NASA/CR–2017-219582

Understanding What It Means for Assurance Cases to "Work"

David J. Rinehart
Architecture Technology Corporation, Campbell, California

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

April 2017

NASA STI Program . . . in Profile

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

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

- TECHNICAL PUBLICATION. Reports of completed research or a major significant phase of research that present the results of NASA Programs and include extensive data or theoretical analysis. Includes compilations of significant scientific and technical data and information deemed to be of continuing reference value. NASA 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

- 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–2017-219582

Understanding What It Means for Assurance Cases to "Work"

David J. Rinehart
Architecture Technology Corporation, Campbell, California

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 NNL16AB09T

April 2017

Acknowledgments

With thanks to NASA's Michael Holloway and Patrick Graydon for guidance and feedback throughout the project, as well as Langley Research Center's Flight Critical Systems Research (FCSR) program. We express our deepest gratitude and respect to the assurance practitioners that took time from their real-world responsibilities to provide us with the invaluable information that forms the foundation of this report. We hope that our work returns value to you in kind.

Available from:

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

Contents

1. Executive Summary

This report is the result of our year-long investigation into assurance case practices and effectiveness. Assurance cases are relevant to aviation as aircraft, ATC, and ATM systems become more complex and automated. Conventional aviation system performance is rooted in simple, well-known systems, extensive human oversight, and conservative procedures. Though successful with respect to safety and reliability, aviation cannot realize critical future improvements (e.g. capacity, efficiency, support for new vehicles, etc.) without adopting new technology, especially automation. This calls for more advanced assurance methods.

Assurance cases are a method for working toward acceptable critical system performance. They represent a significant thread of applied assurance methods extending back many decades and being employed in a range of industries and applications. Our research presented in this report includes a literature survey of over 50 sources and interviews with nearly a dozen practitioners in the field. We have organized our results into seven major claimed assurance case benefits and their supporting mechanisms, evidence, counter-evidence, and caveats.

Of the seven claimed benefits presented in this report, the first explores the fundamental success of assurance cases as indicated by evidence available to date. Though this is a broad stroke compared to the benefits that follow, readers who have not had much exposure to assurance cases may find it an important backdrop. We find that it is not difficult to substantiate basic success in suitable cases. Relevant limitations and caveats are also discussed.

The next three claimed benefits are concerned with comprehensiveness, allocation of responsibility, and organization of assurance information. Comprehensiveness is almost intrinsic to assurance cases. Allocation of responsibility is an extremely interesting aspect of assurance cases (and assurance in general) and there are important emerging benefits to consider. Assurance cases offer flexible organization of information and are also well-suited to supporting notations and electronic tools.

The next benefit we examined, that assurance cases address modern certification challenges, is divided into three elements: safety-criticality, system complexity, and innovative technology. We find that safety-criticality (operation of the system directly impacts human safety) is a dominant element of most assurance case applications. Complexity and innovation may also be present. Based on evidence of field applications, this claim has fairly strong support.

We then consider the claim that assurance cases offer an efficient path to certification compared to alternatives, which brings some of the strongest skepticism concerning assurance cases into focus. There are frequent concerns among practitioners – and some in the literature – about the efficiency of assurance cases. We found strong evidence that this concern is surmountable in practice. There are some key mechanisms which we explore, such as taking advantage of prescription where applicable and leveraging assurance case patterns. Decisions about notations and assurance case management also influence efficiency.

The last claim we examine concerns managing the legal aspect of assurance, for which we find assurance cases to be a good fit.

We conclude with a synopsis of findings. One high-level conclusion is that assurance cases are already widespread and well-established. It would be difficult to perceive this from within any single domain (industry, field of practice, etc.). The research presented here offers the broad view necessary to draw such conclusions. There is much for practitioners and researchers to learn from existing evidence on how assurance cases are working in application today.

2. Scope, Motivation, and Objectives of this Report

As aviation systems become more technologically advanced, complex, and interdependent, maintaining extraordinary levels of safety presents a challenge. Assurance cases represent an important methodological trend that may have a role in addressing this challenge. This potential opportunity is the motivation for our research. Though our research is not specific to aviation, it lies at the root of our motivations and therefore has some effect on the examples and conclusions we focus on.

Assurance cases have become increasingly common in a range of domains over the past several decades. Figure 1 depicts several milestones in the lineage of assurance cases that represent this lengthy history spanning various industries. Most of these examples relate specifically to safety cases which, as discussed in Section 3, "What is Meant by 'Assurance Case'", we consider a fully incorporated subtype of assurance cases. See Section 5.1.3 "Various Historical and Recent Cases" for more detail on these historical milestones.

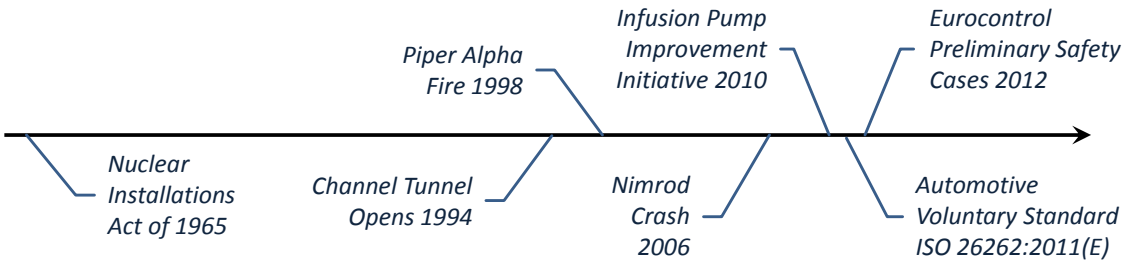

Figure 1: Select Milestones in the Lineage of Assurance Cases

Despite this long and broad history, it is not easy to assess assurance case benefits and performance given the many variables and long timelines associated with safety-critical systems. The purpose of this report and the project behind it is to conduct in-depth research on the benefits and performance of assurance cases. The statement of work for the research project directs it to address "how assurance cases are used in the design, certification, operation, modification, and maintenance of critical systems and what it means for them to be fit for those purposes." As noted in Section 5.1, "Fundamental Claim: Assurance Cases are Successful where Suitable," we are not the first to research this line of assessment. Nonetheless, we hope to contribute substantially to it.

This report is primarily organized around claimed or expected benefits, underlying mechanisms, and the supporting evidence (or counter-evidence) that could be found in connection with them. This central core of the report is found in Section 5, "Claims, Mechanisms, and Evidence for Assurance Case Benefits." In order to unearth this core content, we conducted an extensive literature survey and practitioner interviews. The methods we employed are described in Section 4, "Sources and Methods for this Project." Finally, working backward, Section 3 ("What is Meant by 'Assurance Case'") provides introductory definitions and background information.

Our research team's intent is to approach the subject of assurance case performance from a neutral perspective and let the information revealed by our research speak for itself. The purpose of this report is to bring clarity to the subject of assurance cases, present what benefits can be realistically expected (and conversely, expectations that may be unrealistic), and what mechanisms appear to be behind this performance.

3. What is Meant by "Assurance Case"

"Assurance case" is a relatively new term that fully encompasses the older term "safety case". As we illustrate in Section 5.1.3, "Various Historical and Recent Cases", safety cases extend at least as far back as the 1960s and were common by the 1980s. Assurance cases emerged as a superset term around the 1990s to place other concerns such as security and dependability alongside concerns for safety. We included a fuller historical discussion in our prior report (Rinehart et al. 2015).

In this section we establish a clear definition and scope for the term "assurance case" for the purposes of this report. The following subsections explore this from several aspects.

3.1 Definition

In our prior report, we developed a concise definition which we find useful again here:

> *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).*

This definition incorporates the two elements that most consider fundamental to assurance cases – an explicit argument and high-level goals ("specified concerns").

A slightly more elaborate definition that is commonly cited is the United Kingdom's Ministry of Defence (UK MOD) definition of a safety case (2007):

> *[A safety case is] 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 operating environment.*

This definition is limited to safety (though it is easy to conceptually extend) and offers clarifications. An argument consists of evidence and must be compelling, comprehensible, and valid. The acceptability of a safety case intrinsically depends on the specific application and specific operating environment.

As many past and current precedents for assurance cases are safety cases, both in form and name, readers will see both terms throughout this report. Since we consider safety cases a strict subtype of assurance cases, the terms are equivalent for most purposes. In particular, as many sources present information about safety cases, it is generally safe to extend this to assurance cases and we do so throughout this report without comment unless it is specifically needed.

For those who are new to the terms safety case or assurance case, we wish to establish at the outset that assurance case practices exist alongside many other complementary assurance methods and techniques. It does not replace, for example, prescriptive standards or risk management; in fact, most applications of assurance cases explicitly establish roles for all three. The synergistic implementation of assurance cases among conventional practices was strongly established by the research described in this report (see, for example, Section 5.2.3, "Mechanism: Integration with Conventional Methods").

3.2 Important Variations on Assurance Cases

We consider the core elements of assurance cases to be high-level goals and explicit argumentation. Though there is broad agreement on high-level goals, some sources and precedents take different positions on argumentation. Furthermore, there are numerous non-core

elements of assurance cases that vary in the field of practice. The subsections below explore these variations.

An important consideration we hope to communicate here is that the field of assurance cases is highly variable in important ways. Assurance cases are a general-purpose tool and consequently have been deployed in an amazingly wide range of contexts. (We will substantiate this in much greater detail in Section 5.1, “Fundamental Claim: Assurance Cases are Successful where Suitable”.) On the one hand, this is a credit to the method’s broad appeal. On the other hand, it makes it difficult to discuss and analyze assurance cases; virtually no two examples are alike with regard to important details that have a bearing on success and effectiveness.

3.2.1 Argumentation

The best way to articulate the issue with argumentation in assurance cases is not “should it be present?” but rather “should it be explicit?” The idea of “making the case” is intrinsic in the semantics of the term, which has always connoted the presentation of some type of argument. Especially in the early decades of safety cases, however, the argument was left to implicit construction. Implicit argumentation works well enough for straightforward, simple systems. There are still many examples traditionally called “safety cases” that rely on implicit argumentation, and we note this distinction throughout this report.

About midway through the development and expansion of safety case practices, explicit argumentation came to the foreground. (Though not the only example, this transition is especially notable in the research work of Tim Kelly and John McDermid at the University of York in the 1990s.) Explicit and even structured argumentation is a good fit for assurance cases and is a theme in many modern applications, as will be seen in numerous examples in this report.

Roughly half of our interview sources (see Section 4.2, “Field Interviews”) represented assurance cases as having some significant inclusion of argumentation. The remainder viewed assurance cases through the lens of what we would consider an older formulation that did not explicitly prioritize argumentation. Rather, the focus was on assurance information that was tailored to the system (more than general compliance with standards) and included elements such as risk management and lifecycle safety management. For these non-argumentation assurance case formulations, the applicant was still required to “make the case” but not in the form of explicit argumentation.

3.2.2 Risk Management and Safety Management System (SMS)

As we will examine in detail, assurance cases are very proficient at adding value on top of conventional methods (see Section 5.2.3.1, “Incorporating conventional methods as evidence”). Common hybrid applications of assurance cases incorporate risk management and/or SMS in the assurance case. There are numerous examples of regulators publishing guidance in which they make it clear to safety case applicants that they expect to see risk management and/or SMS included as evidence that their system is safe.

3.2.3 Development vs. Operations

The most immediate and obvious application of assurance cases is to system development. However, in many practical applications, it quickly becomes clear that there are limits to this scope and there is at least one other locus of responsibility: operations. Consequently, in practice, we found both assurance cases that dealt with the safety of a system *as designed and produced* and also separate assurance cases that dealt with the safety of a system *as operated*. To further

complicate matters, the responsible parties for development may or may not be the same as the responsible parties for operation (see Section 5.3, “Benefit Claim: Assurance Cases Improve the Allocation of Responsibility over Prior Norms”). Regardless, there are assurance case examples that vary across this dimension of development vs. operations (and potentially other permutations such as maintenance, system updates, or repurposing).

3.2.4 Scope: Software, Systems, Operations, etc.

Another dimension of variations among assurance cases is the scope that is addressed. Perhaps the most common scope is system safety, where the “system” is on the scale of an aircraft or an infrastructure facility. However, there seems to be an expanding range of scopes to which assurance cases are being applied. In automobiles and medical devices, the primary scope is software assurance. In many military examples, it is not only the systems but also the total operation including humans and procedures. In nuclear waste, it is the stability of geological features over centuries and millennia. These examples and others are discussed in more detail later in this report, especially in Section 5.1.3, “Various Historical and Recent Cases”. The important point for now is the wide range of scopes and contexts, which may be important to consider in understanding the methodology.

3.2.5 Formats

Varying formats and notations is the subject of Section 5.4.3, “Mechanism: Assurance Case Notations”, so we will not go into detail here other than noting the range. Assurance case formats can range from traditional design documentation to electronically-managed graphical structures. The choice of format is linked to important ramifications for factors such as assurance case access, evaluation, and maintenance. In considering any assurance case example, it is generally worth noting what format is considered the norm in that example.

3.3 Classification Scheme

Our prior report (Rinehart et al. 2015) used an assurance case classification scheme to illuminate key characteristics of a range of examples. These are *rigor in argument*, *rigor in evidence*, and *flexibility in process*. We applied this scheme again in the literature survey portion of this project (see Section 4.1, “Literature Survey”). Here we briefly re-introduce the scheme, which is depicted in Figure 2.

Figure 2: A Classification Scheme for Assurance Cases

Rigor in argument is characterized by three levels:

- Implicit: the argument is not clearly stated,
- Explicit: the argument is stated but unstructured (e.g. narrative prose), and
- Structured: the argument is presented using a defined format (e.g. notation).

As mentioned earlier, for our purposes, an assurance case without at least an explicit argument cannot be considered fully aligned with our definition – hence the hatched portion of the scale representing implicit arguments.

Rigor in evidence refers to requiring more extensive, specific documentation to substantiate that an argument is satisfactory. This dimension often correlates to a degree of standard compliance that is relevant to a particular field. There is a connection here to the "patterns" theme we discuss at multiple points later in this report (especially Section 5.6.3, "Mechanism: Role of Assurance Case Patterns"). 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 (e.g. text records), and
- Structured: evidence is organized into a specified format (e.g. data model).

As in argument rigor, we cannot entirely consider assurance cases without at least explicit evidence to match our definition. (Without presented evidence, there is hardly a meaningful argument.) Accordingly we hatch the portion of the scale representing implicit evidence.

Flexibility in process characterizes a fascinating aspect of assurance methods that will emerge repeatedly throughout this report. Early efforts to improve safety (e.g. mid-1900s) yielded increasingly *prescriptive* compliance requirements. This approach certainly increased predictability and streamlined practices. However, it runs into serious limitations, and a counter-trend toward goal-orientation has emerged in recent decades. In many ways assurance cases are able to fuse the two approaches. We explore this dynamic more fully in Section 5.6, "Benefit Claim: Assurance Cases Offer an Efficient Certification Path Compared to ," as well as other sections. For now, we will simply identify the 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 goal-orientation, and
- Goal-Oriented: regulation is *mostly* dominated by general goals and compliance adaptability.

These scales are oriented such that the upward direction is generally toward more modern methods. However, that does not at all imply that the top-level characteristics are the best approach for all or even the majority of assurance case applications. In a particular niche, for example, "explicit – explicit – prescriptive" may function perfectly adequately and represent the most efficient style of assurance case for that application and regulatory environment.

4. Sources and Methods for this Project

The objective of our project – to understand the workings of assurance cases – is dependent on collecting information from relevant sources. This, then, was our primary activity. We pursued relevant sources via two initiatives: a literature survey and interviews of practitioners.

4.1 Literature Survey

A literature study was conducted to identify claims about the benefits (or deficits) of assurance arguments and the mechanisms contributing thereto. As the main venues for publication are oriented around research, the research community's perspective framed the literature survey for the most part (as opposed to the practitioner perspective). Of course, there is some cross-over, for example research publications identifying lessons learned. Furthermore, we explored some non-research published literature (such as regulator publications).

In any case, the purposes of the literature study were as follows:

- Survey the claims of benefit/deficit from assurance cases as understood by the research community.
- Survey the mechanisms of assurance cases in support of these claims.
- Identify the evidence provided by the research community in support of the claims and mechanisms presented.
- Understand assurance argument research within top-tier research publications.
- Understand the domains of application (industries, technology areas) to which assurance arguments were studied in research literature.
- Understand the kinds of assurance cases (syntactic format, style) described in research literature.

4.1.1 Method

4.1.1.1 *Selection of Relevant Publishers/Search Venues*

There is a significant body of written research results concerning assurance arguments. To date, most have appeared within communities representing the engineering of safety critical systems. As a development that occurred after the initial development of the safety case, in which all safety argument might be implicit, explicit assurance arguments can be considered either a) an implicit subset of the safety case research community, or b) an offshoot of safety case engineering philosophy towards an explicit argument-driven approach to the assured engineering of system properties. As a result, there are a key set of engineering research publishers with which a majority of assurance arguments papers will be published.

Likewise, there are a key collection of journals and conferences under which relevant research is most likely to appear. Publication venues such as IEEE and the International System Safety Society were chosen for comprehensive search. Table 1 lists the key venues included in the comprehensive search and the representative publications.

Table 1: Publications Searched for Assurance Cases Literature Survey

Search Venue	Publications with Matching Paper	Type	Discipline
International System Safety Society	International System Safety Conference(ISSC)	Conference	Systems
	Journal of System Safety (aka Hazard Prevention)	Journal	Systems
IEEE	International Conference on Electric Railways in a United Europe		Rail
	International Conference on System Safety and Cyber Security	Conference	Systems
	Digital Avionics Systems Conference (DASC)		Avionics
	Euromicro Conference on Digital System Design (DSD)	Symposium	Embedded systems
	IET Seminar on Safety Assurance	Seminar	
	IET International Conference on System Safety	Conference	Systems
	International Conference on Sizewell B	Conference	Nuclear
	IET Seminar on Railway Safety Assurance	Seminar	Rail
	IET International Cyber Security Conference	Conference	Software/Hardware

Search Venue	Publications with Matching Paper	Type	Discipline
	Aerospace and Electronic Systems Magazine	Magazine	Aerospace/Avionics
	High Assurance Systems Engineering Symposium		Systems
	Colloquium on Understanding Patterns and Their Application to Systems Engineering		
Springer	Safety-critical Systems Symposium	Conference	Systems Engineering
	Operational Research	Journal	Operations
	NASA Formal Methods	Conference	
	Swiss Journal of Geosciences	Journal	Geoscience
	International Conference of Computer Safety, Reliability and Security (SAFECOMP)	Conference	Software/Hardware
Ad Hoc	Deepwater Horizon Study Group	Report	
	Software Engineering Institute	Tech Reports	
	National Research Centre for OHS Regulation, Australian National University	Tech Reports	

4.1.1.2 *Identification of Relevant Papers within Selected Periodicals*

A comprehensive text search for keyword terms was performed over each search venue. The following keyword terms were used:

- safety case
- assurance case
- assurance argument
- safety argument
- argument

For some venues, such as Springer and IEEE, venue search engines were used. For others without a specialized publisher search engine, such as the International System Safety Society, Google Scholar was utilized. The results of this search are included in the survey results presented in Section 4.1.2.

4.1.1.3 *Ad-hoc Inclusion of Papers*

In addition, known sources such as accident investigation reports, and technical reports, from relevant authors and experts were included in the survey results. Examples include reports investigating the Deepwater Horizon accident, as well as technical reports from known experts at the Software Engineering Institute. These are shown in Table 1 under the ‘ad-hoc” search venue.

4.1.1.4 *Characterization of Sources*

Once identified, the papers were read with various characterization activities to perform. They were as follows:

- **Semantic Filter**: The first question to ask was whether the paper actually discussed some form of assurance argument. In some cases, search term matches were false positives. Such papers were discarded and not included in our database of results
- **Research Categorization**: The reader determined context surrounding the research:

    - **Topic:** The system, operation, product, or abstracted area that is the subject of assurance.
    - **Industry:** The industry sector under which research was performed, if any.
    - **Discipline:** The expert discipline of the researchers and their application. Examples include software engineering, systems, or operations.
    - **Perspective:** The nature of the research, whether it was industrial applied research or more abstracted and theoretical work.
- **Argument Categorization**: The reader determined the form of argument in the model of the researchers. This categorization model was described earlier in this report:
    - **Rigor in Argument**: implicit, explicit, or structured argument.
    - **Rigor in Evidence**: implicit, explicit, or structured evidence.
    - **Flexibility in Process**: Unstated, Prescriptive, Goal-oriented
- **Claims Identification**: Research papers state various claims about the benefits and costs of assurance arguments. Readers identified such claims contained in research papers and recorded them. Keep in mind that such claims could be made independent of the hypotheses of a research paper. The claims were recorded in summary form.
- **Mechanism Identification**: Readers identified any mechanisms that authors suggested or stated which constituted a claimed benefit or cost of assurance arguments. These were recorded in summary form.
- **Evidence Identification**: Readers identified any evidence supplied in support of the above mechanisms and claims. In cases where no evidence was given, this was recorded. Results were summarized for each paper.

Each paper was reviewed by at least one researcher. Information was collected in a database and reviewed during research team meetings. In some cases, clarifications were required during discussions and analysis was re-performed to obtain additional fidelity in results.

4.1.2 Literature Survey Characterization

Eighty-two papers identified by the survey were of relevance. That is, after examination it was determined that they contained information about safety cases and/or assurance arguments. After prioritization, seventy were reviewed. What follows is a general characterization of these papers. That is followed by an examination of the forms of “assurance argument” as represented in the literature.

4.1.2.1 *Research Categorization*

Figure 3 shows the number of surveyed papers by year of publication. The number of relevant publications has fluctuated between two and ten up until 2015, with a slight “uptick” in relevant publications within the specified venues in the last decade. The search was conducted in the first month of January 2016.

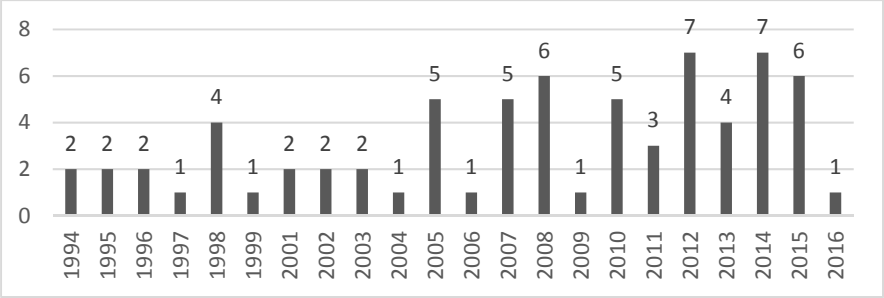

Figure 3: Literature by Publication Year

Figure 4 shows the number of papers by industry sector. The literature survey touched on a wide range of sectors with the predominant themes being transportation and energy. These characterizations turned out to be highly exclusive except for one paper which spanned both "Oil & Gas" and "Nuclear". "Aviation" refers to commercial aviation and includes both air and ground systems. "Military" includes some aviation military systems as well as other types. Note that numerous publications are not associated with any industry sector ("n/a"). These publications are generally about the nature of assurance arguments and safety cases abstracted from specific industry contexts.

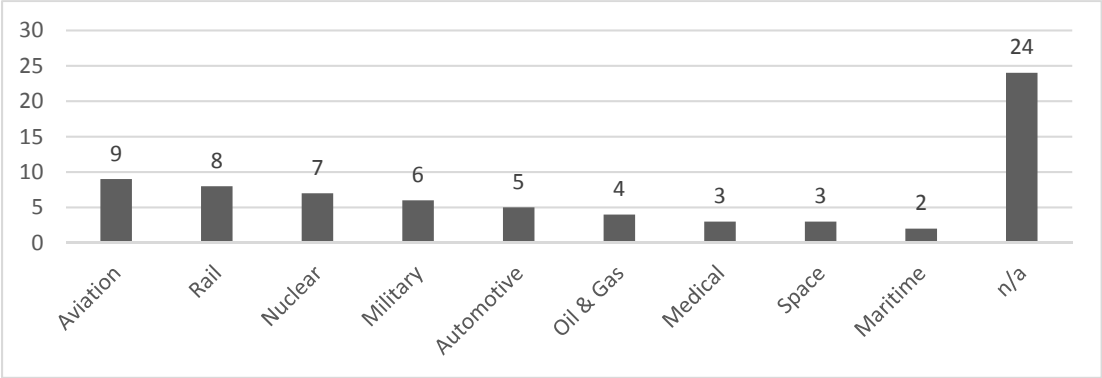

Figure 4: Literature by Industry Sector

Figure 5 shows the number of papers against technical discipline of concern. Note that some of the papers are abstract or general and have no associated discipline ("n/a"). Common disciplines are systems, operations, and software. More than one discipline could be ascribed to a paper if appropriate. Numerous systems-focused papers describe hardware/software systems such as avionics or electronic systems in automobiles. Operations typically concerns processes and procedures. Software indicates that the paper is at least partly about software assurance exclusively and separately from system-level considerations. Hazardous materials safety is also identified and appears in the nuclear industry.

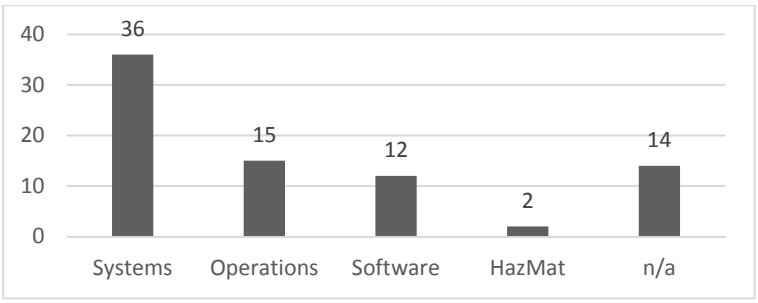

Figure 5: Literature by Discipline

Figure 6 categorizes publications by the perspective of the authors. Perspectives could be characterized as Academic, Practitioner, or Regulator. If appropriate, more than one tag could be used. (We gave ten publications two tags; the rest were single tags.) As shown in Figure 6, the predominant perspective was academic with the practitioner perspective close behind. The regulator perspective had only slight representation. This was not surprising as most regulator contributions to the domain are in the form of regulatory publications, which were not the focus of our survey.

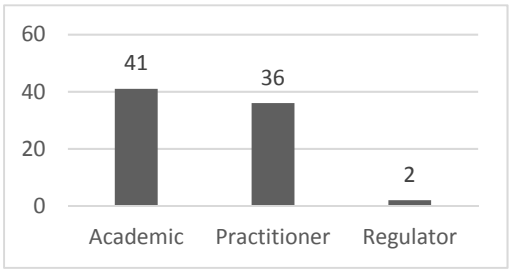

Figure 6: Literature by Author Perspective

In general, there appears to be an even split between academic and practitioner work represented in the literature. Systems research dominates application of safety cases followed closely by abstract and general work. Operations, software, and software/hardware systems follow in publication attention. Most publications do not focus on an industry. Rail is the most common industry of practice in the selected literature. Aviation, Automotive, Nuclear, and Military applications have the next tier of attention in publication.

4.1.2.2 *Argument Notations*

The literature survey endeavored to capture the safety case notation described in publications. Figure 7 shows categorizations of safety case notations as represented by papers. Each paper could be given more than one tag. Goal Structuring Notation (GSN) dominates the case form found in literature. The usage of GSN in these papers varies from simplistic to relatively rigorous. Textual notation (e.g. prose arguments recorded in collections of engineering documents) is the next most common form. A significant number of papers do not identify the form of argument given (“n/a”); it is not stated and no example is provided. Others use modified or less common structures and notations. Four publications explicitly mention using an electronic system (as opposed to document files) as the primary means to create and manage their assurance cases.

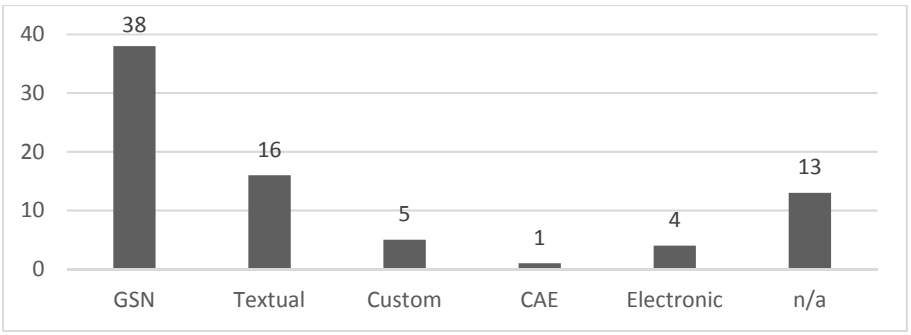

Figure 7: Literature by Safety Case Form

Figure 8 shows a specific extract of the literature survey data: the perspectives "Academic" and "Practitioner" correlated to the forms "GSN" and "Textual". This shows that GSN is much more common than textual forms among academic sources. Among practitioner-oriented sources, GSN is still common but textual forms have a strong presence as well.

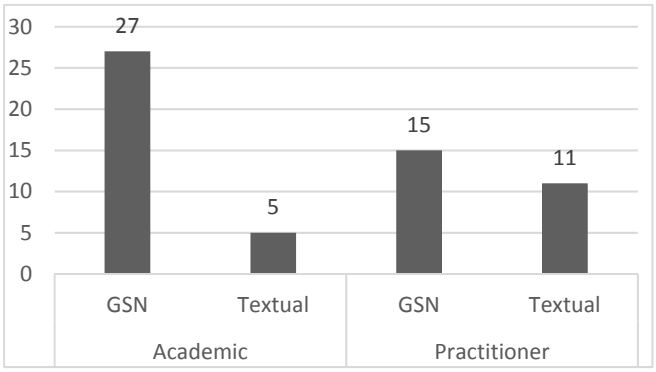

Figure 8: Literature by Argument Form per Perspective

Figure 9 shows the nature of argument form using the categorization of implicit, explicit, or structured argument as described earlier in this report. In some cases, analysis was not applicable or not available ("n/a"). The majority of papers (45) apply a structured approach to argument, in which an assurance argument is documented and organized around a notation that limits the argument narrative to a common syntax. A few papers (9) describe explicit, written argument but without required structure. Some papers (11) discuss assurance cases in which argument is implicit (i.e. the assurance argument is not clearly specified).

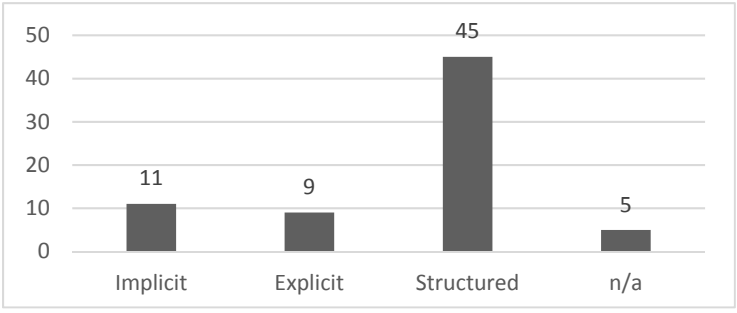

Figure 9: Literature by Rigor of Structure in Argument

Figure 10 shows the rigor of evidence in arguments as discussed in a previous section. Many papers (28) describe explicit evidence with no structural constraints indicated within the the

paper. Nearly as many (27) describe structured evidence, in which some aspect of the evidence follows rules based on process or form. Only one paper appeared to allow evidence to be implicit and focus on argument structure. This is not surprising, as the documentation of evidence in conventional assurance is generally more mature than the documentation of arguments (comparing Figure 10 to Figure 9). For the remainder, the characterization did not apply or was not available ("n/a").

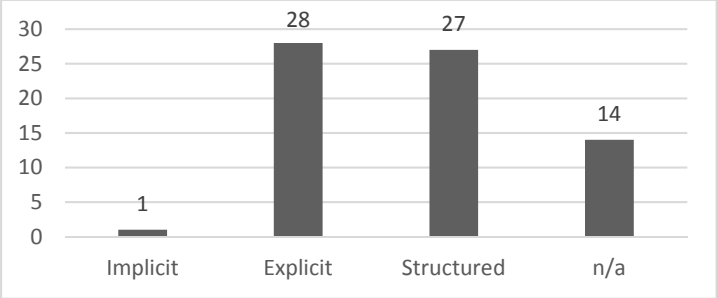

Figure 10: Literature by Rigor of Evidence in Argument

Papers often espouse a process orientation ranging from prescriptive to goal-oriented. Figure 11 shows the form of process defined for an argument construction or analysis as portrayed in papers. Many works (22) do not describe process sufficiently for characterization ("n/a"); those that do either describe goals to accomplish (22), a prescriptive method (17), or a blend thereof (9).

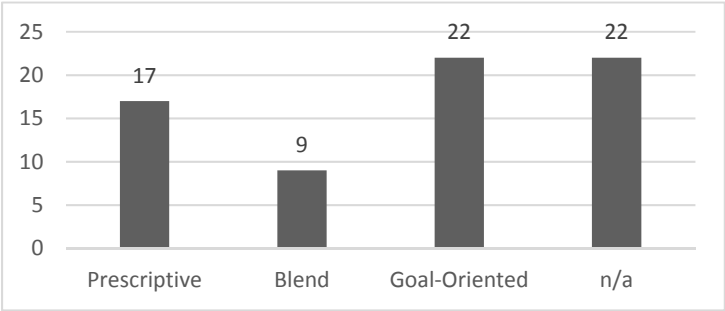

Figure 11: Literature by Rigor of Process to Develop Argument

The most common combination of elements seen in recent literature is GSN with structured evidence and argument. Some papers define processes to achieve successful argumentation, which are often goal-oriented. Older papers tend to focus on documentation based safety cases, often from the oil and gas and nuclear industries. In contrast, most recent papers focus on aviation, automotive, and aerospace sectors and tend to apply explicit and structured arguments, generally using GSN.

4.1.2.3 *List of Sources*

Table 2 lists all relevant sources applied in the study. The author, year, industry, and discipline of each source are listed. For full references, see Section 7, "References".

Table 2: List of Relevant Source Literature

Author	Year	Industry	Discipline
Abdala et al.	2001	Aerospace	Software, Systems
Aiello et al.	2014	n/a	General

Author	Year	Industry	Discipline
Alexopoulos and Konstantopoulos	2004	Maritime	Operations
Ayoub et al.	2012	Medical	Systems
Baik	2015	Nuclear	HazMat
Baram	2011	Oil & Gas	Operations
Barker et al.	1997	Automotive	Electronics Systems
Bishop and Bloomfield	1998	n/a	General
Bishop and Bloomfield	1995	Nuclear	Systems
Björnander et al.	2012	Automotive	Systems
Brain	2014	Nuclear	Operations
Cockram and Lockwood	2003	Military	Systems, Operations
Dardar et al.	2012	Automotive	Electronics Systems
Denny and Pai	2015	Aerospace	Systems
Denny et al.	2012	Aviation	Software
Despotou and Kelly	2005	n/a	General
Despotou and Kelly	2007	n/a	General
Eastwood	2013	n/a	General
Feather and Markosian	2013	Aerospace	Software
Feather and Markosian	2011	Aerospace	Software
Ferrell and Ferrell	2014	Aviation	Software, Systems
Felici	2005	Air Traffic Control	Systems
Geyer et al.	1995	Rail	Operations
Goodenough et al.	2012	n/a	Abstract
Habli and Kelly	2007	n/a	General
Hawkins and Kelly	2010	n/a	General
Holloway	2008	General	n/a
Holmes-Mackie	2005	Rail	Systems
Hopkins	2012	Oil & Gas	Systems, Operations
Inge and Costello	2008	Maritime	Operations
Jolliffe	2005	Aviation	Avionics
Kelly and McDermid	1998	n/a	Abstract
Kelly and McDermid	1999	n/a	Abstract
Larrucea et al.	2015	Aviation	Avionics
Lin and Shen	2015	Medical	Software
Lisagor et al.	2010	n/a	General
Lisagor et al.	2010	n/a	General
Lucas	2008	Aviation	Systems
Maguire and Garside	2008	Military	Operations
Manz and Schneider	2013	Rail	Systems
Mayo	2009	Anonymized	Operations
McDermid	1994	n/a	General
McDermid	1998	Aviation	Avionics
Mistry and Felici	2008	n/a	General
Nair et al.	2014	n/a	Software
Newton and Vickers	2007	n/a	Abstract
Nordland2001	2001	Rail	Systems
Ozols et al.	1998	Military	Systems
Palin and Habli	2010	Automotive	Electronics Systems
Petkova	2003	Rail	Systems
Pierce and Baret	2005	Air Traffic Control	Systems

Author	Year	Industry	Discipline
Reijonen et al.	2015	Nuclear	HazMat
Rich et al.	2007	Military	Operations
Rippon et al.	1996	Nuclear	Systems
U.S. CSB	2015	Oil & Gas	Operations
Shen and Bai	2014	Aviation	Avionics
Shepperd	2006	Rail	Systems
Short and Lucic	2007	Rail	Systems
Standish et al. (a)	2014	General	Systems
Standish et al. (b)	2014	Military	Systems
Stavert-Dobson	2016	Medical	Systems
Storey	2013	Rail	Systems
Sun et al.	2011	n/a	General
Taylor	1994	Military	Systems
Törner and Öhman	2008	Automotive	General
Verrall	1996	Nuclear	Systems, Operations
Weaver et al.	2002	n/a	Software
Wassyng et al.	2010	Abstract	Software
Wilkinson	2002	Oil & Gas, Nuclear	Operations
Zeng and Zhong	2012	General	Software

4.1.3 General Observations from Literature Survey

There is a general split between academic and practitioner research in the literature. While there are more papers of academic paper than practitioner, a significant number of papers report the work of applied developers and researchers in industry, particularly from the UK. The sectors represented in the papers are all from safety critical areas. General areas are transportation, energy, medicine, and military applications.

The majority of papers indicate the use of Goal Structuring Notation (GSN). The next most common discussed form of argument is textual forms such as prose technical documents. The majority of papers, particular more recent ones, describe safety cases with explicit (and often structured) arguments. While not shown in a figure in this report, older papers and those from the nuclear and oil and gas industries tend to be implicit argument documents.

Evidence is almost always explicit, if it is discussed within publications. Many papers make an effort to structure evidence, either to improve arguments or as a byproduct of verification techniques used to generate the evidence.

It should be noted that many academic perspective research papers involve small toy example cases. Case studies are often promised but not well “followed up” or are “glossed over” in the resulting publications. Practitioner reports tend to focus on lessons learned and experience, without presenting to the reader how the complexity of large systems is handled. That is, they do not give significant examples of structure of large safety cases, an area of considerable concern for the effectiveness of the technique as a whole.

4.2 Field Interviews

Field interviews of practitioners were the second major source of information and evidence (the first being the literature survey). The field interviews constitute a unique research asset that our project developed and has used as a foundation for this report. Interviews were conducted at

a total of eleven organizations. Of the eleven, five were government organizations concerned primarily with approval and six were commercial organizations concerned primarily with development. The domains covered by these organizations were: passenger rail, medical devices, passenger aircraft, large defense systems, unmanned aircraft systems, unmanned surface systems, airports, and military aircraft.

Each interview lasted between two and three hours. For each interview, the interviewee selected the attendees after being provided with a summary of the project goals and planned interview protocol. Interviews were conducted at the interviewee's business location.

The format of each interview was a discussion motivated for the most part by the interview protocol document supplied to the participants. Notes were taken during the interviews but no recordings made.

After the interviews were complete, the notes taken during the interviews were transcribed, organized, and missing details were added. These notes were then processed in order to provide the information necessary for this report.

4.2.1 Interview Sources

As part of our methodology with our interview sources, we agreed not to publish identification of individuals or organizations. This allowed the sources to provide us high-value generalized practitioner information without laborious approval processes or implications of speaking on behalf of associates.

For the purposes of this report, then, we identify sources by the letter designations A through K as summarized by Table 3. Given our methodology, there is some inevitable ambiguity in these designations, but it provides a flavor for our pool of interview sources.

Table 3: List of Field Interview Sources

Identifier	Predominant Perspective	Context
A	Regulator	Public infrastructure facilities
B	Consultant	Geographically distributed operations
C	Developer	Vehicle technology
D	Owner	Distributed real-time control systems
E	Operator	Integrated human/technical operations
F	Developer	Autonomous systems
G	Regulator	Large commercial safety-critical systems
H	Regulator	Small commercial safety-critical systems
I	Developer	Vehicle systems
J	Oversight	Safety-critical assurance management
K	Consultant	Assurance of software systems

4.2.2 General Observations from Field Interviews

The major general points resulting from the field interviews were:

- The impression gained was of very widespread use of safety cases both within and across domains.
- Significant belief in the value of safety cases was noted by developers and regulators that had extensive experience with them.
- It is difficult to find or produce empirical evidence of safety case value.
- Interviewees noted that imposing a requirement for a safety case on many organizations is at least initially (and sometimes sustained) met by a negative response.
- Documentation, guidance, examples, and templates are generally lacking; of particular note is the lack of examples of rigorous safety cases. (Sole exception: large development organizations have proprietary examples available to their own staff.) The result is:
    - Difficulty training staff for both developers and regulators.
    - Poor quality safety cases developed by those new to the method.
    - Difficulty making approval decisions by regulators.
- Having to deal with legacy systems is problematic but, even there, safety/assurance cases are making inroads into system maintenance.
- Certification/approval is facilitated by the presence of an assurance case, because the case provides a guide to the supplied materials.

A great deal of variability in many dimension of safety case development was noted after visiting the eleven organizations. Of particular note are the following dimensions of variation:

- **The definition of the term "safety case"**. Some organizations use the term to mean a rigorous safety case and others use the term to mean little more than a collection of documents resulting from the application of safety engineering techniques. In all of the organizations interviewed, the majority are using the term to mean rigorous safety cases.
- **The notation used to define and to document safety cases**. For organizations using rigorous arguments, some use GSN or CAE (Claims, Arguments, and Evidence – another graphical format) to document all of their arguments. Others use these notations for only some of their arguments. The remainder arguments are in plain text (natural language).
- **Certification using safety cases**. Processes for certification vary widely. In most cases, certifiers are involved throughout system development and are given access to the evolving safety case, but this form of access is not universal.
- **Practical use within the organization**. In some organizations, safety cases are used for essentially all projects. In other organizations, safety cases are used differently by different parts of the organization, both vertically (system vs. subsystem vs. component) and horizontally (project 1 vs. project 2). In part this variation arises because of the need to deal with a mix of project ages. In some cases, safety cases have to be retrofitted to legacy systems thereby limiting severely the technology that can be applied compared to the use of safety cases in new developments.

4.2.3 Usage Examples

The way in which safety cases are built and used is illustrated by the following examples. These examples are abstracted and generalized from real descriptions provided to us by interview sources.

4.2.3.1 *Example 1*

The organization is involved in safety-critical systems development. Assurance cases are initiated when the development project of the system starts. The assurance case is exploited during system development to drive the assurance process for the project, to communicate the assurance context to developers, and to assist management in identifying project risk.

The organization's perceived benefits resulting from the use of assurance cases are in the following areas.

- Privacy: Assurance cases can present the argument to the stakeholders while maintaining privacy of the evidence.
- Shared Access: Assurance cases are sharable and viewable by all stakeholders.
- Legal: Assurance case documents fulfill certain legal responsibilities.
- Standards Conformance: Argument fragment assuring conformance to a required standard can be constructed.

4.2.3.2 *Example 2*

The organization develops a safety argument that is documented entirely in GSN and is presented as a series of web pages. The safety case is rigorous but the presentation is limited by the presentation and format requirements imposed by the approval authority. The management of the legal responsibility is complex because of the contributions to the system from a myriad of suppliers.

The organization noted several advantages that accrue from their use of a safety case including:

- The safety case is used as a reference document for the entire engineering and management team.
- When the customer asks questions about safety issues, the answer is always provided by reference to the safety case.
- During development, the safety case is used to derive evidence requirements for assurance.

4.2.3.3 *Example 3*

The organization is involved in safety assessment in a relatively conventional and well-known technology area. The industry relies heavily on existing published standards. The form and structure of safety cases, however, is not made clear by available guidance. Approval and auditing has a fixed structure: (a) lead assessor studies entire case, and (b) subject-matter experts examine specific parts. Auditors frequently develop their own unofficial argument structures as needed to document the rationale they have developed for their own approval recommendation.

4.2.3.4 *Example 4*

The organization is involved in safety assessment in commercial systems. The associated legal framework requires an explicit safety case. However, format and contents may vary widely

per the applicant's discretion. The assessment process is facilitated by the availability of the safety case for the subject system which at least provides a map of the submission materials. Despite the general assurance case framework, it is difficult to tell if the regulatory system is as effective as it could be. In this context, applicants have perhaps an inefficient degree of latitude and a questionable underlying safety culture.

4.2.3.5 *Example 5*

The organization develops large safety-critical systems. Heavy use is made of conventional assurance-oriented standards and methods. The overall safety culture in this organization was built deliberately and is pervasive, serious, and comprehensive.

- Guidance and templates are provided to subsystem development groups together with a preliminary list of hazards.
- Technical experts are sent to professional courses on safety engineering.
- A project safety committee oversees system safety engineering.
- Customers are invited to meetings of the project safety. The organization's goal is to have customer signoff on system safety at the end of development.
- Under the umbrella of a safety case, multiple assurance methods are used: safety management system (SMS), fault trees, software assurance (further segmented into product, process, and organizational arguments), and field monitoring.

4.3 Discrepancies Between Literature and Practice

In the areas of safety case development and safety case approval, there appear to be a significant number of discrepancies between the state of the art as reported in the academic literature and the practice of safety case usage. The literature authored by non-academics tends to be far closer to practice but: (a) does not report on material likely to be in the least way proprietary (where much of the technical detail lies), and (b) does not report complete details of projects because the volume of detail is large.

In this section, the discrepancies noted between the material reported in the literature surveyed in this study and the practice as reported by the interviewees contacted in this study are:

- The academic literature has very little material on dealing with legacy systems although this is an important area of practical application.
- Safety cases in practice are larger than those discussed in the academic literature by a considerable factor.
- The need for official responsibility to be taken for the residual risk in practice dictates elements of safety case development processes and safety case structures.

5. Claims, Mechanisms, and Evidence for Assurance Case Benefits

Based on our literature survey and practitioner interviews, we distilled the perceived assurance case benefits into claims that could be individually assessed. As far as possible, we endeavored to make this set of claims thorough and mutually exclusive. Thoroughness meant that we covered fairly completely the perceived benefits that we discovered in literature and interviews. Mutual exclusivity meant that each claim could be assessed with some degree of independence and minimal overlap with other claims.

Having formulated this set of benefit claims, we then examined the mechanisms that might lie behind these benefits and weighed the evidence for and against the claims. For mechanisms

and evidence, we turned to our resources in the form of literature and interviews. The emerging benefit claims sharpened our focus as the project proceeded to specifically search for relevant mechanisms and evidence.

Below is the list of assurance case benefit claims formulated and considered by our team:

1. The first claim is more fundamental (and essential) than those which follow: assurance cases are **successful in suitable cases**. In other words, they perform at least satisfactorily to achieve the desired assurance goal where they are applied. This basic claim, if substantiated, establishes that assurance cases are viable, feasible, and possibly attractive as an emerging method option.
2. Assurance cases are **more comprehensive than conventional methods alone**. Here comprehensiveness refers to including all relevant means to achieve certification.
3. Regulatory systems based on assurance cases lead to an **improved allocation of responsibility** compared to prior norms.
4. Assurance cases are particularly **effective at organizing the relevant assurance information** necessary to achieve certification. This claim posits that assurance cases are relatively intuitive, navigable, etc.
5. Assurance cases offer a solution to **certifying modern systems** with respect to attributes that are problematic for other methods. Specific attributes of concern include safety-criticality, high system complexity, and novelty.
6. Assurance cases provide an **efficient path to certification** compared to other approaches by providing focus and direction for the certification. The result is minimal unnecessary work and expeditious completion of the necessary work.
7. **Due diligence** is encouraged and established by assurance case processes. As system behaviors become more complicated and consequential, this is increasingly important to developers and operators.

Each of these benefit claims is explored in detail in the following subsections.

5.1 Fundamental Claim: Assurance Cases are Successful where Suitable

This first claim is unique in comparison to the six claims that follow. It is general and foundational for the others (which enumerate more specific claims). To some extent, this first claim is an overlay for the purpose of this paper as a whole. This paper's title, "What It Means for Assurance Cases to 'Work'," places the focus on achieving success with assurance cases. A good place to start, then, is considering success in the broadest terms.

Despite the generality that makes this claim an outlier relative to the others presented in this paper, we include it for several reasons. First, there are prominent opinions and significant evidence on both sides the claim. It is a significant theme in the literature and practices we researched, and therefore we would be remiss not to address it directly. Second, the remainder of the claims in this paper largely hinge upon this fundamental claim. Third, it is a claim of paramount importance to practitioners who are considering applying an assurance case method.

Several mechanisms of basic success are covered under later claims. For example, to the extent that assurance cases are more comprehensive than alternatives (Section 5.2), it is reasonable to consider that a contributor to success. Similar statements could be made about claims concerning efficiency (Section 5.6) and effective organization of information (Section

5.4). In this section, we restrict our scope to higher-level mechanisms that are not addressed later.

5.1.1 General Claim and Associated Evidence

The general claim is that assurance cases, as we've defined them, are reasonably successful at least in a significant number of instances where they are applied. "Suitable" is difficult to nail down; it is also a major topic woven through this paper. However, if an assurance case method is attempted and successful, then we can at least retroactively assume it is a suitable instance. In other places in this paper, for example Section 5.6, "Benefit Claim: Assurance Cases Offer an Efficient Certification Path Compared to ," we explicitly discuss some cases that are clearly *not* suitable, so we can at a minimum identify examples near the ends of the suitability spectrum.

If a reasonable expectation of assurance case success were not taken to be provisionally true, assurance cases would not be attempted by practitioners. Correspondingly, we take this claim as implicit in the many applications of assurance cases (especially safety cases) that seriously apply the method. We consider a wide range of such precedents below in Section 5.1.3, "Various Historical and Recent Cases." The large majority of these precedents support the claim, although we will also discuss one counter-example in that section.

Fundamental success of assurance cases is a difficult claim to prove with certainty at this point in time for the inescapable reason that final success can only be conclusively demonstrated in the decades that follow the application of an assurance case. On this timescale, the method is still young. As Hopkins (2012) states, "There are huge difficulties in trying to assemble empirical data on the effectiveness of safety case regimes. One of the most significant is that that since major accident events are rare it is difficult to compile statistics that demonstrate trends… Given these difficulties, it goes without saying that quantitative cost-benefit analysis cannot be carried out."

We found some supportive evidence in the literature in the form of expert analysis. Though the weight of it at present may not be conclusive, if it continues to grow in substantially the same way, it represents increasingly strong support for the claim. Two studies we found in the literature were in the form of high-level evaluations of the success of assurance (or safety) cases. In "Safety cases: Success of Failure," Wilkinson (2002) writes that "the near universal opinion of managers and most of the workforce at hazardous installations is that safety cases have been very successful." Törner and Öhman (2008) reported a similar study of effectiveness entitled "Automotive Safety Case: A Qualitative Case Study of Drivers, Usages, and Issues". ("Drivers" is used in the sense of "reasons for a safety case," not the sense of vehicle operators). Both these studies lend support to the claim that the assurance case approach is reasonably successful while calling attention to certain caveats.

There is also a relevant point of evidence in the safety record of the Eurotunnel railway link between the UK and France (a.k.a. the "Chunnel"). The development of the Eurotunnel employed fairly cutting-edge safety processes (for the mid-90s); running a high volume of trains underground and underwater for 50km presents unique and substantial risks. The Eurotunnel safety case approach certainly went beyond general-purpose standards and was goal-oriented (Evans 1995). However, it lacked explicit argumentation, and it bears similarity to what we would now call a Safety Management System (SMS). Nonetheless, it stands as a partial example of assurance case methods. After 22 years in service and over 366 million passengers (Eurotunnel Group 2016), the Eurotunnel is often cited as a safety case success story. As of 2012, there were no significant incidents to passengers (Wake 2012). There were three fire

incidents (1996, 2006, and 2008), each involving heavy vehicles being shuttled by rail (none were occupied). In each fire incident, the safety response functioned as planned in the safety case.

Our interviews also found the dominant belief among practitioners that assurance cases (usually safety cases) are a step toward improved, more successful outcomes. One must take this with a proverbial grain of salt since many of these practitioners are advocates of the method. Nonetheless, what we found in the field carries much more weight than theoretical support for an unproven method. For some interviewees, applied assurance case practices go back decades (interview sources B, E, I, J, K) and large-scale examples range from transportation infrastructure and vehicles to military systems to medical devices (all sources A–K). The impression drawn from these interviews is that the method is spreading, in some instances it is already quite mature, and the general sense is that its fundamental value is well-established.

The growing popularity of safety cases could be a transitory phenomenon. However, given available evidence, it seems more likely that growth in the field is an indicator that the fundamental claim is substantially valid and adoption will continue (especially as the bounds of "suitability" clarify with time). As Wassyng rightly points out, assurance cases are not a "panacea," but our research generally indicates that the method is finding success in a range of applications when deployed properly as a hybrid with existing conventional methods.

5.1.2 Essential Conditions for Assurance Cases

Literature, practice, and common sense bear out that mere *pro forma* application of assurance case methods will not necessary lead to success. That is, there are contextual conditions and implementation elements that can undermine the method and make it ineffective. Failure as a result of lacking supporting conditions does not necessarily reflect on the method as a whole.

Furthermore, it is important to be aware of the most essential conditions for success. Hopkins (2012) formulates just such a list of "five basic features":

- "A risk- or hazard-management framework."
- "A requirement to make the case to the regulator."
- "A competent and independent regulator."
- "Workforce involvement."
- "A general duty of care imposed on the operator."

Each of these five features would be a good subject for discussion and analysis, but that is not our aim at present. More importantly, Hopkins' list reinforces the broader point that a contextual weakness could lead to an assurance case failure even if the method itself is otherwise sound. Hopkins offers as a specific example: "A safety case regime will almost certainly fail where safety cases are not scrutinized by a competent regulator." Other assurance case experts might offer somewhat different lists than Hopkins, but the underlying point remains: it is both possible and consequential to fail to provide the essential conditions for assurance case success. A good example of this is the well-known Nimrod aircraft crash, which is discussed in Section 5.1.3.5.

Some conditions are concrete, such as Hopkins' requirements for a risk- or hazard-management framework and imposed duty of care (which would typically be expressed in regulations). Other conditions, though they may be just as essential, are more subjective: what exactly constitutes "making the case"? How does one measure regulator competence or

workforce involvement? The only practical answers involve expert judgment and require practitioners to determine these factors for themselves.

On the subject of a strong, independent regulator, (Dahle et al. 2012) comments on a real-world regulatory debate where this essential condition resulted in an organizational shifting of assignments: “The responsibility for safety on the UK shelf [offshore industrial operations] was transferred from the Department of Energy to the Health and Safety Executive. Intention behind this separation is mainly to avoid goal conflicts between safety and production aspects.” Various sources have also noted the need for adequate regulator review which sometimes requires significant resources and investments in expertise. This is discussed further in Section 5.1.6, “Mechanism: The Challenge of Objective and Sufficient Evaluation”.

5.1.3 Various Historical and Recent Cases

Our literature survey brought to light many instructive examples of assurance cases. This section presents an overview of those which are relevant to the claim at hand that assurance cases are acceptably successful where suitable. Given the nature of the content, this section is based solely on our literature survey and not our interviews.

5.1.3.1 *Assurance Cases in the Nuclear Industry*

Perhaps the earliest adopter of safety cases was the nuclear power industry, which deals with one of the most intrinsically dangerous technologies developed by mankind. J. M. Brain noted the forerunner status of nuclear safety cases (2014): “The earliest legal requirement for a Safety Case in the UK come from the Nuclear Installations Act of 1965 so the nuclear industry has now has almost 50 years experience of producing and updating Safety Cases to support equipment and operations.”

Many early nuclear facility safety cases did not explicitly incorporate argumentation, but the implicit argument was clear – that facilities and procedures were adequately safe to operate. Early safety cases appear to focus on comprehensiveness: there is a unified framework for documenting and addressing all relevant safety concerns. There is a strong element of implicit high-level goal-orientation in this approach as well. Early safety cases were an important step beyond prescriptive compliance and fragmented safety initiatives.

Before long, argumentation as an explicit concept emerged in the context of nuclear industry safety cases. For example, G. S. Verrall documented in 1996 the safety case efforts for the Sizewell B nuclear reactor in the UK. Verrall wrote that the safety managers worked to produce “a documented set of ***arguments*** which provide justification that operation of the nuclear facility throughout its complete lifecycle will meet the stringent standards required by the NII” (emphasis added).

The long track record of assurance cases in the nuclear industry provides some evidence that it is fundamentally sound and successful.

5.1.3.2 *Assurance Cases in Oil & Gas Industry*

Though it came to assurance case practices later, similar evidence is available from the oil and gas industry. The Piper Alpha oil platform fire in 1988 and subsequent inquiry resulting in the Cullen Report (Cullen, 1990) is often cited as a turning point toward safety case methods (Wilkinson 2002).

Spurred by the Deepwater Horizon blowout in the Gulf of Mexico, Michael Baram (2011) presents an interesting comparison of oil and gas regulatory schemes between the US and Norway. Baram's perspective is not necessarily that of assurance cases. The analysis is favorable toward Norway's approach, which has resulted in no major accidents since 2002 despite a track record of several prior to that. The Norwegian scheme features goal-orientation, a well-resourced regulator, and workforce engagement.

These elements of the Norwegian scheme overlap significantly with assurance cases. We discuss goal-orientation more in Section 5.1.4 below, "Mechanism: High-Level Goal-Orientation." Competent regulators and workforce engagement align with two of the features presented by (Hopkins 2012) as essential to safety case success. Explicit argumentation is notably missing from the Norwegian approach. Still, the Baram (2011) analysis provides support for the fundamental viability and success of methods at least related to assurance cases.

5.1.3.3 *Assurance Cases in Medical Devices*

Assurance case methods (specifically safety cases) have found application in the medical domain as well (Stavert-Dobson 2016, Health Foundation 2012). A specific example of interest is infusion pumps.

In 2010, the US FDA launched an "Infusion Pump Improvement Initiative". Infusion pumps are used routinely throughout hospital care, primarily to administer intravenous fluids. The ubiquity of infusion pumps creates a market very much like a mass-produced commercial product; however, unlike most commercial devices, the possibility of life-threatening mishaps is very real. "From 2005 through 2009, FDA received approximately 56,000 reports of adverse events associated with the use of infusion pumps, including numerous injuries and deaths. During this time period, 87 infusion pump recalls were conducted by firms to address identified safety concerns." (FDA 2010)

One of the FDA's responses was to institute a safety assurance case element in the infusion pump approval process. In "Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff" (FDA 2014), the FDA recommends information to be submitted for infusion pump approval. In addition to specific design documentation and a hazard analysis, the FDA recommends a safety assurance case: "The safety assurance case (or safety case) consists of a structured argument, supported by a body of valid scientific evidence that provides an organized case that the infusion pump adequately addresses hazards associated with its intended use within its environment of use. The argument should be commensurate with the potential risk posed by the infusion pump, the complexity of the infusion pump, and the familiarity with the identified risks and mitigation measures."

The US is not the only country where assurance cases are working into medical regulatory systems. The incorporation of assurance cases by the UK National Health Service (NHS) is larger-scale than the infusion pumps example above. Through its standard SCCI0129, "Clinical Risk Management: its Application in the Manufacture of Health IT Systems" (UK HSCIC 2015), the UK NHS applies safety case methods along with others to medical information technology (IT) systems. "The use of such Health IT Systems is becoming increasingly widespread and the functionality is becoming more sophisticated. However, it must be recognised that failure or incorrect use of such systems have the potential to cause harm to those patients that the system is intended to benefit." The standard goes on to describe how its methods are explicitly drawn from "high-risk settings." This shows an intentional adoption of safety cases from other domains

(presumably such as nuclear and petrochemical energy) as a technique that is well-suited to modern, safety-critical systems.

At a high level, these safety cases from the medical field are excellent examples of the assurance case methods targeted by our research: there is a clear argument and the intention is comprehensive coverage. This provides some support to the basic claim of acceptability from a domain that is quite unique relative to many other applications (nuclear, military, vehicles, etc.).

5.1.3.4 *Assurance Cases in Automotive Technology*

Automotive technology is an interesting domain with regard to assurance regulations. Generally speaking, regulation is light, basic, and simplistic. Nonetheless, automobile control and navigation systems have developed rapidly in step with technological advances. Vehicles on the road today have not only highly integrated, computerized control systems (e.g. engine control, anti-skid braking, and traction control systems) but also advanced navigation sensors and self-driving features. This combination of regulation and technology has led to such odd juxtapositions as NASA officially analyzing Toyota software to search for a life-threatening potential failure mode in relation to a large-scale lawsuit (Gamble and Holzmann 2011). The fatal crash involving Tesla's "self-driving" feature in Florida (Neumann 2016) further illustrates this trend that automotive assurance regulation is increasingly behind the curve of automotive technology.

ISO 26262:2011(E) "Road vehicles – Functional safety" is the most relevant automotive standard for assurance of the electronic systems. It is prescriptive and voluntary; furthermore, no compliance information must be provided to regulators. Still, it does constitute evidence that the automotive domain has been aware of safety case methods for at least 5-10 years. Its definition of safety case is modern and argument-oriented: "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." Unfortunately, we have not found any available real-world examples of automotive safety cases conforming to ISO 26262, most likely due to the voluntary nature of compliance (and manufacturer reluctance to expose themselves to possible liability challenges).

There is one automotive safety case example that we discovered in our literature survey and that is from relatively early development of integrated electronic controls: the Jaguar Electronic Throttle in the late 1990s. The safety case was apparently internally motivated – either within the manufacturer or its underwriter – by concerns this relatively new electronic system could be unsafe relative to preceding fully mechanical controls. Then, as now, assurance information was not externally required: "In the automotive industry, there is no 'regulator' to whom such a safety case should be submitted" (Barker et al. 1997). Lloyd's of London was brought in as an independent assessor. Based on the literature written about it, the Jaguar safety case appears to be a good, early example of comprehensiveness and flexibility. The safety case was used as a framework for multiple conventional assurance methods and prescriptive standards. "The project was completed successfully and resulted in a high quality product accompanied by a reasoned, fully documented argument for its safety. This approach is therefore seen as both feasible and beneficial, and will be used on future projects." (Barker et al. 1997)

Though much of the automotive assurance state of the art is opaque outside the walls of automotive manufacturers, there are signs that assurance cases are a significant element of current approaches in those circles.

5.1.3.5 *Case Study: Nimrod Aircraft System*

No historical overview of assurance cases would be complete without mention of the Nimrod aircraft crash, which could be called the most famous safety case failure to date. It has been covered by many sources including our prior report on assurance cases (Rinehart et al. 2015).

In brief, the Hawker Siddeley Nimrod was a UK Royal Air Force maritime reconnaissance aircraft (now retired). The design originated in the 1960s and the fleet was updated several times. In September 2006, a Nimrod experienced an in-flight fire over Afghanistan and crashed, killing all 14 crew members. The UK government instituted a review led by Sir Charles Haddon-Cave.

The Haddon-Cave review developed into a sharp critique of safety case practices because a safety case analysis had been completed for the aircraft just the prior year (2005). The circumstances, unfortunately, created a situation in which there was little intrinsic motivation for a serious and well-resourced review of the aircraft. The last major design change had been in 1989 and the aircraft had a long service record, leading to the perception that there could be no major flaws because they would have been encountered in the field. The UK military initiated the Nimrod safety case as a routine matter of adopting safety cases in general. The Nimrod was one of many systems for which safety cases were produced as a result of the change. As the aircraft was already fielded and considered "safe", the result was a safety case effort that was about as *pro forma* as it could have possibly been. As the Haddon-Cave report (2009) stated it, "The Nimrod Safety Case became essentially a paperwork and 'tick-box' exercise."

Interestingly, the safety case analysis did make some headway on dealing with the underlying issue – but it did not go far enough. During safety case review, the aircraft contractor (BAE) identified the hazard that eventually led to the crash. However, it was buried in inconsequential hazards and was not managed appropriately. The independent safety assessor (another contractor, Qinetiq) was ineffective as an agent of regulatory oversight. Though it demonstrates many missteps and mistakes, to be fair, the Nimrod safety case came closer to averting the accident than what would have otherwise occurred if the UK military had not ordered the review. However, the failings of the safety case initiative tragically resulted in a missed opportunity to avoid the accident and crew deaths.

As Stavert-Dobson (2016) states: "…the value of the safety case can quickly be eroded should it be seen as an administrative exercise or a simple means to an end to satisfy management, a regulator or contractual requirement." This is perhaps the most important conclusion to be drawn from the Nimrod safety case failure.

How does the evidence of the Nimrod example relate to the perceived benefit in question, that assurance cases are acceptably successful where suitable? It certainly illustrates that there are limitations to the practical success of assurance cases. In other words, it is evidently possible to implement assurance case methods in such a way that they are not as successful as desired. Furthermore, there is no reason to think that the practitioners involved in the Nimrod analysis were outside the mainstream, although they were later characterized as inexperienced in the Haddon-Cave report. That is, the example demonstrates (in tragic fashion) that fairly typical practitioners can fail to achieve assurance using safety case methods.

Nonetheless, it would be taking the evidence too far to say that the Nimrod example invalidates the perceived general benefit in question in any significant way. Practitioners and theorists alike are well aware that any method can be misapplied, and superficial compliance (as in the Nimrod analysis) is a common threat to many assurance methods. There is nothing in the retroactive critique of the Nimrod failure that suggests that the assurance case approach is: (a)

inherently less successful than alternative methods, or (b) flawed in some fundamental way. We can hope that the identified pitfalls (such as lack of rigor and weak oversight) are not repeated by future applications of the method.

5.1.3.6 *Case Study: Harrier Aircraft System*

Application of safety case methods to the Harrier aircraft system provides something of a counterpoint to the failures of Nimrod. The two aircraft are very much contemporaries, both being UK military aircraft originating in the 1960s. Both are considered legacy aircraft with, to some extent, proven records prior to the adoption of safety cases.

However, where the Nimrod record is marred by a major accident in spite of its safety case, Harrier has been successful. Per (Lucas et al. 2007): "Furthermore in the last 6 years of development the Harrier project has never failed to meet a key milestone objective and has delivered on-time, on-budget and to, or exceeding, the required military capability. It has done so within an increasingly safety conscious environment and without compromising safety. This has not been an easy task as long-established processes have been challenged."

There are many interesting details in the Harrier safety case example. Though the body of the safety case is not publicly available, it appears to be a good example of a complete, large, practical application that yielded real-world success. The team used Goal Structuring Notation (GSN) at the top level of the safety case and eventually transitioned from manual documentation to assistance from electronic safety case tools (see Section 5.4.4, "Mechanism: Assurance Case Scalability and Supporting Tools") to relieve the difficulty of burdensome safety case maintenance. The initiative subdivided into at least two hierarchical safety cases: a low-level safety case for the mission computer and its software, and a high-level safety case for the whole aircraft (based, where possible, on legacy performance). Over the course of multiple years, the assurance team managed several upgrades and new weapons systems.

5.1.4 Mechanism: High-Level Goal-Orientation

An important basic mechanism that may contribute directly to the success of assurance case methods is that they focus inherently and structurally on the end goal rather than intermediate (or indirect) objectives. Relative to conventional prescription, rather than focusing on compliance with standards that apply generally, the top level of a safety assurance case focuses on the specific system. Structurally, an assurance argument starts and ends with the high-level assurance goal. A properly argument-oriented assurance case calls for the high-level goal to be substantially proven by argument; the many supporting details should systematically work through this challenge. Assurance cases are, in principle, flexible enough to accommodate anything that pertains to the high-level goal.

In contrast, we do not know of any alternative method that links so holistically to the high-level goal. Prescription-oriented methods rely on implicit assurance that following guidelines appropriate to a general class will succeed with individual instances. This may be true and effective to some extent but it has several weaknesses, including that it does not address unique or innovative aspects of individual instances (for more on this, see Section 5.5.4, "Mechanism: Managing Certification of Innovative Technology"). Prescription excels at propagating best practices. This has a positive influence on assurance but it does not correlate directly to high-level goals.

Safety assurance methods such as fault trees, failure mode and effects analysis (FMEA), and risk management – any of which may be found in practice as part of or in lieu of a safety case –

are *technique-oriented*. They do not begin with the high-level goal, but rather begin by looking at the system from a particular perspective and following through with specified processes. These also have a beneficial influence on assurance and have a place in modern practice. However, they can have blind spots to potential flaws that do not align with the model at the core of their methodology. For example, fault trees are very good at identifying and working through the ramifications of component failures; they are not as good at identifying user-oriented failures because these do not align well with the technique's model. Risk management and a safety management system (SMS) have less specific technique models and therefore tend to be more flexible to a range of concerns. Assurance cases could be said to go a step broader (the only core model is argumentation) and correlate more directly to the motivating assurance goals.

It should be noted that goal-orientation is not unique to assurance cases. Argumentation has a natural affinity to goal-orientation, as demonstrated by the adoption of GSN to express many assurance cases (Kelly, 1998). However, it is possible to adopt goal-orientation without explicitly adopting argumentation. We discuss this further in the next section (5.1.5, "Mechanism: Centrality of Explicit Argumentation").

Accident prevention often calls for the resolution of competing factors and tradeoffs. For example, the gas line rupture and fire at a Chevron facility in Richmond, CA (2012) was the result of a slow-acting corrosion mechanism with complex dependencies on metallurgical composition. Some critical factors could not be known without 100% inspection and laboratory testing of the components in question (U.S. CSB 2015). Chevron (and relevant authorities) had a range of safety mechanisms in place including standards compliance, safety culture improvements, and topical initiatives (such as managing corrosion). However, these did not produce enough mitigation action to avert the accident. Since a goal-oriented assurance case was not used, we cannot speculate as to whether or not it would have been more successful. It does, however, illustrate a context in which goal-orientation could provide motivation and direction. Over and above the relevant parties paying attention to standards compliance, safety culture mechanisms, and directed activities, it would seem that increased focus on the high-level goal, "Ensure that this facility is acceptably safe to operate" and the subsequent follow-through could have motivated better resolution of the lingering corrosion hazards.

In fairness, it is possible that a properly constructed high-level risk management system would have had a similar beneficial influence in this example. It is also possible that a risk management system could call for the development of an assurance case to satisfactorily mitigate risks! Once again, many hybrid combinations of methods are possible.

One of the recommendations resulting from the Richmond fire reads as follows: "Develop a method to assign accountability at Chevron to determine whether any new… recommended program or industry best practice… must be followed to ensure process safety or employee personal safety. This method shall include monitoring of these practices and guidance at a refining system level and at the refinery level. Develop a tracking system to monitor the progress of implementing these selected practices and guidance to completion." (U.S. CSB 2015) In other words, as new high-level hazard information comes to light, ensure that it is managed properly. This, in essence, recommends a new high-level goal mechanism.

On the other hand, one substantial criticism of assurance cases is that they are *too* high-level. The concern here is that, if practitioners start with nothing more than a high-level goal, their guidance is too vague and they have too much freedom to convince themselves of assurance – to the detriment of the real safety produced. This is perhaps the tradeoff of a high-level

methodology and the reason why it should be applied as part of a hybrid along with lower-level methods (see Section 5.2.3, “Mechanism: Integration with Conventional Methods”). (Wassyng 2010) cautions against the “almost complete absence of control of creativity” and goes on to state: “… if the safety case approach does not impose more prescriptive software dependent requirements for certification, we are not solving the basic software certification problem, or for that matter, the problem for embedded devices. It will still be possible, and maybe easy, for people to present apparently convincing arguments to substantiate their claims using evidence that they are free to choose. Of course, certifying authorities do not have to accept the validity of the evidence or of the argument – but that is no better, and in fact no different, from many certification regimes in existence today.” We find this overly simplistic in favor of prescription (which is not the only path to improved assurance), but nonetheless it reflects a concern that we encountered more than once in our research: that assurance cases are too open-ended in connection with their high-level goal-orientation. We revisit another aspect of this concern in Section 5.2.2, “Mechanism: Systematic Approach”.

5.1.5 Mechanism: Centrality of Explicit Argumentation

An important mechanism that we found to be an undertone from many sources is, as (Stavert-Dobson 2016) and others summarize it, “making the implicit, explicit”. Looking at assurance methods through the lens of argumentation, one can make the general observation that conventional methods could be characterized by the implicitness of their argumentation. Process-based assurance (e.g. ISO 9001 or CMMI compliance), though shown effective by a vast body of practical application, has little to do with individual systems or even technologies. Process compliance provides indirect evidence of assurance – and furthermore that evidence may part of an implicit argument (not explicitly stated). Technology-specific methods such as fault trees are more directly connected to system specifics, but still not necessarily explicitly drawn into an overall argument for assurance. When fault tree analysis is generated and presented, the *implication* is that the system is sufficiently safe and robust, but the high-level significance is rarely documented (outside of assurance cases) in an explicit, systematic way. Argument-based assurance cases force practitioners to be explicit. For further discussion of this, please see Section 5.3.3, “Mechanism: Explicit Argumentation as a Responsibility”.

Furthermore, framing the assurance challenge as an argument immediately brings a critical and oppositional undertone to the activity that seems appropriate for critical systems – and this should contribute to successful assurance in the end. Efforts directed at assurance are continually drawn back to the central concerns: Is the assurance case convincing? Are we sufficiently certain of assurance? What are the weak points in the argument? In assurance cases, conducting prescribed activities alone is not adequate. Neither is it adequate to document an argument merely to the satisfaction of its authors. The assurance case must hold up under expert challenges to the stated argument. This leads to our next section on evaluation.

5.1.6 Mechanism: The Challenge of Objective and Sufficient Evaluation

The practical efficacy of evaluation is rarely described in literature, but we encountered it frequently in our interviews. Prescriptive compliance, despite its serious shortcomings, has the attractive quality of tending toward unambiguous, objective assessment. Goal-orientation and assurance arguments are much more flexible but potentially prone to subjectivity. As Wassyng (2010) states: “It is not good enough that the producer of the product supplies the evidence and the argument(s) in the safety case. What does matter is that the certifying agent cannot expect the

same type of evidence and the same type of argument each time. The certifying agent thus has less chance of building expertise that will help in future submissions. This lack of expertise, or lack of appreciation of some of the finer points perhaps in the argument, may easily lead to the certifying agent not detecting a subtle flaw. Again, safety case templates could help alleviate this problem." (This quote not only restates the challenge of assurance argument evaluation, but also raises templates – which we group with patterns – as a mitigation. See Section 5.6.3, "Mechanism: Role of Assurance Case Patterns".)

Leveson raises concerns about "confirmation bias" (2011), but this is only a serious threat when regulators do not provide an effective counter-balance to applicants. To repeat a quote from (Hopkins 2012): "A safety case regime will almost certainly fail where safety cases are not scrutinized by a competent regulator." Under assurance case methods, regulators may require additional resourcing, but there is no reason to think that this is an unreasonable expense for commensurate gains in assurance performance. Multiple sources cite a well-resourced regulator as a necessary component of any effective assurance regime.

In fact, the incorporation of expert, independent review and judgement appears to exist in many regulatory systems regardless of assurance case methods. Aside from our interviews, our team is familiar with the FAA Designated Engineering Representative (DER) system in which technical experts are explicitly qualified and used to review and approve critical technical details. Some UK processes use a similar mechanism oriented around Independent Safety Assessors (ISAs). The Norwegian offshore oil and gas regulatory system described in (Baram 2011) is an example of a system that extensively leverages expert evaluation without any explicit assurance case methods.

Therefore, an interesting research question is how expert evaluators react to assurance cases. Since evaluation can be done with our without assurance cases, do they make the task easier or harder? Interview source B could speak to this and indicated that, in their experience, safety cases had taken on a fairly standard form and consequently evaluation was generally straightforward. (It should be noted, though, that B's industry uses safety cases that are largely an umbrella for risk management. Even so, argument constructs were deliberately used in the evaluation process to ensure sound approval decisions.) Interview source H was also in a position to comment on this question. In their regulatory system, assurance cases were more variable in form and content. Nonetheless, they expressed the view that assurance cases made the job of evaluation easier; the key to this improvement seemed to be that the assurance case forced applicants to articulate their logic and this facilitated clear, substantive engagement with the evaluator.

Interview source K indicated that assurance cases are useful not only for review by official evaluators, but also for review by all stakeholders. They expressed concern about the perils of evaluation, however, stating that safety cases do work but only when qualified participants are involved and they apply the appropriate level of rigor. As in the Nimrod case, it is a real possibility that assurance case evaluation degenerates to inadequate levels.

Expert, independent evaluation was also a strong theme with interview source I. In this case, it was really part of the safety culture. Expert judgement was viewed as an indispensable element of safe project execution and appeared to be maintained independent of other specific methodologies (for example, whether a safety case approach or safety management system approach was used). The view among conscientious practitioners appears to be that objective

assessment is essential regardless of method; assurance case practitioners that we talked to indicated that assurance cases facilitate rather than impede objective assessment.

5.1.7 Conclusions

Concerning the fundamental claim that assurance cases are successful where suitable, our research finds that:

- The expanding adoption of safety case regimes across multiple industries over the course of several decades provides strong support for this claim.
- Certain elements are essential, such as evaluation by a well-resourced and competent regulator.
- Goal-orientation and explicit argumentation are core strengths of assurance case methods. These are typically employed in combination with the complementary strengths of other conventional methods.
- Assurance evaluation remains a challenge but on balance appears to benefit rather than suffer from the adoption of assurance case methods.

5.2 Benefit Claim: Assurance Cases are More Comprehensive than Conventional Methods Alone

5.2.1 General Claim and Associated Evidence

By "comprehensive," this claim refers to the ability of assurance cases to incorporate everything relevant to assurance and certification. Complex systems have many different types of potential flaws, both in design and operation. Examples of types of flaws include unanticipated system modes, human factors weaknesses, structures that could fail under stress, software bugs, etc. Some flaws tend to emerge during design review, some during verification test, and some during operation. Most conventional assurance methods tend to detect a subset of flaw types. Assurance cases, it is claimed, have the beneficial property of operating at a higher level than other methods and comprehensively integrate across flaw types, evidence types, and contributing lower-level methods.

Like many claimed benefits, assurance cases can only be considered "comprehensive" relative to certain other methods. Table 4 lists several conventional methods and their general shortcomings with respect to comprehensiveness. It is vital to understand, however, that in practice it is *not* a matter of replacing a conventional method (such as risk management) with an assurance case. It is a matter of choosing an assurance case as a method that overarches risk management (and other conventional methods). The comprehensiveness of assurance cases stems from its ability to effectively integrate a wide range of other appropriate methods.

Table 4: Conventional Methods and Comprehensiveness

Method	Comprehensiveness Shortcomings	Method References
Risk Management	Minimal opportunity for decomposition (tends to produce long lists of individual risks), but covers more types than most methods. Weak on process-based improvements (e.g. safety culture, best practices).	(Boehm 1991)
Safety Management System (SMS)	Unifies a range of assurance measures (safety processes, lifecycle management, risk management, etc.). Relatively good comprehensiveness, but limited by inflexibility (does not adapt well).	(FAA 2006)

Probabilistic Risk Assessment (PRA)	Extends processes associated with risk management, and correspondingly shares the same comprehensiveness shortcomings (see above).	(Stamatelatos and Dezfuli 2011)
Fault Trees	Well-suited to particular types of flaw analysis (for example, failures in a system of related functional units). However, difficult to apply to other flaw types (such as human factors).	(U.S. NRC 1981)
Failure Mode and Effects Analysis (FMEA)	Primarily a reliability analysis methodology. Like Fault Trees, works best with functional unit failures. An extended version (FMECA) adds criticality analysis of failure modes but has similar coverage limits.	(U.S. DoD 1980)

Furthermore, it could reasonably be claimed that assurance cases not only *support* comprehensiveness but *encourage* it. By starting with the requirement to sufficiently make an argument for assurance, the job is not complete until the case is made. If conducing conventional or expected assurance methods leaves weaknesses in the argument, an assurance case directs practitioners to new, complimentary processes and evidence. These are generally diverse from what has already been done and therefore contribute to more comprehensive results.

Our interviews validated that comprehensiveness is a perceived benefit among assurance case practitioners. Interviewee C commented that safety cases help to develop the right requirements and help to avoid missing requirements. This comment lends some substance to the desired property that assurance case argumentation inherently encourages pragmatic comprehensiveness (that is: not only avoid missing things, but also refine to include the right things).

5.2.2 Mechanism: Systematic Approach

One of the benefits of safety cases identified by (Stavert-Dobson 2016) is "systematic thinking." To a certain extent, this is inherent and intuitive: given the requirement to make an argument, the next natural consideration is how to break down the task most appropriately. Assurance cases are flexible and extensible, and therefore respond well to whatever systematic decomposition is selected.

However, there is a significant counter-trend both in literature and especially in practice. The countering view is that assurance cases offer so much flexibility – such high-level goals – that there is no *self-evident* way to go about systematically proving the argument. Part of the difficulty is the relative newness of assurance case practices. As described by (Brain 2014):

> "Clearly, a structured approach is required with the type and frequency of planned maintenance and test activities required for the Safety Case identified at the outset in order to enable the activities required to keep the case current and reliable to be carried out efficiently in a cost effective manner. … A proven approach to Safety Case structuring would be preferred. Unfortunately, such proof does not yet exist for the long term Safety Case (and even for relatively short term cases)."

The authors here are proponents of assurance cases and proceed to suggest some structuring principles, but the fact that they must articulate and address the challenge illustrates our point.

This difficulty involving structure and systematic progress has also been researched for software development safety cases. (Hawkins and Kelly 2010):

> "… constructing safety arguments for the software aspects of systems (software safety arguments) is challenging. When following a prescriptive approach, the developer of the software knows clearly from the outset the processes that must be followed, and the

techniques that must be used. This helps with the planning and management of the development project. In contrast to this, when adopting a safety argument based approach, the necessary activities and processes are not specified up front. Instead the high level objectives are specified, and the developer must determine what techniques and evidence are necessary and sufficient to construct a compelling safety argument. Identifying what evidence will be sufficient to demonstrate that the contribution of the software to the safety of the system is acceptable is a major challenge."

This is echoed in the experience of NASA space systems researchers attempting to implement a safety case (Feather and Markosian 2011): "Despite the well-written guidance on how to go about development of safety cases… we found it daunting to get started."

Consequently, many practitioners find themselves at a loss as to exactly how to proceed systematically. There are many ways the argument could be made, but how do they know which are dead ends or fall short, and which would be acceptable to a regulator? For this reason, we detected through numerous practitioner interviews a resistance to assurance cases – not necessarily among the active users of assurance cases that we interviewed, but among colleagues from whom they tried to gain participation. One way to characterize the objection is that assurance cases are ambiguous with regard to proceeding systematically.

This mechanism cannot be addressed entirely in isolation from another theme among assurance case methods: patterns. We treat these more thoroughly in Section 5.6.3, "Mechanism: Role of Assurance Case Patterns." Assurance case patterns can be established by a regulator to communicate to applicants an acceptable high-level argument structure. It is not necessarily the *only* acceptable structure, but it provides guidance for how an argument *could be* acceptably organized. This is often a vital starting point for applicants. From a provided pattern, they are in a much better position to move ahead systematically with their assurance efforts.

Furthermore, our research produced some evidence that the "systematic approach" mechanism may not be so difficult in the longer run – as practitioners get used to the methods and establish new norms and expectations. One interviewee (J) represented an organization that was relatively mature in their use of assurance cases. They used assurance cases as the basis of a structured approach very much in line with the aspirations of academics and theoreticians: they started the assurance case early, used weak areas of the argument to steer their development and test decisions, and set up collaboration mechanisms so that all relevant staff could contribute to assurance case development. For this particular interviewee, assurance cases are so integrated into their internal processes that it is difficult to imagine how they would operate without them. At present this is the minority of field practices, but it is a positive indicator that assurance cases can be a powerful structuring mechanism as practitioners get more familiar with it.

5.2.3 Mechanism: Integration with Conventional Methods

By its critics, assurance cases are sometimes drawn in contrast with conventional methods, for example "safety case vs. prescriptive safety". However, in many ways, this is a false dichotomy. For the most part, assurance cases operate at a higher level of abstraction than conventional methods and therefore function well as an integration mechanism that overarches them. That is, the most appropriate long-term way to think about assurance case methodology adoption is as the top (integration) level of a new hybrid approach to assurance management.

5.2.3.1 *Incorporating conventional methods as evidence*

The Jaguar electronic throttle example mentioned earlier provides an example of comprehensively integrating conventional methods within the framework of an assurance case. As reported by Barker, Kendall, and Darlison (1997), the safety case incorporated:

- software safety and quality proofs,
- system-level safety management (design through production),
- compliance with IEC 1508,
- compliance with ISO 9000-3,
- compliance with MISRA guidelines,
- fault tree analysis, and
- failure mode and effects analysis (FMEA).

The Jaguar example shows clearly and practically how a safety case can overarch and integrate results from conventional methods.

Numerous interview sources (e.g. A, G, I) explicitly mentioned using conventional standards and methods at lower levels such as system implementation and software design. It is the norm in all the detailed examples we encountered. One interview source (E) stated that the differential cost of constructing an assurance case – that is, the cost over and above what would be done without an assurance case – is essentially zero, because it simply integrates everything that needs to be done anyway as a matter of good engineering.

5.2.3.2 *Organizational decomposition of assurance methods*

Another interesting observation from our field interviews was that, where assurance cases are used, they may only used by a subset of the organizational network involved in producing and operating the system. An assurance case might be deployed at the upper level of technical management, and conventional methods might be deployed at the lower levels of design, implementation, and operation. For example, a safety management group might write, own, and maintain a safety case. This group might work with high-level designers to steer assurance efforts; however, lower-level designers and implementers might work only to the standards and methods flowed down to them. They may have no practical visibility into the safety case, and there may be no need or benefit to such visibility. Their job is more focused by attending to conventional methods. Their conventional efforts are integrated into the total safety picture by practitioners working at a higher level of analysis and planning.

One reason that assurance cases may be tended by specialists is practical: real-world assurance cases can be so large that those who manage them do not have time for anything else, and those who are concerned with technical design or operations do not have time to come up to speed. “Typically a safety case for a moderately sized system, along with the reports that constitute the primary supporting evidence, can result in a pile of paper several inches thick (larger systems safety cases have filled library shelves).” (Cockram and Lockwood, 2003)

Our interviews suggested some tension concerning this dynamic, however, as there is a genuine desire to create access to the assurance case by as large a subset of the organization as possible. Interview source I captured the benefit they are seeking by stating that it is easier to explain safety to technical experts than to explain technical detail to safety experts. It can be a dangerous assurance approach to have safety largely in the hands of safety experts because they are not the ones that have a deep understanding of the technical and operational risks. Hence there must be a strong link, somehow, between the assurance case management and technical

expertise. In the case of interview source I, they tended to use fairly simple safety case formats and constructs which made the content more accessible internally. They also invested in safety training for technical managers and other staff.

Likewise, the notion that assurance cases are primarily only used by the upper levels of assurance management is somewhat at odds with a subset of literature that emphasizes making assurance cases accessible to all practitioners involved. "…structure makes the safety case readable and comprehensible to casual as well as expert readers" (Stavert-Dobson 2016). Many would not associate safety cases with "casual readers" so this certainly implies a wide audience! One subtle effect here could be that it should be easier for non-experts to *read* an assurance case (and perhaps use it for navigation purposes) than to *create* or *modify* it – similar to the way that many people can comprehend an accident report but few have the expertise to write it. The accessibility of an assurance case has important implications for maintenance and evaluation (see Section 5.1.6, "Mechanism: The Challenge of Objective and Sufficient Evaluation).

To conclude, we find significant variations (and competing strategies) in how organizations draw the lines to define practical access to assurance cases. There are ramifications for notations and analytical capabilities as well (see Section 5.4.3, "Mechanism: Assurance Case Notations"). While it is possible that mature argumentation practices could someday permeate practice to the point that lower-level designers and implementers interact directly with sub-arguments allocated to them, this is a sophistication that is not common in current activities, although we did find some advanced practitioners moving in that direction. However, where possible, most successful applications today appear to be taking the general approach that specialists deal with the high-level assurance case construction and flow down more conventional requirements to functional project groups (for example, requiring software development to meet certain standards and conduct certain analyses).

5.2.4 Mechanism: High Level of Abstraction

There is a relationship between this mechanism and the one discussed earlier in Section 5.1.4, "Mechanism: High-Level Goal-Orientation." The distinction is that, in this mechanism, we discuss how high-level conceptual positioning serves comprehensiveness specifically rather than successful assurance in general.

By starting with a high level of abstraction – in essence, "Why should we believe this system is safe (or secure, dependable, etc.)?" – assurance cases are flexible to any structure, arguments, and evidence that effectively serves the high-level concern. There is a fundamental contrast in this regard as compared to most assurance methods, which prescribe a particular process and inherently make no suggestion of comprehensiveness apart from that method. For example, a risk management approach leads to certain risk identification and mitigation processes. This approach exists at what might be designated a medium level of abstraction: flexible to any type of risk, but requiring every issue in scope to be cast as a risk. (For example, subsystem failures and management failures are all risks put through the same processes even though they are very different in nature.) Assurance cases operate at a higher level of abstraction and lead to any type of lower-level method (such as risk management) that strengthens the argument.

Examples that we encountered in our research illustrate this mechanism of high-level abstraction yielding comprehensive assurance. The Jaguar electronic throttle example is one, demonstrating abstraction across lower-level assurance methods. Another example is shown in Figure 12, which is an excerpt from (Eurocontrol 2012).

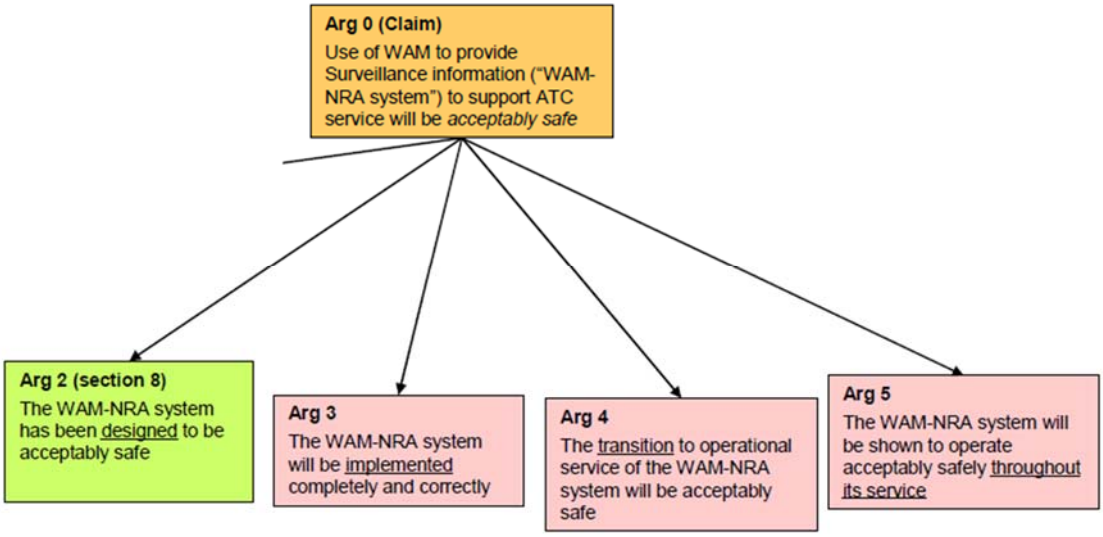

Figure 12: Excerpt from Eurocontrol WAM PSC High-Level Argument

The very simple decomposition shows another type of high-level comprehensiveness: uniting safety concerns across the system lifecycle (design, implementation, transition, and operation). This high-level decomposition leads easily to next-level argument decomposition and so forth until the complete argument is deemed sufficient.

5.2.5 Conclusions

Concerning the claimed benefit that assurance cases are more comprehensive than conventional methods alone, our research finds that:

- General indicators substantially support the claim.
  - Literature clearly reflects the value of assurance cases with respect to comprehensiveness.
  - Practitioner interviews indicated the same.
  - Assurance case argumentation tends to make it more abstract by design than most conventional methods (risk management, SMS, etc.) – that is, less constrained by specific techniques and processes.
- An important caveat is that practitioners may find it difficult to proceed comprehensively (systematically) in the absence of an effective guiding pattern for assurance case structure. Patterns may be provided by experience or regulator guidance.
- We found ample field examples of assurance cases overarching more traditional methods (integration at a higher level of abstraction).
- There is some tension in practice concerning where to draw the boundaries of organizational access to assurance cases – whether it should lean toward management by specialists or lean toward maximizing access by non-experts. This dynamic relates not only to practical comprehensiveness but also notational rigor (see Section 5.4.3) and efficiency (see Section 5.6).

5.3 Benefit Claim: Assurance Cases Improve the Allocation of Responsibility over Prior Norms

5.3.1 General Claim and Associated Evidence

One of the seminal motivations for assurance cases is the desire to focus practitioners on their responsibility for real safety as opposed to *pro forma* compliance with regulations. A good example is the response to the Piper Alpha oil platform disaster in 1988 (167 dead, 61 survivors) which triggered an investigation and the publication of the Cullen Report. "The Cullen Report also did away with traditional prescriptive safety legislation in favor of a more progressive 'goal-setting' model" (Turner 2013). The essential conclusion was that major accident sequences may be impossible to prescriptively predict. Therefore, a prescriptive approach to safety is prone to falling short in cases of high safety-criticality and/or complexity in design and operation. Since 1992 safety cases have been required for UK offshore oil and gas facilities.

The concept of "duty holder" is a powerful one that has taken hold in literature and practice. The U.K. Ministry of Defence (MOD) defines the duty holder as "A MOD person with specific responsibilities for the safety management of the system" (00-56). The distinction is subtle but extremely important: there is a person who holds a duty for safety, not merely a responsibility to comply with prescriptions. (We discuss some of the legal ramifications of this in Section 5.7, "Benefit Claim: Assurance Cases Provide a Practical, Robust Way to Establish Due Diligence.") Bloomfield & Bishop (2010) present one strength of safety cases as "to prevent safety from being seen as the responsibility of the regulator rather than the service provider."

Also embedded in the concept of assurance cases is the understood mechanism that the responsible party must "make the case" to the regulator. This is a more open-ended responsibility than prior norms. Assurance cases are somewhat novel in explicitly requiring the applicant to make a successful argument. While the *de facto* necessity of convincing the regulator has been a reality in a multitude of past examples, assurance cases require it to be explicit and defensible.

Most of the evidence we found concerning this claimed benefit organizes well into the mechanism sections that follow (5.3.2, 5.3.3), so it is presented in context accordingly.

5.3.2 Mechanism: Clarification and Localization of Responsibility

The reality of large systems development is that multiple organizational units are involved, forming a complex web of roles and responsibilities that have a vital impact on successfully developing and fielding the system. In many of the interrelationships between these entities, there is a regulatory component and an associated assurance methodology. Additionally, many entities find it appropriate to adopt internal assurance methods to fulfill their respective responsibilities. Our field interviews suggest that assurance cases can play a valuable role in this web of organizations and responsibilities. However, the detailed application of assurance cases is far from simple in the relatively complicated stakeholder environments that are frequently encountered.

An overview survey of systems development life cycle (SDLC) literature suggests that the primary perspective is *what activities and processes* happen (or should happen) (FAA System Safety Handbook, 2000; Ericson, 2005; Grady, 1998). There is relatively less emphasis on *roles* in SDLC – that is, what organizations/groups are in the picture, how they relate to each other, and what their responsibilities are. One reason for this is undoubtedly that there is great variability in the organizational structure of SDLC. Kossiakoff and Sweet (2003) comment on this within the limited context of systems engineering activities: "… despite its central

importance to the success of a given system development project, the systems engineering function will usually need to adapt to preexisting organizational structures. … This means that the systems engineering activity must span not only a number of different disciplines but also several independent companies." Even this broad statement does not go far enough for our purposes. In many of the systems addressed by this report, not only were multiple independent companies involved, but also multiple government entities and associated structures with roles in specification, ownership, and operation (in addition to regulation).

The U.S. Department of Transportation (2009) identifies at least a few broad "Roles and Responsibilities in Systems Development," documenting the following structure:

- System's Owner
  - Project Sponsor
  - Stakeholders
- Systems Engineering Assistant
  - In-House Staff
  - Independent Verification and Validation
  - System Manager
- Development Team
  - In-House
  - Systems Integrator

While its identification of some distinct roles is helpful, it is still inadequate compared to some of the system contexts we encountered in our research. There is no representation of more complicated subcontracting and supplier relationships as well as technical operations.

A somewhat realistic, representative organizational structure encountered in our field interviews is shown in Figure 13.

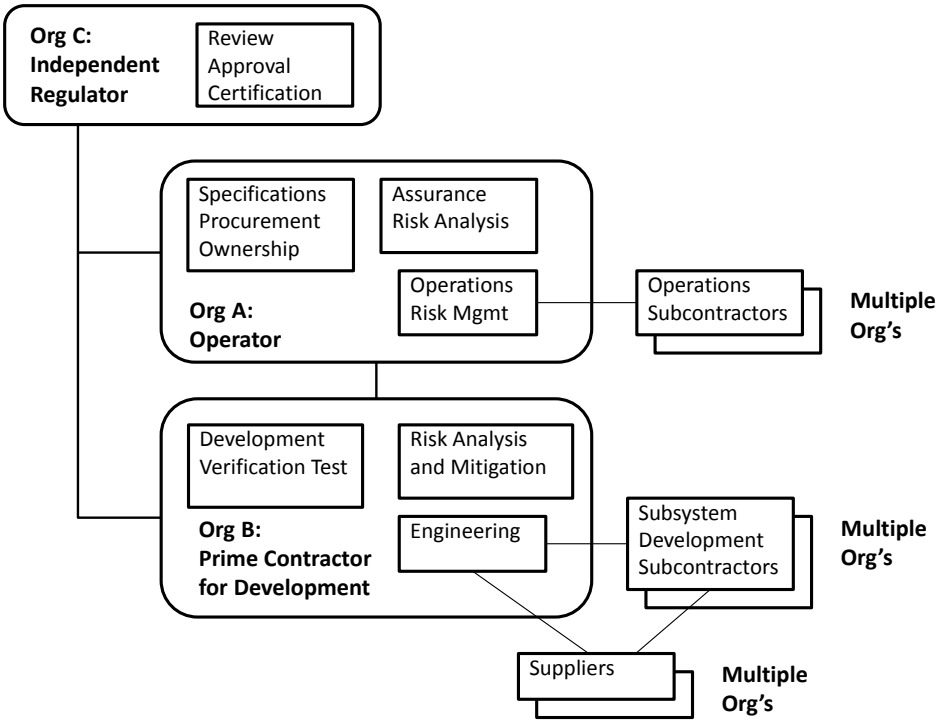

Figure 13: Realistic Organizational Structure for Large System Examples

The organizational complexity shown in Figure 13 is fairly typical for large, complex systems. Our team encountered several variations on the theme:

- government as both operator and regulator,
- prime contractor as both developer and operator,
- separation between ownership/operations and specification/development (as in commercial systems),
- separate ownership and operations organizations,
- etc.

Furthermore, there is a large and important set of variations that deal with modified and upgraded systems. The main point is that it is far from trivial to assign assurance responsibilities to such a network, and there are further complications when it comes to mapping methodologies (such as assurance cases) to the responsibilities. Figure 14 shows a hypothetical subdivision of assurance cases in an environment of complex responsibility mappings.

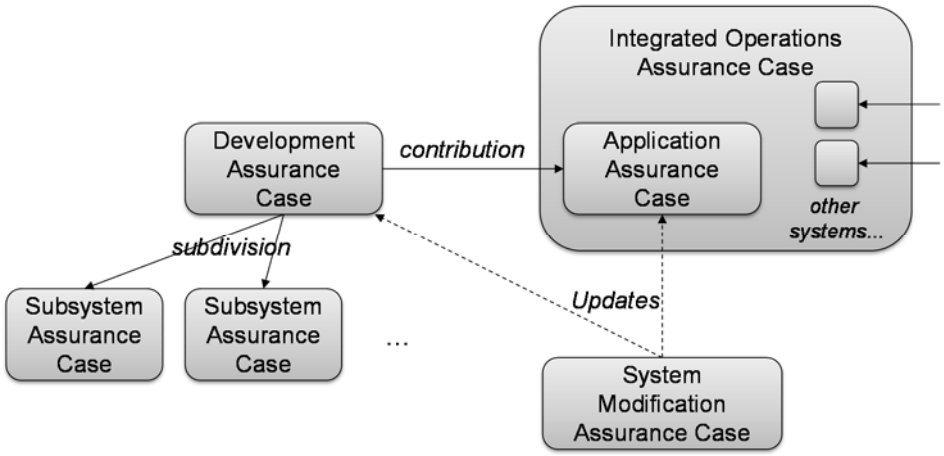

Figure 14: Generalized Practical Subdivision of Large System Assurance Case

Regardless of exactly how it is accomplished, one of the appeals of assurance cases is in clarifying the responsibility for assurance and deliberately moving it closer to the most appropriate parties. “Experience suggests that the main benefit of a safety case comes from the process that the operator has to go through to prepare the case. Thus it is not the document or suite of documents, called the safety case, that should be seen as the greatest product of safety case regulations, rather it is the process of preparing the case and the improvements in the hardware and managerial arrangements that are identified as necessary. The operator of the installation will always know it better than any regulator and the requirement to produce a safety case is intended to ensure that they know it even better.” (Wilkinson 2002) Interview source E stated that a breakthrough for their organization was realizing the role and importance of *ownership* of the assurance case.

What we see in our practitioner interviews is a variety of ways in which assurance case method integration has played out, depending on the nature of the organizational responsibilities network. In relatively simple or small systems, assurance cases may be fairly self-contained. In large or complex systems, the management of responsibilities may tend to produce assurance cases that are necessarily subdivided. Interview source E saw a range of decompositions within the regulatory schemes in which they were involved; they cited one scheme that divided assurance cases into a design case and an operational case, and another scheme that required them to be unified. We did not see evidence that one approach was inherently better than

another, rather that each was appropriate for different system types and configurations of stakeholders and responsibilities. Also, aside from separating design and operations, interview source E had also seen success with subdividing assurance cases by separate subsystems and/or separate applications.

The regulatory environment we discussed with interview source F is an informative example. The system in question is a multi-year (likely multi-decade) undertaking with numerous organizations participating as stakeholders. The owner of the system holds responsibility for essential safety as designed and built. Safety case analysis is outsourced to an organization with relevant expertise; this expert organization documents and maintains the safety case working closely with development contractors. The expert organization has some oversight of development, but ultimately evaluation of safety assurance is done by the system owner.

In this environment described by interview source F, several variants or by-products of the assurance case had to be produced. The system owner had responsibilities ascribed to it in several categories (such as human safety, environmental impact, etc.). The system owner owed different regulators a range of specific assurance products for review. However, the system owner was not directly the operator of the system. In fact, there were several operators of the system, each with unique applications. Each of these operators bore responsibility for details of their usage. The expert organization was also involved in working with these operators and generating the assurance cases that each of them needed to manage their particular responsibilities.

The above description of Interviewee F's regulatory environment illustrates one real-world example in which responsibility allocation is both compelling and complicated. It is not easy to sort out assurance in an environment such as this, with or without assurance cases. In this example, assurance cases were used and at least made the decomposition of a complex set of responsibilities clear and manageable.

5.3.3 Mechanism: Explicit Argumentation as a Responsibility

A common phrase in the literature is that party responsible for assurance must "make the case" for it. "Where previously prescriptive standards were used as the main certification device, the responsibility is now being placed with the developers to *argue* a safety case." (Kelly 1998). Explicit argumentation reinforces proper responsibility allocation between regulator and applicant. If an applicant provides a vague or unsubstantial argument, the regulator can reply along the lines of "you have not yet adequately made the case." The regulator can also direct them to established guidance on what types of arguments are acceptable. The process is back in the applicant's hands to fix the argument before the conversation can even begin as to whether or not system assurance is adequate. This exact process was noted in our interview with source H, who indicated that an assurance case provides a map of the relevant body of information and explains why the applicant believes it's important (that is, what conclusions they believe the information supports). In other words, the argument directs the applicant to explicitly explain how they have met their responsibilities.

On this point, it is again helpful to contrast the process featuring explicit argumentation with the conventional process that occurs in many regulatory systems. If, for example, regulations require applicants to provide design information and test data, applicants are likely to feel that they've done their part once that documentation has been delivered. Even if guidance states that they are responsible for assurance, their *de facto* responsibility is to deliver documents. If assurance is not clear to the regulator, any pushback to the applicant will be viewed to some

extent as obstructionism. The applicant is in a position that, in their view, they've done what is required and the regulator is being difficult and levying additional, subjective requirements.

One example we encountered in literature illustrates this point. (Dahle et al. 2012) describes the re-evaluation of Australian regulation for offshore oil and gas in response to the Montara oil spill in 2009. "In some areas the Commision wants to have a more prescriptive regulatory approach, for instance developing more detailed standard for drilling operations. … The Australian authorities, however, showed a more reluctant attitude towards this recommendation as it was believed to transfer responsibility from the companies to authorities." In this example we see a conscious decision not to pursue additional prescription because the responsibility allocation in goal-oriented methods (such as assurance cases) is preferred.

If explicit argumentation is required as in assurance cases, the applicant's responsibility is further reinforced in practice. The process of documenting explicit argumentation is likely to prompt applicants to proactively strengthen weak points, which has a beneficial effect before the submission is even made. Once a submission is made to the regulator, it is the regulator's job to assess the quality of the argument. The key point is that there are clear roles assigned to the applicant (to construct a sufficient argument and provide evidence) and regulator (to review, accept, reject, and provide feedback).

5.3.4 Conclusions

Concerning the claimed benefit that assurance cases improve the allocation of responsibility over prior norms, our research finds that:

- Allocating and managing assurance responsibilities can be very daunting in the large networks of interrelated stakeholders such as found in many systems encountered in the field today.
- The claim is supported by: (a) our interviews which included practitioners stating this from experience, and (b) by literature sources discussing it.
- Our literature survey results also suggest that responsibility allocation is a relatively weak area of conventional, prescriptive methods and frameworks such as systems development lifecycle (SDLC). This lends support to the claim that assurance cases (and possibly other goal-oriented methods) are an improvement relative to conventional methods such as these.

5.4 Benefit Claim: Assurance Cases Organize Information More Effectively than Conventional Methods

5.4.1 General Claim and Associated Evidence

This benefit claim states that assurance cases capture the relevant content in a way that is more intuitive and quicker to navigate than conventional methods (especially for those who do not specialize in safety, such as managers and technical staff). Effective organization, thus described, presumably translates to greater effectiveness in associated processes such as production, revision, and review. This in turn allows stakeholders (developers, operators, regulators, etc.) to do their jobs more quickly and with less frustration.

One dimension of this is simply the ability to scale up to a large amount of information. For large safety-critical systems, the body of assurance information is huge. Assurance cases provide a scalable way to subdivide, cross-link, and explain the body of information. We examine this dimension in more detail in Section 5.4.4 below.

At a slightly more subtle level, there is the intent that assurance cases will lead to better communication between the various parties that must interact over them – most prominently, regulators and applicants. Stavert-Dobson (2016) identifies "aiding communication amongst stakeholders" as one of the benefits of a safety case. This improved communication seems to have been noted especially by regulators in alignment with Wilkinson's statement (2002) that assurance cases yield "better oversight by the regulator."

Of course, to address this claim completely, one must consider how effectively conventional methods organize information. A method like risk management is inferior on a first-order basis: the method tends to produce enumerated lists of risks lacking decomposition and high-level structure. A method like safety management system (SMS) is more comparable. An SMS generally incorporates a range of processes (including risk management) and, correspondingly, a range of documentation formats for organizing assurance information. Within an SMS's prescribed structure, it organizes information quite effectively. However, the prescribed structure is not necessarily sufficient or efficient (see Section 5.6, "Benefit Claim: Assurance Cases Offer an Efficient Certification Path Compared to "). An SMS is a good way to organize assurance information according to static, well-known processes. It is not a good fit for assurance activities that are dynamically evolving to meet high-level goals.

At the risk of muddying the waters, the above critique that a given SMS is limited by prescription would be somewhat irrelevant if that SMS called for the development of an argument-based assurance case. Such a hybrid is conceivable (although we have not encountered any in practice). The converse is also possible, as mentioned in Section 5.2.3.1, "Incorporating conventional methods as evidence" – the existence of a prescriptive SMS could be used in the higher-level arguments and evidence of an assurance case. In some literature, there is a blurry line between well-organized SMS documentation, a "safety case," and an assurance case that is light on argumentation. Here we maintain the distinction that an SMS is essentially prescribed processes without flexible argumentation (unless explicitly called for by the inclusion of an assurance case). By contrast, an assurance case by our definition always has at least some stated high-level goals and argumentation.

Practitioners in the field also gave us insights on assurance cases as a means of organizing information. Interview source E emphasized that assurance cases must be living, dynamic documentation that must not sit on the shelf unused. This same source stated that assurance cases provide a route to diagnosing a problem. Descriptions like these suggest that practitioners in the field turn to assurance cases to organize their efforts in a way that is relevant and pragmatic.

5.4.2 Mechanism: Explicit Argumentation and Assurance Case Structure

T. Kelly wrote in 1998: "… a commonly observed failing of safety cases is that the *role of the safety argument is neglected*. In such safety cases, many pages of supporting evidence are often presented (e.g. hundreds of pages of fault trees or Failure Modes and Effects Analysis tables), but little is done to explain how this evidence relates to the safety objectives. The reader is often left to guess at an unwritten and implicit argument." The underlying criticism here is that often assurance information has minimal and superficial organization; the recommended improvement is to organize along the lines of an explicit argument.

Our field interviews supported this view, especially from the regulator side. Returning to interview source H, explicit argumentation was identified as one of the key benefits of the method – as compared to a loosely-prescribed system that preceded it. Previously an applicant might essentially state, "We believe this system is safe because of this stack of documents." If

the regulator disagreed, it was up to them to counter unstated logic (presume the applicant's argument). A presumed argument often does not coincide with the applicant's (undocumented) reasoning, resulting in frustration and inefficient back-and-forth between the applicant and regulator. In contrast, using assurance cases with explicit arguments, the regulator can zoom in on the point of concern and provide counter-argument such as, "I disagree with this claim because …" or "The evidence provided with this claim is not sufficient as presented, and the weak area is …" Source E stated that these new feedback processes with assurance cases were concise and clear as compared to prior experience.

5.4.3 Mechanism: Assurance Case Notations

There is a high degree of variety and a range of opinions in the assurance cases field concerning notations used to document an assurance argument. In a prior report (Rinehart et. al, 2015), we identified an array of argument notations:

- Goal Structured Notation (GSN)
- Claims, Arguments, and Evidence (CAE)
- Object Management Group (OMG) Structured Assurance Case Metamodel (SACM)
- Textual Forms including:
  - high-level templates such as sectional outlines
  - free-text patterns using well-understood elements such as claims, evidence, reasons, qualifiers, rebuttals, etc.

There is a general tradeoff concerning notations is shown in Figure 15. There are advantages and adherents across the spectrum. Some sources prefer the analytical power of a format like GSN, while others prefer the intuitiveness of a textual template.

Figure 15: Assurance Case Notation Tradeoffs

GSN is an important topic in this area as it is widely used and promoted by academics (Kelly and Weaver 2004, Palin and Habli 2010, Witulski 2016). Certainly it connects to an aspect of research interest, which is attempting to move toward more rigorous argument analysis (targeting eventual proof to some extent). However, our practitioner interviews suggested limited adoption of GSN in the field. GSN in practice seems to lend itself to assurance case specialists who can invest the time in learning the relevant graphical definitions and argument patterns. However, there appears to be a significant body of practitioners who find the format unwieldy. Where it is used (or proposed for use) in the field, it appears to be used in simple structures as opposed to more advanced argument structures present in academic literature (Kelly and McDermid 1998, Weinstock and Goodenough 2009).

There certainly were some practitioners who used and valued GSN. Of our eleven interviewees, three indicated that they routinely worked with GSN. Three more indicated partial use of GSN (for high-level arguments or certain submissions). The format also had its detractors – two interview sources noted an aversion to "GSN wallpaper." Use of GSN tended to be more prominent among assurance experts as opposed to technical staff and management.

Perhaps the most important take-away from our research on this subject is that the rigorous use of a structured graphical format like GSN is by no means essential for assurance cases. The majority of successful assurance cases we encountered in the field use more informal argument notations such as free text, outlines, tables, and simple graphs (in some cases what might be called degenerate GSN). The obvious motivation is accessibility to experts whose input is necessary for the assurance case. As noted in Section 5.2.3, "Mechanism: Integration with Conventional Methods," interview source I made the salient observation that it is easier to explain safety to a technical expert than technical details to a safety expert. It stands to reason, then, that it is desirable to use formats which make the assurance documentation more accessible to technical contributors that are not assurance experts.

A noteworthy observation of our research is a discrepancy between academia and practitioners is that many academics are focused on pushing the bounds of rigorous, analytical argument evaluation whereas practitioners are largely focused on argument forms that facilitate practical human judgement. Someday there may be greater synergy between these perspectives, but at present they are quite separate. For example, research literature addresses some topics such as GSN contracts (Despotou 2007) and theories of confidence (Goodenough et al. 2012). While these represent potentially important future directions, the practitioners we interviewed are focused on practical, human-oriented, judgement-based evaluation. All of our interview sources were involved in robust assurance case evaluation based on human expert judgement; none used formal or analytical argument evaluation. Evaluation literature among practitioners focuses on expert processes (e.g. safety case review guidelines such as UK HSE 2008).

Nonetheless, advanced notations in assurance cases offer the future potential for formal, analytic evaluation. Presently, assurance arguments are based upon inductive logic, i.e., a logic in which general conclusions are inferred from specific observations allowing for the possibility that a conclusion is, in fact, false. Researchers (Rushby 2015) have suggested the documentation of assurance arguments using a novel structure in which the argument is based upon deductive logic, i.e., a logic in which conclusions are drawn from premises such that, if the premises are true, a conclusion must be true. In this structure, all uncertainty is located in the assessment of the evidence. If this were possible, the argument itself could be mechanically checked.

Simple type checking could be integrated into statements in assurance cases thereby allowing limited but possibly useful analysis. For example, if a set of hazards were defined by enumeration in a set such that each hazard was associated with a unique symbol then strategies such as "Argue over all credible hazards" would define at least part of the expected content of the associated subgoals. Checking that all elements of the set had at least been mentioned and that no member had been mentioned more than once provides at least a simple check on the content of the subgoals. Although this is merely at the level of checking for typographical errors and simple omissions, such errors are not unlikely in a large assurance case.

Rigorous arguments do not preclude the use of methods such as risk management and safety management systems. Frequently, such systems make use of probabilistic risk analysis (PRA) leading to decisions being based on probabilities that one or more hazards will arise. Although the analysis conducted in PRA is formal, the resulting probabilities are almost universally conditional on a number of factors for which probabilities are either unavailable or untrusted. The advantage of rigorous arguments in such circumstances is that they allow entities such as probabilities to be included in the argument in such a way that the valid contribution of the entities to belief is clear and explicit.

The selection of argument notation (and associated technical rigor) is a weighty one for practitioners. If the assurance argument can be comprehended fully only by a few extensively trained experts, it poses a threat to one of their fundamental needs: to reach consensus that the assurance argument (and underlying activities) are sufficient. Conversely, the more transparent and accessible the argument, the easier it is to achieve efficient communication and consensus among the necessary stakeholders. From this perspective, it is not surprising to observe that practitioners appear to lean in the direction of simpler argument notations.

5.4.4 Mechanism: Assurance Case Scalability and Supporting Tools

There is a significant amount of literature and practice in the area of support tools for assurance cases. These usually included features for graphical presentation, data entry, scaling up, and interactive navigation.

Although many practitioners manage without them, the need for supporting digital, software-based assurance case tools is not difficult to identify. As described in (Kelly 1998): "The totality of evidence and argument required to meet many of today's certification standards can be huge. The engineer constructing the safety case can often be left with the unenviable task of attempting to present a safety argument that overarches thousands to tens of thousands of pages of evidence." Conventional large-system design teams are well-acquainted with reams of documentation, and the document-oriented approach is still seen among many practitioners. Nonetheless, in today's context of digital information management, the appeal of assurance case software tools is clear.

We reviewed several literature sources about digitally managed safety cases. Cockram and Lockwood (2003) summarize the motivation and objectives: "The challenge to safety engineers is to produce safety cases that are quickly readable, intelligible and auditable even when a large amount of material is required. We describe the problems in developing complex safety cases using traditional development methods and the opportunities to address these problems by the development of an electronic safety case."

Some of our interviewees mentioned using electronic tools specifically designed for assurance cases (Interviewees F and J) and we expect that one or two others did as well, although it didn't come up explicitly in our interviews. It seems reasonable to expect that, as notations and practices settle among assurance case practitioners, supporting tools will become more common and beneficial.

5.4.5 Conclusions

Concerning the claimed benefit that assurance cases organize information more effectively than conventional methods, our research finds that:

- In general, the claim is supported both by literature and our field interviews.
- SMS is a well-organized conventional method, but its range is limited by prescribed assurance processes.
- Advanced formats such as well-formed GSN are not necessary for successful assurance cases in the field; rather, most practitioners use simpler formats and appear to benefit from accessibility for non-experts.
- At the more advanced end of assurance case notations, there is the future potential for more rigorous argument analysis, although this remains a research area and we did not find any fielded examples.

- Assurance case supporting software tools are fairly common but not yet used by the majority of practitioners.

5.5 Benefit Claim: Assurance Cases Address Modern Certification Challenges

5.5.1 General Claim and Associated Evidence

This benefit claim presents assurance cases as a solution to many of the emerging challenges in certification. Moderns systems are expanding the boundaries of complexity and safety-criticality. In addition to these characteristics, innovative systems are generally difficult to manage from an assurance perspective because precedents are scarce (e.g. applicable standards).

Existing certification approaches are severely strained by these characteristics. Assurance cases, according to this claimed benefit, manage these aspects significantly better than conventional alternatives. In the extreme, assurance cases could make certification achievable where it might otherwise have been practically out of reach.

Some of the fields in which assurance case use is being employed or explored substantiate this claim in general. As mentioned in Section 5.1.3.1, "Assurance Cases in the Nuclear Industry," the nuclear power industry was one of the earliest adopters of assurance cases (Verrall 1996, Brain 2014). NASA researchers have experimented with assurance cases (Feather and Markosian 2011). More prominently, NASA has published related guidance about "risk-informed safety cases" (NASA 2014). In the following three mechanism sections (5.5.2, 5.5.3, and 5.5.4) we examine examples such as these broken down into three sub-areas: safety-criticality, complexity, and innovative technology.

What is perhaps slightly obscured by the following sections is that assurance cases are a good fit for a synergy of multiple "modern" factors (safety-criticality, complexity, and innovation). Evidence of this in literature and field application is significant, which lends weight to the claimed benefit. Table 5 summarizes domain areas relevant to this point. (In Table 5, we are conservative and general in indicating modern characteristics).

Table 5: Presence of Safety-Criticality, Complexity, and Innovative Technology in Researched Domains

Domain	Safety-Critical	Complex	Innovative Tech	Encountered in Literature	Encountered in Interviews
Manned Aircraft	✓	✓		✓	✓
Small Unmanned Aircraft	✓		✓		✓
Large Unmanned Aircraft	✓	✓	✓		✓
Nuclear Power	✓	✓		✓	
Radioactive Waste	✓			✓	
ATC/ATM Systems	✓	✓	✓	✓	✓
Space Systems	✓	✓	✓	✓	

One feature that is clear from Table 5 is the predominance of safety-criticality as an applied concern, which is the subject of the next section.

5.5.2 Mechanism: Managing Increasing Safety-Criticality

A specific mechanism of the broader claim is that assurance cases handle safety-criticality better (for the purposes of assurance) than alternatives. The trend in systems development and society in general is toward greater reliance on technology; correspondingly, there is increasing safety-criticality in such systems. That is, setting aside for the moment technological novelty, the quality of interest is that many new systems will be expected to make decisions and act within situations that have ramifications for life and limb. There are many examples of this including self-driving vehicles, energy infrastructure, medical devices, and space launch systems.

What advantages might assurance cases have in managing safety-criticality that conventional methods do not have? The most significant advantages are likely *comprehensiveness* (see Section 5.2) and *flexibility* in the context of safety-critical requirements. Assurance cases can be extended in whatever direction is necessary to reach the desired level of assurance. This does not necessarily mean that assurance cases are the best method for *every* safety-critical application, but this advantage is likely to be compelling in at least some applications.

The fact that assurance cases were adopted by the nuclear industry – and that the industry has stayed on that track for many decades – provides some evidence for assurance case suitability to manage safety-criticality. Granted, nuclear power systems are not especially complex or modern in the normal sense of engineering state of the art (compared to, say, a distributed traffic system or high-performance computing). However, the nuclear industry can be thought of as an early adopter for safety-critical technological issues in general. It is certainly extraordinarily safety-conscious and deals in large, high-consequence systems.

In the case of oil and gas infrastructure, adoption was not academic or gradual; it was in response to large-scale accidents. As noted by (Dahle et al. 2012):

> "At an institutional or regulatory level, the three offshore accidents resulted in a more independent and stronger regulatory regime. … In the new regulatory regime all offshore facilities needed to conduct a Safety Case, which is based on risk analysis on each facility. (Store Norske Leksikon, 2009) The safety case approach is also recommended in the Macondo investigation report. In the safety case the industrial operating actors have to prove that the facilities and operations are sufficiently safe."

(It is also noteworthy in this quote that risk analysis is considered part of the safety assurance case – even considered the basis for it. The two method approaches, risk and argumentation, are used together in a complementary hybrid.)

Assurance cases appear to continue to find application at the boundaries of extreme safety concerns. One such example is in long-term storage of radioactive waste, which could be said to present safety threats not only to current populations but many future generations as well. Baik et. al (2015) document the use of safety case methods for this purpose: "A safety case is the synthesis of evidence, analyses and arguments that quantify and substantiate a claim that the repository will be safe after closure and beyond the time when active control of the facility can be relied on." Though this example necessarily focuses on geology more than technology, it shows how assurance cases have a very strong appeal where safety is critical: they are focused and systematic while adapting easily to the specific assurance goals dictated by the context. (Using assurance cases for long-term storage of radioactive waste is also an example managing novelty, that is, assurance for which there is no sufficient precedent. This is essentially the focus of Section 5.5.4 below, "Mechanism: Managing Certification of Innovative Technology".)

In addition to many literature examples of assurance cases used in safety-critical systems, we also found that safety-criticality was virtually constant throughout our practices study. All our interview sources (A–K) used assurance cases to manage safety first and foremost.

We can state based on our evidence that safety-criticality is a dominant concern among assurance case practitioners. We can also state that those practitioners appear to be satisfied with the way they handle safety-criticality, especially with regard to the clarity and maintainability of well-designed assurance cases. This does not necessarily mean that assurance cases are the best choice for all safety-critical applications. There are countering opinions in the literature along the lines that the only sensible response to safety-criticality is increased prescription, and that assurance cases are too open-ended to be trusted with safety-criticality. Nonetheless, the balance of our evidence supports the claim that assurance cases manage safety-criticality well compared to other methods – perhaps qualified by dependence on contextual factors and practitioner skill.

5.5.3 Mechanism: Managing Increasing System Complexity

Another element of the broader claim is that assurance cases handle system complexity better than alternatives. Referring to complexity here, it is important to call to mind the many levels and types of systems subject to assurance. For example, as organizations become more operationally complex, there are systems of human roles and procedures that call for assurance-oriented scrutiny. While certain types of system complexity are associated with well-known assurance methods (for example, dependency in software systems or fault trees in hardware systems), other types of system complexity are emerging that are ill-suited to conventional methods.

Several of our literature survey sources used assurance cases to deal with organizational complexity. For example, Inge and Costello (2008) are concerned with end-to-end arguments for inter-departmental functions in a military organization. It is difficult to imagine an alternative method that can apply to a case like this as easily as an assurance case. One can imagine doing a general risk assessment, but it does not carry the same orientation to a high-level objective for the functioning of the organization.

Air traffic management and control systems present another unique example of complexity. ATM/ATC systems are infrastructure-intensive, high-tech, must operate virtually around the clock without interruption, and interface other systems (old and new) around the world. Recent assurance regulations for ATM/ATC (UK CAA 2010, Eurocontrol 2012) reflects a shift toward assurance cases.

Several of our interview sources (D, E, I) are involved in applying assurance cases to large, complex systems. Interestingly, these organizations also tend to have the most prominent issues managing a more complicated web of assurance responsibilities (see Section 5.3.2, “Mechanism: Clarification and Localization of Responsibility”) than other applied examples. Also, system complexity, like safety-criticality, is intrinsically linked to large volumes of assurance information. Again we refer to Section 5.4 for a specific discussion of this aspect.

5.5.4 Mechanism: Managing Certification of Innovative Technology

Innovative technology is making inroads into system roles for which there is little or no effective precedent. A potential advantage that assurance cases have in these cases is that they expand readily to unconventional analysis and evidence. Examples of relevant innovative systems include unmanned aircraft systems (UAS) and self-driving cars (Lutin et al. 2013). Cybersecurity is similarly facing new and unprecedented technological challenges. Prescription

and standards are of minimal use at the level of total system assurance because the novelty of these systems and their individual, specific weaknesses.

One argument with regard to difficult novel technologies is expressed by Wassyng et al. (2011): "…engineers should avoid innovation, at least of a certain kind, exactly because they want predictability and safety." This approach may suffice in limited examples, but it does nothing to assist with the adoption of new technologies that is practically inevitable. One could argue for slower adoption of new technology, but our research suggests that this approach is wholly impractical – technology adoption is charging ahead in some applications far faster than conventional methods could comfortably match.

Furthermore, there is always a gap between what can be prescribed and what is being built, the only question is how large. Interview source C specifically brought up this mechanism, asserting that standards are always "behind the curve" of operational systems and safety cases help to efficiently fill in the gaps. This dynamic can be seen going back many decades; one example is the Piper Alpha oil platform disaster in 1988. The problem is especially acute in highly innovative systems. One can go a step further, though, and say that it is not *only* a problem in highly innovative systems. For various reasons – low risk tolerance, narrow field of representative systems, etc. – the inevitable gap between what is covered by standards and what is critical to assurance may become unacceptable. Assurance cases can bridge over these gaps. C stated that assurance cases help developers to navigate the gaps efficiently. Without assurance case analysis, developers tend to pile on lots of over-engineering to compensate for areas of uncertainty. Over-engineering may be morally commendable, but unguided by sound reasoning, it can be an unnecessary barrier to progress.

5.5.5 Conclusions

Concerning the claimed benefit that assurance cases address modern certification challenges, our research finds that:

- A dominant thread through assurance case applications is safety-criticality as a modern assurance concern. It is often the first priority of practitioners. On balance, assurance cases appear well-suited to managing safety-criticality compared to other methods, although differing views in the literature suggest that this is not always the case. Assurance cases seem especially compelling for safety-criticality in combination with other difficult factors such as novelty and high-level requirements.
- Our literature review and interviews substantiate that assurance cases are useful to bridge the gap between available prescription and a satisfactory level of assurance. In modern systems this gap appears to be dominated by innovative and complex aspects of the application.
- Among assurance case examples in literature and practice, there is strong and broad representation of modern systems. We take this as indirect but significant evidence in support of the claimed benefit.

5.6 Benefit Claim: Assurance Cases Offer an Efficient Certification Path Compared to Other Approaches

5.6.1 General Claim and Associated Evidence

The essence of this perceived benefit is that assurance cases will reasonably limit unnecessary expenditures of resources in the achievement of certification. There are several factors involved in reasonably limiting assurance expenditures:

- Does the assurance method call for activities that are more expensive than other sufficient approaches?
- Does the method enable participants to complete their contributions quickly and cost-effectively?
- Is the certification process using the method reasonably clear and free of unanticipated risks that it will encounter delays or failure?

Generally speaking, we did not encounter evidence of serious concerns for the first two points – the cost of assurance case activities and ability to complete contributions quickly and cost-effectively. Most literature and practitioners indicate that assurance cases are largely an overlay on activities they already need to do and that assurance cases make their execution clearer and more expeditious. Assurance cases provide a "big picture" to drive activities and coordination. Stavert-Dobson (2016) cites "flexible integration of evidence" as one of the strengths of assurance cases and this report reinforces that point in other sections (e.g. 5.2.3.1, "Incorporating conventional methods as evidence"). The caveat to this might be concerns about managing large assurance cases and more abstract formats/notations. If only a few expert practitioners can effectively construct, interpret, and modify the assurance case, and a large team is needed to complete the process, this can create an inefficient execution dynamic. However, we did not encounter a substantial real-world example of this, perhaps precisely because it is intuitively undesirable and avoided by practitioners.

A more substantial concern we encountered is that assurance cases introduce new risks that the certification process will encounter delays or failure. Coming from a certification environment dominated by prescriptive standards, this is an understandable concern. Conceptually, in a prescriptive assurance world, if you "complete the checklist" properly, then you have a high degree of certainty that you can achieve certification. Of course, the introduction of other judgement-oriented methods such as risk analysis and safety management has already eroded some of this certainty. Still, many practitioners are disconcerted by a new requirement to build an argument in an assurance case; it is perceived as unclear exactly what they need to do to get over the certification bar. Both of the mechanism sections below investigate aspects of this concern (5.6.2, "Mechanism: Prescriptive Standards are Preferable Where Adequate" and 5.6.3, "Mechanism: Role of Assurance Case Patterns").

Colloquial evidence from the field (as gathered by our interviews) made it clear that many practitioners are at least initially concerned about the efficiency of assurance cases. "H" experienced the transition from a prior conventional system to a system based on assurance cases. For the first year or two, applicants were generally nervous and skeptical about the new system. Assurance cases were initially seen as a burden and a barrier to expeditious certification. However, after experience achieving certification under the new assurance case system, the general opinion of applicants was that the process was no more burdensome than the prior system, and some preferred it and submitted assurance cases where it was optional but not

required. Interview source “E” also mentioned large-scale cases of voluntary adoption of assurance cases (though not required or requested by regulators).

Another interview source (“A”) indicated that their regulatory community was still experiencing pushback and reluctance from suppliers. From this source’s perspective, safety case requirements were viewed by developers and suppliers as burdensome and unclear. Whether or not this changes over time remains to be seen. It seems likely that at least some increased familiarity and acceptance will occur.

It is important to note that efficiency is not a one-size-fits-all property. A methodology can be efficient in one context and not in another. In this regard, the abstract nature of assurance cases (see 5.2.4, “Mechanism: High Level of Abstraction”) seems to make them remarkably flexible. Assurance arguments can range from a few pages to hundreds of thousands of pages. The field examples we examined spanned both ends of this spectrum. One could conclude, though, that the efficiency *advantages* of assurance cases appear to be more compelling in more difficult assurance contexts, such as high complexity, large scope, or safety-criticality. That is, assurance cases have an advantage over alternative methods in these cases where conventional methods may struggle to provide the necessary level of assurance.

5.6.2 Mechanism: Prescriptive Standards are Preferable Where Adequate

Our practitioner interviews clearly revealed that many system developers and operators prefer prescriptive standards over argument-based methods. Working to prescriptive standards is a clear-cut, well-characterized process. It is difficult to find a reception for assurance cases where a prescriptive approach does an adequate job.

Note that we are contrasting here with *prescriptive standards*, not all standards. As described in our prior work (Rinehart et al. 2015) standards are a general-purpose mechanism for systematizing just about anything, including non-prescriptive approaches. The process of standardizing semi-prescriptive and non-prescriptive methods such as risk management and safety management is constantly underway and applies to assurance cases as well. (For example, ISO 26262 is a standard that at least partially defines safety cases.)

The pressing question is: at what point does the adequacy of prescriptive standardization run out? We have touched on some of the factors in previous sections (for example, see Section 5.5, “Benefit Claim: Assurance Cases Address Modern Certification Challenges”). The boundary of prescriptive adequacy is depicted in Figure 16.

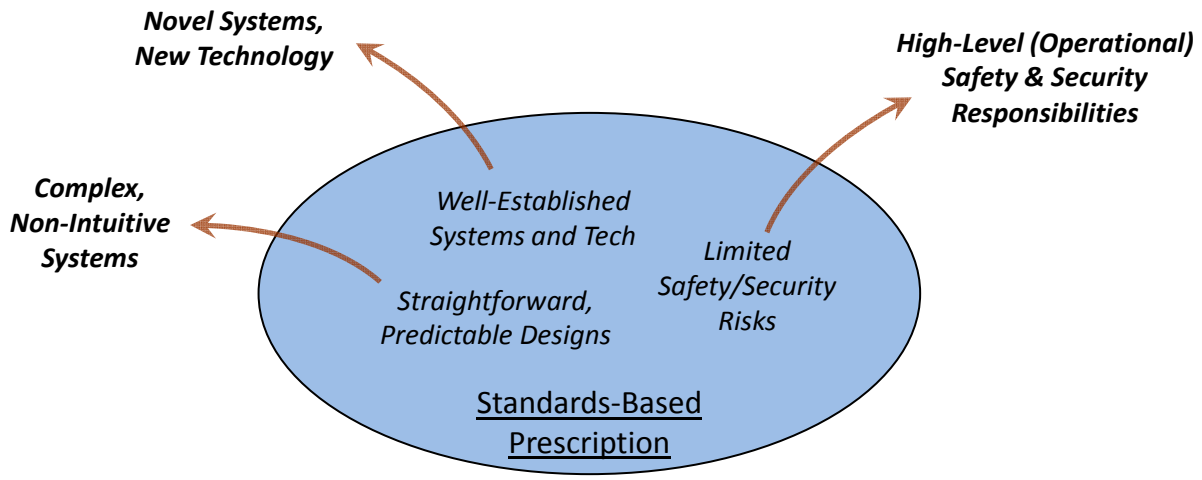

Figure 16: Limitations of Standards-Based Prescription

The area within the boundary shown in Figure 16 is an area of high efficiency for prescriptive methods. Within this zone, assurance cases will typically be less efficient or, in any case, offer little benefit over the needed prescription. Within this zone, it could be argued that assurance cases are *not* efficient for a reason mentioned earlier: compliance is more open-ended and therefore introduces new risks for delayed or failed certification. By comparison, prescriptive standards offer a path to certification that is clearly-defined and low-risk. For this reason, where prescription is adequate, we do not expect assurance cases to be adopted in general (and neither would we recommend it based on our research).

Some sources take a strong stand against assurance cases without acknowledging the distinctions shown in Figure 16. For example, Wassyng et al. (2011) offer civil engineering prescriptive standards (in a well-established, straightforward context) as an instructive precedent for software engineering (a context featuring high complexity and new technology). In our view this misses a crucial point of distinction. Prescriptive approaches can only stretch so far before becoming ineffective.

The problem is not that prescription must be replaced, but rather that it needs supplementing and a higher level of integration. As we discuss in Section 5.2.3, “Mechanism: Integration with Conventional Methods”, assurance cases properly deployed work with standards and other methods rather than replacing them. As Hopkins (2012) states: “One of the misconceptions in the US about safety case regulation is that it involves the abandonment of prescription. That is not so. A safety case requires that technical standards be specified and regulators can then enforce those standards. Moreover there remains room for prescriptive, government-imposed regulation.”

We find, then, that there is substantial evidence for efficient assurance cases for high-level goals (incorporating complex, system-specific factors) and elements such as safety-criticality and new technology. On the other hand, in well-established and straightforward areas, prescription is likely to be more desirable. How does this play out among practitioners? A common theme in our research examples that related to large and safety-critical systems was that, at some level of system decomposition, the focus transitions from the high-level assurance case to low-level prescriptive standards. This phenomenon came up in our discussion with interview source “A”. In their experience, parts suppliers almost invariably prefer to be outside the assurance case process. They prefer to supply their parts to specifications and standards-based prescriptions

because that is simpler and requires a minimum amount of customization for individual customers. In such cases, the primary operator and primary developer might develop and manage the assurance cases, but flow down only specifications and standards to the suppliers. Subsystem developers fall within a gray zone of these options and could be tailored either direction.

5.6.3 Mechanism: Role of Assurance Case Patterns

The expressed need for assurance case patterns has been evident in the literature for a long time (Kelly and McDermid 1998, Rich et al. 2007, Hawkins and Kelly 2010, Palin and Habli 2010). Patterns came up repeatedly in our literature survey. The essential function of this mechanism can be summarized in both a positive and negative sense:

- Patterns save practitioners a substantial amount of time and effort by leveraging starting points for assurance cases that are proven and well-known.
- Patterns avoid the situation that applicants are directed to "make the case" with so much latitude that they don't know how to start and perceive high risk that they will invest in a direction that is later found to be unacceptable to the regulator.

We note that there are at least two ends of a spectrum for the term "pattern" as it concerns assurance cases. At the one end, a pattern can refer to a general argument construct (an "*abstract pattern*"). This is the type of pattern we encountered most frequently in academic literature. For example, Rich et al. (2007) present detailed GSN patterns for safety concerns related to human factors. Such patterns tend to be more general than a particular domain and more technical in their arrangement.

At the other end of the spectrum, a pattern can refer to what is essentially an assurance case outline for a specific regulatory system (a "*template pattern*"). In many cases different terms are used for this type of regulatory guidance: outline, template, recommended contents, etc. Such patterns tend to be less technical (e.g. section headers rather than GSN) and specific to the domain.

We include both abstract and template patterns in our discussion here because they are both part of the same efficiency mechanism – that is, providing applicants with specific guidance as to what type of assurance argument to construct.

A regulator typically does not require a specific abstract pattern, although they may include it in their recommendations and/or refer to academic literature on the subject (as in US FDA 2014). Template patterns from regulators are typically more explicit and are, if not literally required, highly recommended. They essentially communicate what type of assurance case the regulator expects to see and would prefer to see. Following the template makes communication easier between applicant and regulator and simplifies the training and analysis required by each.

An example of a template outline is in the implementation guidance portion of the UK NHS standard SCCI0129 (2016) (which, by the way, is a good example of useful, substantive, but not overwhelming guidance provided by a regulator to applicants). After presenting what defines a safety case, argumentation, and so on, the standard presents this "representative content" of a "Clinical *Safety Case* Report" (emphasis added):

1. Introduction
2. System Definition / Overview
3. Clinical Risk Management System
4. Clinical Risk Analysis

5. Clinical Risk Evaluation
6. Clinical Risk Control
7. Hazard Log
8. Test Issues
9. Summary Safety Statement
10. Quality Assurance and Document Approval
11. Configuration Control / Management

This approach shows a combination of safety case and hazard/risk management techniques, which is not uncommon in the examples we studied. On the surface, it is perhaps less than explicit regarding argumentation, but supporting text in the standard discusses argumentation. There is certainly conceptual room in sections such as "Clinical Risk Control" for argumentation. Also like many other examples, the argumentation tends to be more free-form and document-oriented than one typically finds in academic literature where GSN and other graphical formats are used predominantly.

We also encountered a counter-example of this mechanism in our field interviews – that is, an example in which very little pattern-type guidance was provided by the regulator to applicants. In this example, we were able to review a set of safety case submissions responding to this mostly pattern-free regulatory guidance. In our judgement, there was a wide range of quality levels in the arguments submitted. Approximately two-thirds of the submissions included fairly superficial arguments and one-third included solid, substantive arguments. We do not mention this as a critique of the regulatory process in question; the regulator in this example seemed to be able to offer flexibility to applicants which may have have been instrumental in decreasing applicant resistance to the requirement for argumentation.

Nonetheless, the example illustrates a key problem: if applicants are given flexibility (that is, not provided with effective patterns), they may make low-quality submissions which could introduce inefficiency. If regulators can offer flexibility commensurate with a wide range of argument forms and types, the process may be workable. If, however, regulators essentially have high expectations but do not communicate it to applicants in the form of pattern guidance, there is a strong chance of inefficiency (and frustration). In any case, our research suggests that defining regulatory expectations in the form of patterns is an evolving challenge.

In some cases, well-resourced regulator-applicant communication and interaction can to some extent take the place of explicit pattern guidance. Well-resourced interaction is the essential feature described in (Baram 2011) concerning the success of Norwegian offshore oil and gas facilities. There are also elements of this alternative mechanism (individualized interaction rather than explicit patterns) in the FAA DER, UK ISA, and similar process mechanisms (see Section 5.1.6, "Mechanism: The Challenge of Objective and Sufficient Evaluation").

5.6.4 Conclusions

Concerning the claimed benefit that assurance cases offer an efficient certification path compared to other approaches, our research finds that:

- Practitioner evidence strongly indicates that the claim must be qualified. Prescriptive standards are still preferred (and believed to be more efficient) where

sufficient; that is, where systems are well-established, straightforward, and low-risk.

- Evidence suggests that patterns are an important potential mechanism to facilitate efficiency and mitigate potential inefficiencies (specifically risks of delayed or unsuccessful certification).
- For complex, novel, safety-critical, and/or high-level assurance, available evidence from practitioners and literature substantiates the claim that assurance cases achieve certification efficiently relative to other approaches.

Based on our practitioner interviews, the primary advantage that assurance cases appear to have with regard to efficiency is that they focus efforts on what is important for the achievement of real assurance. Relevant standards compliance remains a part of successful certification. It is in the areas beyond standards compliance where assurance cases excel. Where other methods (e.g. risk and safety management) provide implicit coverage, assurance cases provide explicit argumentation for coverage. The practitioners we interviewed held the expert opinion that this explicit argumentation has the effect of efficiently resolving the essential concerns of certification.

5.7 Benefit Claim: Assurance Cases Provide a Practical, Robust Way to Establish Due Diligence

5.7.1 General Claim and Associated Evidence

There is a distinct thread of thinking among the literature and practice that an accepted assurance case secures some legal protection of the developer/manufacturer/owner/operator in the event of a major loss event. This legal protection is in the form of what is generally called "due diligence." In legal terminology, "due diligence" aligns with "necessary diligence", which is defined as (Black 1910): "That degree of diligence which a person placed in a particular situation must exercise in order to entitle him to the protection of the law in respect to rights or claims growing out of that situation, or to avoid being left without redress on account of his own culpable carelessness or negligence." Due or necessary diligence is an important concept to organizations and individuals associated with advanced systems. Developers, owners, and operators will be expected, both generally and to some extent legally, to meet or exceed the appropriate level of diligence.

An important precedent concerning legal safety responsibility is the development of the term "as low as reasonably practicable" (ALARP) associated with UK regulations. It is often identified with goal-oriented specification of duties. As stated by the UK Health and Safety Executive (2016), "Using 'reasonably practicable' allows us to set goals for duty-holders, rather than being prescriptive… Deciding whether a risk is ALARP can be challenging because it requires duty-holders and us to exercise judgement." An ALARP approach offers a balance of flexibility and responsibility. The legal origin of the concept can be traced back at least as far as a UK case in 1949 (Edwards v. National Coal Board, [1949] 1 All ER 743): "'Reasonably practicable' is a narrower term than 'physically possible' … a computation must be made by the owner in which the quantum of risk is placed on one scale and the sacrifice involved in the measures necessary for averting the risk (whether in money, time or trouble) is placed in the other, and that, if it be shown that there is a gross disproportion between them – the risk being insignificant in relation to the sacrifice – the defendants discharge the onus on them." In other

words, duty holders must work to reduce risks at least to the point that additional efforts outweigh the risk reduction (see Figure 17).

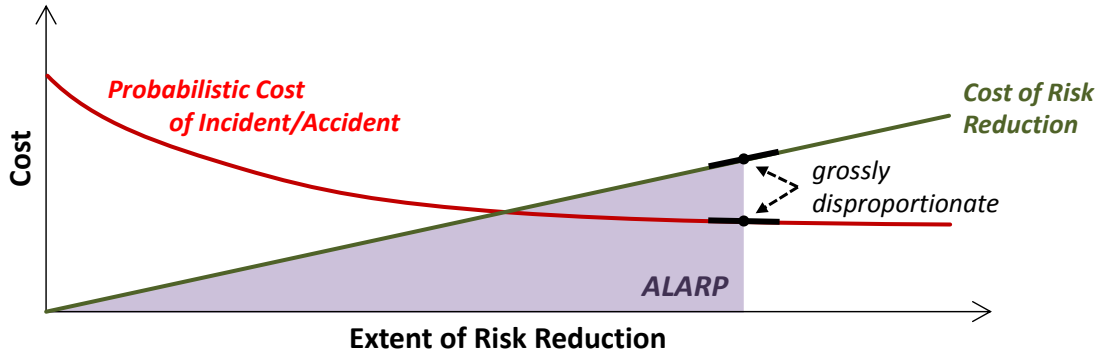

Figure 17: Visualization of the ALARP Standard

Though there is some understandable discomfort among practitioners with the uncertainties of ALARP judgements, it is more balanced and realistic than some alternative legal standards (which might stand on somewhat arbitrary absolute safety thresholds or more binding responsibilities). The ALARP standard withstood a 2007 legal challenge by the European Commission which essentially charged that it did not go far enough to place responsibility on duty holders (UK HSE 2007). The fact that it is criticized from both sides (applicants and regulators) suggests that it is a fairly balanced legal standard.

At least in the UK, the legal establishment of ALARP has gone hand in hand with the progressive adoption of safety cases. One of our interview sources active in developing safety-critical systems in the UK essentially said that it's impossible to comply with ALARP without developing a safety case. In other words, within that regulatory framework, legal compliance drives practitioners toward assurance case methods.

In a general sense, having systematic (see Section 5.2.2) and well-considered assurance practices – which certainly may include assurance cases – goes a substantial way toward addressing due diligence concerns (associated with ALARP or any other such legal responsibility). "There have been few legal tests but in the event that an organisation finds itself subject to a challenge, the presence of an SMS, safety policy and safety case helps to demonstrate adherence to good practice and the regard in which an organization holds safety and risk management." (Stavert-Dobson 2016) However, this type of protection is limited to the general and not to the specific ("the presence of," in contrast to the contents of).

At a deeper and more specific level, assurance cases seem to be better suited to establishing due diligence than alternative methods. For example, in the following quote, one can see the practitioners thinking of how they could use specific assurance rationales to justify their decision to field the system. Note here that "safety assessment" refers to a structured process that is very similar to constructing and evaluating an assurance argument: "Safety assessment in the motor industry is not currently a mandatory requirement, and hence its justification is subject to commercial considerations. The extensive safety and design assessment described in this paper involved significant effort at a commensurate cost to Jaguar; a cost that would be difficult to justify in terms of a direct return on investment... However, the results from the assessment would undoubtedly be used as defence evidence, should Jaguar ever find itself in a product liability situation involving the electronic throttle." (Barker et al. 1997)

Based on our team's experience both on this project and prior efforts, we can state that it quickly becomes clear that few practitioners are eager to display their assurance cases to anyone beyond what is required by regulation. Most organizations using safety cases are reluctant to show detailed contents. Where we have gained access to such information, it is almost invariably after agreeing to protections that restrict us from disseminating it beyond our team.

Is the reluctance of practitioners to reveal their assurance cases counter-evidence to the claim that they achieve legal protection by their use of assurance cases? We believe that would be drawing the wrong conclusion. In general practitioners express confidence in their assurance cases. They are as reluctant or more so to reveal similar details that are not associated with assurance. The reticence, then, is accounted for by at least two factors: (1) minimizing legal exposure by reducing the number of potential sources of legal action (some of which could be frivolous but expensive), and (2) concern that some details included in the assurance case could release information that is a competitive advantage.

The following sections examine specific mechanisms underlying the claimed benefit.

5.7.2 Mechanism: Explicit Argumentation and Justification of Belief

A major mechanism behind this claimed benefit is specifically due to the inclusion of explicit argumentation. Assurance case arguments compel practitioners to get right to the point of due diligence: "Why do you believe this (system, process, etc.) is sufficiently safe?" We did not encounter any other assurance method that so directly pertains to due diligence. Even if an argument is later found to be inadequate on some point, at least an assurance case tangibly demonstrates that the correct question was asked and presents all the assurance information in a manner directed at answering the right question. That is, it exposes everything that was done in an arrangement suitable for responding to due diligence challenges.

By comparison, non-argument methods (such as standards compliance) establish some degree of due diligence, but often do not get to the substance of real legal responsibility. At worst, it may only demonstrate pro forma compliance (all the boxes were checked). At best, it shows that rational, intentional efforts were made toward due diligence. If the prescription involved is fits the application, compliance may make very substantive progress. However, a pitfall with some conventional assurance methods is that the difference between "good" diligence and "poor" diligence is easily obscured by details, and truly relevant factors may not be documented.

Many aspects of conventional processes do not incorporate any high-level / cross-cutting due diligence (nor documentation of it). Standards-based methods address a class of concerns, but only those within the scope of the standard. As mentioned in Section 5.6.2, this works well for common, straightforward systems and operations. However, uncommon aspects are not handled well by standards-based methods. Risk-based and safety management methods are more effective at comprehensive coverage, but again the full picture with regard to due diligence is only inferred. One could still ask, "Why do you believe the set of risks is sufficiently complete? Why are the safety management practices sufficient?" In our research, only assurance cases offer a method that comprehensively directs practitioners to document their efforts at due diligence concerning both common and uncommon aspects using appropriate means.

5.7.3 Conclusions

Concerning the claimed benefit that assurance cases provide a practical, robust way to establish due diligence, our research finds that:

- evidence is sparse as there are not many legal examples to examine,
- expert opinion (where available) strongly supports the claim, and
- the argument basis of assurance cases provides analytical justification.

Though we did not find a plethora of supporting evidence, we found far less contradicting evidence (virtually none). Of course, the mere use of assurance case methods does not ensure that a developer, manufacturer, owner, or operator will not be found legally liable for an accident. Nonetheless, our research suggests that practitioners that properly use argument-based assurance cases along with other required practices will be on relatively strong footing (compared to alternative methods) with regard to legal due diligence.

6. Conclusions

6.1 Synopsis of Findings

The most significant findings – that is, those which we consider most noteworthy to prospective practitioners, especially in aviation – are summarized as follows:

1. Goal-orientation and explicit argumentation are core strengths, which typically overarch complementary conventional methods.
2. Assurance case practices are already widespread and well-established. It is currently applied in a minority of suitable contexts. Increasing adoption clearly appears to be the trend.
3. Not all applications include both goal-orientation and explicit argumentation. Goal-orientation has a longer track record and is more widespread. Implicit argumentation ("making the case") is an old and well-established concept; the transition to explicit argumentation is more recent and less mature.
4. Assurance evaluation remains a critical challenge. In some ways, assurance cases are not unlike other methods in this regard. Competent, well-resourced regulator evaluation is essential. In other ways, assurance cases introduce new dynamics such as the need for a common, baseline understanding of the argument structures employed.
5. Practitioners may find it difficult to proceed comprehensively (systematically) in the absence of an effective patterns (both abstract argument patterns and applications-specific template patterns). Patterns can be provided by guidance or obtained by experience.
6. There is some tension concerning where to draw the boundaries of organizational access to assurance cases. There are pros and cons to both ends of the spectrum: management by specialists vs. maximum access by non-experts.
7. Allocating and managing assurance responsibilities can be very daunting in the large networks of interrelated stakeholders such as typical in the field. Assurance cases confront this explicitly and offer coherent ways to assign and subdivide responsibilities.
8. Advanced features (well-formed GSN, argument analysis) are important academic and research topics. However, they are neither common nor necessary for successful assurance cases in the field. Most practitioners use simpler forms. There may be a

general lack of established simpler argument notations (simpler than GSN) for explicit argumentation.

9. Assurance cases are useful to bridge the inevitable gap between available prescription and a satisfactory level of assurance (especially safety). This gap is exacerbated by innovative technology and system complexity, which strike at the heart of modern certification challenges.
10. Prescriptive standards are preferred and likely more efficient where they are sufficient. Prescription is generally sufficient in well-understood, straightforward, and/or low-risk cases.
11. Patterns, especially application-specific templates, are important enablers of efficiency.
12. Assurance case arguments explicitly document justification of belief that responsibilities have been met. As such, they are fairly unique among assurance methods in the extent to which they support efforts to establish due diligence, ALARP, and related legal thresholds.

6.2 Overview of Claimed Benefits

We provide an overview of the seven claimed benefits explored by our research in the following paragraphs.

Fundamental Claim: Assurance Cases are Successful where Suitable. The claim is well-founded, especially considering the historical range of examples and expert consensus.

Benefit Claim: Assurance Cases are More Comprehensive than Conventional Methods Alone. Of its various specific perceived strengths, comprehensiveness is probably the easiest to substantiate. There is strong evidence from intrinsic properties, literature, and field practices.

Benefit Claim: Assurance Cases Improve the Allocation of Responsibility over Prior Norms. This claim appears well backed by evidence and addresses an aspect of assurance that is otherwise weakly managed by conventional methods.

Benefit Claim: Assurance Cases Organize Information More Effectively than Conventional Methods. This claim appears to be true with caveats. A high degree of notational rigor, though desirable for other reasons, can the accessibility of assurance cases (e.g. for proper integration and evaluation). Assurance case tools are also an important factor in the practical reality of this benefit.

Benefit Claim: Assurance Cases Address Modern Certification Challenges. This is largely well-supported by evidence, especially for safety-criticality, which is a dominant feature in literature and field examples. Complexity and technical innovation are common additional elements. Technical innovation is noteworthy as this is a weak area for prescription.

Benefit Claim: Assurance Cases Offer an Efficient Certification Path Compared to Other Approaches. This is the most challenged of the claims we researched. Many practitioners have strongly-held concerns about efficient certification with assurance cases. However, we did not find this to be a widespread problem in practice. Patterns (especially templates) are a strong factor in assurance case efficiency. Also, experience tends to normalize practices and reduce efficiency concerns.

Benefit Claim: Assurance Cases Provide a Practical, Robust Way to Establish Due Diligence. This claim appears to be well-founded mostly by virtue of the explicitness of assurance case arguments.

6.3 In Closing

The research described in this report used wide-ranging methods (literature survey and interviews) to explore the real working success of assurance cases. The method is growing and maturing. It is our hope and belief that the work described here offers insights for practitioners and future research.

7. References

Abdala M, Lahoz C, de Lemos R. 2001. Diversity of safety arguments in the validation of a sounding rocket destruction system. In *International System Safety Conference*. 801-810.

Aiello M, Hocking A, Knight J, Rowanhill J. 2014. SCT: A Safety Case Toolkit. In *IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)*. 216-219.

Alexopoulos AB, Konstantopoulos N. 2004. New elements in international maritime standards: Developing a safety case approach for the treatment of tanker incidents. *Operational Research* 6(1):55-68.

Ayoub A, Kim B, Lee I, Sokolsky O. 2012. A Safety Case Pattern for Model-Based Development Approach. In *Proceedings of NASA Formal Methods: 4th International Symposium*. Goodloe AE, Person S (editors). Springer Berlin Heidelberg. 141-146.

Baik MH, Park T-J, Kim IY, Jeong J, Choi KW. 2015. Development of a natural analogue database to support the safety case of the Korean radioactive waste disposal program. *Swiss Journal of Geosciences* 108(1):139-146.

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.

Barker S, Kendall I, Darlison A. 1997. Safety Cases for Software-intensive Systems: an Industrial Experience Report. In *Safe Comp 97: The 16th International Conference on Computer Safety, Reliability and Security*. 332.

Bishop P, Bloomfield R. 1998. A Methodology for Safety Case Development. In *Industrial Perspectives of Safety-critical Systems: Proceedings of the Sixth Safety-critical Systems Symposium*. Redmill F, Anderson T (editors). Springer London. 194-203.

Bishop P, Bloomfield R. 1995. The SHIP Safety Case Approach: A Combination of System and Software Methods. In *Safety and Reliability of Software Based Systems: Twelfth Annual CSR Workshop*. 107-121.

Björnander S, Land R, Graydon P, Lundqvist K, Conmy P. 2012. A Method to Formally Evaluate Safety Case Evidences against a System Architecture Model. In *IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*. 337-342.

Black, Henry Campbell. 1910. *Law dictionary*. West Publishing Company.

Bloomfield R, Bishop P. 2010. Safety and Assurance Cases: Past, Present and Possible Future – an Adelard Perspective. In Dale C, Anderson T (eds.) *Making Systems Safer, Proceedings of the Eighteenth Safety-Critical Systems Symposium*, Bristol, UK, pp. 51-67.

Boehm BW. 1991. Software risk management: principles and practices. *IEEE Software* 8(1):32-41.

Brain JM. 2014. Learning from experience: how can we produce a nuclear safety case to outlast the station? In *9th IET International Conference on System Safety and Cyber Security*.

Cockram T, Lockwood B. 2003. Electronic safety cases: Challenges and opportunities. In *Current Issues in Safety-Critical Systems: Proceedings of the Eleventh Safety-critical Systems Symposium*. Springer. 151-162.

Cullen, WD (1990). *The public inquiry into the Piper Alpha disaster*. London:H.M. Stationery Office. ISBN: 0101113102.

Dahle IB, Dybvig G, Ersdal G, Guldbrandsen T, Hanson BA, Tharaldsen JE, Wiig AS. 2012. Major accidents and their consequences for risk regulation. In *Advances in Safety, Reliability and Risk Management: ESREL 2011*. Berenguer G, Grall A, Soares G (editors). Taylor & Francis Group: London. 33-41.

Dardar R, Gallina B, Johnsen A, Lundqvist K, Nyberg M. 2012. Industrial Experiences of Building a Safety Case in Compliance with ISO 26262. In *IEEE 23rd International Symposium on Software Reliability Engineering Workshops (ISSREW)*. 349-354.

Denney E, Pai G. 2015. A Methodology for the Development of Assurance Arguments for Unmanned Aircraft Systems. In *33rd International System Safety Conference (ISSC)*.

Denney E, Pai G, Habli I. 2012. Perspectives on software safety case development for unmanned aircraft. In *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. 1-8.

Despotou G. 2007. *Managing the Evolution of Dependability Cases for Systems of Systems*. Doctoral dissertation, University of York.

Despotou G, Kelly T. 2005. Using Scenarios to Identify and Trade-off Dependability Objectives in Design. In *Proceedings of the 23rd International System Safety Conference*.

Despotou G, Kelly T. 2007. Design and development of dependability case architecture during system development. In *25th International System Safety Conference*.

Eastwood R, Kelly TP, Alexander RD, Landre E. 2013. Towards a safety case for runtime risk and uncertainty management in safety-critical systems. In *8th IET International Cyber Security Conference*. 1-6.

Ericson CA II. (2005). *Hazard Analysis Techniques for System Safety*. John Wiley & Sons, Inc., Hoboken, NJ.

Eurocontrol. 2012. *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/surveillancewam-nra-psc1-2.pdf. Accessed 7 January 2015.

Eurotunnel Group. 2016. *Traffic Figures*. http://www.eurotunnelgroup.com/uk/eurotunnel-group/operations/traffic-figures/. Accessed 28 September 2016.

Evans AW. 1995. Railway Safety Cases and Railway Risk Assessment in Britain. In *4th International Conference on Competition & Ownership in Land Passenger Transport*. 170-188.

Federal Aviation Administration (FAA). 2000. *FAA System Safety Handbook*.

Federal Aviation Administration (FAA). 2014. *Safety Management System Manual*. Version 4.0. Air Traffic Organization (ATO).

Feather M, Markosian L. 2013. Architecting and generalizing a safety case for critical condition detection software an experience report. In *2013 1st International Workshop on Assurance Cases for Software-Intensive Systems (ASSURE)*. 29-33.

Feather MS, Markosian LZ. 2011. Building a Safety Case for a Safety-Critical NASA Space Vehicle Software System. In *IEEE Fourth International Conference on Space Mission Challenges for Information Technology*. 10-17.

Felici M. 2005. Modeling safety case evolution – Examples from the air traffic management domain. In *International Workshop on Rapid Integration of Software Engineering Techniques*. 81-96.

Gamble E, Holzmann G. 2011. *Logic Model Checking of Unintended Acceleration Claims in the 2005 Toyota Camry Electronic Throttle Control System*. Jet Propulsion Laboratory, California Institute of Technology. Presentation.

Geyer TAW, Morris MI, Hacquart RY. 1995. Channel Tunnel Safety Case: development of the risk criteria. In *International Conference on Electric Railways in a United Europe*. 164-167.

Goodenough JB, Weinstock CB, Klein AZ. 2012. *Toward a Theory of Assurance Case Confidence*. Software Engineering Institute.

Grady JO. 1998. *System Validation and Verification*. CRC Press.

Habli I, Kelly T. 2007. Safety Case Depictions vs. Safety Cases - Would the Real Safety Case Please Stand Up? In *2nd Institution of Engineering and Technology International Conference on System Safety*. 245-248.

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. Accessed 7 January 2015).

Hawkins RD, Kelly T. 2010. A Systematic Approach for Developing Software Safety Arguments. *Hazard Prevention*, 46(4):25-33.

Health Foundation. 2012. *Evidence: Using safety cases in industry and healthcare*. ISBN 978-1-906461-43-0.

Holloway C. 2008. Safety Case Notations: Alternatives for the Non-Graphically Inclined? In *3rd IET International Conference on System Safety*. 1-6.

Holmes-Mackie N. 2005. New developments in Safety Case preparation. In *IEE Seminar on Safety Assurance*. IET Ref. No. 2005/11081.

Hopkins A. 2012. *Explaining 'Safety Case'*. National Research Centre for OHS Regulation, Australian National University.

Inge JR, Costello GT. 2008. End-to-End Reviews: A New Approach to Providing Assurance that a Complex Organisation is Effectively Managing Safety. In *Proceedings of the 26th International System Safety Conference*.

International Organization for Standardization (ISO). 2011. *Road vehicles – Functional safety*. ISO 26262:2011(E).

Jolliffe G. 2005. Producing a safety case for IMA blueprints. In *24th IEEE Digital Avionics Systems Conference (DASC)*. 14.

Kelly TP. 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. Accessed 7 January 2015.

Kelly T, McDermid J. 1998. Safety Case Patterns – Reusing Successful Arguments. In *IEEE Colloquium on Understanding Patterns and Their Application to Systems Engineering (Digest No. 1998/308)*.

Kelly TP, McDermid JA. 1999. A Systematic Approach to Safety Case Maintenance. In *International Conference on Computer Safety, Reliability, and Security*. Springer Berlin Heidelberg.

Kelly T, Weaver R. 2004. The goal structuring notation–a safety argument notation. In *Proceedings of the Dependable Systems and Networks Workshop on Assurance Cases*.

Kossiakoff A, Sweet WN. 2003. *Systems Engineering: Principles and Practice*. John Wiley & Sons, Inc.

Larrucea A, Perez J, Agirre I, Brocal V, Obermaisser R. 2015. A Modular Safety Case for an IEC-61508 Compliant Generic Hypervisor. In *2015 Euromicro Conference on Digital System Design*. 571-574.

Leveson N. 2011. The Use of Safety Cases in Certification and Regulation. *Journal of System Safety* 47(6).

Lin C-L, Shen W. 2015. Applying Safety Case Pattern to Generate Assurance Cases for Safety-Critical Systems. In *IEEE 16th International Symposium on High Assurance Systems Engineering (HASE)*. 255-262.

Lisagor O, Bozzano M, Bretschneider M, Kelly T. 2010. Incremental Safety Assessment: Enabling the Comparison of Safety Analysis Results. Submitted to *28th International System Safety Conference (ISSC)*.

Lisagor O, Sun L, Kelly T. 2010. The illusion of method: challenges of model-based safety assessment. Submitted to *28th International System Safety Conference (ISSC)*.

Lucas J. 2008. Safety Case Experiences from Harrier. In *Improvements in System Safety*. Redmill F, Anderson T (editors). Springer London. 77-91.

Lutin JM, Kornhauser AL, & Lerner-Lam E. 2013. The revolutionary development of self-driving vehicles and implications for the transportation engineering profession. *ITE Journal* 83(7):28. Institute of Transportation Engineers.

Maguire R, Garside A. 2008. Development of an Electronic Safety Case for a Military Communication, Command and Control System. In *3rd IET International Conference on System Safety*.

Manz H, Schnieder E. 2013. Implementation of the normative safety case structure for satellite based railway applications. In *IEEE International Conference on Intelligent Rail Transportation (ICIRT)*. 203-208.

Mayo P. 2009. Creating a competence argument to support a safety case. In *4th IET International Conference on Systems Safety*. 1-6.

McDermid J. 1994. Proving the design in the safety case. In *IEE Colloquium on Designing Safety-Critical Systems*.

McDermid JA. 1998. Safety analysis of hardware/software interactions in complex systems. In *Proceedings of the 16th International System Safety Conference*.

Mistry M, Felici M. 2008. Implementation of Change Management in Safety Cases. In *Formal Aspects of Safety-Critical Systems*.

Nair S, de la Vara JL, Sabetzadeh M, Briand L. 2014. An extended systematic literature review on provision of evidence for safety certification. *Information and Software Technology*. 56:689-717.

National Aeronautics and Space Administration (NASA). 2014. *NASA System Safety Handbook – Volume 2: System Safety Concepts, Guidelines, and Implementation Examples*. Version 1.0. NASA/SP-2014-612.

Neumann PG. 2016. Automated Car Woes – Whoa There! *Ubiquity*, July 2016.

Newton A, Vickers A. 2007. The Benefits of Electronic Safety Cases. In *The Safety of Systems: Proceedings of the Fifteenth Safety-critical Systems Symposium, Bristol, UK*. Redmill F, Anderson T (editors). 69-82.

Nordland O. 2001. Presenting a Safety Case – A Case Study. In *Proceedings of 20th International Conference on Computer Safety, Reliability and Security (SAFECOMP)*. 56-65.

Ozols M, Eastaughffe K, Cant A, Collignon S. 1998. DOVE: A tool for design modelling and verification in safety critical systems. In *16th International System Safety Conference*.

Palin R, Habli I. 2010. Assurance of Automotive Safety – A Safety Case Approach. In *Proceedings of 29th International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2010)*. Schoitsch E (editor). Springer Berlin Heidelberg. 82-96.

Petkova M. 2003. EMC and the safety case. In *EMC Assurance in a Railway Environment*. IEE Ref. No. 2003/10332.

Pierce R, Baret H. 2005. Structuring a Safety Case for an Air Traffic Control Operations Room. In *Constituents of Modern System-safety Thinking: Proceedings of the Thirteenth Safety-critical Systems Symposium*. Redmill F, Anderson T (editors). Springer London. 51-64.

Reijonen HM, Russell Alexander W, Marcos N, Lehtinen A. 2015. Complementary considerations in the safety case for the deep repository at Olkiluoto, Finland: support from natural analogues. *Swiss Journal of Geosciences*. 108:111-120.

Rich KJN, Blanchard H, McCloskey J. 2007. The Use of Goal Structuring Notation as a Method for Ensuring that Human Factors is Represented in a Safety Case. In *2nd IET International Conference on System Safety*. 217-222.

Rinehart DJ, Knight JC, Rowanhill J. 2015. *Current Practices in Constructing and Evaluating Assurance Cases with Applications to Aviation*. NASA/CR–2015-218678.

Rippon JP, Bratby PAW, Smedley C. 1996. Safety Case Support For Sizewell 'B' Enhanced Cycles. In *International Conference on Sizewell B - The First Cycle*. 123-127.

Rushby J. 2015. On the Interpretation of Assurance Case Arguments. In *2nd International Workshop on Argument for Agreement and Assurance (AAA 2015)*, Vol. 9. Kanagawa, Japan.

Shen X, Bai Y. 2014. Architectural considerations in integrated modular avionics (IMA) system safety case construction. *IEEE Aerospace and Electronic Systems Magazine*. 29:26-33.

Shepperd CB. 2006. Safety case study. In *The 9th Institution of Engineering and Technology Professional Development Course on Electric Traction Systems*. 358-364.

Short R, Lucic I. 2007. Victoria Line Upgrade – System Safety Case. In *IET Seminar on Safety Assurance*. 1-37.

Stamatelatos M, Dezfuli H. 2011. *Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners*. 2nd Edition. NASA/SP-2011-3421.

Standish M, Auld H, Caseley P, Hadley M. 2014(a). Safety case development: a process to implement the safety three-layered framework. In *9th IET International Conference on System Safety and Cyber Security*. 1-11.

Standish M, Auld H, Caseley P, Hadley M. 2014(b). The safety three-layer framework: a case study. In *9th IET International Conference on System Safety and Cyber Security*. 1-8.

Stavert-Dobson A. 2016. *Health Information Systems: Managing Clinical Risk*. Springer International Publishing.

Storey J. 2013. Safety case approach for the Victoria line re-signalling project. In *IET Seminar on Railway Safety Assurance: Management and Method in a Safe Network*, 1-19.

Sun L, Lisagor O, Kelly T. 2011. Justifying the validity of safety assessment models with safety case patterns. In *6th IET International Conference on System Safety*. 1-6.

Taylor JR. 1994. Developing Safety Cases for Command and Control Systems. In *Technology and Assessment of Safety-Critical Systems: Proceedings of the Second Safety-critical Systems Symposium*. Redmill F, Anderson T (editors). Springer London. 69-78.

Törner F, Öhman P. 2008. Automotive Safety Case A Qualitative Case Study of Drivers, Usages, and Issues. In *11th IEEE High Assurance Systems Engineering Symposium*. 313-322.

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/. Accessed 4 September 2014.

UK Civil Aviation Authority (CAA). 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. Accessed 7 January 2015.

UK Health and Safety Executive (HSE). 2007. *European court supports UK safety laws (Case C127-05 European Commission v United Kingdom)*. Press release C007:07 dated 14 June 2007.

UK Health and Safety Executive (HSE). 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. Accessed 7 January 2015.

UK Health and Safety Executive (HSE). 2016. *ALARP "at a glance"*. http://www.hse.gov.uk/risk/theory/alarpglance.htm. Accessed 30 September 2016.

UK Health and Social Care Information Centre (HSCIC). 2015. *Clinical Risk Management: its Application in the Manufacture of Health IT Systems - Specification*. Version 4.0, dated 08.12.2015.

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

U.S. Chemical Safety and Hazard Investigation Board (CSB). 2015. *Final Investigation Report: Chevron Richmond Refinery Pipe Rupture and Fire*. Report No. 2012-03-I-CA.

U.S. Department of Defense (DoD). 1980. *MIL-STD-1629A: Procedures for Performing a Failure Mode, Effects and Criticality Analysis.*

U.S. Department of Transportation. 2009. *Systems Engineering Guidebook for Intelligent Transportation Systems*. Version 3.0. Federal Highway Administration, California Division.

U.S. Food and Drug Administration (FDA). 2010. *Infusion Pump Improvement Initiative*. Center for Devices and Radiological Health.

U.S. Food and Drug Administration (FDA). 2014. *Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff*. Center for Devices and Radiological Health. OMB Control Number: 0910-0766.

U.S. Nuclear Regulatory Commission (NRC). 1981. *Fault Tree Handbook*. Vesely WE, Goldberg FF, Roberts NH, Haasl DF. NUREG-0492.

Verrall GS. 1996. Safety Case Management At Sizewell B. In *International Conference on Sizewell B - the First Cycle*. 89-93.

Wake C. 2012. *Key developments in the Channel Tunnel safety rules and the wider EU framework*. Channel Tunnel Safety Authority, Office of Rail Regulation. Presentation dated September 2012.

Wassyng A, Maibaum T, Lawford M, Bherer H. 2010. Software certification: Is there a case against safety cases? *Monterey Workshop*. 206-227.

Weaver R, McDermid J, Kelly T. 2002. Software safety arguments: Towards a systematic categorisation of evidence. In *International System Safety Conference*.

Weinstock CB, Goodenough JB. 2009. *Towards an assurance case practice for medical devices*. Carnegie-Mellon University. No. CMU/SEI-2009-TN-018.

Wilkinson P. 2002. *Safety cases: Success or failure?* National Research Centre for OHS Regulation, Australian National University.

Witulski A, Austin R, Evans J, Mahadevan N, Karsai G, Sierawski B, LaBel K, Reed R, Schrimpf R. 2016. Goal Structuring Notation in a Radiation Hardening Assurance Case for COTS-Based Spacecraft. In *GOMAC Tech 2016 Government Microcircuits Applications & Critical Technologies Conference*. Presentation.

Zeng F, Lu M, Zhong D. 2012. Software Safety Certification Framework Based on Safety Case. In *2012 International Conference on Computer Science & Service System (CSSS)*. 566-569.

8. Appendix

8.1 Literature Survey Database

To complete our literature survey and document our characterizations and other extracted information, we developed a modified BibTeX database format. Three examples from this database are provided below.

```
@InProceedings{Ayoub2012,
  Author = {Ayoub, Anaheed and Kim, BaekGyu and Lee, Insup and Sokolsky, Oleg},
  Booktitle = {Proceedings of 4th NASA International Symposium NASA Formal Methods
(NFM 2012)},
  Year = {2012},
  Address = {Berlin, Heidelberg},
  Editor = {Goodloe, Alwyn E. and Person, Suzette},
  Month = {April},
  Pages = {141--146},
  Publisher = {Springer Berlin Heidelberg},
  Chapter = {A Safety Case Pattern for Model-Based Development Approach},
  Doi = {10.1007/978-3-642-28891-3_14},
  Groups = {Completed},
  ISBN = {978-3-642-28891-3},
  Uac-claims = {None},
  Uac-comments = {The paper is about a prototyping/demonstration activity at the
University of Pennsylvania on an assurance case for software in a drug infusion pump.
So the application is real but the work is about a pattern they developed.},
  Uac-discipline = {Systems},
  Uac-evidence = {None},
  Uac-flex-process = {Goal-Oriented},
  Uac-form = {GSN},
  Uac-industry = {Medical},
  Uac-mechanisms = {None},
  Uac-perspective = {Academic, Practitioner},
  Uac-review-date = {2/19/2016},
  Uac-reviewer = {J. Knight},
  Uac-rigor-arg = {Structured},
  Uac-rigor-ev = {Structured},
  Uac-topic = {The paper describes a safety case pattern for the software used in
drug infusion pumps where the software derives from model-based development. Use of
the pattern is illustrated by instantiating the pattern for a particular pump being
developed by the University of Pennsylvania.},
  Url = {http://dx.doi.org/10.1007/978-3-642-28891-3_14}
}

@TechReport{Baram2011,
  Title = {Preventing Accidents in Offshore Oil and Gas Operations: the US Approach
and Some Contrasting Features of the Norwegian Approach},
  Author = {M. Baram},
  Institution = {Deepwater Horizon Study Group},
  Year = {2011},
  Month = {January},
  Type = {Working Paper},
  Owner = {drinehart},
  Timestamp = {2016.02.24},
```

```
  Uac-comments = {Example is in the negative - what did not work in Deepwater vs.
what appears to work better in Norwegian approach. However, assurance cases are never
explicitly mentioned. The upshot of the regulatory argument is that less mechanistic,
less "calculable" approaches are better - assigning a high level of responsibility on
operators with non-adversarial supervision but less emphasis on hard limits and
violations/sanctions.},
  Uac-discipline = {Operations},
  Uac-evidence = {US vs. Norwegian records are offered as evidence. The
definitiveness of this is questionable but the cited mechanisms probably have some
merit.},
  Uac-flex-process = {[Prescriptive, Blend, Goal-Oriented, n/a]},
  Uac-form = {None},
  Uac-industry = {Oil & Gas},
  Uac-mechanisms = {Several mechanisms are cited for relative success:
    * Assigning high-level responsibility to operators vs. assigning responsibility
to agencies and emphasizing compliance.
    * Requiring broad functions without prescription / with guidance and non-
adversarial supervision vs. a prescriptive, policing, adversarial approach.
    * Relying on trust, supervision, and expertise vs. relying on mistrust, fear of
sanctions, and liability.
    * Inclusion of workers and unions vs. non-involvement.
    * A high target for cost/benefit w.r.t. level of safety without strict
calculation vs. strict calculation of less ambitious cost/benefit-LOS targets.},
  Uac-perspective = {Academic, Regulator},
  Uac-review-date = {1/26/2016},
  Uac-reviewer = {K. Swanson, D. Rinehart},
  Uac-rigor-arg = {[Implicit, Explicit, Structured, n/a]},
  Uac-rigor-ev = {[Implicit, Explicit, Structured, n/a]},
  Uac-topic = {This document is a working paper from the study group analyzing the
Deepwater Horizon accident. It discusses aspects of accident prevention in the oil
and gas industry, contrasting US operations to those of Norway. It does not discuss
safety or assurance cases, but rather examines the issue from a regulatory aspect,
mostly focusing on industry standard practices and inspection procedures.}
}

@InProceedings{inge2008end,
  author = {Inge, JR and Costello, Capt and others},
  title = {End-to-End Reviews: A New Approach to Providing Assurance that a Complex
Organisation is Effectively Managing Safety},
  booktitle = {Proc. 26th International System Safety Conference},
  year = {2008},
  uac-claims = {1) Assurance cases can be used to make end-to-end assurance arguments
for inter-departmental functions. 2) An effective assurance case can be made for
safety in an SMS (Safety Management System) that has RCSs (RiskControl Systems), as
each RCS is an interdepartmental function. 3) Thus arguments support a better
assurance vehicle than modular spot-checks on RCS functions of each department. RCSs
(Risk Control Systems), each RCS can be treated as a arguments that Assurance of
safety requires assurance of interdepartmental coordination and not just spot audits
of departments in an SMS (Safety Management SYstem). A Risk Control System is a unit
of function distributed across various offices and workplaces. Many RCSs make up a
SMS. Typically, spot audits of departments test their responses to various RCS
scenarios.},
  uac-discipline = {Human Management},
  uac-evidence = {The paper demonstrates construction of a safety argument to human
organization interactions in an SMS (Safety Management System) based organization for
```

```
military shipping. This application demonstrated the effectiveness of the overall
argument structure, the strength of an end-to-end argument for an example RCs, and
thus, that the argument and the abiltiy to include department interactions in an end-
to-end argument for all involved RCSs.},
  uac-flex-process = {Prescriptive},
  uac-form = {GSN},
  uac-industry = {Maritime, Military},
  uac-mechanisms = {Identify the RCSs in an SMS. Perform an end-to-end assurance
argument for each RCS given the template arguments of this paper. Include evidence
for department interaction success. Combine RCS arguments into an overall argument
that assures operation of each and every RCS assures system safety. In summary, this
is a strategy claiming that Safety of th system is then assured if all RCSs are end-
to-end assured. Thus safety is an argument of end-to-end assurance of each and every
RCS.},
  uac-perspective = {Practicioner},
  uac-review-date = {2/10/2015},
  uac-reviewer = {J. Rowanhill},
  uac-rigor-arg = {Structured},
  uac-rigor-ev = {Structured},
  uac-topic = {Military shipping/logistics safety},
  url = {http://safety.inge.org.uk/20080711-Inge2008_End_to_End_Reviews-U.pdf}
}
```

8.2 Field Interview Outline

For our practitioner interviews, we developed a protocol script to normalize our conversations and focus on the information we wanted. Excluding orientation materials, the central portion is provided below.

Introduction

- Personnel, roles and backgrounds
- Presentation of study goals and procedures

General

- Establish roles of organization in assurance case practices:
  - Regulator, developer, operator.
- Establish roles of individuals:
  - Author, reviewer, manager, certify/approve.
- Programmatic details:
  - When was use of assurance cases initiated?
  - Was the assurance case approach imposed or self started?
  - Number of engineers involved and their roles?
  - Liaison of this organization with others?
- Domains:
  - Civil aero, defense, rail, healthcare, etc.?
- Top-level requirement:
  - How derived/agreed?
  - How stated?
  - Typical technical properties being address (e.g., safety for human life, environmental protection, security, etc.)
- Technology used:

    - Rigorous, explicit argumentation?
    - Notations – natural language, spreadsheets, GSN, etc.?
    - Assurance case representation – document, web site, other?
    - How are cases built and presented?
    - Are confidence arguments used? If so, how, when and where?
- Evidence:
    - Forms of assurance evidence – FMECA, FTA, HazOp, etc.?
    - Software – testing, formal verification?
    - How is evidence collected, represented, stored?
- Process:
    - Process used for assurance case activity (build, review or certify, choose)?
    - Use of assurance case by developers? Managers? Quality assurance?
    - Does the assurance case affect/manage system development process?
    - Assurance case quality control – are there internal audits?
- Pragmatics:
    - What is the training burden?
    - Are you able to find qualified employees?
    - Are employees happy with the technology?
    - Are guidance and examples provided by regulator?
    - Use of patterns? Pattern libraries? Fullsized frameworks?
    - Reuse of assurance case from "similar" products?
    - Any system failures even with an assurance case?
    - Number of system successes with assurance cases?
- Statistics:
    - How many assurance cases has the organization developed/approved?
    - Distribution of scale of projects using an assurance case,
    - Number of domains within which assurance cases developed/approved?
    - Distribution of development/approval times?

Assurance Case Benefits

- Benefits expected and seen?
- What problems solved?
- What needs are met?
- What are the necessary conditions and assurance case elements to realize these benefits?
- Empirical measurements/indicators of benefits? Reduced development time? Better management control? Better products? Lower development costs?
- Do staff generally feel there is value?
- Does the SC lead to more or less overall project effort?
- What alternative methods might be options if an SC/AC were not used? Pros and cons?

Developers Only

- Do you use assurance arguments during system design to evaluate design options?
- Do engineers designing system modifications use assurance cases to familiarize themselves with the systems they will modify?
- Who reads the assurance argument before system deployment, and for what purpose

Operators Only

- Do you use the designers' pre-operational assurance case to familiarize themselves with the designers' assurance rationale?
- Who reads the assurance argument after system deployment, and for what purpose?

Regulators Only

- If an argument is presented, how do you determine whether the argument is compelling?
  - What assessment process is used?
  - How long does it take?
  - Are determinations generally that argument is compelling or not?
- Do you use the assurance case to assess:
  - Degree of completeness of hazard analysis?
  - Degree of completeness of hazard mitigation?
  - Degree to which evidence is adequate?
  - Degree to which evidence was properly collected and handled?
  - Appropriate and correct use of statistical methods?
  - Other items?

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01- 04- 2017	Contractor Report	

4. TITLE AND SUBTITLE

Understanding What It Means for Assurance Cases to "Work"

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Rinehart, David J.; Knight, John C.; Rowanhill, Jonathan

5d. PROJECT NUMBER

5e. TASK NUMBER

NNL16AB09T

5f. WORK UNIT NUMBER

999182.02.85.07.01

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NASA Langley Research Center
Hampton, VA 23681-2199

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSOR/MONITOR'S ACRONYM(S)

NASA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

NASA-CR-2017-219582

12. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified - Unlimited
Subject Category 62
Availability: NASA STI Program (757) 864-9658

13. SUPPLEMENTARY NOTES Langley Technical Monitor: C. Michael Holloway

14. ABSTRACT

This report is the result of our year-long investigation into assurance case practices and effectiveness. Assurance cases are a method for working toward acceptable critical system performance. They represent a significant thread of applied assurance methods extending back many decades and being employed in a range of industries and applications. Our research presented in this report includes a literature survey of over 50 sources and interviews with nearly a dozen practitioners in the field. We have organized our results into seven major claimed assurance case benefits and their supporting mechanisms, evidence, counter-evidence, and caveats.

15. SUBJECT TERMS

Argument; Assurance; Case; Epistemology; Safety

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			STI Help Desk (email: help@sti.nasa.gov)
U	U	U	UU	78	19b. TELEPHONE NUMBER *(Include area code)* (757) 864-9658