

The existence of a wide variety of standards in all areas of assurance raises concerns about the role and even the need for assurance cases. Conformance to standards has been the means by which essentially all safety-critical industries have been regulated worldwide for decades. For example, standards such as ARP 4754a (SAE 2010) and ARP 4761 (SAE 1996) are in routine use for systems engineering in the aviation industry, and the use of DO-178B for software assurance dates back to 1992 (RTCA 1992).

Many standards are prepared by committees of expert volunteers, and a typical standard embodies the knowledge and experience of those volunteers. Though standards are often criticized in various ways, the fact that standards document the composite knowledge of many experts is a major benefit. Advantages of standards in the field of assurance can be summarized as:

- **Technology completeness.**

The technology stated explicitly in standards is often quite comprehensive.

- **Subject to scrutiny.**

The development and use of a standard frequently facilitates extensive examination of the content. Maintenance of the standard permits clarification and correction.

- **Established technical level.**

An entity deemed conformant with a standard meets an established technical level with a high (although unknown) probability.

With these advantages, what are the disadvantages of standards? Some disadvantages of standards can be summarized as:

- **Unknown assurance performance.**

Despite the incorporation of proven techniques and technologies, the results of applying those techniques and technologies in the form required for conformance with a standard is generally unknown. In other words, conformance with a given standard does not necessarily ensure that a system meets a prescribed assurance goal.

- **Lack of flexibility.**

Conformance with a standard usually means conformance with all of the provisions of the standard irrespective of whether those provisions are suitable for the subject system or adequate for the subject system. Although some standards incorporate provisions to adjust the definition of conformance so as to allow variation, such provisions tend to be poorly defined and are rarely used.

- **Development cost.**

The cost of developing a standard is usually born by the volunteers that develop the standard. The cost is usually considerable, and this limits volunteers to interested parties who have the assets necessary to support the activity.

- **Maintenance cost.**

Standards are rarely if ever assessed prior to deployment. Usage of a standard frequently reveals defects or omissions that need to be addressed. In addition, changing technology frequently imposes the need to update the standard to incorporate technical advances.

Given the availability of standards and their established track record, what motivates the need for assurance cases? The key to answering this question lies in the first disadvantage of standards listed above. A standard is essentially a statement of requirements irrespective of whether the standard prescribes objectives or techniques. Although an implicit rationale exists for the stated requirements, the rationale is rarely stated, and the developers of the standard might not be aware that a rationale is motivating decisions about the content of a standard.

Importantly, the modern view is that standards and assurance cases are complementary not competing technologies. As noted in Section 2, the significant advance that results from the introduction of an assurance case is that the rationale for belief in assurance of a system property is stated explicitly. Where assurance cases have come into practical use, conformance with standards is not the essential property that is required by regulators. Rather, the provision of an assurance case that embodies a compelling, comprehensive and valid argument is the property regulators require.

Freed from rigorous and complete conformance with standards as a regulatory requirement, standards can be used as a source of technical insight and guidance. Conformance with a specific element of a relevant standard can be used to guide the preparation of evidence for subsequent use in an assurance case.

### 3.9 A Classification Scheme for Assurance Cases

In surveying assurance cases in various domains, we find that there are several key characteristics that help to understand and characterize the range of examples. These are *rigor in argument*, *rigor in evidence*, and *flexibility in process*.

***Rigor in argument*** concerns the most active dimension of assurance case evolution: structured argumentation. In fact, it is the inclusion of organized, intentional argumentation that is a key defining characteristic of modern assurance cases. We use three levels for this characteristic:

- Implicit: the argument is not clearly stated,
- Explicit: the argument is stated but in an unstructured (narrative prose) way, and
- Structured: the argument is presented using a defined format (argument model).

Expert consensus is that examples which feature implicit argumentation should not generally be called assurance cases at all. We include some of them in our pool of examples anyway, because their users apply the label assurance (or safety) cases to them; and, therefore, they serve to illustrate the range of usage of the terms. Also, the implicit argument examples we include are generally noteworthy for other. However, we will make a point to caveat such examples.

***Rigor in evidence*** refers to an earlier movement in the history of assurance cases (and safety cases and related regulatory processes) toward requiring more extensive documentation to substantiate compliance. This dimension often correlates to compliance standards that have been developed to regulate a particular field. The initial achievement of compliance standards is specifying what constitutes acceptable behavior (or best practices); a following achievement is specifying what evidence is required to show that the standards have been met. We use three levels for this characteristic:

- Implicit: compliance is required, but specific documented evidence is not required,
- Explicit: evidence is captured with minimal formatting (for example, text records), and
- Structured: evidence is organized into a specified format (for example, data model).

As in argument rigor, although less clearly, it could be said that assurance cases with only implicit evidence do not really qualify to be called assurance cases. This is especially true from the standpoint that without evidence, there is no meaningful argument. Therefore, we also caveat this category as being more accurately identified with “so-called” assurance cases.

***Flexibility in process*** characterizes another important dimension in the evolution of assurance cases. An early movement in the effort to improve safety was for regulators to become increasingly *prescriptive* in their compliance requirements. In other words, to state it strongly, compliance was achieved by doing specific things a specific way, and no other ways were acceptable. This approach does have some desirable advantages, such as increasing safety predictability and streamlining practices across an industry. However, it also runs into distinct disadvantages. The most important disadvantage is that, as systems and processes become more complex, it becomes virtually impossible to prescribe safe practices that cover every potentiality. Safety “holes” emerge that may be rare but can be disastrous. Attempts to plug these holes aggravate another problem with high prescription: the regulated industry becomes unacceptably constrained by regulatory overhead and inflexibility. Also, compliance can become mindless and outsourced to box-checkers, without real safety awareness.

In response to these downsides, there began a shift toward *goal-orientation* (safety outcomes) which, for example, strengthens the “culture of safety” (so that behavior can be optimized on the

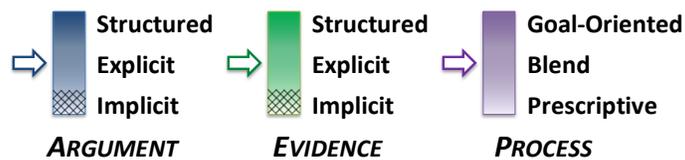
fly in dangerous situations). When “one size fits all” becomes too onerous, there are gains to be found by relaxing prescription and engaging in intelligent tailoring.

We use three levels for this characteristic:

- Prescriptive: regulation is *mostly* dominated by specifics that apply to all,
- Blend: incorporates a fairly even mix of prescription and flexibility, and
- Goal-Oriented: regulation is *mostly* dominated by general goals and compliance adaptability.

Finally, we note that there is generally a synergy between increasing argument rigor and goal-oriented compliance – both of which are positive trends in the domain of assurance cases. Structured arguments naturally allow for a range of ways to make the case (flexibility) while ensuring that the argument and supporting evidence are clearly presented. This, in turn, facilitates scrutiny and approval with confidence.

For each assurance case example, we describe the three characteristics above graphically as shown in Figure 9. The arrows indicate where on the three scales a given example falls.



**Figure 9: Assurance Case Examples Graphical Characterization**

These scales are organized so that the upward direction corresponds with progress toward more advanced, modern assurance cases. For argument and evidence, this means additional rigor and structure. For prescriptive vs. goal-oriented, this means movement toward goal orientation. While these trend indications are significant, it is important to note that many properties of individual examples are not captured by these few characteristics. Therefore, an example that is graphically represented as “structured – structured – goal-oriented” is not necessarily “good”; it could have serious flaws in other ways. Similarly, an “implicit – implicit – prescriptive” example is not necessarily “bad”; it might function quite adequately in its particular niche.

As mentioned above, the “implicit” levels of argument and evidence rigor are specially marked to indicate that examples in these categories cannot be called proper assurance cases. However, we do have some examples in these categories because they may be called “assurance cases” (however improperly), and they may be important to include in our survey for other reasons.

We will use the above classification scheme throughout the next section, which is the central section of this report: assurance case examples.

## 4. Example Uses of Assurance Cases

Our goal in this section is to compile a wide-ranging list of the existing uses of assurance cases on real projects worldwide. A tabular summary is provided in Table 3. Details for each example are provided in the following subsections.

**Table 3: Summary of Assurance Case Examples**

Name	Domain	Organizations*	Standards / Regulations*	Notations*	Classification†
Offshore Oil and Gas	Energy	U.K. HSE Norway PSA U.S. API & COS	U.K. SI 2005 No. 3117 API RP 75	Textual	ESB EEG IEP
GDA of Nuclear Plants	Energy	U.K. ONR & EA	ONR-GDA-GD-001	Textual	EEP
CAP 670 & 760	Aviation Infrastructure	U.K. CAA	CAP 670 CAP 760	Textual	SSB
WAM Preliminary Safety Case	Aviation Infrastructure	Eurocontrol	WAM PSC	Textual GSN	SEG
Risk-Informed Safety Case	Aerospace Vehicles	NASA Office of Safety and Mission Assurance	NASA System Safety Handbook Vol. 1	Textual Graphical	SSG
Triton UAS	Aerospace Vehicles	U.S. Navy	NAVAIR INST 13034.4	GSN	SSB
RAF Nimrod	Aerospace Vehicles	U.K. RAF	U.K. MoD JSP318B U.K. Defence Std 00-56 U.K. MoD BP1201	Textual	IEG
European Rail SMS	Railways	European Railway Agency	E.U. Directives 2001/14/EC, 2004/49/EC, 2008/57/EC	Textual	ISP
U.K. Rail Safety Cases	Railways	U.K. HSE	(not known / obsolete)	Textual	ISP
ISO 26262	Automobiles	ISO	ISO 26262	Textual	EEP
Infusion Pumps	Medical Devices	U.S. FDA	FDA 510(k)	Textual GSN	SEB
Generic Pacemaker Assurance Case	Medical Devices	University of Pennsylvania	(none)	GSN	SEG

\* not exhaustive

† see section 3.9

The information shown in Table 3 (and in following subsections) is based on literature research. The way in which we characterize assurance cases in these examples is our own, and may or may not reflect the view of the issuing organizations or other parties in the domain.

## 4.1 Energy Sector

The energy sector has been particularly productive in safety case and assurance case innovations. Reasons for this may include the following characteristics:

- Large, long-term infrastructure systems,
- Impact on public health and safety, and
- Significant employment sector, that is, ongoing risk exposure of employees.

### 4.1.1 Offshore Oil and Gas

The offshore oil and gas industry has been the context for some noteworthy recent history on the development of safety cases; and, more broadly, approaches to safety in large, complex, risk-intensive systems. The Piper Alpha disaster in 1988 was a major stimulus for regulatory change in the U.K. for offshore oil platforms. The Deepwater Horizon catastrophe in the Gulf of Mexico (2010) again brought this industry to the forefront of much debate.

The Transportation Review Board (TRB) issued a thorough Special Report on offshore oil and gas regulation in 2012 (Transportation Research Board of the National Academies (2012)). While this section draws on many sources, it uses the TRB Special Report as a centerpiece, and highlights the same international examples. Consequently, the subdivisions in this section focus on the U.K., Norway, and the U.S. These three countries have been compared and contrasted by additional sources (Baram 2010 and Engen 2012).

#### 4.1.1.1 Synopsis

##### U.K.

The defining incident for an assurance-case-type approach to safety for U.K. oil platforms was the Piper Alpha disaster in 1988. With 167 workers perishing within two hours (there were only 61 survivors), “it remains the worst disaster in the history of the oil and gas industry” (Turner 2013).

As a result of the disaster, Lord Cullen was called upon to conduct an inquiry and make recommendations. Certain technical recommendations were naturally expected; however, the Cullen Report (Cullen 1990) went much further and came to embody a major shift in safety regulation. The enquiry quickly determined that avoiding the same, specific failure mode in the future would be unsatisfactory; in Lord Cullen’s words, “Major accidents are relatively rare – history does not repeat itself in the same fashion” (Jeffrey 2013). Therefore, attention broadened to the management of safety in various forms. For example, “training, monitoring and auditing had been poor” and “there had not been an adequate assessment of the major hazards and methods for controlling them.” The conclusions and recommendations cut to the core methods of safety regulation: “The Cullen Report also did away with traditional prescriptive safety legislation in favor of a more progressive 'goal-setting' model” (Turner 2013).

Following the Cullen Report, a wide range of reforms was instituted in the U.K. The Health and Safety Executive (HSE) was tasked to be the primary regulatory agency, and a key legal shift went into effect in 1992 with the passage of “Offshore Installations (Safety Case) Regulations” (current version: 2005). We will look more closely at these in the following sections.

## Norway

Norway's offshore oil and gas regulation initially featured very comprehensive, strict, and specific oversight. However, this did not produce the desired outcomes: "experience with this approach, including several blowouts and several high-profile tragedies—most notably the loss of 123 lives on the *Alexander L. Kielland*—was not as desired" (TRB 2012). Specific criticisms included a passive attitude on the part of regulated companies and a tendency to find ways to meet the letter of the law rather than ensure real safety.

Consequently, Norway's Petroleum Safety Authority (PSA) shifted "from prescriptive to performance-based regulation," which transferred greater responsibility (and greater latitude) to regulated companies for the satisfaction of broader safety objectives. "The term 'inspection' was replaced with the preferred term 'supervision,' and 'approvals' was replaced with 'consents'." (TRB 2012) The main features of the current Norwegian approach include collaboration (with operators, unions, etc.) to improve safety, flexibility in meeting safety goals, proactive risk management, and expert review (PSA 2013, Engen 2012).

## U.S.

The predominant regulatory framework in the U.S. is the Outer Continental Shelf Lands Act (OCSLA), initially enacted in 1953 and actively amended ever since. Until 2010, the Minerals Management Service (MMS) was the U.S. agency responsible for offshore oil and gas regulation in conjunction with its role administering leases. However, the Coast Guard was given the enforcement role for "workplace safety regulation" including scheduled and unscheduled inspections and investigations related to death, serious injury, fires, and "major" spills (Baram 2011). Note that this conflates personal (small-scale) safety with process (large-scale) safety, which the TRB notes do not necessarily correlate (TRB 2012, pg. 30).

A significant component of the safety framework for offshore oil and gas in the U.S. has historically been voluntary industry adoption of safe practices, for example the Recommended Practices from the American Petroleum Institute (API) (TRB 2012). This trend has continued with the recent establishment of the Center for Offshore Safety (COS).

One aspect of the U.S. system that has drawn criticism is its tension between public and private interests, with the government expected to strike a difficult balance between. "...industry and regulators are viewed as adversaries because companies are expected to be opportunistic and agencies are expected to prescribe and police their behavior, where companies lobby against new 'burdensome' regulations and agencies are under constant pressure from industry, states, Congress, and the President to be accommodating to business and other economic interests yet somehow prevent harms." (Baram 2011)

The *Deepwater Horizon* disaster in 2010 prompted a flurry of regulatory reform. MMS was reorganized. Currently, the predominant regulatory agency is the Bureau of Safety and Environmental Enforcement (BSEE). (Note that some current initiatives tie back to an interim agency, the Bureau of Ocean Energy Management, Regulation and Enforcement – BOEMRE.)



**Figure 10: Deepwater Horizon**  
(Photo by US Coast Guard)

Part of the public debate that followed *Deepwater Horizon* included consideration of the safety-case-based approach typified by the U.K. (and the flexible-but-intensive approach typified by Norway). We will look briefly at this and current regulation in the sections below.

#### 4.1.1.2 *Role of Assurance Case*

##### **U.K.**

Safety cases play a very prominent role in the U.K.’s oversight of offshore oil and gas activities; in fact, it could be said to be one of the defining examples of safety cases. One of the key legal elements is U.K. Statutory Instrument (SI) 2005 No. 3117, “The Offshore Installations (Safety Case) Regulations 2005,” (United Kingdom 2005) which requires that operators submit a safety case to HSE at least 6 months before expected operation of a facility. Operation may not commence until the safety case is accepted. The safety case must be revised when appropriate or when directed, and it must be reviewed every 5 years or when directed.

##### **Norway**

The Norwegian system does not explicitly require the creation of an instrument called a “safety case” or “assurance case.” It does require the creation of a safety management process and emphasizes the management of risks (see PSA 2013) and features a system of frequent audits that are designed to maximize partnership between operators, regulators, unions, etc. (TRB 2012, Engen 2013). The effect of this does bear similarity to the aim of safety cases – to establish a structured, flexible mechanism for exploring safety sufficiency. It is also noteworthy that the Norwegian regulatory functions are relatively well-resourced (Leveson 2011).

##### **U.S.**

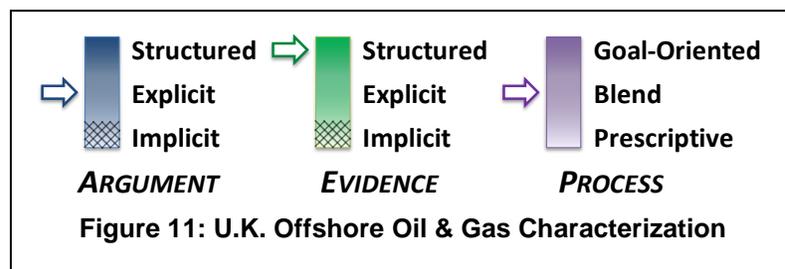
Current U.S. offshore drilling regulation does not *require* anything like a safety case or assurance case; the closest guidance is voluntary compliance with API Recommended Practice (RP) 75, “Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities” (American Petroleum Institute 2004). Formulation of this RP goes back to 1993. In line with this, Safety and Environmental Management Systems (SEMS) is the subject of the TRB report. Similar in principle to reforms in Norway and elsewhere, “SEMS is a safety management system (SMS) aimed at shifting from a completely prescriptive regulatory approach to one that is proactive, risk based, and goal oriented in an attempt to improve safety...” (TRB 2012). While some progress has been made on the adoption of SEMS, it currently remains voluntary.

As mentioned earlier, the aftermath of *Deepwater Horizon* did bring to the forefront a U.S. discussion of U.K.-style safety cases. The primary concern specific to safety cases raised in a critique by Prof. Leveson of MIT is confirmation bias: if operators/developers set out to make the argument that a system is sufficiently safe, they may have an inherent bias against uncovering real inadequacies (Leveson 2011). However, this is really a critique of a particular *formulation* of a safety case, not the intrinsic properties of a safety case. Operational expedience can subvert actual safety whether safety cases are used or not – and regardless of the method, a critical evaluation must be made at some point. Rigorous argumentation, done properly, exposes weakness as well as adding confidence. Safety case approaches can and do incorporate elements of counter-argument and fault-finding (as demonstrated by the common inclusion of risk management in safety case approaches). While it is important to guard against confirmation bias, this is a separate concern from the central feature of safety cases (organized argumentation).

#### 4.1.1.3 Characterization of Assurance Case

##### U.K.

Within our scheme, the U.K.’s offshore oil and gas regulatory system fits as “explicit argument, structured evidence, blended process.” This is somewhat typical of current U.K. regulation, which does not emphasize the argument, is energetic about assembly of evidence in the safety case, and has a tempered approach to process flexibility (see Figure 11).



SI 2005 No. 3117, Schedule 2 identifies fourteen items to include in a safety case for the operation of an installation. Seven of these could be considered “informational” (design documents, site plans, etc.). The remaining seven follow the post-Cullen approach of identifying high-level safety requirements and making satisfaction the responsibility of the operator. These high-level objectives include:

- Show consultation with safety representatives;
- Show compliance with Prevention of Fire and Explosion, and Emergency Response (PFEER) regulations;
- Describe measures to protect persons from toxic gas, explosion, fire, heat, [etc.]; and
- Identify safe limits of operation.

While these may seem surprisingly general, they do link to more detailed lower-level regulations (such as PFEER).

U.K. regulations for offshore oil and gas do not specify a graphical or structured format for safety cases. However, it is not difficult to envision how the above list might be formatted as a GSN diagram as the starting point of safety case, see Figure 12:

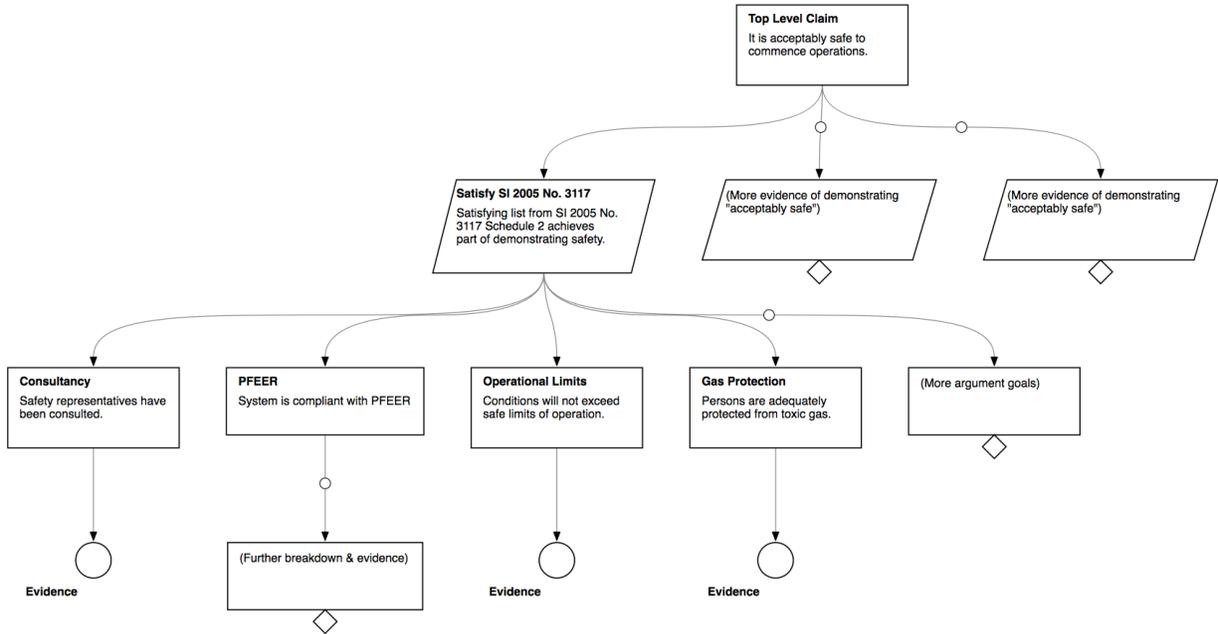


Figure 12: Graphical Translation of Part of U.K. Oil and Gas Regulation

### Norway

An assurance case approach would certainly fit within the Norwegian model; that is, as a way to organize a particular operator's adoption of a collection of processes, technical standards, and risk mitigations to achieve the desired level of safety. However, the structure of the safety management system and its artifacts is not prescribed.

Within our scheme, clearly the flexibility of the Norwegian approach is its dominant feature, as shown in Figure 13.

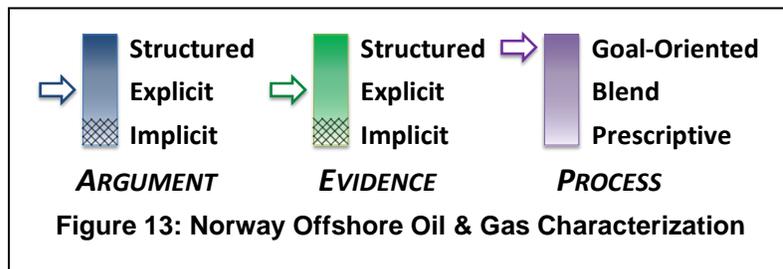


Figure 13: Norway Offshore Oil & Gas Characterization

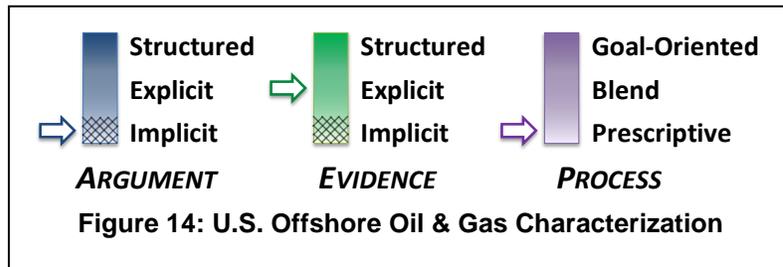
### U.S.

As mentioned above, the U.S. does not require safety cases or assurance cases. The TRB advocates the following elements of SEMS:

- inspections,
- audits,
- key performance indicators, and
- whistleblower program.

These could easily be elements of a safety case. Certainly, the principle of making SEMS “holistic” (TRB 2012) is similar to the motivating impulse of assurance cases (which could be characterized as holistic with explicit argumentation).

However, given the lack of high-level objectives and emphasis on basic safety processes, the current U.S. approach is considered heavily implicit and prescriptive (see Figure 14).



#### 4.1.1.4 Outcomes

##### U.K.

There has not been another major accident in the U.K. since *Piper Alpha*. Oil & Gas UK, the relevant industry group in the U.K., reports a “significant fall in the Lost Time Injury Frequency Rate for the UK since 1997” (Oil & Gas UK 2008).

HSE also reports statistics on hydrocarbon releases, such as the graph in Figure 15.

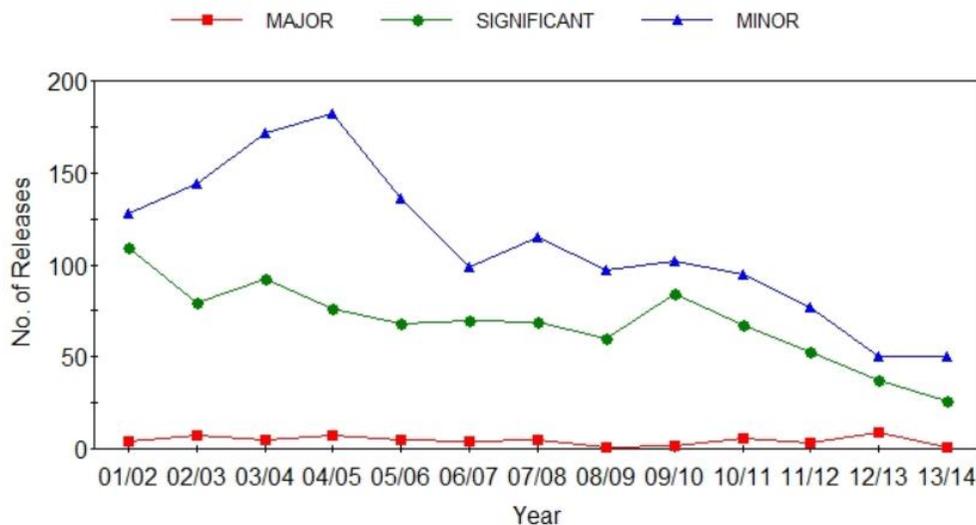


Figure 15: [https://www.hse.gov.uk/hcr3/report/graphs\\_public.asp](https://www.hse.gov.uk/hcr3/report/graphs_public.asp) captured 5 March 2014

##### Norway

(Henrikson 2012) summarizes fairly positive outcomes with the Norwegian system:

- No major oil spills since 1977,
- No major accidents since 1981, and

- Use of hazardous chemicals drastically reduced between 1997 and 2010.

He also mentions, as do other sources, that the system is relatively costly.

## U.S.

Changes made since *Deepwater Horizon* are new enough that clear outcomes are not yet available. In addition, comprehensive incident reporting is only beginning to take hold in U.S. offshore oil and gas.

### **4.1.2 Generic Design Assessment (GDA) of Nuclear Plants**

#### 4.1.2.1 *Synopsis*

Great Britain began its Generic Design Assessment (GDA) program in 2006/2007. The purpose of this program is to vet proposed nuclear reactor designs. Developers must submit a safety case for reactor designs (phase 1) and then amend it for site-specific installation plans (phase 2). Safety cases are central to phase 1 approval and are thus a crucial element of safety assessment in future U.K. nuclear plant operations. Acceptance must be obtained from the Office for Nuclear Regulation (ONR) and the Environmental Agency (EA).

Four plant designs were submitted to the GDA process in 2007. As of 2013, only one design has been accepted – AREVA’s EPR reactor. The GDA program processed the plant design from 2007 through March, 2013. Safety issues were discovered and amended within submitted safety cases so that final safety case documentation satisfied GDA authorities (Office for Nuclear Regulation 2013a). The other design parties have asked to halt the acceptance process.

In 2014, a Hitachi-General Electric plant design began the GDA process. Westinghouse may attempt a restart of the GDA process.

#### 4.1.2.2 *Role of the Assurance Case*

Due to the findings of a 2006 report by the Health and Safety Executive (Office for Nuclear Regulation 2008), it was suggested that future nuclear plants be built with safety case analysis early in project development. The GDA was established to vet plant designs through safety cases submitted during the design phase.

The Design acceptance phase of the GDA process has four steps involving a safety case (Office for Nuclear Regulation 2014a), summarized as follows:

1. **Submission Request:** A designer prepares to submit initial documentation and enters into agreement with the ONR and EA.
2. **Review of a Preliminary Safety Report (PSR):** The designer submits a Preliminary Safety Report (PSR). The PSR must present any claims about the design’s safety. It must also detail the methodologies that will be used to produce the safety case argument and evidence justifying these claims. This preliminary report must demonstrate ALARP (As Low as Reasonably Practicable) safety, which is referred to by the ONR as So Far As Is Reasonably Practicable (SFAIRP).
3. **Analysis of a Pre-Construction Safety Report (PCSR):** The designer submits a PCSR in which the arguments for the safety of the design are presented in detail. In this phase, safety arguments are scrutinized closely and in detail. The arguments must be of sufficient detail to “substantiate the claims made in the PSR” (Office for Nuclear Regulation 2014a) of step 2 for the entire plant lifecycle. The report must also include a

fault analysis, safety function categorization, and safety classification of design structures, systems and components. It must clearly identify where more work will be done in step 4.

4. **Final Evidence for the PCSR:** The designer submits any remaining evidence required to justify the arguments of the PCSR. In this phase, evidence for the safety case is scrutinized closely and in detail. This is the most time consuming part of the process.

The ONR will issue a Design Approval Certificate (DAC) if and only if the analysis of the safety case passes step 4. Additional documentation and processes are vetted but are outside the scope of this report.

Steps 3 and 4 of the process apply sampling from the regulator. Even under this regime, regulators cannot consume the entire safety case argument.

Once a design is approved, it can undergo phase 2 site-specific safety case analysis. The entire phase 1 and phase 2 safety case development process is summarized in the ONR guidelines (Office for Nuclear Regulation 2014a), as shown in Table 4 **Error! Reference source not found.**

**Table 4: Safety Documents and Stages of Nuclear Plant Approval**

Report	Input To
PSR	Assessment in Phase One Step 2
Generic PCSR	Assessment in Phase One Steps 3 and 4
Updated Generic PCSR	Assessment of GDA Issue responses (if required)
Site-specific PCSR	Phase Two Site specific and Licensing assessment
Pre-Commissioning Safety Report	Prior to (inactive and active) commissioning

#### 4.1.2.3 Characterization of Assurance Case

The “purpose, scope, and content” of nuclear safety cases” are defined in the ONR Technical Assessment Guide T/AST/051 (Office for Nuclear Regulation 2013b). Safety cases must follow the ‘claims’, ‘arguments’ and ‘evidence’ approach. Note that these components are the focuses of phase 1 GDA steps 2 through 4, respectively.

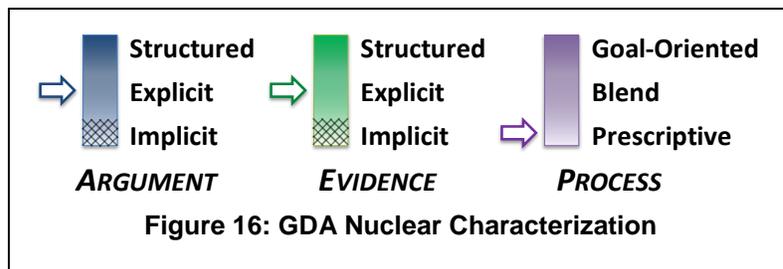
According to (Office for Nuclear Regulation 2013b), a nuclear safety case should answer the following questions:

- What does the safety case cover?
- What does the site/facility, etc., look like (site layout, design, key features)?
- What must be right and why?
- How is this achieved?
- What can go wrong?
- What prevents/mitigates against it going wrong?
- What if it still goes wrong?
- Are the risks ALARP?
- What could be done to make it safer; what areas need further work, and what are the limitations and uncertainties?

- What must be done to implement the safety case?
- How long will the safety case be valid?
- What happens at end-of-life?

Guidance does not specify the structure and scope of the safety case, leaving that as a matter to the applicant licensee. However, it suggests a hierarchy of documents. The top tier can be a summary or Safety Report. It should contain a summary of safety arguments, refined in further documents into details and evidence. Further documents define the evidence in detail. It is recommended that safety cases be divided into a separate safety case for each lifecycle phase of a facility. Safety cases can also be divided into safety cases for subcomponents of a facility, which are elements of input to an overall safety case.

More than anything else that could be said of the GDR process, shown in Figure 16, is that it is highly prescriptive. The technology is presumably well-known, and the public safety implications so high, that predictability and caution is valued above all else.



ONR’s “Safety Assessment Principles for Nuclear Facilities” (Office for Nuclear Regulations 2008) outlines what should be contained in the safety case via Safety Case Principles SC3 – SC6. We condense and summarize this information table in the list below:

- **SC.3: For each life-cycle stage, control of radiological hazards should be demonstrated by a valid safety case that takes into account implications from previous stages and for future stages.**

All risks should be addressed in a safety case before they actually exist. Constraints for subsequent life-cycle stages should be explicitly detailed. Decommissioning should be considered in all previous life-cycle stage safety cases.

The content and depth of a safety cases varies from stage to stage of development, with increasing detail from design through operation.

- **SC.4: A safety case should be accurate, objective, and demonstrably complete for its intended purpose.**

A safety case should:

1. Link to information to show the facility is safe and will remain so;
2. Support arguments with appropriate evidence, experiments and analysis;
3. Accurately reflect the proposed activity of the facility;
4. Explicitly argue for how ALARP has been satisfied; and
5. Identify monitoring that will underpin operational assumptions.

A safety case should contain:

1. Identification of the hazards and their potential, systematically;
2. Identification of failure modes through systematic fault sequence identification;
3. A demonstration of conformation to nuclear engineering good practice and principles (This must include demonstration of ‘defense in depth’);
4. A demonstration that engineering rules are applied appropriately;
5. A demonstration that ionizing radiation dosing to all people is within regulatory limits and ALARP;
6. An analysis of possible faults through design and probabilistic analyses, and severe accident analysis as appropriate and showing hazards and risks are ALARP;
7. Information to show that radioactive waste management and decommissioning have been addressed; and
8. The basis for the management of safety for people, plant, and procedures (This includes management, training, maintenance, instructions, rules, and contingencies).

To demonstrate ALARP, the safety case should:

1. Identify and document all options considered;
  2. Provide evidence of the criteria used in option selection; and
  3. Support comparison of cost and benefit for options where large differences appear.
- **SC.5: Safety cases should identify areas of optimism and uncertainty, together with their significance, in addition to strengths and any claimed conservatism.**  
The safety case should take a balanced view of risks. Areas of uncertainty and optimism should be balanced with adequate conservatism.  
Potential weaknesses in the design of the safety case should be identified clearly. Mitigation for these weaknesses should be identified. Issues remaining to be addressed should be clearly explained.
  - **SC.6: The safety case for a facility or site should identify important aspects of operation and management required for maintaining safety.**  
The important aspects of operation and management required to maintain safety should emerge from the safety case.  
The safety case for each life-cycle stage should include:
    1. The required maintenance, inspection, and testing regimes assumed for the case to remain valid;
    2. The operating conditions required to ensure the facility is kept in a safe condition; and
    3. Inputs to emergency planning.

From this guidance, we conclude that the ONR’s requirements for a safety case specify an informal but explicit argument over explicit evidence.

#### 4.1.2.4 *Outcomes*

The four phases of GDA follow the structure of the safety case in vetting claims, arguments, and evidence. Evidently, the process has been very difficult for vendors from outside of Great Britain to adopt. ONR noted this difficulty: “Understanding the UK regulatory approach and expectations for presentation of safety case claims, arguments and evidence was a challenge for the Requesting Parties towards the beginning of GDA” (Office for Nuclear Regulations 2013c).

We should also note that the ONR has admitted to underestimating the manpower required for a thorough safety case analysis. Each stage of the GDA can take from 6 months to two years, with estimates being very open for this relatively new process. Furthermore, it is critical to note the ‘sampling’ nature of the analysis. Even the regulator does not have sufficient resources to fully vet the entire safety case argument of the designer.

From 2007 through 2014, the activity of the GDA process can be summarized as follows from their activity reports (Office for Nuclear Regulations 2013a, 2014a):

**Throughput:** 1 of 4 reactor designs accepted

**Staff Hours (government):** ~10000

**Documents (applicants):** ~1000s

**EPR Reactor Design (AREVA):**

Identified Issues: 31

Issues Satisfied by Safety Case Amendment: 31

Status: Process exited with design approval

**AP1000 Design (Westinghouse):**

Remaining Issues: 51

Status: Process exited with remaining issues

**ABWR Design (Hitachi-GE):**

Status: Entering phase 2 technical assessment

## 4.2 Aviation Infrastructure

### 4.2.1 U.K. Civil Aviation Authority CAP 670 & 760

CAP 670 and 760 are both issued by the Civil Aviation Authority of the United Kingdom:

- “CAP 670: Air Traffic Services Safety Requirements.” The Third Issue, Amendment 1/2013, 13 June 2013 was the version reviewed for this study. The current version is dated 23 May 2014 (UK Civil Aviation Authority 2014).
- “CAP 760: Guidance on the Conduct of Hazard Identification, Risk Assessment, and the Production of Safety Cases.” The first edition was dated 13 January 2006. The current version is dated 10 December 2010 (UK Civil Aviation Authority 2010).

#### 4.2.1.1 Synopsis

CAP 670 is a lengthy document that covers all aspects of air traffic services: overall regulation, air traffic control (ATC), engineering, flight information services (FIS), communication, navigation, surveillance, weather, and so on. CAP 670 and other CAA regulations coexist and fit together with EU-level regulations as well developed by the European Aviation Safety Agency (EASA) and EUROCONTROL.

Only portions of this document concern assurance cases (specifically, safety cases). The relevant sections/subsections include:

“Part B, Section 1: ATS Certification, Designation and Approval”

→ “APP 01: Safety Management Systems”

→ “Appendix A to APP 01: SMS: Additional Guidance” (references CAP 760)

“Part B, Section 3: Systems Engineering”

→ “SW 01: Regulatory Objectives for Software Safety Assurance in ATS Equipment”

→ “Part 3: Guidance”

→ “Appendix A to SW 01: Identification of AELs”

→ “Appendix B to SW 01: Argument and Evidence Concepts”

CAP 760 is shorter and much more tightly focused. This document explicitly associates hazard analysis methods (such as FMECA, HAZOP, Event Trees) and traditional risk assessment with safety cases.

#### 4.2.1.2 Role of Assurance Case

CAP 670 provides a straightforward practical definition concerning role: “Safety assurance documentation contains **argument** and **evidence** that the system meets or exceeds the appropriate standard of safety.” Safety cases are integral to the regulatory structure set up in CAP 670. The format is flexible, but an arrangement of argument and evidence must be assembled into a safety case to satisfy CAP 670. Assurance documentation must be submitted to the CAA for approval before certain activities may be executed.

The terms “unit safety assurance documentation” and “Unit Safety Case” (USC) are used interchangeably in CAP 670; both refer to what we consider a safety case. CAP 670 presents it as integrated with a Safety Management System (SMS). Safety assurance documentation must be submitted to CAA for approval. Safety case activity may be required for current operations or changes to current operations.

CAP 670 presents a sequence for safety assurance documentation, such that it is provided at several stages in the system development process (shown in Table 5).

**Table 5: CAP 670 Process by Stage**

Stage	Documentation Contents
System Description, Requirements and Hazard Identification [Specification]	<ul style="list-style-type: none"> <li>• Reason for and overview of changes</li> <li>• Safety objectives and regulatory requirements</li> <li>• Operational and functional requirements</li> <li>• Risk assessment to identify hazards</li> <li>• Assumptions and Responsibilities</li> </ul>
Justification of Selected System or Operational Change [Design Complete]	<ul style="list-style-type: none"> <li>• Demonstrate meeting requirements (safety, operational, etc.) – including installation, commissioning, and operation</li> <li>• Often need assurance information from suppliers</li> <li>• Mitigations for deficiencies</li> </ul>
Physical Integration and Handover into Routine Operation [Deployment]	<ul style="list-style-type: none"> <li>• Safe integration of changes</li> <li>• Appropriate staffing and training</li> <li>• Procedures for transition (including reversion)</li> <li>• Summarize hazards and resolutions</li> </ul>

Regarding safety assurance of *changes* to operations, CAP 670 specifies that the following might trigger additional safety case activity:

- Installation and commissioning of a system,
- Modification to in-service equipment,
- Change to maintenance arrangements,
- Withdrawal of a service or facility, or
- New or changed procedure.

While CAP 670 mentions risk management in association with assurance documentation, CAP 760 is entirely devoted to the subject. CAP 760 draws the connection between risk and safety cases (and standards and requirements) very succinctly:

*“International regulations and standards require [ESARRs referenced] ... a risk assessment and mitigation process... The result of the assessment should be documented and this is typically achieved by developing a Safety Case. The term 'Safety Case' is used in respect of a set of one or more documents that include claims, arguments and evidence that a system meets its safety requirements.”*

As for the role of CAP 760, it is also clearly stated: “The purpose of this document is to provide guidance to aerodrome operators and ANSPs on the development of a Safety Case and, in particular, on hazard identification, risk assessment and the mitigation techniques that may be used.” As in CAP 670, it is reiterated that a safety case is a “living document” that will be progressively built up over the course of a project.

CAP 760 presents the following summary of system lifecycle and associated safety activities. This bears similarities to portions of CAP 670 and is shown in Table 6.

**Table 6: CAP 760 and System Lifecycle**

<b>Lifecycle Phase</b>	<b>Activities</b>
Feasibility and Concept	<ul style="list-style-type: none"> <li>• high-level hazard identification and risk assessment</li> <li>• identify applicable safety regulatory requirements</li> </ul>
Design and Development	<ul style="list-style-type: none"> <li>• additional risk assessment</li> <li>• compliance matrices</li> </ul>
Tender and Contract	<ul style="list-style-type: none"> <li>• supplier processes and compliance</li> <li>• hazard logging</li> <li>• contractual safety aspects</li> </ul>
System Realization	<ul style="list-style-type: none"> <li>• change management / safety impacts</li> <li>• risk assessment and mitigation activity</li> </ul>
Transition to Service	<ul style="list-style-type: none"> <li>• evidence of meeting safety requirements (results of tests and trials)</li> <li>• regulatory approval</li> </ul>
On-going Operation and Maintenance	<ul style="list-style-type: none"> <li>• operational and maintenance risks/mitigations</li> <li>• corrective action</li> </ul>
Changes	<ul style="list-style-type: none"> <li>• depending on situation, all phases above</li> </ul>

Decommissioning	<ul style="list-style-type: none"> <li>• assess safety impact of removal</li> <li>• removal risk mitigation</li> </ul>
-----------------	--

CAP 760 goes on to present a seven-step process for risk assessment and mitigation:

1. System description,
2. Hazard and consequence identification,
3. Estimation of the severity of the consequences of the hazard occurring,
4. Estimation/assessment of the likelihood of the hazard consequences occurring,
5. Evaluation of the risk,
6. Risk mitigation and safety requirements, and
7. Claims, arguments and evidence that the safety requirements have been met and documenting this in a safety case.

Though there are connections to assurance case concepts throughout – such as the application of ALARP after step 5 – it is the sole focus of step 7. Chapter 3, section 7 of CAP 760 details this step and is especially informative about the construction of safety cases. A safety case structure (outline) is provided, including key section “System Assurance” which includes claims, arguments, and evidence.

CAP 760 further explicitly integrates a number of risk analysis techniques (FMECA, HAZOP, Event Trees) with the seven-step process and thus safety cases. The document closes with the subject of “Required Level of Confidence in Evidence” (Appendix G).

#### 4.2.1.3 *Characterization of Assurance Case*

CAP 670 is not explicit about the format of safety cases. Regarding safety assurance of current operations, the document provides some guidance for what major areas to include in documentation, such as:

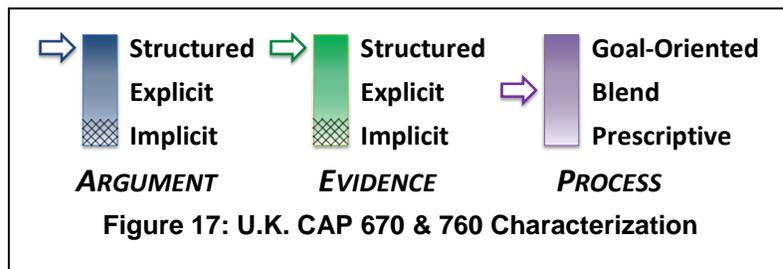
- Describe the SMS,
- Description of operation,
- Safety assessment of operation,
- Compliance with regulations, and
- Operational procedures.

CAP 760 presents GSN as a specifically appropriate graphical representation of safety arguments. More importantly, it provides a safety case structure as guidance, but not strictly required. Although this structure is described in the context of associated risk management processes, the structure is not limited to that perspective; however, it is somewhat tailored to the types of large systems typical of Air Traffic Services). A list of the sections is provided in Table 7 (skipping *pro forma* content such as title page).

**Table 7: CAP 760 Safety Case Structure (abridged)**

Executive Summary
Scope
Functional Description
System Description
System Operation
System Design
Design Dependencies
Assumptions
Safety Objectives
Safety Requirement Derivation
Safety Requirements
Statutory Safety Objectives and Requirements
System Assurance [claims and arguments]
Limitations and Shortcomings
Ongoing Monitoring
Conclusion

In its construction and principles, CAP 670/760 is a relatively modern example. Its inclusion of argument is more advanced and explicit than almost any other examples available. Likewise, it is thorough with respect to evidence and appears to be moderately flexible. Our classification scheme applied to CAP 670/760 is shown in Figure 17.



#### 4.2.1.4 Outcomes

CAP 670 and 760 provide excellent reference material on assurance (safety) cases; but unfortunately, we do not have access to information concerning how it has been applied in specific cases. Nonetheless, they clearly establish the regulatory process that assurance documentation (safety cases) will be produced by air traffic services (ATS) system providers and approval will be based on this documentation.

#### 4.2.2 Eurocontrol Wide-Area Multilateration (WAM) Preliminary Safety Case

The primary source for this section is the Eurocontrol publication “Preliminary Safety Case for Air Traffic Control Service in Non-Radar Areas using Wide-Area Multilateration (WAM) as sole means of surveillance” (Eurocontrol 2012a). Note: Eurocontrol has produced several

Preliminary Safety Cases (PSCs), including for ADS-B surface coverage, ADS-B in radar areas, and ADS-B in non-radar areas. All contain similar structures and utilizations. These and associated documents have been produced as part of the Eurocontrol CASCADE programme.

#### 4.2.2.1 Synopsis

As concluded by the Eurocontrol review document SRC 51 (Eurocontrol 2012b): “The Preliminary Safety Case for WAM-NRA sets out a generic argument and structure to support the claim the use of WAM ... will be acceptably safe.” Furthermore: “Implementers may choose to make use of elements of the PSC, for example the generic set of safety arguments... but must not rely on it alone.” As such, the WAM-NRA PSC provides a starting point for a full safety case to be developed by Eurocontrol member organizations. It limits itself to: (1) a generally acceptable framework and (2) detailed arguments in the area of WAM abstract (“logical”) design.

#### 4.2.2.2 Role of Assurance Case

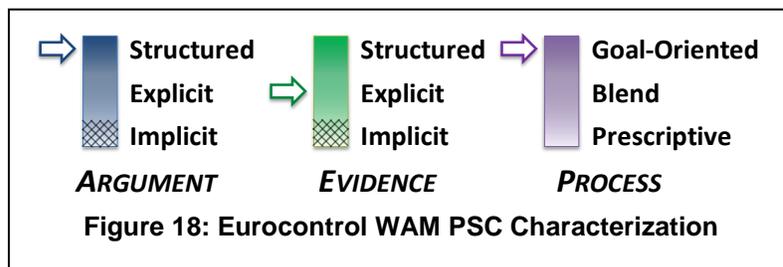
This assurance case example is strictly a safety case. Furthermore, it is intentionally incomplete; it is designed to provide a starting point for specific instances of WAM. “... The aim of this PSC is to be an input to the Air Navigation Service Providers (ANSPs) to produce their own full safety cases (in accordance with the requirements of the local regulator) for a local implementation of WAM-NRA... ANSPs wishing to implement the WAM-NRA system in their own airspace should then consider the information and processes presented in this PSC.” (Eurocontrol 2012a, pg. 15) This document proposes that specific, complete “Local Safety Cases” be produced following the included structure and guidance.

The PSC focuses its detail on the safety argument for the *design* (as opposed to implementation or any other life-cycle phase.). It also “does not prescribe the physical implementation and in particular whether WAM function is passive or active. This will be a local decision on how to achieve the safety requirements identified in this PSC (e.g. probability of detection requirements).” (Eurocontrol 2012a pg. 14) For this reason, the PSC refers in many places to the “logical design” of WAM. Since this document is independent of implementation details (including hardware and its specifications), it limits itself to arguments about the fundamental, abstract characteristics of WAM.

The greatest value of the PSC is in presenting a structure for arguing that a particular WAM instance is acceptably safe for ATC services. This is done both through an extensive GSN structure/diagram and the sections and subsections of the document.

#### 4.2.2.3 Characterization of Assurance Case

As the PSC provides a high-level template for an argument-based safety case, see Figure 18, it clearly encourages argument structure and goal-orientation.



Much of the document explores wide-area multilateration in principle and correlates it to existing radar requirements.

The PSC (Eurocontrol 2012a) organizes its material according to the following argument structure:

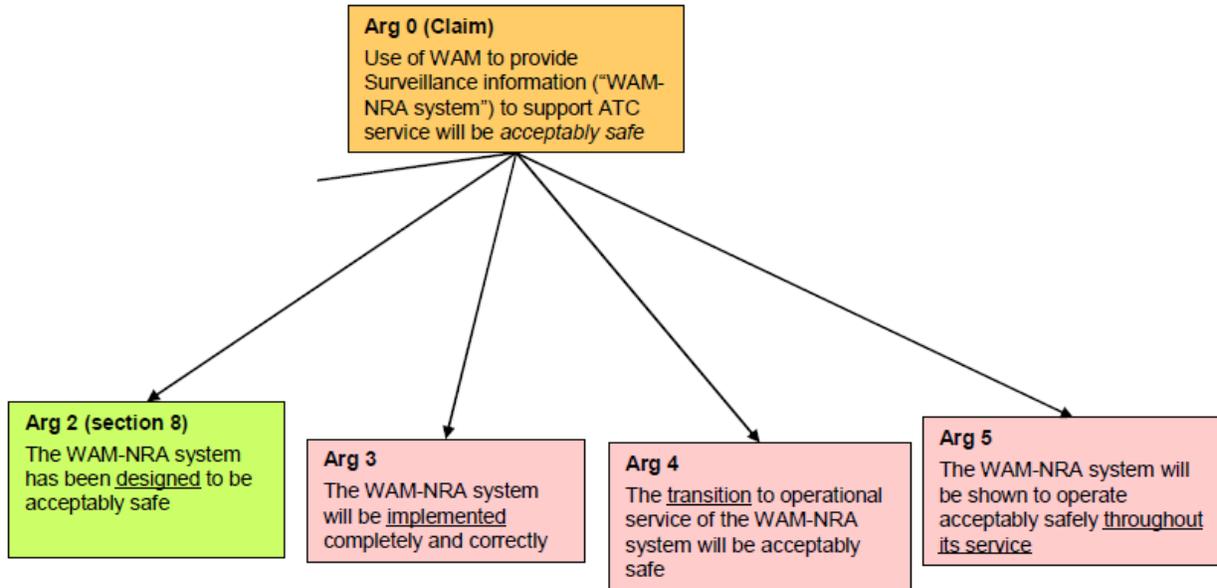
- Overall Safety Argument  
(subdivided into Arg 1 and Arg 2, with placeholders for additional sub-arguments)
  - ATC Service Definition – Arg 1
  - WAM-NRA Design – Arg 2  
(subdivided into multiple sub-arguments: Arg 2.1, 2.2, ...)
    - Appropriate Safety Targets Derivation – Arg 2.1
    - Design Satisfaction of Safety Targets – Arg 2.2  
(subdivided into multiple sub-arguments: Arg 2.2.1, 2.2.2, ...)
      - Logical Design Description – Arg 2.2.1  
(subdivided into sub-arguments 2.2.1.2 through 2.2.1.4)
        - Description of the WAM-NRA Logical Design – Arg 2.2.1.1
        - Differences Between WAM-NRA and Reference Designs – Arg 2.2.1.2
        - WAM-NRA Safety Requirements – Arg 2.2.1.3
        - External Elements – Arg 2.2.1.4
      - WAM-NRA Design Correctness – Arg 2.2.2
      - Logical Design Robustness – Arg 2.2.3  
(subdivided into sub-arguments 2.2.3.1 and 2.2.3.2)
        - Reaction to Abnormalities of the Environment – Arg 2.2.3.1
        - Reaction to Abnormalities of the External Systems – Arg 2.2.3.2
      - Mitigation of Internal Failures – Arg 2.2.4  
(subdivided into sub-arguments 2.2.4.1 through 2.2.4.5)
        - Hazards Identification – Arg 2.2.4.1
        - Hazards Effect Assessment and Severity Assignment – Arg 2.2.4.2
        - Determination of Pe Values and Safety Objectives – Arg 2.2.4.3
        - Hazard Causes Identification and Internal Mitigation Means – Arg 2.2.4.4
        - Safety Requirements and Assumptions – Arg 2.2.4.5
    - Logical Design Realism – Arg 2.3
    - Trustworthiness of the Evidence for the Logical Design – Arg 2.4

As is shown by the structure above, much of the document is dedicated to Argument 2.2, “Design Satisfaction of Safety Targets.” Within this, several common assurance case patterns can be seen.

The first is the top-level emphasis on service definition and safety targets (that is, safety requirements). In order for safety (or assurance of any kind) to be successfully argued, the essential functions and applicable criteria must be sufficiently clear. This is a key early concern in any assurance case. In the case of this PSC, many of these details are identified by reference to existing documentation previously developed for related systems (such as radar and ADS-B).

Next is the inclusion of a subsection specifically arguing that the *design* is acceptably safe. This is a useful foundational argument for the following reason: if the design is *not* safe, there is no reason to progress further (for example, to implementation and maintenance aspects) until that is resolved. Furthermore, though it only provides part of the full argument, the PSC lays out a

useful high-level decomposition pattern as shown in Figure 19 below (Eurocontrol 2012a, pg. 30).



**Figure 19: Eurocontrol WAM PSC High-Level Argument (excerpt)**

This pattern breaks down the overall claim into independent arguments directed at *design*, *implementation*, *transition*, and *operational service*. This is a useful and intuitive breakdown – as part of an assurance case – since each of these tend to address different and unique critical considerations.

The third noteworthy pattern is the explicit inclusion of a hazard management element (Arg 2.2.4). This links the safety case to well-established and effective hazard management practices (as indicated by the subsections: hazard identification, assessment, mitigation, etc.). Including this element in the safety case brings to bear powerful best practices from the field of hazard analysis.

#### 4.2.2.4 Outcomes

The WAM PSC has been further reviewed (Eurocontrol 2012b). The document is somewhat brief and primarily reinforces the scope limitations and appropriate uses of the PSC by member states. It is not known if any European ANSPs have used the PSC yet to produce a complete WAM Safety Case.

### 4.3 Aerospace Vehicles

Assurance cases of various types are available for aerospace vehicles. However, information access restrictions are common. NASA has published guidance that is applicable especially to space systems, though we do not have specific examples. We have some information about the Triton UAS safety case, although it is limited to very high-level information. Perhaps one of the most accessible examples in this domain is the U.K. Nimrod aircraft, since much has been written about its (very poor) safety case in the aftermath of a tragic accident in the Nimrod fleet. There is a safety case for Thales Watchkeeper (for the U.K. Ministry of Defence), but it is not

publically available. There is also rumored to be a safety case for Global Hawk for the U.S. Air Force.

### 4.3.1 NASA Risk-Informed Safety Case (RISC)

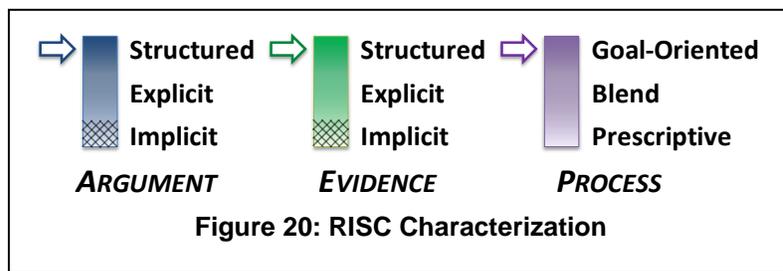
#### 4.3.1.1 Synopsis

As part of its safety process guidance published by the Office of Safety and Mission Assurance (OSMA), NASA has published a model for a Risk-Informed Safety Case (RISC) (Dezfuli et al. 2011). A second, related volume is expected soon. The guidance is relatively new, and we are not aware of the completion of any RISCs to date. (Feather and Markosian 2011) describe their development of a “feasibility” safety case within NASA for a particular instance of operational software, though it is not specifically a RISC. This feasibility safety case was scoped to cover the safety-critical Abort Failure Detection, Notification and Response (AFDNR) system from the Constellation space program. The Feather and Markosian example predates the publication of RISC guidance; but, regardless, it is noteworthy as an example of NASA’s potential movement toward assurance cases for at least some domains.

Though we do not have examples, we can certainly characterize RISCs as they are defined by the published guidance, which is the approach we take in this section.

#### 4.3.1.2 Role of Assurance Case

Likely related to its relative newness, RISC appears (see Figure 20) to be quite advanced in its use of structured argumentation, structured incorporation of evidence, and flexibility.



These characteristics seem fitting for a safety-critical but technologically unique and innovative field of systems.

NASA clearly presents RISC development as a process that parallels the entire systems development process. “...System safety activities are neither auxiliary to nor duplicative of those systems engineering processes that have the potential to affect safety. Rather, system safety activities are integrated into systems engineering processes in a manner that best assures optimal safety throughout these life cycle phases” (Dezfuli et al. 2011).

RISC is shaped by two fundamental principles:

- Meeting or exceeding the minimum tolerable level of safety established by the stakeholders, and
- Being as safe as reasonably practicable (ASARP).  
(ASARP is similar to ALARP, but phrased in terms of positive safety performance rather than negative risk reduction.)

Major stages include:

- Safety Objectives (Hierarchy) [during systems engineering],
- Integrated Safety Analysis (ISA) [during systems engineering],
- Develop the RISC and Safety Claims, and
- Evaluate RISC / Proceed or go back.

The construction of a RISC matches well our definition of an assurance/safety case, including the primary elements of claims, evidence, and arguments. This is shown in the following quotation from (Dezfuli et al. 2011): “It is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is or will be adequately safe for a given application in a given environment.”

#### 4.3.1.3 Characterization of Assurance Case

The RISC top-level argument structure is demonstrated in Figure 21. It is a good example of argument decomposition using well-stated claims.

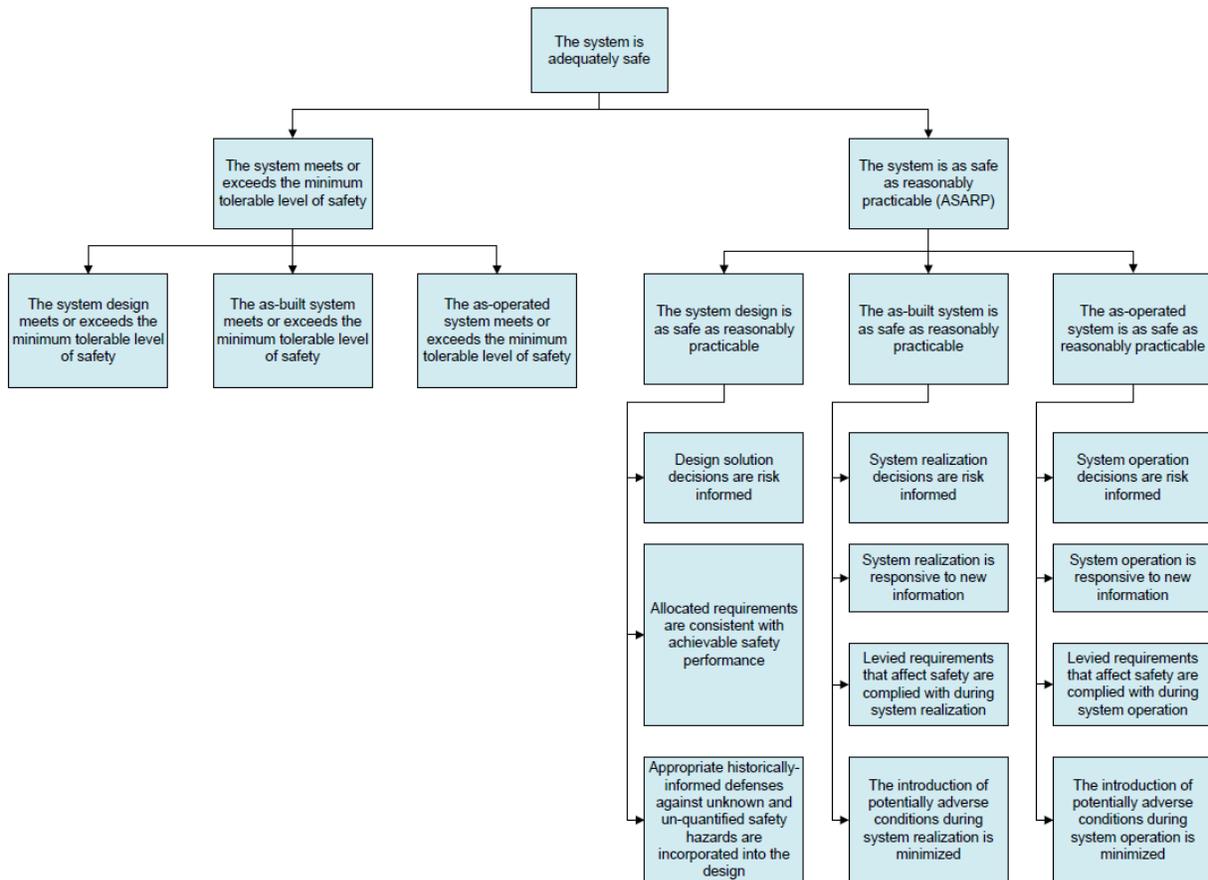


Figure 21: Top-Level Claims of Example RISC (Dezfuli et al., 2011)

RISC further supports mapping arguments to claims. A simple format is used which is less precise than GSN. Nonetheless, the reasoning is clearly stated and easy to follow (see Figure 22).

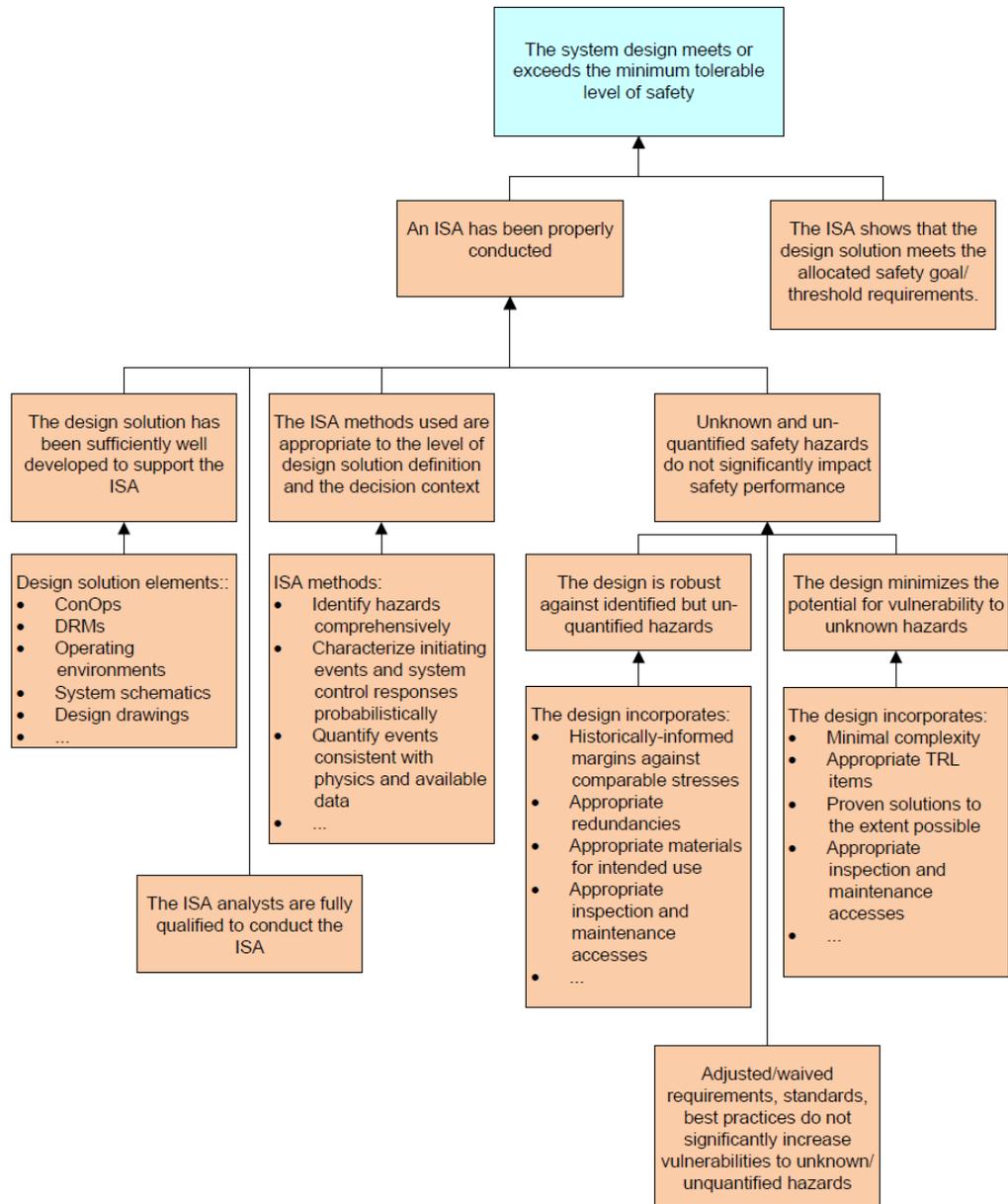


Figure 22: Example RISC Claim and Argument (Dezfuli et al., 2011)

RISC evaluation is covered (Dezfuli et al. 2011, pg. 86):

*“For each claim in the RISC, it is the task of the decision-maker to:*

- 1. Understand the technical basis (i.e., evidence) behind the claim.*
- 2. Question the technical basis of the claim to determine its validity.*
- 3. Provide judgment as to adequacy of the claim.”*

Checklists are also provided to guide and facilitate evaluation.

#### 4.3.1.4 Outcomes

The definition of RISC was published in 2011, with a second volume expected soon. We do not know of any systems that have produced a full RISC.

## 4.3.2 Navy Triton UAS

### 4.3.2.1 Synopsis

The Northrop Grumman MQ-4C Triton, pictured in Figure 23, is an unmanned aircraft system developed for the United States Navy. The system provides persistent maritime surveillance capability for the U.S. Navy, complementing the Boeing P-8 Poseidon maritime patrol aircraft's anti-submarine warfare, anti-surface warfare mission. The MQ-4C Triton's global, maritime mission requires the air vehicle to operate in foreign and U.S. national airspace, as well as international airspace, using Instrument Flight Rules and due-regard operating rules, as defined in civil and Department of Defense regulations. Compliance with due-regard operating rules requires U.S. Navy development and certification of an on-board Sense and Avoid (SAA) system capable of maintaining safe separation between the Triton unmanned aircraft and all other aircraft.



**Figure 23: MQ-4C Triton**  
(Photo by US Air Force)

### 4.3.2.2 Role of Assurance Case

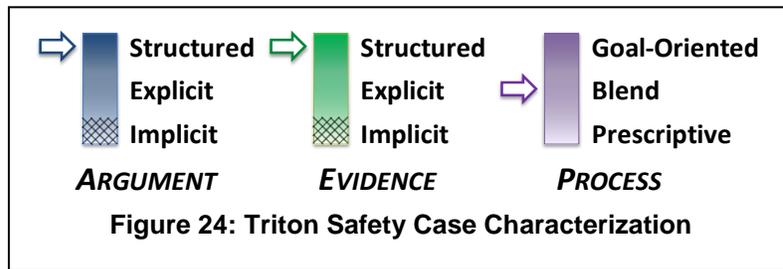
The safety case developed for Triton supports airspace integration and is specifically focused on due-regard operations. Triton due-regard operations are novel; no existing U.S. Navy processes exist to inform certification of due-regard operation. Development of a rigorous safety case for a Sense and Avoid system for use during due-regard operations was viewed as the best approach to mitigate technical and programmatic risk. The safety case was recently adopted by the Naval Air Systems Command (NAVAIR) as a method for achieving SAA certification with the promulgation of NAVAIR INST 13034.4 “Policy for Certification of Sense and Avoid Systems for Employment with Unmanned Aircraft Systems.” The instruction defines a safety case as:

*“Safety Case. The process by which a formally documented body of evidence is created that provides a convincing and valid argument that a system is safe for a given application in a given environment. The safety case documents the safety requirements for a system, provides evidence that the requirements have been met, and documents the argument linking the evidence to the requirements. Elements of the safety case include safety claims, evidence, arguments, and inferences.”*

The airspace-integration safety case developed for Triton assumes, but does not argue, airworthiness or mission suitability. Airworthiness certification and determination of mission suitability is handled through existing U.S. Navy processes.

#### 4.3.2.3 Characterization of Assurance Case

The Triton airspace-integration safety case (see Figure 24) is advanced in its use of assurance-case tools and comprehensive application of the assurance-case paradigm.



The Triton airspace-integration safety case includes GSN arguments comprising over a thousand claims and broad evidence incorporating expert judgment, bench testing, modeling and simulation, and flight tests. The safety case is developed following a rigorous process through which the arguments are matured in consultation with subject-matter experts, reviewed by technical-area experts, and used as the basis for the negotiation of evidence requirements.

Approval of the Triton airspace-integration safety case follows a process similar to that of airworthiness certification. Technical-area experts approve domain-specific portions of the safety case at the leaves of the argument, based on review of evidence and the recommendation of their subject-matter experts. These approvals flow up the argument as evidence for consideration by higher-level technical-area experts until all portions of the argument have been signed off on.

#### 4.3.2.4 Outcomes

The Triton airspace-integration safety case is not publicly available. Nevertheless, experience gained in early stages of development of the safety case was incorporated into NAVAIR INST 13034.4 “Policy for Certification of Sense and Avoid Systems for Employment with Unmanned Aircraft Systems.” The instruction is available in electronic form from NAVAIR.

### 4.3.3 RAF Aircraft Nimrod and Related

#### 4.3.3.1 Synopsis

In September of 2006, an RAF Nimrod aircraft, pictured in Figure 25, suffered a catastrophic in-flight fire resulting in the deaths of the entire crew of 14 on board. The accident cause was traced back to fuel leaked during air-to-air refueling and hot exposed ducting. The primary source for information in this section, unless otherwise noted, is “The Nimrod Review” by Charles Haddon-Cave which was the definitive report on the subject produced for the U.K. government (Haddon-Cave 2009).



**Figure 25: The Nimrod Aircraft**

("Nimrod MRA4 1" by Ronnie Macdonald is licensed under [CC BY 2.0](https://creativecommons.org/licenses/by/2.0/))

What makes the Nimrod case such an instructive example is that a partial safety case for it *had been completed* after design, implementation, and modifications were complete. The aircraft originally entered service in 1969, including a safety-critical design change relative to the preceding design (the Comet). Additional design changes were made in 1979 and 1989. It was, in fact, a combination of the three design changes that led to the accident in 2006. Safety cases were not introduced by the U.K. Ministry of Defence until well after the last design change. However, as mandated, a safety case was created between approximately 2002 and 2005 which reviewed the safety of the aircraft. As the report states, “The Nimrod Safety Case represented the best opportunity to capture the serious design flaws in the Nimrod which had lain dormant for years.” The Nimrod Safety Case received intense scrutiny after the accident and was found to be seriously deficient. Since then, it has served as an important real-world example of how *not* to develop safety cases.

#### 4.3.3.2 Role of Assurance Case

Updates to safety regulation within the U.K. military led to the publication of JSP318B “Regulations of the Airworthiness of Ministry of Defence Aircraft” (4<sup>th</sup> Edition) in 2002 (UK Ministry of Defence 2002). JSP318B prominently features Safety Management Systems (SMSes), Safety Cases, and the principle of As Low As Reasonably Practicable (ALARP). This mirrored evolutionary changes at the broader level of military systems regulation in Defence Standard, “Safety Management Requirements for Defence Systems” (UK Ministry of Defence 2004). Hazard management remained a required element even as there were shifts in the higher-level structure of safety processes and documentation. Both JSP318B and 00-56 were primarily written for new systems. Within the U.K. military aviation organization, further guidance on applying new regulations to legacy aircraft was provided in BP1201, as referenced in (Haddon-Cave 2009). BP1201 emphasized the combination of SMS, Safety Case, and Hazard Log for military aircraft systems; furthermore, it introduced the concept of an “implicit Safety Case” for legacy systems. While the intent is understandable, this unfortunately set up a tendency to be less rigorous for in-service designs and to assume that aircraft currently flying without major incidents were presumably safe. This was especially true for the Nimrod, which was widely regarded as a safe and proven aircraft. Though this was an option for the Nimrod, to their credit,

safety oversight elected to develop an explicit safety case. There was some uncertainty on this point early in the development of the safety case; regardless, the fundamental weaknesses of the safety case were in the execution of it, not the regulatory form.

A Safety Management Plan (SMP) that defined the SMS specifically for Nimrod was issued in early 2002. The SMP established a Platform Safety Working Group (PSWG) and roles such as an Integrated Project Team (IPT) and Team Leader (IPTL), a Safety Advisor, a Safety Manager, and Independent Safety Assessors (ISAs). Hazard management processes were defined at the low level (daily) and oversight level (every 3-6 months).

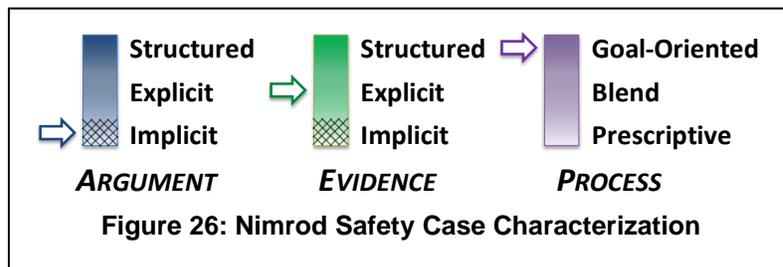
Though the SMP was reasonably well-constructed, in practice there was little motivation to question the safety of the aircraft. As reported in a 2002 feasibility study by BAE (Haddon-Cave 2009):

*“By virtue of a range of traditional methods (certification and qualification/integrity testing), there is an intrinsic high level of confidence in the prevailing acceptable level of safety of the Nimrod types. However, there is currently a lack of structured argument and supporting evidence formally recorded and maintained in order to support the requirements of forthcoming legislation and to achieve compliance with the requirements of JSP318B Edition 4. Hence the reason for the overall task to compile, record, monitor and maintain an aircraft level SC for the Nimrod MR Mk2 and R Mk 1 types.”*

In other words, before real safety case development even started, the authoring organization all but declared that it would be an exercise in documentation and actual safety would be taken for granted. This became a recurring theme throughout the initiative. Sure enough, “The Nimrod Safety Case became essentially a paperwork and ‘tick-box’ exercise.”

#### 4.3.3.3 Characterization of Assurance Case

We characterize the Nimrod Safety Case (see Figure 26) as “Implicit – Explicit – Goal-Oriented.” The argument for safety was not explicitly made or, if it was, it was in appearance only. The evidence was, in fact, explicit, and this is demonstrated by the fact that a deeper inspection of the risk documentation later helped to determine what went wrong. The initiative was also goal-oriented, especially because it was a legacy system, and there was systemically and *de facto* a high degree of latitude in making the safety case.



The safety case was written by BAE Systems, which was the supplier of the aircraft. The process featured a Fault Tree Analysis at the highest level and Zone Hazard Analyses (ZHA) at lower levels. Hazard management techniques formed the bulk of the safety case effort. There

was essentially no argumentation or evidence from design of the analysis; apparently the service record of the aircraft along with hazard analysis was considered adequate to build a safety case.

Though ZHA was not done particularly thoroughly, the hazard that eventually caused the crash was identified and noted in general terms by two separate teams, and subsequently entered into the hazard database. Both ascribed relatively low “initial probabilities” which, later in the process, was given too much weight. Furthermore, the hazard identification system was overburdened with so-called hazards (about 1,300, many of which were unrealistic or slight variations on others). Later “rationalization” of the hazard database reduced the number down to 105: 66 Functional Hazards and 39 Zonal Hazards). The specific hazard in question remained identified as one of the 105.

The role of the Independent Safety Assessor, Qinetiq, was apparently undermined by the perception of the IPTL (from the MoD) that their criticisms were indirect ways to generate business for themselves. Haddon-Cave somewhat vindicates Qinetiq, but in any case, the independent assessment clearly did not function as intended. Qinetiq’s recommendations were frequently brushed aside, and the “independent assessor” was *de facto* pressured to relax its standards.

The safety case development (largely a risk mitigation exercise) was badly under-resourced. The majority of the mitigations had to be developed under severe pressure, and consequently they were of low quality and riddled with errors and inconsistencies. Such was the case for the hazard that eventually caused the Nimrod crash – though portions of the mitigation documentation are tantalizingly correct (such as the identification of a single point of failure fire hazard), the net effect of several flaws in the mitigation argument was that the risk was tolerable.

In the end, the Nimrod Safety Case was accepted primarily because serious inadequacies at the deeper levels were hidden and glossed over. Specific weaknesses in the Nimrod Safety Case are identified in the following subsections.

### *Inexperienced Practitioners*

The authors of the safety case at BAE, according to Haddon-Cave, had never produced a safety case before. Due in part to organizational boundaries, some participants were not the best possible for their roles. For example, some BAE engineering experts were used who were not very familiar with the Nimrod, whereas RAF line engineers had extensive experience with Nimrod safety issues. One of the supporting documents, the Fire & Explosion Report, was written by a manager who wasn’t even present at the (relatively cursory) aircraft examinations on which the report was based.

### *Programmatic Pressure*

Furthermore, there was an early commitment to unrealistic budget and schedule constraints. The acceptable cost of the Nimrod Safety Case was about 1/10<sup>th</sup> the known cost of the (then completed) Harrier Safety Case. The safety case was written in two six-month phases – the first of which was largely hazard identification, and the second of which was risk mitigation. Six months is hardly enough time to develop an understanding of the safety issues that might be present in a large, complex aircraft (let alone draft and vet a comprehensive document on the subject). The budget for phase 2 worked out to about 5 man-hours per hazard, which was, again, at least about 1/10<sup>th</sup> a more reasonable allocation. There was an assumption that each hazard would yield to a search through design documents, test reports, etc. in lieu of substantial

analysis. When suitable documents were largely not to be found, the project had, in effect, no good options.

#### *Gross Mismanagement of Hazards*

The hazard analysis process was rushed and shoddy. At the time of completion, it was covered up that 12 of 66 functional hazards and 22 of 39 zonal hazards remained “Unclassified” (that is, had not been sufficiently worked to classify the risk). In total about 40% of the hazards remained “Open” (work incomplete). Inappropriate reliability data was included in calculations, and subjective judgment was under pressure to arrive at conclusions that even catastrophic hazards were tolerable due to low probability. In the detailed risk assessment data, frequent references were made to more work being required, but this was ignored at the program level in the rush to declare the aircraft “safe” that everyone had, apparently, already decided from the outset was “safe.”

#### 4.3.3.4 *Outcomes*

Unfortunately, the outcome of the Nimrod Safety Case is well-known: it failed to identify and correct a fairly straightforward technical risk, resulting in a fatal aircraft loss. Lessons that can be drawn from the example include:

- Safety should never be assumed, neither should the objective be to “demonstrate that \_\_\_\_ is acceptably safe.” The objective presumes the conclusion; the system in question may *not* be acceptably safe, which is the very reason for producing a safety case.
- Design modifications can radically change the risk characteristics of a system. In the case of Nimrod, its 30 years of safe operation were largely irrelevant (a red herring, in fact) because the 1989 design change was a critical factor in the failure mode. In terms of certain risks, the Nimrod was a different aircraft post-1989 than it was pre-1989.
- Inadequate participation and inadequate review and oversight can allow critical issues to slip through the cracks. Just because an assurance case uses the proper form and procedures does not ensure that it is actually valid and complete. In-depth expert examination from more than one stakeholder seems the minimum necessary measure to ensure validity.
- Budget/schedule pressure and internal mistrust can be toxic to the effective development of an assurance case. Professional judgment is required and will vary from person to person; judgments have repercussions for mitigation strategies, costs, and schedule. It is essential that, barring obvious malfeasance, team members trust each other’s good intentions. Professional opinions deserve merit and should not be discounted.

## **4.4 Rail (Infrastructure and Vehicles)**

In this section we have a pair of examples that are, so to speak, genealogically related. The first example, the European Rail Safety Management System, is the current regulatory regime for rail infrastructure and vehicles in the European Union (EU). It is oriented around the concept of a Safety Management System (SMS), which brings with it a certain safety philosophy. The second example predates the first and represents the U.K. Rail safety regulation prior to integration with

the EU. As such, it emphasizes the safety-case-oriented trends emerging in the U.K. during that time period (which, it should be noted, were not necessarily in favor of *argument-based* safety cases, but they did establish the name “safety case” and emphasize evidence).

As we will see, both examples rely on implicit argumentation. However, there is a distinction that is worth highlighting. The SMS approach tends to imply safety based on the adoption of *beneficial management processes*. In contrast, implicit safety cases such as in the U.K. Rail example also imply safety, but on a different basis: the *collection of evidence* that the system is safe. Neither example explicitly states their arguments. Each uses a slightly different implied argument for safety.

#### **4.4.1 European Rail Safety Management Systems**

##### **4.4.1.1 Synopsis**

The European Railway Agency is responsible for organizing interoperable and safe rail across the European Union. It facilitates the integration of two key railway system elements:

- **Infrastructure Management (IM):** Owners and operators of rail track and related equipment.
- **Railway Undertaking (RU):** Owners and operators of rail vehicles including freight and passenger service.

Three key directives from the European Parliament mandate the European Railway Agency’s work. These are as follows:

- **2001/14/EC:** Establishes an open/shared market whereby RUs within the European Union can openly travel the IMs of countries across the EU.
- **2004/49/EC:** Requires each RU and IM present a Safety Management System, or SMS, that can be assessed by the safety administration of each nation of the EU.
- **2008/57/EC:** Simplifies some aspects of creating an SMS and sets in motion a plan to eventually provide a single SMS structure template for IMs and another for RUs.

Therefore, the Safety Management System is the means of safety assurance in European Union rail. Work continues to unify the definition of an SMS and standardize its implementation.

A traditional SMS covers many aspects of safety not traditionally thought of as part of a safety assurance argument. For example, it may include future safety goals for an organization and include active elements to influence behavior within an organization. Therefore, Safety Management often subsumes an explicit Safety Assurance Case as an umbrella under which assurance occurs. Safety Management Systems are traditionally found in healthcare, aviation, rail, and maritime systems where they operate similar to quality assurance conventions.

We note that the European Railway Agency refers to the SMS as follows (European Railway Agency 2014a): “Implementing all relevant elements of an SMS in an adequate way can provide an organisation with the necessary assurance that it controls and will continue to control all the identified risks associated with its activities, under all conditions.”

Therefore, we consider the role of SMS for European Rail as an assurance case for two reasons:

- The European Railway Agency refers to the SMS in terms of assurance.

- The U.K.’s rail system previously applied safety cases, but has since adopted the European Railway regime as mandated by the European Union. Therefore, we can compare and contrast the two approaches to assurance.

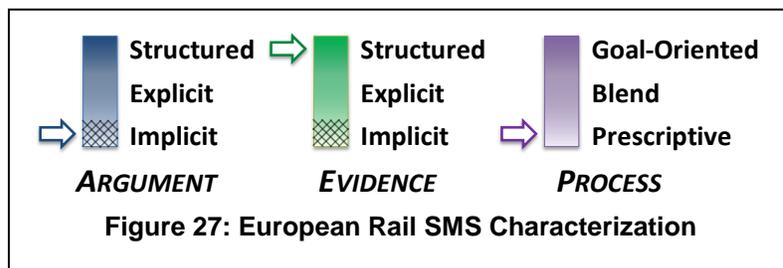
For the remainder of this section, we will consider the European Railway SMS to be an example of an informal assurance case.

#### 4.4.1.2 Role of Assurance Case

The SMS is a necessary requirement for operation of an RU or IM within the European Union. All nation states within the EU must receive the SMS for a RU or IM, and must issue a safety certificate on the basis of reviewing the SMS. As the SMS is a live document, this review is theoretically continuous. A certified SMS is necessary but not sufficient for an RU or IM to operate legally within a member nation. Nations may maintain additional regulations.

#### 4.4.1.3 Characterization of Assurance Case

The European rail safety regulation is, in many ways, very traditional. It emphasizes collecting and recording a comprehensive body of evidence, shown in Figure 27. This is, in some ways, appropriate given that the railway system is very well-known and not particularly complicated – that is, the risks tend to be very transparent.



A Safety Management System consists of a large set of categories into which documentation, procedures, and evidence are placed. The structure of these categories forms an implicit argument of safety assurance.

In the case of the European Railway Agency SMS, this categorical structure is called the “SMS Wheel.” The wheel represents categories of evidence and procedure designed to assure system safety. As examples:

- “Risk Assessment” category provides evidence about potential hazards and likelihoods.
- “Emergency Plans” provide document hazard mitigation strategies.
- “Leadership” provides evidence for organized managerial responsibility for safety.
- “Continuous Improvement” procedures document means for maintaining quality of operations to maintain and improve safety standards.

While a comprehensive study of SMS exceeds the bounds of this work, we note that these and other SMS categories, when combined, are oriented to enact but also assure system safety. It is this assurance of safety that allows nation states to offer safety certificates upon acceptance of an SMS. In 2013, legislation was proposed that will enable the ERA to issue safety certificates to

vehicle and rail operators anywhere in the EU by 2019. Compliance with the SMS would be a key requirement of such certification.

#### 4.4.1.4 *Outcomes*

The European Railway Agency released its 2014 biannual safety report (European Railway Agency 2014b). Amongst its key findings are the following

- According to the latest available common safety indicators data, railway safety continued to improve across the EU in 2012, with 2,068 significant accidents resulting in 1,133 fatalities and 1,016 people seriously injured. This represents a 7% drop in the number of significant accidents and a 5% drop in casualties compared to 2011.
- “... improvement continues to slow...” [in safety gains]
- “The safety performance of EU Member States varies considerably, with a more than ten-fold difference in risk for all categories of railway users. This implies that there is clear potential for improvement in numerous areas, as there has been no significant reduction in risk variations over the last ten years.”

Overall, the report’s data suggests a significant drop in serious accidents in 2008-2009, followed by relatively gradual reduction in serious accidents from 2009 through 2012.

In 2013 there were two high profile train accidents, including the most deadly passenger train crash in 15 years in Spain (July 24). However, Christopher Carr, head of safety for the ERA indicated at the time that “The timing is unfortunate but I don’t think we see this as the start of a trend and we don’t see evidence of that in the data we have so far” (Hall and Spence 2013).

### **4.4.2 U.K. Rail Safety Cases: 1994 - 2006**

#### 4.4.2.1 *Synopsis*

From 1994 to 2006, the United Kingdom’s rail industry assured safety through the application of a safety case regime. In 2006, the U.K. transitioned from the use of safety cases to the SMS-driven approach as required in European Union directive 2004/49/EC, as discussed in Section 4.4.1. A majority of this section is taken from “Supplement F: Safety case use in the railway industry”, which is a supplement to “Using safety cases in industry and healthcare: a pragmatic review of the use of safety cases in safety-critical industries – lessons and prerequisites for their application in healthcare” (Medhurst and Embrey 2012).

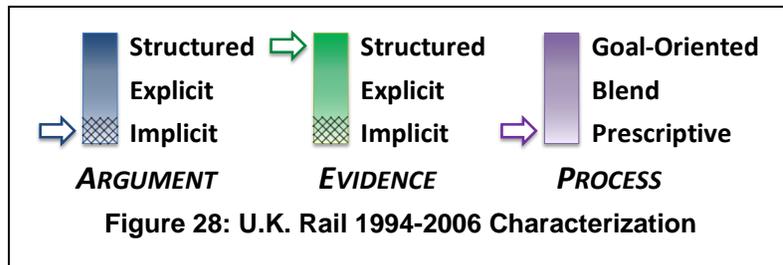
#### 4.4.2.2 *Role of Assurance Case*

Safety cases became required of U.K. rail in response to the privatization of the industry in 1994. At that time, the Railway Regulations of 1994 included the need for safety case with all elements of rail industry, including infrastructure and train operations. The HSE was charged with verifying compliance of industry and auditing of safety cases.

There was a two-tier approach to safety case audit. Rail infrastructure submitted its safety cases to HSE. Rail carriers and train operators submitted their safety case to both rail infrastructure and the HSE for review. In this way infrastructure was able to check the assumptions and methods of operators on the infrastructure. Formal approval of a safety case by all predecessor parties in the hierarchy was required in order to legally operate within the U.K.

#### 4.4.2.3 Characterization of Assurance Case

Though the older U.K. railway regime was in name a “safety case,” whereas the successor European system is an “SMS,” the two are categorized the same according to our scheme, shown in Figure 28.



Rail industry safety cases are effectively traditional U.K. safety cases. A safety case consists of the following elements (Medhurst and Embrey 2012):

- *Duty Holder*: Description of the responsible party for the safety of a system.
- *Risk Assessments*: Comprehensive documentation of risk, “including methodology, results and the implementation of risk control measures.”
- *Health and Safety Management System*: A description of the safety management system in place for the system. This included evidence for its effectiveness and auditing procedures.
- *Technical Description*: A technical description of the system in question.
- *Operations and Maintenance Procedures*: A description of procedures used to operate and maintain the system.
- *Training and Competency*: Description of training methods and competency assessment techniques for staff.
- *Cooperation*: Description of methods for cooperation with other systems in rail.
- *Emergency Response and Incident Investigation*: A Description of methods.
- *Development Plan*: A plan for the continuation, maintenance, and ownership of the safety case and its required evidence.

These are all of the typical elements found in a safety case required by the U.K.’s Health and Safety Executive. Note that the safety case subsumes the Safety Management System (SMS) of the rail entity, whereas in European Union regulations of Section 4.4, the SMS subsumes an assurance argument. The standard HSE Safety Case is by nature a structured safety assurance argument in which evidence is displayed explicitly, but the argument itself is implicit.

#### 4.4.2.4 Outcomes

(Medhurst and Embrey 2012) indicates that the strength of SMS methodologies in rail is in its impact on the evidential structure of safety cases, as compared with industries such as petrochemical. In other words, the safety management approach further discretized and regularized the categorization of evidence for use in safety assurance.

As with other HSE initiatives, compliance with safety case regulations was complete, and may have helped identify hazards and mitigation with the London Underground system amidst the fragmentation of privatization (Medhurst and Embrey 2012). The authors also note that there is no analytic evidence in support of the effect of the safety case regime on safety in U.K. rail. However, accidents per kilometer travelled continued to decline in inverse proportion to time over the safety case regime.

## 4.5 Automobiles

### 4.5.1 ISO 26262

#### 4.5.1.1 Synopsis

The ISO 26262:2011(E) standard is entitled “Road vehicles — Functional safety” (International Organization for Standardization 2011b) and was developed by the automotive industry. The standard is an adaptation of IEC 61508 and is designed to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles.

The development of ISO 26262:2011(E) was undertaken with no legal requirement. Thus, conformance is voluntary, and there is no regulatory oversight. The voluntary nature of the standard means that safety cases developed within the automotive industry do not have to leave the associated development organizations. This is likely the primary reason that there are no publicly available ISO 26262 safety cases available for inclusion in this report.

The standard is important for this study, because it is:

- the only standard applicable to the automotive industry,
- aimed at the electrical and electronics systems in automobiles, and
- mandates the development of a safety case.

ISO 26262:2011(E) is based upon a system-development V process model. Detailed hardware-development and software-development process models are included. The standard partitions target systems into four different Automotive Safety Integrity Levels (ASILs), A through D, with level D being the most critical.

ISO 26262:2011(E) is composed of 10 separate volumes. The first volume is a detailed glossary of terms and covers all of the major terms that usually cause confusion. Some of the key definitions from the standard are as follows:

- **Safety:** absence of unreasonable risk.
- **Unreasonable risk:** risk judged to be unacceptable in a certain context according to valid societal moral concepts.
- **Safety case:** argument that the safety requirements for an item are complete and satisfied by evidence compiled from work products of the safety activities during development. NOTE Safety case can be extended to cover safety issues beyond the scope of ISO 26262:2011(E).
- **Safety goal:** top-level safety requirement as a result of the hazard analysis and risk assessment. (Note: one safety goal can be related to several hazards, and several safety goals can be related to a single hazard.)

Volumes 2 through 9 partition the safety engineering process mostly by lifecycle phase as defined by the V model. The tenth volume is a guidance document that includes detailed guidance and worked examples of fault-tree analysis and the associated probability calculations.

Despite the fact that a safety case has to be constructed to establish compliance, the standard provides no guidance on the development of the safety case, how it should be presented, how it should be evaluated, or how the safety case should be validated and verified. There are virtually no links from the body of the standard to the safety-case requirement.

ISO 26262:2011(E) is a prescriptive standard which defines process requirements in extensive detail and includes numerous tables that identify technology choices and associated technology recommendations for the different ASILs. From the safety perspective, an important requirement set by the standard is a detailed hazard analysis. From the hazard analysis, the standard calls for the development of safety requirements that mitigate the hazards to acceptable levels.

Combining the standard’s requirement for a hazard analysis with the standard’s detailed process requirements results in a prescriptive standard that, if followed, causes a great deal of the essential evidence for a safety case to be developed. Thus, the bulk of the standard supports the requirement for development of a safety case extensively.

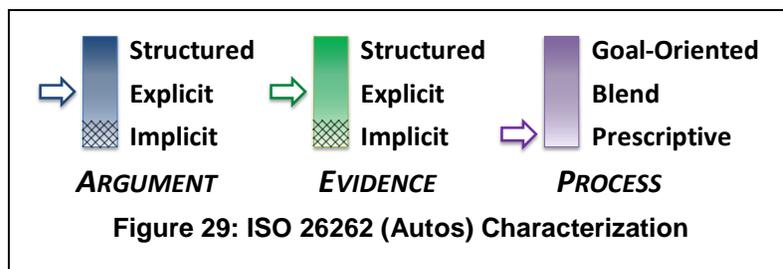
#### 4.5.1.2 Role of Assurance Case

Although the term “safety case” is defined in volume 1, the glossary, the term is enhanced in section 5.3.1 of volume 10 (the guidance) as follows:

*“The purpose of a safety case is to provide a clear, comprehensive and defensible argument, supported by evidence, that an item is free from unreasonable risk when operated in an intended context.”*

#### 4.5.1.3 Characterization of Assurance Case

ISO 26262:2011(E) is very thorough in the processes and technologies that it prescribes, but it is in the sense of “highly explicit” rather than “structured.” Though the regime is not mandatory (which is a form of flexibility), it is nonetheless intrinsically prescriptive as described above and characterized in Figure 29.



The limited statement about the role of the safety case in the mechanism set up by ISO 26262:2011(E) is defined in section 6.4.6 of volume 2 of the standard, “Management of functional safety.” Specifically, the standard states:

#### “6.4.6 Safety case

*6.4.6.1 This requirement shall be complied with for items that have at least one safety goal with an ASIL (A), B, C or D: a safety case shall be developed in accordance with the safety plan.*

*6.4.6.2 The safety case should progressively compile the work products that are generated during the safety lifecycle.”*

Use of the ASILs in defining what is expected from a safety case would be expected, especially for ASIL D systems. For ASIL D systems, Annex E of volume 2 is entitled: “Example of a functional safety assessment agenda (for items that have an ASIL D safety goal).” Despite the expected role of the safety case in safety management, Annex E only mentions the safety case once and then only as an item in the safety management plan.

Section 11 of volume 4 is entitled: “Release for production.” The only mention of the safety case in this section is that having one is a prerequisite for release.

#### 4.5.1.4 Outcomes

We have not found specific examples of safety cases developed using ISO 26262 or reports of conformance with the complete standard. Research papers published by authors from Jaguar Land Rover suggest that that company has built safety cases for ISO 26262:2011 (E) compliance, although no details have been released (Habli et al. 2013, Palin & Habli 2010, Palin et. al. 2011). It is likely that there are other unreleased efforts to implement ISO 26262 at least in part.

## 4.6 Medical Devices

Medical devices are engineered systems that provide a service to patients by treating injuries and illnesses, mitigating their effects, or providing data that can be used by physicians or other devices.

As the complexity, sophistication and number of medical devices has increased, so has concern over their safety. Defining “safety” for a medical device is more difficult than in most other safety-critical domains, because the notion of “acceptable residual risk” is variable. For example, the degree of residual risk that is acceptable for a medical device is much lower for generally healthy children than for elderly adults with a life-threatening disease. A much higher level of residual risk is acceptable for the elderly adults because of the serious nature of their situation. This distinction must be possible for medical devices, although nothing similar arises in other safety-critical domains.

The U.S Food and Drug Administration uses the following definition of safety (Food and Drug Administration 2013):

*“There is reasonable assurance that a device is safe when it can be determined, based upon valid scientific evidence, that the probable benefits to health from use of the device for its intended uses and conditions of use, when accompanied by adequate directions and warnings against unsafe use, outweigh any probable risks. The valid scientific evidence used to determine the safety of a device shall adequately demonstrate the absence of unreasonable risk of illness or injury associated with the use of the device for its intended uses and conditions of use.”*

Even though this definition is not motivated by the explicit use of safety cases, the form and content of the definition is remarkably close to the definition that would be used in a safety case. This circumstance makes the adoption of safety cases in the medical-device domain somewhat simpler than might be expected.

In this section we present: (1) a summary of the issues in medical device safety, (2) a discussion of the use of safety cases with drug-infusion pumps, and (3) an overview of the assurance case developed at the University of Pennsylvania for a generic (i.e., non-proprietary) pacemaker.

According to supplement G of the report ‘Using Safety Cases in Industry and Healthcare’, “Despite the benefits, software failure poses a number of additional risks to patient safety; moreover, the complexity of software poses significant challenges for regulators to ensure their safety and confirm that they perform to the manufacturer’s specification” (Bloomfield et al. 2012).

(Thimbleby 2013) points out that user interaction failures cause significant damage to caregivers in addition to patients; poor interface design and ignoring detectable errors is almost universal in the current generation of medical devices. Poor user interface design leads to misreading the device or entering bad information. Ignoring detectable errors on the device (such as unreasonable dosages or flow rates) leads to devices acting in a less safe manner than they otherwise could in partnership with an operator.

#### **4.6.1 Infusion Pumps (Food and Drug Administration)**

##### **4.6.1.1 Synopsis**

The FDA is now requiring that, for new infusion pumps, an assurance case for medical device safety must be included in their pre-market filing (Food and Drug Administration 2014). An infusion pump, shown in Figure 30, provides controlled, direct drug delivery into a patient’s body over time.



**Figure 30: Medical Infusion Pump**

(“EDK Pump 1” by Daniel Schwen is licensed under [CC BY-SA 3.0](https://creativecommons.org/licenses/by-sa/3.0/))

The reason for this requirement is that the FDA is seeing a strong increase in the number of reported infusion pump failures – with serious repercussions to patients – for which the cause is

either poor design or poorly handled software errors (Bloomfield et al. 2012). In particular, they summarize the FDA’s findings about failures occurring due to:

1. software defects,
2. user interface issues, and
3. mechanical and electrical failures.

Thus, new devices require a formal safety assurance case be filed with new devices in the 510(k) process.

The FDA Software Engineering Lab produced a Generic Patient Controlled Analgesic (GPCA) infusion pump model (Food and Drug Administration 2011). This model is made available to the public. According to the FDA, the purpose of this model is to:

- “1. Demonstrate the use of model-based development techniques for engineering medical device software,*
- 2. Provide a base open-source reference model that can be extended and modified to develop specific implementations of PCA pump software, and*
- 3. Provide a reasonably complex medical design for researchers to use in developing, refining, and improving theories and methods needed to develop certifiably dependable medical devices.”*

In general, the purpose of the GPCA is to support research into model-oriented software development. In addition, the FDA has released hazard analyses and safety requirements (FDA, 2011). This project has been extended to the Generic Infusion Pump (GIP) which is an infusion pump design meant as a safe reference architecture for industry (Real-Time Systems Group 2014a, Food and Drug Administration 2011).

The University of Pennsylvania has participated in the Generic Infusion Pump (GIP) project implementation. They have contributed safety cases and processes in an attempt to assure the safety of the GIP for use in patients as an assured example of the GPCA reference architecture (Real-Time Systems Group 2014b). Collaboration with Swansea University and Queen Mary University provided safety assurance for the user interface.

#### 4.6.1.2 Role of Assurance Case

The GIP project is a substantial contribution to its domain by emphasizing a structured, comprehensive argument regarding the safety of a technical system that is well-known but still moderately complex. Infusion pumps are also interesting as being relatively low-cost and mass-produced (relative to the other examples in this report). Given these considerations, the safety case is impressively advanced, as indicated in Figure 31.

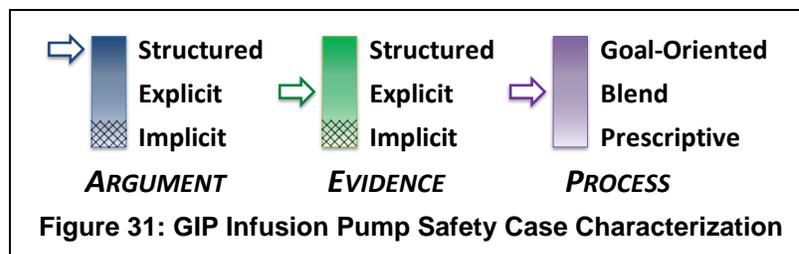


Figure 31: GIP Infusion Pump Safety Case Characterization

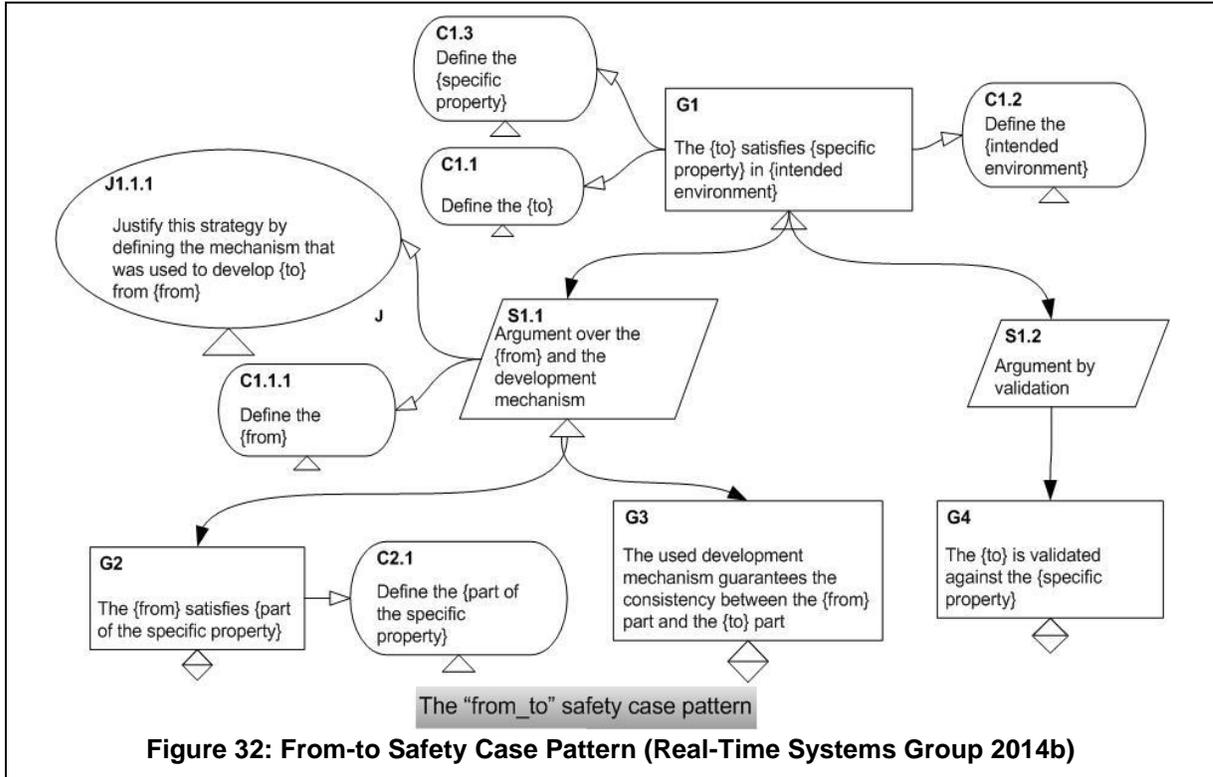
The safety case in the GIP project serves two key roles:

1. It is an assurance of safety for the operation of GIP in patients.
2. It is a guidance product that is built in tandem with the GIP implementation in order to produce the safe software implementation.

In other words, the GIP is not just a post-production artifact assuring safety; it is applied during development to guide and assure implementation meets safety requirements (Real-Time Systems Group 2014a, 2014b).

#### 4.6.1.3 Characterization of Assurance Case

The GIP safety case uses GSN to explicitly present the safety case. Evidence is explicitly provided and linked within the safety case. Its placement is not structured but limited to GSN notation. While the safety case is not prescriptive in form, it does include common patterns. For example, University of Pennsylvania researchers recommend a specific goal state notation pattern, the “from-to” pattern (Real-Time Systems Group 2014b), as shown in Figure 32.



This pattern is a recommendation, but not a constraint. Thus, the safety cases presented are a blend of prescribed (recommended) patterns and best-fit-for-use adaptation.

#### 4.6.1.4 Outcomes

(Masci et al. 2013) used a user interface safety case to produce confidence arguments about the safety argument. The authors argue that a systematic confidence argument construction

identifies deficits in the assurance case, either in argument or evidence. Through this approach, they identified deficits in the evidence for their infusion pump user interface safety case.

The authors further argue that their approach demonstrates the benefits of a “synergistic use of model-based development and safety cases in developing interactive software for a medical device user interface prototype.”

#### 4.6.2 Generic Pacemaker Assurance Case

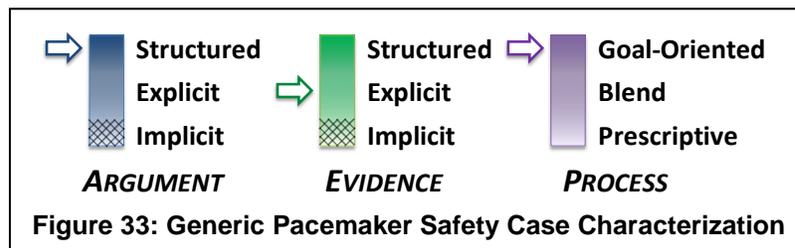
##### 4.6.2.1 Synopsis

In order to facilitate research into medical device safety, Boston Scientific released a previous generation pacemaker model into the public domain. Researchers were encouraged to produce certifiably safe implementations of the model as part of a Software Certification Consortium Grand Challenge (Méry et al. 2014).

Researchers at the University of Pennsylvania produced an implementation of the generic pacemaker (Jee et al. 2010). This software was developed using the model-oriented development mode of verifying properties of a model, generating code formally verified to match the model, and then demonstrating further properties over the generated code. They then produced a safety case for the implementation. In their words: “We created an assurance case to demonstrate that the implemented code is safe to operate, with the intention of providing a guiding example of assurance cases to be possibly used in the certification process of pacemaker software.”

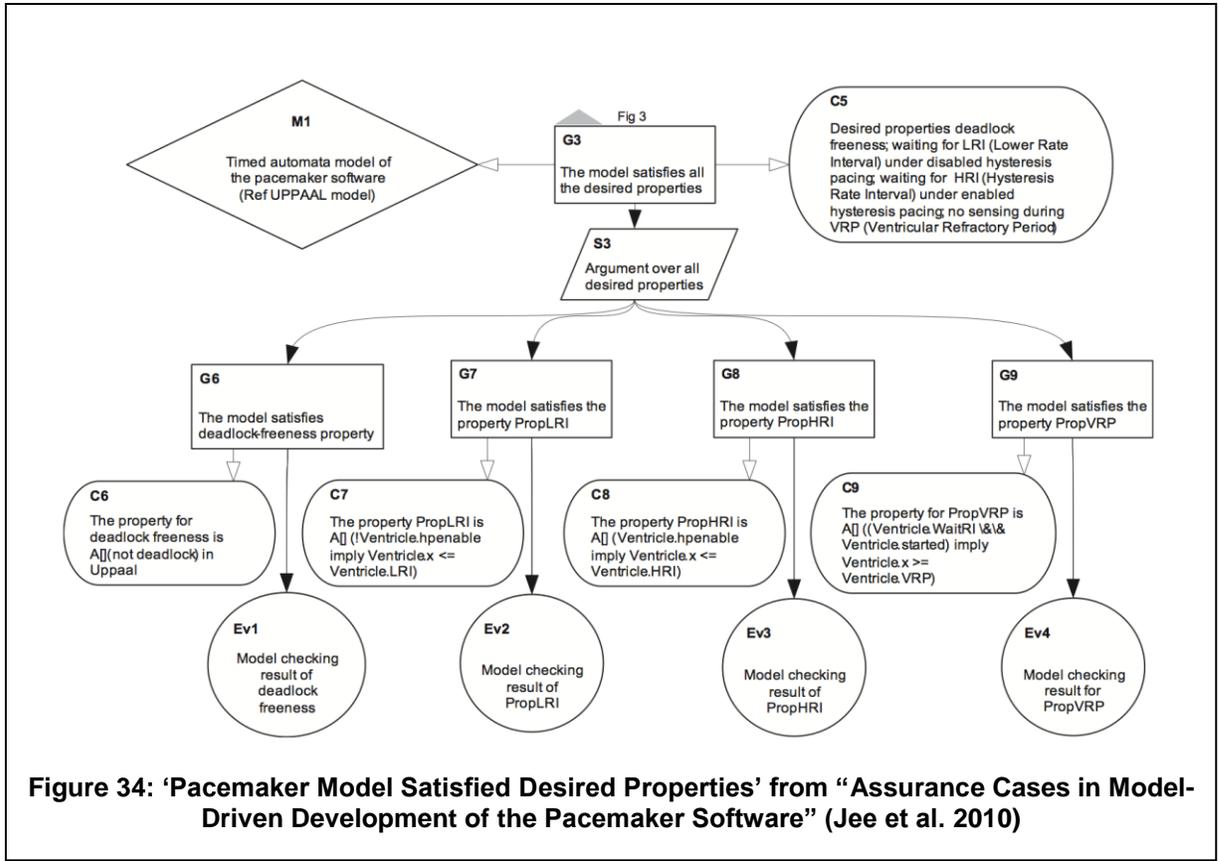
##### 4.6.2.2 Characterization of Assurance Case

The nature of this example is similar to that of the infusion pump, with some additional flexibility. Classification according to our scheme is shown in Figure 33.



The pacemaker software safety case produced by the University of Pennsylvania is written in GSN. The safety case is decomposed specifically to match a general argument about model-based software implementations. Namely, that the steps of the process cause the software implementation to match a model, and that the model meets safety requirements.

More specific safety case arguments relate to the properties desired on the Pacemaker model. For example, (Jee et al. 2010) define part of the argument related to the model. We reproduce their diagram below in Figure 34. This section of GSN describes the specific properties required for the pacemaker. Note that the evidence consists of formal model checking results.



**Figure 34: ‘Pacemaker Model Satisfied Desired Properties’ from “Assurance Cases in Model-Driven Development of the Pacemaker Software” (Jee et al. 2010)**

The produced safety case is formal with structured argument and explicit evidence. Its structure is individualized for the safety case in question.

#### 4.6.2.3 Outcomes

The resulting safety case was limited to (1) pacemaker software (2) in a specific mode, for (3) arguments limited to model-based software design. A more rigorous and complete safety case would have been out of scope for their research efforts (Jee et al. 2010). This work points out that the size of a safety case required, even for a single medical device, if it is to be complete in its assurance of safety. Resultantly, the authors’ further work will seek to improve scaling composition of safety cases for standard industrial use.

## 5. Assurance Case Evaluation

This section presents a review and summary of assurance-case evaluation technology and techniques.

Note that evaluation of interest here is of the assurance case. Much has been written about the related topic of the evaluation of safety assessment. This related topic is about the evaluation of the methods used to conduct the safety assessment of a particular system, such as associated hazard analysis or fault-tree analysis. Evaluation of safety assessment is not covered here.

NASA describes evaluation this way in relation to its definition of Risk-Informed Safety Cases (RISC) (Dezfuli et al. 2011): “Evaluation of the RISC is the means by which reasonable assurance of adequate safety of the system can be obtained by the responsible oversight organization. As in a legal case, the ‘burden of proof’ is on the RISC developer to make the case for safety to a critical, and skeptical, approval authority. Deficiencies in either the safety of the system or in the quality of the RISC must be addressed in order for the oversight organization to have reasonable assurance that the system is adequately safe.”

Assurance-case evaluation is a complex topic, because there are many different properties that might be required of an assurance case and because different stakeholders view the various properties differently. Section 5.1 summarizes the different assurance-case properties of interest and Section 5.2 summarizes the interests of the various stakeholders.

Conformance with one or more existing prescriptive standards is sometimes used as part of an overall approach to the development of an assurance case. The various activities or objectives required by a standard are viewed as producing evidence and for claims to be justified by the implicit assurance case embodied in the standard. A system assurance case then refers to the use of the standard. This technology is reviewed in Section 5.3.

Some organizations that use assurance cases (especially those that use safety cases) have defined specific evaluation procedures and codified those procedures in the form of either a standard to which an assurance case must conform or guidance that must be followed in preparing the assurance case. The various organizational standards and guidance documents are discussed in Section 5.4.

Various items of theoretical research have been conducted to answer basic questions about assurance-case evaluation. Section 5.5 surveys the theoretical work in the area of evaluation.

### 5.1 Evaluation Stakeholder Roles

Different stakeholders evaluate the assurance case for a subject system in different ways. The stakeholders and their interests include:

- **Developer**

Those responsible for the design/implementation of the system in question. Developers are responsible for making sure that the design and implementation match the assurance case, and that the assurance case matches the requirements set forth by regulators.

- **Regulator**

Those responsible for regulation that must make a deployment decision about a system based on the associated assurance case. They will be concerned primarily with protection of the public interest.

- **Owners**

Those who have material responsibility for the system in question through financial investment. They will be concerned with the overall business case for the system.

- **Suppliers**

Those responsible for contributing components to the system in question. Suppliers must not violate the constraints and assumptions of the assurance case. In particular, they often must provide evidence to support the claims of the case with respect to their services and supplies.

- **Operators**

Those responsible for the installation and operation of the system in question. Operators must not violate the constraints and assumptions of the assurance case while operating the system. Going ‘out of bounds’ of the assurance case reduces the value of the assurance case (and can nullify it). The potential violation of assurance case constraints and assumptions has led to the concept of an *operational assurance case* designed to argue the goal that such violations will occur with acceptably low frequency. Operators may need to develop and provide evidence for such an operational assurance case.

- **General Public**

Members of the general public are primarily interested in the residual risk that remains in a deployed system (although few members of the public would ever describe their interests in quite those words). For a safety-critical system, safety is both defined and argued in a safety case, and members of the public might expect to be provided access to the safety case for a system in order to make an individual evaluation of the rationale for the residual risk being acceptable. One example of providing this access is the U.K. government publication “The United Kingdom’s Fifth National Report on Compliance with the Convention on Nuclear Safety Obligations” (Department of Energy & Climate Change 2010). This document states: “To allow public participation in the process, GDA (Generic Design Assessment) was designed specifically to be open and transparent.”

## 5.2 Properties of Interest

Evaluation of an assurance case requires assessment in several different although not entirely independent dimensions. Each of the dimensions corresponds to a property of interest, and the dimension associated with a property identifies the range of values that the property can have. Some properties of interest are the following:

- **Compelling Argument**

The argument in an assurance case must be compelling. That is, the argument must convince the observer of the truth of the top-level goal. Or, in other words, that the desired property of the associated system holds.

- **Valid Argument**

The argument in an assurance case must be an accurate representation of the rationale for belief in the top-level goal.

- **Complete Argument**

An assurance case must document the rationale for belief in the associated property of the subject system completely.

- **Confidence**

Evaluation of an assurance case relies upon examination of many components of the case including evidence, contexts, and inferences. Those examinations must be able to trust the presented material. That is, there must be confidence that the associated material reflects the true state of the system of interest.

- **Transparency/Readability**

An assurance case is an explicit documentation of the rationale for belief that a given subject system possesses a property of interest. That the documentation is explicit immediately facilitates scrutiny by any stakeholder or interested party. To facilitate scrutiny, the assurance case must be readable and sufficiently transparent that important information is accessible.

- **Certiability**

An important role of an assurance case is to facilitate approval of the associated system. Many important systems must be certified by a government agency before deployment. The assurance case must support this process by facilitating the mechanisms of approval.

- **Facilitate System Development**

An assurance case is not intended to be a burden placed on developers. Rather, an assurance case is intended to support developers by: (a) providing a reference during development for why the subject system is using the techniques and technology that it is, (b) facilitating development decisions by supporting reasoning during the selection process, and (c) supporting development managers in assessing the state of the development.

- **Intellectual Property Protection**

An assurance case contains a lot of descriptive material about the subject system, and various amounts of that material could be proprietary or classified. Thus, an assurance case needs to facilitate evaluation but do so in such a way as to protect the contained intellectual property.

- **Modularity**

In practice, assurance cases are large complex documents. Both construction of an assurance case and the associated evaluation are facilitated by modularity to the extent that modularity permits a “plug and socket” approach to both construction and evaluation.

- **Extensibility**

An assurance case should always be extensible. The need to change some aspect of an assurance case arises because of either: (a) changes in the operating conditions of the subject system, (b) changes in the system itself as a result of repair or upgrades, or (c) defects detected in the assurance case.

- **Multiple Properties**

The traditional role of an assurance case has been to provide the rationale for belief that a specified system has a specified property. The most common property of interest has been safety. Increasing interest in security has motivated the need to consider arguments

documenting the rationale for two or more properties. Of special interest are safety and security, because a security failure can lead to a system entering a hazardous state.

- **Integrity**

No information is lost (unless it is intentional), and all information gained or lost is attributed to one or more authors.

### **5.3 Conformance with Standards**

As discussed in Section 3.8, assurance cases and standards are complementary. This synergy is well illustrated in the area of assurance case evaluation. Development practices that yield evidence for an assurance case can be based on details documented in a standard in which case the standard is transformed into structured guidance. Recognized engineering standards that in some cases have been in use for protracted periods (DO-178B, for example, has been in use since 1992) can be viewed as excellent sources of guidance.

The most prominent organization that requires an assurance case (actually a *safety* case) for production safety critical systems is the U.K. Ministry of Defence. All systems built for the U.K. Ministry of Defence that have any safety implications are required to have a safety case.

The Ministry's requirement is stated in standard MoD 00-56 (U.K. Ministry of Defence 2007). Issue 5 is the latest draft version of MoD 00-56 and is presently under review. A draft of Issue 5 of MoD 00-56 states:

*“13.2 Safety Case. The Contractor shall produce a Safety Case or Safety Cases for a PSS as defined in the SMP.*

*13.2.1 The Contractor shall ensure that the Safety Case consists of a structured argument, supported by a body of evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment.”*

(In this standard, the meaning of the acronyms in the quoted text are: PSS – Products, Services and/or Systems; SMP – Safety Management Plan.)

Issue 5 makes explicit and extensive provision for the use of related engineering standards. Specifically, a draft of Issue 5 states:

*“6.1.1 The Contractor shall identify civil, open or other standards, or good practice, where they are used in full or partial fulfilment of the requirements of this Standard, and document the means by which any differences to this Standard will be resolved.*

*6.1.7 The Contractor should show that use of civil, open or other standards or good practice is appropriate for their Contract (eg ARP4754/DO-178 in an air application, or ISO 26262 in an automotive application).”*

Thus, evaluation of the resulting safety case where the safety case includes use of standards relies in part on assessment of conformance with the standard and documentation of differences.

The possible use of a standard in the context of an assurance case and the associated role of conformance with the standard as a significant part of evaluation of an assurance case is an excellent transition path for development organizations familiar with the current portfolio of standards.

## 5.4 Assurance Case Standards and Guidance Documents

This section examines various standards and guidance documents that have been developed in different domains. The materials discussed are tailored to the needs of the sponsoring domain yet might offer significant value to the aviation community. This section does not discuss ISO/IEC 15026, since that standard is generic and aimed strictly at assurance cases. ISO/IEC 15026 is discussed in Section 5.5.

Evaluation of an assurance case can be based upon an assurance-case standard. Note that in this circumstance, the standard is about the assurance case itself, not the engineering techniques used in development of the system. Thus, evaluation would be equivalent to an assessment of conformance with the assurance-case standard. In developing an evaluation approach for assurance cases in any particular domain, examination of existing standards might be useful. Caution must be exercised, however; because, as noted in Section 4, the term has different definitions in different domains.

Some examples of what are stated to be assurance case standards are:

- **Offshore Installations**

The Health and Safety Executive in the United Kingdom has developed extensive documentation including evaluation requirements for safety cases for offshore installations (UK Health and Safety Executive 2006, UK Health and Safety Executive 2008). The documents are informal and use the term “safety case” in a thoroughly informal and domain-specific sense. Nevertheless, the material is extensive and worth review as a source of assurance-case quality criteria.

- **Nuclear Installations**

The Office for Nuclear Regulation in the United Kingdom has developed a detailed guidance document for safety cases in the nuclear domain. The notion of a safety case used by the Office of Nuclear Regulation is summarized as (Office for Nuclear Regulation 2013b):

*“The primary purpose of a safety case is to provide the licensee with the information required to enable safe management of the facility or activity in question.”*

*“A safety case should communicate a clear and comprehensive argument that a facility can be operated or that an activity can be undertaken safely.”*

Relevant sections of the guidance document include (listed under the group heading of “Advice to Assessors”):

- Section 5 – Definition of a Nuclear Safety Case
- Section 6 – The Purpose of a Safety Case
- Section 7 – Overall Qualities of a Safety Case
- Section 8 – The Structure and Content of a Safety Case

These sections of the guidance document provide a wealth of information relevant to evaluation that can be adapted quickly to other domains.

Of particular note are Appendices 1 and 2 of this guidance document. They are entitled:

- Appendix 1 - “Common Problems with Safety Cases”
- Appendix 2 - “Nimrod Review – Safety Case Shortcomings and Traps”

Appendix 1 is a detailed list of problems and as such forms an excellent basis for at least one phase of a safety-case evaluation procedure. Appendix 2 as the name implies is a detailed list of shortcomings and traps that are explained carefully and thoroughly. Again, Appendix 2 would form the basis of a phase of a safety-case evaluation procedure.

Also of note in this standard is Table 1. This table provides a detailed mapping between nuclear plant design and development stages and the associated activities that are required for the safety case. The table can be modified easily to provide a similar mapping to other domains.

- **Nuclear Waste**

The International Atomic Energy Agency (IAEA) has developed extensive guidance for the disposal of nuclear waste (International Atomic Energy Agency 2012). The guidance is detailed and contains valuable material that could be adapted to other domains relatively easily. Assessment of nuclear waste disposal plans and procedures uses safety cases, and the IAEA guidance offers a great deal of valuable material on safety case evaluation. The notion of a safety case used by the IAEA is semi-rigorous. The guidance contains the following text that summarizes what the IAEA regards as the role of a safety case:

*“The safety case provides a basis for decision making and is presented to the relevant decision makers for their review and consideration. The parties interested in the safety case may include regulators, the general public and other interested parties. These parties will decide for themselves the extent to which they are convinced by the reasoning that is presented, and whether they share the confidence of the operator developing the safety case. The confidence of the interested parties in the findings of the safety case should, however, be enhanced if the arguments and evidence are presented in a manner that is open and transparent, and all relevant results are fully disclosed and subject to quality control and independent review.”*

Along with this notion of the role of the safety case, the IAEA guidance includes a variety of advice on safety-case quality (and hence what might be checked as part of evaluation) including the following:

*“Independent peer review should play an important role in building confidence in the safety case for a radioactive waste disposal facility.”*

*“Confidence in the safety case may also be enhanced by the use of multiple lines of reasoning. The use of multiple lines of reasoning may add value to the safety case by providing a range of different arguments that together build confidence in certain data, assumptions and results. Furthermore, certain arguments may be more meaningful to specific audiences.”*

*“If the evidence, arguments and analyses do not provide sufficient confidence to support a positive decision, then the safety case, the facility design or even the disposal concept may need to be revised.”*

Importantly, the IAEA guidance addresses the need to address both quantitative and qualitative aspects of a safety argument:

*“The conclusions drawn from the quantitative assessment should be supplemented by qualitative arguments and assessments.”*

The guidance contains specific material on the following topics:

- Requirements for the safety case and safety assessment,
  - Role and development of the safety case,
  - Components of the safety case,
  - Evolution of the safety case,
  - Documentation of the safety case,
  - Uses of the safety case, and
  - Regulatory review process.
- **Air Traffic Control**

Eurocontrol has published a wide range of documents on many aspects of safety assessment, safety documentation, and safety cases (Eurocontrol 2007, Eurocontrol 2009).

## **5.5 ISO/IEC 15026-2**

ISO/IEC 15026-2 is part two of four parts of ISO/IEC 51206. The standard is entitled: “Systems and software engineering – Systems and software assurance”, and part two is subtitled: “Assurance case.” According to the standard (International Organization for Standardization 2011a):

*“The purpose of this part of ISO/IEC 15026 is to ensure the existence of types of assurance case content and restrictions on assurance case structure thereby improving consistency and comparability among instances of assurance cases and facilitating stakeholder communications, engineering decisions, and other uses of assurance cases.”*

*“The standard specifies minimum requirements for the structure and contents of an assurance case.”*

This standard is the only standard for assurance cases developed by a standards organization.

The majority of ISO/IEC 15026-2 provides structural guidelines for an assurance case. The structural guidelines are presented in the form of a grammar (or graph rule-set) extending from general goals towards supporting evidence. The components of the 15026’s structural definitions are generally well understood by the community, and conform to the basic components often found in structured assurance cases.

ISO/IEC 15026 does not require, however, that an assurance case directly represent itself using their structural model. Instead, a 15026-compliant assurance case needs map explicitly from its argument to the ISO/IEC 15026 structure. So long as the mapping is complete, clear, explicit, and the resulting mapped argument obeys the required structural rules, then an assurance case is considered 15026 compliant.

ISO/IEC 15026 defines an overall structure of an assurance to consist of five principal components: claims, arguments, evidence, justifications and assumptions. Unlike more familiar structural definitions, the standard uses the notion of a justification for a method of argumentation rather than a strategy. The defined structure is presented in a rather obscure and unexplained mathematical form.

The mathematical form is supplemented by a set of requirements on the structure that are defined in English. For example, nodes may not refer to themselves. This applies transitively. Thus, all sub-nodes represent recursive detail refinement. In general, a case consists of one or more top-level claims, each supported with a justification and an argument. Arguments consist of further claims, sub-arguments, assumptions, and evidence. Both sub-claims and assumptions can result in further decomposition into argument. Sub-claims are explicitly defined as requiring argumentation. Assumptions tend to be more limited by conditions. They may or may not require a sub-claim depending on the nature of what is assumed.

The ISO/IEC 15026-2 standard describes both structural and semantic requirements for an assurance case. Through their combination, 15026-2 enhances the goals of various stakeholders through the safety case.

The five component types should be sufficient such that the argument can be explicitly mapped to these element types. If such a mapping is incomplete, an assurance case cannot be 15026 compliant. Further, the mapping must be made explicit in order for an assurance case to be 15026 compliant. Readers should not need to deduce a mapping.

These semantic constraints fall into several general categories:

1. *Consistency*: Basic utility must follow in the assurance case. *Non sequitur* is not conformant to the standard. For example, an argument's conclusion must imply its claim, or that the statement of an argument describes and uses its sub-contents.
2. *Explicitness*: Where possible, assurance components are called out explicitly, such as that arguments state their case as well as show subcomponents, that arguments and claims have justification, and that evidence is tangible.
3. *Scope*: Claims and all subcomponents explicitly call out limits in their applicability where they occur. All sub-components can operate within these constraints. This can both enable assumptions and limit required arguments.
4. *Graded Risk/Confidence*: Where applicable, components model the probability of their veracity and the risks they create, rather than assume a binary model of veracity and risk.

## 5.6 Documentation Review

In evaluation of an assurance case, much of what is required rests on human insight. The form of an assurance case is, for the most part, not amenable to mechanical analysis. Further, the content of the assurance case is embodied in natural language semantics.

In evaluation, human insight is strengthened by systematic procedures and associated tools. A simple example of this is provided by the U.K. HSE's "Safety Case Handling and Assessment Manual" (UK Health & Safety Executive 2013) for the gas and pipeline industry, which comprises documentation processes and reviewer guidelines. This can also be seen clearly in the field of software inspections. Software inspections routinely use techniques such as Fagan Inspections (Fagan 1986), Phased Inspections (Knight & Myers 1993), and Active Reviews (Parnas & Weiss 1985). These techniques can be adapted easily to provide the same benefits to assurance argument evaluation as has been measured in software development.

## 5.7 Assurance Argument Evaluation Theory

The most difficult part of assurance-case evaluation is determination of the first three properties listed in Section 5.1, the degree to which the included assurance argument can be considered to be *compelling*, *valid* and *complete*. We will refer to these properties as the three

*essential* properties. If the argument linking the evidence to the top-level goal is lacking any of the essential properties, then whether an assurance case possesses the rest of the assurance case properties is not important.

The development of arguments that possess the three essential properties in assurance cases is known to be hard. The difficulties arise from many sources, but a key difficulty is the fact that arguments in assurance cases tend to be mostly *inductive*. Belief in a claim relies upon evidence that might support the claim (enumerative evidence) or raise doubt about the claim (eliminative evidence). Whereas deductive logic is inherently objective, inductive logic necessarily includes an element of human belief. Thus, the role of evaluation of assurance arguments is to provide an answer to the question: “Should the top-level goal in the assurance argument be believed?”

Many researchers have attempted to provide a rigorous basis for arguments. In this section, we summarize these efforts.

### **5.7.1 Baconian Probability**

(Goodenough, Weinstock, and Klein 2013) introduced the notion of *eliminative induction* into the assurance case literature. This approach is novel and quite different from the other approaches to argument evaluation that have been developed. The basis of eliminative induction is defeasible reasoning (Pollock 2008).

The concept is best summarized in the abstract from the authors’ original publication on the topic (Goodenough et al. 2012):

*“Assurance cases provide an argument and evidence explaining why a claim about some system property holds. This report outlines a framework for justifying confidence in the truth of such an assurance case claim. The framework is based on the notion of eliminative induction—the principle (first put forward by Francis Bacon) that confidence in the truth of a hypothesis (or claim) increases as reasons for doubting its truth are identified and eliminated. Possible reasons for doubting the truth of a claim (defeaters) arise from analyzing an assurance case using defeasible reasoning concepts. Finally, the notion of Baconian probability provides a measure of confidence based on how many defeaters have been identified and eliminated.”*

Importantly, this approach addresses the issue of argument evaluation from the opposite perspective to that used in other approaches. The usual direction is to try to determine why an argument as presented should be believed. As has been pointed out by (Leveson 2011), there is a chance that confirmation bias could affect the assessment. By focusing on defeaters, eliminative induction is actively attempting to determine why the argument should not be believed.

### **5.7.2 Bayesian Belief Networks**

A Bayesian Belief Network (BBN) is a graphical model of a set of dependent probabilities. Some researchers are exploring the use of BBNs to evaluate arguments (Denney et al. 2011). In argument evaluation, a BBN can be used to try to compute a probability of belief in the various goals in the argument, particularly the top-level goal. The limiting factor in such computations is the extent to which the argument relies on qualitative evidence. For example, human judgment is basically an opinion and as such is qualitative. To deal with qualitative items, one can map qualitative assessments to values between 0 and 1. Critics of efforts to quantify belief using

probabilistic methods including BBNs question, among other things, the accuracy of mapping inherently qualitative notions to specific probability values or intervals.

### **5.7.3 Argumentation Theory**

Argumentation theory is the study of general reasoning and includes areas such as debate, persuasion, negotiation, legal argument, political argument, and dialog.

Some researchers in argumentation theory have developed formalized systems of argumentation that support reasoning about properties of arguments. (Tang et al. 2012), for example, have developed a formal system for reasoning about what they characterize as trust and belief. This work is actually in the context of decentralized systems in which decisions have to be made based on information obtained from autonomous agents. The paper states:

*“... we introduce a formal system of argumentation that can be used to reason using information about trust. This system is described as a set of graphs, which makes it possible to combine our approach with conventional representations of trust between individuals where the relationships between individuals are given in the form of a graph. The resulting system can easily relate the grounds of an argument to the agent that supplied the information, and can be used as the basis to compute Dungian notions of acceptability that take trust into account.”*

This technology can be transferred to evaluation of assurance arguments where the notion of trust is replaced with the notion of belief in a claim.

### **5.7.4 Operational Definition**

The three essential properties (compelling, valid and complete) have intuitive meanings but are not defined precisely in any assurance case documentation. Of particular note is the U.K. Ministry of Defence standard 00-56 which requires delivery of a safety case with the three essential properties but does not define the terms.

(Graydon, Knight and Green 2010) offered a definition of the three essential properties using an *operational* definition. A set of testable properties were defined, and, if an assurance case (more particularly a safety case as required by 00-56) could be shown to possess those testable properties, then the assurance case was defined to have the three essential properties. Evaluation of an assurance case could thus be focused on testing for these properties.

## **5.8 Argument Structural Analysis**

Fundamentally, an assurance case can take any form that provides confidence in an argument to the reader. However, many of the goals of an assurance case, such as readability, certify-ability, modularity, and integrity, benefit from a more *formal* and *regular* structure to the argument.

Throughout Section 4, assurance cases were shown to take on different levels of formality and structure in their argumentation and presentation of evidence. It can be argued that as assurance cases move towards application by larger sets of stakeholders, and the stakeholders demand quality in achieving the properties itemized in Section 5.1, it will be imperative that assurance cases take on a more regular structure.

Regular, well-defined structure aids an assurance case in several key respects:

- it classifies the make-up of an argument into a discrete set of a component types, and

- it regularizes the structure between components.

This order improves the ability of stakeholders to:

- Detect invalidity and unsoundness in the argument.
- Detect gaps in the completeness of the argument.
- Decompose the argument into modules.
- Extend the argument.
- Audit changes and assign ownership and rationale to changes.

And perhaps most importantly,

- Divide-and-conquer in assessing the credibility of the argument.

In essence, well-defined structure *improves* the ability of the reader to judge the utility of the argument. In this section, we will consider how structural formalisms can be applied in the analysis of an assurance cases for various stakeholders, including designers and regulators.

Note that structural integrity of an assurance case *is not* sufficient to conclude *soundness or validity*. That is, the premises of the assurance case can be false, and even if they are true, the conclusion of the assurance case can be false.

Most importantly, common assurance case structures are not, generally speaking, sufficient to be logical calculi, even when formalized. They cannot be used to compute the truth of an argument. This differentiates an assurance case from a deductive logic, where structural compliance along with sufficient information can be used to compute validity and soundness.

The purpose of structure in the safety case, as described above, is to aid the human reader in the interpretation of an argument. This is not to say, however, that logical assertions are not part of an assurance case. In fact, there is increasing use of sound and valid logical argument within assurance cases both as evidence and argumentation. Regular structure aids in the injection of formal logic within an assurance case.

By themselves, structural constraints tend to aid the goals of stakeholders in organization of the case, such as with respect to *readability, integrity, modularity, and extensibility*. Combined with semantic constraints, they can aid in the determination of correctness, confidence and completeness by regulating required analysis over an organized structure.

## 6. Conclusion

We believe this report satisfies our objective to introduce assurance cases to an interested audience, specifically from the perspective of potential applications to aviation. This report seeks to be a unique resource to present assurance cases not only at the conceptual level, but also through real-world examples. Those considering assurance cases need to see not just the concepts, but also the applied methods that have been successful (or, in some cases, informatively unsuccessful). This report provides a wide range of assurance case data points so as to serve as a springboard for more focused investigation. We hope that the classification scheme we've developed is useful to a broad audience for characterizing and understanding the shades of distinction between various applications of assurance cases.

We assert that the foundation, examples, and evaluation of assurance cases we've reviewed above are a valuable consideration from the perspective of aviation in the U.S. and abroad. Assurance cases are a good fit for aviation, which is dominated by safety-critical, technologically advanced, highly integrated systems. We have seen both conceptually and by example that assurance case processes should be consistently integrated in parallel with system development processes. Any steps toward assurance case adoption can (and should) be slow and steady. Such a movement could start with assurance cases being employed to organize and validate current system assurance requirements, identifying opportunities for flexibility and efficiency. Assurance cases could next provide the requisite logic for alternative approaches that further strengthen and streamline system assurance.

For further reading (in addition to what is referenced in context throughout this report), we specifically recommend the following sources:

- “A Methodology for Safety Case Development” (Bishop and Bloomfield 1998). This short paper is slightly dated, but still it is a straightforward and pragmatic introduction to constructing argument-based cases for system assurance.
- “Reviewing Assurance Arguments – A Step-By-Step Approach” (Kelly 2007). This paper provides an excellent starting point on the subject of assurance case assessment. It is well-written, practical, and a quick read (5 pages).
- “An Introduction to System Safety Management in the MOD” (UK Ministry of Defence 2011). This document is sometimes called the “white book”. As noted above, the United Kingdom government has played a significant role in developing the principles behind safety cases and assurance cases. This resource is not as explicit as it could be about argumentation, perhaps reflecting some conservatism in the state of official regulation. Otherwise, especially considering its brevity, it covers an impressive range and integrates safety cases with traditional methods such as risk management.
- “Software Assurance Using Structured Assurance Case Models” (Rhodes et al. 2009). This document, produced by the US National Institute of Standards and Technology, is another impressively brief resource, this reflects a certain track of assurance case development within the U.S. and does a good job of placing argumentation front and center.

In closing, we express our hope that this is a valuable resource for the aviation community and the burgeoning field of assurance case practitioners.

## 7. References

- Adelard (1998). *ASCAD: Adelard Safety Case Development Manual*. Available from <http://www.adelard.com/resources/ascad/> (last accessed January 7, 2015).
- Alexander, R., Hawkins, R. & Kelly, T. (2011). *Security Assurance Cases: Motivation and the State of the Art*, Issue 1.1. CESG/TR/2011/1. University of York. [http://www-users.cs.york.ac.uk/~rda/York%20CESG%20security%20case%20report%20i1\\_1.pdf](http://www-users.cs.york.ac.uk/~rda/York%20CESG%20security%20case%20report%20i1_1.pdf) (last accessed January 7, 2015).
- Ankrum, T. S. (2004). *Assurance Case Frameworks: Part of High Confidence Software MSR*. (Presentation) MITRE - Software Engineering Center. [http://www.sigada.org/locals/dc/200403\\_Ankrum\\_Assurance\\_Case.ppt](http://www.sigada.org/locals/dc/200403_Ankrum_Assurance_Case.ppt) (last accessed January 7, 2015).
- American Petroleum Institute (2004). Recommended Practice for Development of a Safety and Environmental Management Program for Offshore Operations and Facilities . API RP 75 (R2008).
- Baram, M. (2011). *Preventing Accidents in Offshore Oil and Gas Operations: the US Approach and Some Contrasting Features of the Norwegian Approach*. Deepwater Horizon Study Group. [http://ccrm.berkeley.edu/pdfs\\_papers/DHSGWorkingPapersFeb16-2011/PreventingAccidents-in-OffshoreOil-and-GasOperations-MB\\_DHSG-Jan2011.pdf](http://ccrm.berkeley.edu/pdfs_papers/DHSGWorkingPapersFeb16-2011/PreventingAccidents-in-OffshoreOil-and-GasOperations-MB_DHSG-Jan2011.pdf) (last accessed January 7, 2015).
- Bishop, P. & Bloomfield, R. (1998). A Methodology for Safety Case Development. In F. Redmill & T. Anderson (ed.), *Industrial Perspectives of Safety-Critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium*. Birmingham, UK. <http://www.adelard.com/papers/sss98web.pdf> (last accessed January 7, 2015)
- Bloomfield, R. (2012). Assurance Cases: Divide and conquer or divide and fall? *2012 Annual Computer Security Applications Conference*. Orlando, Florida.
- Bloomfield, R., Chozos, N. & Cleland, G. (2012). *Supplement G: Safety case use within the medical devices industry*. Supplement to Using safety cases in industry and healthcare. [http://www.health.org.uk/media\\_manager/public/75/publications\\_pdfs/Safety%20cases\\_supplement%20G.pdf](http://www.health.org.uk/media_manager/public/75/publications_pdfs/Safety%20cases_supplement%20G.pdf) (last accessed January 7, 2015).
- Cullen, The Hon. Lord W. Douglas (1990). *The public inquiry into the Piper Alpha disaster*. London: H.M. Stationery Office. ISBN: 0101113102.
- Denney, E., Pai, G. & Habli, I. (2011). Towards Measurement of Confidence in Safety Cases. *5th International Symposium on Empirical Software Engineering and Measurement*. Banff, Alberta, Canada.
- Department of Energy & Climate Change (2010). The United Kingdom's Fifth National Report on Compliance with the Convention on Nuclear Safety Obligations. <http://www.onr.org.uk/cns5.pdf> (last accessed January 7, 2015).
- Dezfuli, H., Benjamin, A., Everett, C., Smith, C., Stamatelatos, M. & Youngblood, R. (2011). *NASA System Safety Handbook: Volume 1, System Safety Framework and Concepts for Implementation* (Version 1.0). NASA/SP-2010-580.
- Emmet, L. (2008). *International Standardisation of Assurance Cases*. (Presentation) Adelard LLC. [http://www.adelard.com/asce/user-group/7-Jun-2011/International\\_standardisation\\_Assurance\\_cases\\_Emmet\\_v01b.pdf](http://www.adelard.com/asce/user-group/7-Jun-2011/International_standardisation_Assurance_cases_Emmet_v01b.pdf) (last accessed January 7, 2015).
- Engen, O. A. (2012). Risk regulatory regimes of the Norwegian Petroleum Sector and the “Nordic model”. *36th Annual Center for Oceans Law and Policy Conference*. Halifax, Nova Scotia, Canada.
- Ericson, II, C. A. (2006). A Short History of System Safety. *Journal of System Safety*, 42(3).

Eurocontrol (2012a). Preliminary Safety Case for Air Traffic Control Service in Non-Radar Areas using Wide Area Multilateration (WAM) as Sole Means of Surveillance. (Edition 1.2)  
<https://www.eurocontrol.int/sites/default/files/content/documents/nm/surveillance/cascade/surveillance-wam-nra-psc1-2.pdf> (last accessed January 7, 2015).

Eurocontrol (2012b). SRC Document 51: Review of the Wide Area Multilateration for Non Radar Areas (WAM-NRA) Preliminary Safety Case. (Edition 1.0)  
<http://www.eurocontrol.int/sites/default/files/article/content/documents/single-sky/src/src-docs/src-doc-51-e1.0.pdf> (last accessed January 7, 2015).

Eurocontrol (2009). EUROCONTROL Guidance Material for Short Term Conflict Alert - Appendix B-3 - Outline Safety Case for STCA System. (Edition 2.0)  
[http://www.eurocontrol.int/sites/default/files/field\\_tabs/content/documents/nm/safety/appendix-a-reference-stca-system.pdf](http://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/nm/safety/appendix-a-reference-stca-system.pdf) (last accessed January 7, 2015).

Eurocontrol (2007). Airport Collaborative Decision Making (A-CDM) Safety Case Guidance Material. (Version 1.1)  
[http://www.eurocontrol.int/sites/default/files/field\\_tabs/content/documents/nm/airports/cdm-safety-case-guidance-january-2007.pdf](http://www.eurocontrol.int/sites/default/files/field_tabs/content/documents/nm/airports/cdm-safety-case-guidance-january-2007.pdf) (last accessed January 7, 2015).

European Railway Agency (2014a). SMS: Introduction.  
<http://www.era.europa.eu/tools/sms/Pages/Introduction.aspx> (last accessed September 4, 2014).

European Railway Agency (2014b). *2014 Railway Safety Performance in the European Union*.  
<http://www.era.europa.eu/Document-Register/Documents/SPR2014.pdf> (last accessed January 7, 2015).

European Union (2008). Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rail system within the Community. Official Journal L 191, P. 0001 - 0045.

European Union (2004). DIRECTIVE 2004/49/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2004 on safety on the Community's railways and amending Council Directive 95/18/EC on the licensing of railway undertakings and Directive 2001/14/EC on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification (Railway Safety Directive). Official Journal L 220, P. 0016 - 0039 .

European Union (2001). Directive 2001/14/EC of the European Parliament and of the Council of 26 February 2001 on the allocation of railway infrastructure capacity and the levying of charges for the use of railway infrastructure and safety certification. Official Journal L 075, P. 0029 - 0046 .

Fagan, M. E. (1986, July). Advances in Software Inspections. *IEEE Transactions on Software Engineering*, SE-12(7), 744-751.

Food and Drug Administration (2013). Medical Device Classification Procedures: Determination of safety and effectiveness. 21CFR860.7. U.S. Department of Health and Human Services.  
<http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=860.3> (last accessed January 7, 2015).

Food and Drug Administration (2011). FDA Infusion: Infusion Pump Software Safety Research at FDA. U.S. Department of Health and Human Services. Last updated 04/21/2011,  
<http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202511.htm>. (last accessed September 4, 2014).

Food and Drug Administration (2014). Guidance for Industry and FDA Staff - Total Product Life Cycle: Infusion Pump - Notification [510(k)] Submissions (Draft). U.S. Department of Health and Human Services, December 2, 2014.  
<http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM209337.pdf> (last accessed January 7, 2015).

- Goodenough, J. B., Weinstock, C. B. & Klein, A. Z. (2013). Elimination Induction: A Basis for Arguing System Confidence. *35<sup>th</sup> International Conference on Software Engineering*, San Francisco, California. <http://www.sei.cmu.edu/library/assets/whitepapers/ICSE%20NIER%202013%20Eliminative.pdf>. (last accessed September 4, 2014).
- Goodenough, J. B., Weinstock, C. B. & Klein, A. Z. (2012). *Toward a Theory of Assurance Case Confidence*. CMU/SEI-2012-TR-002. Software Engineering Institute. [http://resources.sei.cmu.edu/asset\\_files/TechnicalReport/2012\\_005\\_001\\_28161.pdf](http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_28161.pdf) (last accessed January 7, 2015).
- Graydon, P., Knight, J. & Green, M. (2010). Certification and Safety Cases. *Proceedings of the 28<sup>th</sup> International System Safety Conference*. Minneapolis, Minnesota. <http://www.cs.virginia.edu/~jck/publications/ISSC.2010.pdf> (last accessed January 7, 2015).
- Greenwell, W. S., Knight, J. C., Holloway, C. M. & Pease, J. J. (2006). A Taxonomy of Fallacies in System Safety Arguments. *Proceedings of the 24th International System Safety Conference*. Albuquerque, New Mexico. <http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20060027794.pdf> (last accessed January 7, 2015).
- GSN Committee (2011). Draft GSN Standard Version 1.0. <http://www.goalstructuringnotation.info/> (last accessed December 2, 2014).
- Habli, I., Birch, J., Monkhouse, H., Rivett, R., Higham, D., Botham, J., Palin, R., Bradshaw, B. & Jesty, P. (2013). Safety Cases and Their Role in ISO 26262 Functional Safety Assessment. *32nd International Conference on Computer Safety, Reliability, and Security*. Toulouse, France.
- Haddon-Cave, C. (2009). *The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006*. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/229037/1025.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf) (last accessed January 7, 2015).
- Hall, M. & Spence, T. (2013). Safety official sees no link between EU rail liberalisation, fatal accidents. EurActive.com online article, <http://www.euractiv.com/transport/link-eu-rail-liberalisation-fata-news-529582>. (last accessed September 4, 2014).
- Henriksen, D. E. (2012). Managing environmental risks in the Norwegian offshore oil and gas business. Presentation. Rio de Janeiro. [http://www.riela.org/pdfs/rio\\_2012/10-Dag%20Henriksen.pdf](http://www.riela.org/pdfs/rio_2012/10-Dag%20Henriksen.pdf) (last accessed January 7, 2015).
- Holloway, C. M. (2013). Making the Implicit Explicit: Towards An Assurance Case for DO-178C. *31st International System Safety Conference*. Boston, Massachusetts. <http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20140002745.pdf> (last accessed January 7, 2015).
- Holloway, C. M. (2008). Safety Case Notations: Alternatives for the Non-Graphically Inclined? *Proceedings of 3rd IET International Conference on System Safety*. Birmingham, UK. <http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20080042416.pdf> (last accessed January 7, 2015).
- International Atomic Energy Agency (2012). The Safety Case and Safety Assessment for the Disposal of Radioactive Waste. IAEA Safety Standards Series SSG-23. [http://www-pub.iaea.org/mtcd/publications/pdf/pub1553\\_web.pdf](http://www-pub.iaea.org/mtcd/publications/pdf/pub1553_web.pdf) (last accessed January 7, 2015).
- International Organization for Standardization (2011a). Systems and software engineering – Systems and software assurance – Part 2: Assurance case. ISO/IEC 15026-2:2011.
- International Organization for Standardization (2011b). Road vehicles – Functional safety. ISO 26262:2011.
- International Organization for Standardization (2009). Information technology-Security techniques-Evaluation criteria for IT security-Part 1. ISO 15408-1:2009.

- Jee, E., Lee, I. & Sokolsky, O. (2010). Assurance Cases in Model-Driven Development of the Pacemaker Software. *4th Int. Symposium On Leveraging Application of Formal Methods, Verification and Validation (ISoLA)*. Crete.
- Jeffrey, K. (2013). Review: Lord Cullen - what have we learned from Piper Alpha? [http://www.findingpetroleum.com/n/Review\\_Lord\\_Cullen\\_what\\_have\\_we\\_learned\\_from\\_Piper\\_Alpha/044b5113.aspx](http://www.findingpetroleum.com/n/Review_Lord_Cullen_what_have_we_learned_from_Piper_Alpha/044b5113.aspx). (last accessed September 4, 2014).
- Kelly, T. & Weaver, R. (2004). The Goal Structuring Notation – A Safety Argument Notation. In *Proceedings of the Dependable Systems and Networks 2004 - Workshop on Assurance Cases*. Florence, Italy.
- Kelly, T. P. (2007). Reviewing Assurance Arguments – A Step-By-Step Approach. In *DSN 2007: The 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. Edinburgh, Scotland.
- Kelly, T. P. (1998). *Arguing Safety – A Systematic Approach to Managing Safety Cases*. Doctoral dissertation, University of York. <http://www-users.cs.york.ac.uk/tpk/tpkthesis.pdf> (last accessed January 7, 2015)
- Knight, John C. and Myers, E. Ann (1993). An improved inspection technique. *Communications of the ACM CACM*, 36(11), 51-61.
- Leveson, N. (2011). The Use of Safety Cases in Certification and Regulation. *Journal of System Safety*, 47(6), Nov-Dec.
- Masci, P., Ayoub, A., Curzon, P., Lee, I., Sokolsky, O. & Thimbleby, H. (2013). Assurance-Based Development of the Generic PCA Infusion Pump User Interface Prototype. <http://www.eecs.qmul.ac.uk/~masci/works/drafts/NASAFM2013-draft.pdf> (last accessed January 7, 2015).
- McDermid, J. A. (1994). Support for Safety Cases and Safety Arguments using SAM. *Reliability Engineering and System Safety*, 43, 111-127.
- Medhurst, J. & Embrey, D. (2012). *Supplement F: Safety case use in the railway industry*. Human Reliability Associates. Supplement to Using safety cases in industry and healthcare. [http://www.health.org.uk/media\\_manager/public/75/publications\\_pdfs/Safety%20cases\\_supplement%20F.pdf](http://www.health.org.uk/media_manager/public/75/publications_pdfs/Safety%20cases_supplement%20F.pdf) (last accessed January 7, 2015).
- Méry, D., Schätz, B. & Wassying, A. (eds) (2014). The Pacemaker Challenge: Developing Certifiable Medical Devices. *Dagstuhl Reports*, 4(2), 17-37. [http://drops.dagstuhl.de/opus/volltexte/2014/4543/pdf/dagrep\\_v004\\_i002\\_p017\\_s14062.pdf](http://drops.dagstuhl.de/opus/volltexte/2014/4543/pdf/dagrep_v004_i002_p017_s14062.pdf) (last accessed January 7, 2015).
- Northrop Grumman (2014). Photo Release – Northrop Grumman, U.S. Navy Complete Initial Flight Testing of the Triton Unmanned Aircraft System. Press Release - <http://www.globenewswire.com>. (last accessed September 4, 2014).
- Object Management Group (2013). Structured Assurance Case Metamodel (SACM). <http://www.omg.org/spec/SACM/1.0/PDF/> (last accessed January 7, 2015).
- Office for Nuclear Regulation (2014a). *New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties* (ONR-GDA-GD-001 Revision 1). U.K. Health and Safety Executive. <http://www.onr.org.uk/new-reactors/ngn03.pdf> (last accessed January 7, 2015).
- Office for Nuclear Regulation (2014b). *Generic Design Assessment Progress Report: Reporting Period April - June 2014* (TRIM 2014/184570). U.K. Health and Safety Executive. <http://www.onr.org.uk/new-reactors/reports/gda-quarterly-report-april-june-2014.pdf> (last accessed January 7, 2015).

Office for Nuclear Regulation (2013a). *Generic Design Assessment Progress Report: Reporting Period December 2012 – August 2013* (TRIM 2013/306704). U.K. Health and Safety Executive. <http://www.onr.org.uk/new-reactors/reports/gda-progress-report-1212-0813.pdf> (last accessed January 7, 2015).

Office for Nuclear Regulation (2013b). *The Purpose, Scope, and Content of Safety Cases* (NS-TAST-GD-051 Revision 3). U.K. Health and Safety Executive. [http://www.onr.org.uk/operational/tech\\_asst\\_guides/ns-tast-gd-051.pdf](http://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-051.pdf) (last accessed January 7, 2015).

Office for Nuclear Regulation (2013c). *Summary of Lessons Learnt during Generic Design Assessment (2007 – 2013)* (ONR-GDA-SR-13-001 Revision 0). U.K. Health and Safety Executive. <http://www.onr.org.uk/new-reactors/reports/onr-gda-sr-13-001.pdf> (last accessed January 7, 2015).

Office for Nuclear Regulation (2008). *Safety Assessment Principles for Nuclear Facilities* (2006 Edition, Revision 1). U.K. Health and Safety Executive. <http://www.onr.org.uk/saps/saps2006.pdf> (last accessed January 7, 2015)

Oil & Gas UK (2008). *Piper Alpha: Lessons Learnt, 2008*. <http://www.oilandgasuk.co.uk/cmsfiles/modules/publications/pdfs/HS048.pdf>. (last accessed September 4, 2014).

Palin, R. & Habli, I. (2010). Assurance of Automotive Safety: A Safety Case Approach. *Proceedings of the 29th International Conference on Computer Safety, Reliability, and Security*. Vienna, Austria.

Palin, R., Ward, D., Habli, I. & Rivett, R. (2011). ISO 26262 Safety Cases: Compliance And Assurance. *Proceedings of the IET 6th International System Safety Conference*. Birmingham, UK.

Parnas, D. L. and Weiss, D. M. (1985). Active design reviews: principles and practices. *ICSE '85 Proceedings of the 8th International Conference on Software Engineering*, pp. 132-136, IEEE Computer Society Press, Los Alamitos, CA.

Parsons, M. & Hunter, C. (2010). Patterns in Safety-Related Projects. *Proceedings of the Eighteenth Safety-critical Systems Symposium*. Bristol, UK.

Patu, V. (2013). Introducing Our New Method of Writing Systems Assurance Cases. *E-Learn 2013: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education 2013(1)*, 1566-1575. Chesapeake, Virginia.

Petroleum Safety Authority of Norway (2013). Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (the management regulations). Online / English Version. (Retrieved from [www.psa.no](http://www.psa.no), updated annually, last accessed September 4, 2014).

Real-Time Systems Group (RTG) (2014a). Generic PCA Infusion Pump Reference Implementation. University of Pennsylvania. <http://rtg.cis.upenn.edu/medical/gpca/gpca.html>. (last accessed September 4, 2014).

Real-Time Systems Group (RTG) (2014b). Assurance Cases for Medical Devices. University of Pennsylvania. [http://rtg.cis.upenn.edu/medical/assurance\\_cases.html](http://rtg.cis.upenn.edu/medical/assurance_cases.html). (last accessed September 4, 2014)

Rhodes, T., Boland, F., Fong, E., Kass, M. Software Assurance Using Structured Assurance Case Models, NIST Interagency Report 7608, May 2009. <http://nvlpubs.nist.gov/nistpubs/ir/2009/ir7608.pdf> (last visited January 7, 2015).

RTCA (2011). Software Considerations in Airborne Systems and Equipment Certification. DO-178C.

RTCA (1992). Software Considerations in Airborne Systems and Equipment Certification. DO-178B.

SAE (2010). Guidelines for Development of Civil Aircraft and Systems. ARP4754a.

SAE (1996). Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment. ARP4761.

Thimbleby, H. (2013). Improving safety in medical devices and systems. *2013 IEEE International Conference on Healthcare Informatics*. Philadelphia, Pennsylvania.

Toulmin, S. E. (1958). *The Uses of Argument*. Cambridge University Press.

Transportation Research Board of the National Academies (2012) *Evaluating the Effectiveness of Offshore Safety and Environmental Management Systems* (Special Report 309). Committee on the Effectiveness of Safety; Environmental Management Systems for Outer Continental Shelf Oil & Gas Operations. <http://onlinepubs.trb.org/onlinepubs/sr/SR309.pdf> (last accessed January 7, 2015).

Turner, J. (2013). Sea change: offshore safety and the legacy of Piper Alpha . Offshore-Technology.com. <http://www.offshore-technology.com/features/feature-piper-alpha-disaster-anniversary-offshore-safety/>. (last accessed September 4, 2014).

UK Civil Aviation Authority (2014). CAP 670: Air Traffic Services Safety Requirements. <http://www.caa.co.uk/docs/33/CAP%20670%2023%20May%202014.pdf> (last accessed January 7, 2015).

UK Civil Aviation Authority (2010). CAP 760: Guidance on the Conduct of Hazard Identification, Risk Assessment and the Production of Safety Cases: For Aerodrome Operators and Air Traffic Service Providers. <http://www.caa.co.uk/docs/33/CAP760.pdf> (last accessed January 7, 2015).

UK Health & Safety Executive (2013). Safety Case Handling and Assessment Manual. PM/Permissioning/04 Version 8. <http://www.hse.gov.uk/offshore/scham/scham-version-8-2013.pdf> (last accessed January 7, 2015).

UK Health & Safety Executive (2008). Offshore Installations (Safety Case) Regulations 2005 - Regulation 13 - Thorough Review of a Safety Case . (Offshore Information Sheet 4/2006, Revised and Reissued July 2008). <http://www.hse.gov.uk/offshore/sheet42006.pdf> (last accessed January 7, 2015).

UK Health & Safety Executive (2006). A Guide to the Offshore Installations (Safety Case) Regulations 2005. (Draft). <http://www.hse.gov.uk/consult/condocs/offshore.pdf> (last accessed January 7, 2015).

UK Ministry of Defence (2011). An Introduction to System Safety Management in the MOD. [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/27552/WhiteBookIssue3.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27552/WhiteBookIssue3.pdf) (last visited January 7, 2015).

UK Ministry of Defence (2007). Safety Management Requirements for Defence Systems. (DEF STAN 00-56 Issue 4).

UK Ministry of Defence (2004). Safety Management Requirements for Defence Systems. (DEF STAN 00-56 Issue 3).

UK Ministry of Defence (2002). Regulations of the Airworthiness of Ministry of Defence Aircraft. JSP318B, 4th Edition.

United Kingdom (2005). The Offshore Installations (Safety Case) Regulations 2005. Statutory Instrument 2005 No. 3117.

Weinstock, C. B., Goodenough, J. B. & Hudak, J. J. (2004). *Dependability Cases* . CMU/SEI-2004-TN-016). Software Engineering Institute.

Wlad, J. (2006). DO-178B and the Common Criteria: Future Security Levels. *COTS Journal: The Journal of Military Electronics & Computing*.

**REPORT DOCUMENTATION PAGE**

*Form Approved  
OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.  
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

<b>1. REPORT DATE (DD-MM-YYYY)</b> 01-01 - 2015		<b>2. REPORT TYPE</b> Contractor Report		<b>3. DATES COVERED (From - To)</b> 09/2013 - 09/2014	
<b>4. TITLE AND SUBTITLE</b>  Current Practices in Constructing and Evaluating Assurance Cases With Applications to Aviation				<b>5a. CONTRACT NUMBER</b> NNL13AA06B/NNL13AC56T	
				<b>5b. GRANT NUMBER</b>	
				<b>5c. PROGRAM ELEMENT NUMBER</b>	
<b>6. AUTHOR(S)</b>  Rinehart, David J.; Knight John C.; Rowanhill, Jonathan				<b>5d. PROJECT NUMBER</b>	
				<b>5e. TASK NUMBER</b> 3.7	
				<b>5f. WORK UNIT NUMBER</b> 534723.02.02.07.10	
<b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b> NASA Langley Research Center Hampton, Virginia 23681				<b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>  850-035085	
<b>9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b> National Aeronautics and Space Administration Washington, DC 20546-0001				<b>10. SPONSOR/MONITOR'S ACRONYM(S)</b>  NASA	
				<b>11. SPONSOR/MONITOR'S REPORT NUMBER(S)</b> NASA/CR-2015-218678	
<b>12. DISTRIBUTION/AVAILABILITY STATEMENT</b> Unclassified - Unlimited Subject Category 62 Availability: NASA STI Program (757) 864-9658					
<b>13. SUPPLEMENTARY NOTES</b> Final Report  Langley Technical Monitor: C. Michael Holloway					
<b>14. ABSTRACT</b>  This report introduces and provides an overview of assurance cases including theory, practice, and evaluation. This report includes a section that introduces the principles, terminology, and history of assurance cases. The core of the report presents twelve example uses of assurance cases from a range of domains, using a novel classification scheme. The report also reviews the state of the art in assurance case evaluation methods.					
<b>15. SUBJECT TERMS</b>  Argument; Assurance; Assurance case; Claims; Evidence; Safety; Safety case					
<b>16. SECURITY CLASSIFICATION OF:</b>			<b>17. LIMITATION OF ABSTRACT</b>	<b>18. NUMBER OF PAGES</b>	<b>19a. NAME OF RESPONSIBLE PERSON</b>
<b>a. REPORT</b>	<b>b. ABSTRACT</b>	<b>c. THIS PAGE</b>			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	87	<b>19b. TELEPHONE NUMBER (Include area code)</b> (757) 864-9658