Arguing The (Safety) Case(s) For Space

Dr Andy Quinn MSc PhD MRAeS CEng

Saturn Safety Management Systems Ltd, Bath, BA2 9BR, UK

ABSTRACT

Space safety demands that appropriate levels of rigour are applied to license applications in order to demonstrate that the 'system' (spaceport, operator, vehicle etc.) is compliant to the stated requirements. As there are different and novel space vehicles, it is clear that prescriptive requirements are not appropriate and that performance (and risk) based requirements are more suitable. In the US, the FAA-AST regulations are not prescriptive and require an applicant to submit a Safety Review Document to cover the key regulatory requirements. The document's main headings relate to relevant Code of Federal Regulations Part 400 requirements and therefore the applicant's descriptions and 'solutions' to each requirement are essentially the compliance statements (or evidence). The document could therefore be described as the 'safety case'; or can it?

A safety case can mean different things to different people, in different countries. The ICAO definition is '*A document which provides substantial evidence that the system to which it pertains meets its safety objectives'*. In the UK, the term 'Safety Case' is used in respect of a set of one or more documents that include claims, arguments and evidence that a system is safe. Another UK definition is that a safety case is defined as '*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.*

The supporting arguments are the spine of a safety case as these explain the rationale of how lower-level goals (or claims) can help substantiate the overall goal (of safety/compliance) and as well as explaining how the evidence can be interpreted to meet the goals.

The paper presents different safety case formats and the rationale why, if properly argued (constructed), safety cases can assist, rather than hinder, regulators and operators alike. The author of this paper contends that regulations for space activities should be performance based (and not overly prescriptive) and that a formal and *structured argument* can assist regulators in assessing the compliance to appropriately rationalised requirements and a structured argument, with justifications and assumptions can assist the operator's case for award of a launch license.

1. INTRODUCTION

Primarily in the UK, but adopted (and adapted) within other countries, a safety case, and associated report, is a means to convey the attributes of a system such that a regulator can approve its use. A safety case can be defined as [1] '*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'.*

Although originating in the UK in the early 1970's, the safety case concept was elevated due to disastrous events and the subsequent inquiry recommendations that prompted a dramatic change in regulation and approaches to safety management.

The Deepwater Horizon accident occurred in 2010 [2] and lessons identified included taking a more performance and risk-based approach and by articulating this within a safety case: *Recommendation A2: The Department of the Interior should develop a proactive, risk-based performance approach specific to individual facilities, operations and environments, similar to the "safety case" approach in* ***the North Sea***.

The Deepwater disaster occurred after the UK's North Sea disaster in **1988** (Piper Alpha) whereby Lord Cullen [3] made 106 specific recommendations to initiate a new and improved safety regime and in particular, the safety case regime.

As well as recommending less prescriptive approaches, another important recommendation transferred oversight of the

offshore oil & gas industry from the Department of Energy to the Health & Safety Executive (HSE). This then brought the risks under the ALARP principal whereby residual risks of a system are to be 'As Low As Reasonably Practicable' (within the HSE's Tolerability of Risk framework).

So when should we use a safety case regime? Is it just for complex systems or safety critical systems or should everything have a safety case? What about cost and what is proportionate? Figure 1 attempts to illustrate the 'new product, new market = high complexity/high risk' approach, per the Ansoff Matrix.

		Solution	
		Familiar	**Unfamiliar**
Problem	**Familiar**	Minimal argument and standard evidence from the domain i.e. certificates of design	Focused argument on reasons for novel solution, plus the appropriate evidence
	Unfamiliar	Minimal argument and standard evidence from another domain i.e. use of recognised standards	Extensive argument and evidence, with substantial independent scrutiny and application of novel standards and technology i.e. Space Launch Operations

Figure 1: Safety Case Complexity – based Ansoff Matrix

During the lifecycle of a system (from concept, development, manufacture, testing, in-service operation, disposal) the point of the safety case is to challenge whether the system is 'acceptably safe' for instance. During the SC development (and by using rigor and challenge) this would undoubtedly provide some aspects which are not fully substantiated; hence this would mean a recommendation can be made to either improve the design or processes, or having identified a residual risk, then the point is to highlight this (not to hide this). The design team would then have to provide evidence that this has been analyzed (or state that this will be analyzed during the next phase) and hence may require a concession. This may be (or may not) acceptable for this stage of the safety case because of the risk classification i.e. if a risk was identified as intolerable or a design requirement had not been substantiated and further re-design is not practicable, then the point of the safety case would be to say 'stop'. An example could be the X37B project – whereby the design seemed to be fine, but then the programme was cancelled after the technical assurance report provided evidence that the design was not robust, mainly due to poor reliability (of the design and of the reliability processes). In this example, the safety engineer constructing the safety case would have identified this during the concept or development stages, using a properly constructed argument to challenge the design, and processes and hence would have saved a lot of time and money being invested in a novel but non-starting project (the project was stopped in 2001, but could have been stopped 2 years previous using the SC methodology).

2. TYPES OF SAFETY CASE ARGUMENT

Qualitative Argument; this will be used throughout the SC as the author details compliance to standards and requirements; some of which may have an indirect link to the system's desired attributes (competency of personnel's qualifications and experience, certain Quality Assurance aspects, etc.).
Quantitative Argument; here the author will set a probabilistic target (as a goal) and then argue by quantitative statistical reasoning, to establish whether the analysis meets the objective (through reliability, availability, maintainability predictions and performance analysis and modelling etc.).
Deterministic Argument; this relies on axioms, logic and proof.

	Attribute	
	Fault-Tolerance	**Reliability/ Availability**
Goal/Claim	Safety is maintained under stated failure conditions	System reliability meets the stated objective
Requirement	Subsystem 'X' shall be 2-Fault Tolerant	Subsystem 'X' Loss of Function shall be 1x10-4 per mission
Design Features	Redundant channel Zonal separation	Hardware component reliability
Evidence	FMECA FTA Design Review	FTA CMF

Figure 2: Example Claims, Arguments, Evidence Attributes

3. SAFETY CASE CONSTRUCT

The SC is best constructed as a team effort starting with the Top Goal/Claim i.e. System 'X' is acceptably safe to operate in context 'Y'. What we are trying to communicate is a clear, comprehensive and *defensible* argument (case) with supporting evidence. So this sounds like legal jargon – exactly the point! The SC is attempting to justify a system is safe to operate (for complex systems with severe risks) and that the system has met the legislative requirements. Why? – such that, in the event of a catastrophic/critical outcome, the operator can provide a defensible argument (in a court of law if appropriate) that the legislation was complied with and that all that was reasonably practicable to prevent the accident was done.

After the Top Goal/Claim is established then the context in which the system is operating in needs to be defined, along with assumptions.

The strategy (or argument) then evolves by '*arguing over effective design in accordance with 'X' standards and 'Y' means of compliance and that the system is operated and maintained effectively and that all hazards have been identified and managed within an effective Safety Management System'* for instance.

Then the next level down provides the goals/claims to support this strategy, and so on, until the lowest goals/claims are as far as you can derive (with the arguments), whereby the analyst/team provide the evidence. Here we are looking for a true/false solution (evidence) but of course there will be conclusions whereby partial substantiation has been achieved – thus prompting re-design or operating limits/procedures etc.

There is **Direct Evidence**: this is evidence which is clearly linked directly to the goal/requirement itself (test evidence, analysis, historical data, compliance matrices – to standards, Verification Cross-Reference Matrix, etc.) i.e. evidence could be a test result showing that a safety critical parameter is within tolerance.

Then there is **Indirect (Backing) Evidence** that supports the direct evidence, giving it credibility i.e. a qualified and experienced engineer using certified test equipment.

The evidence is presented at the lowest level in the safety case as depicted in Figure 3:

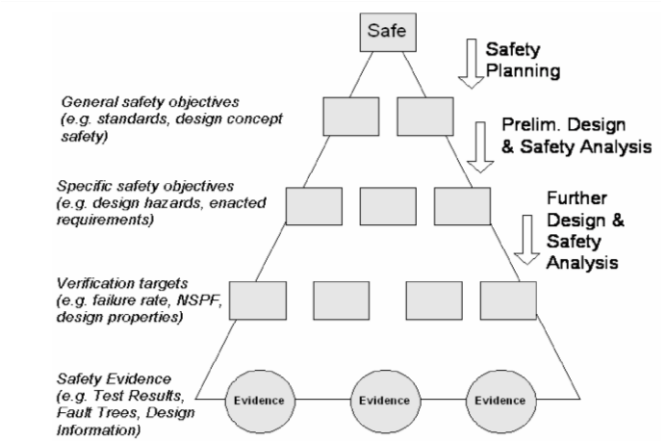

Figure 3: Safety Case Construct

An aircraft has many systems and subsystems that combine to present the overall SC. So for instance, propulsion system requirements are flowed down to the engine manufacturer to produce an engine SC. This engine system SC will then have a specific Top Goal such that the engine operation is acceptably safe on aircraft 'X' and meets its safety objective of $<1x10^{-4}$ per flying hour (per engine) resulting

in a Hazardous event; note in aviation an engine cannot result in a catastrophic event by itself (per Certification Specifications). Figure 4 below depicts a Total Safety case hierarchy diagram for an air-launched suborbital vehicle with similar systems/ subsystems to that of an aircraft (with the obvious differences of the rocket engine etc.).

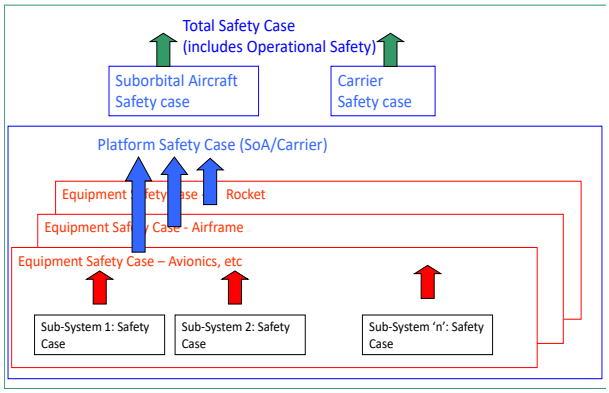

Figure 4: Safety Case Hierarchy

3.1. Safety Case Notations

There are different ways to present a safety case and this depends on the complexity of the system under consideration. A simple system can be described in a document report and have a Tabular safety argument. For more complex systems, in the UK, we recognise the following two notations:

Goal Structuring Notation (GSN). The GSN notation was developed at York University and further developed there by Professor Tim Kelly. A generic GSN example is in Figure 5:

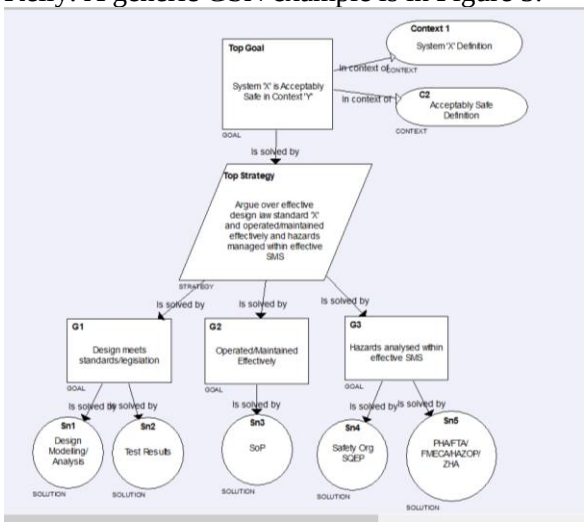

Figure 5: Goal Structuring Notation – simple example using the Adelard Assurance and Safety Case Environment Tool [5]

The Claims, Argument, Evidence (CAE) notation is in Figure 6. The CAE methodology was developed in the UK by Adelard in the Assurance and Safety Case Environment (ASCE) tool. This is an interactive tool whereby the author can 'open' the nodes and write the claims, arguments and evidence. Diagrams and tables can be imported and the nodes can be linked to each other and references can link to reports (analysis/test results etc.) directly when viewing in the ASCE 'Browser'. This is considered a very useful tool for a regulator for instance when interrogating the evidence and arguments.

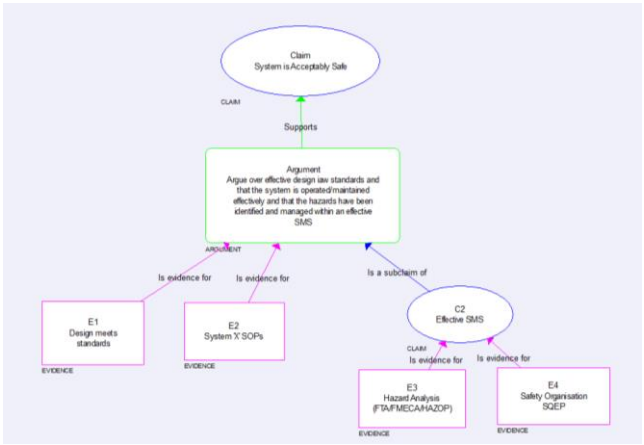

Figure 6: Claim Argument Evidence – simple example using the Adelard Assurance and Safety Case Environment Tool [5]

3.2. Spine Of The Safety Case

The supporting arguments are the spine of a safety case as these explain the rationale of how lower-level goals (or claims) can help substantiate the overall goal (of safety/ compliance) and as well as explaining how the evidence can be interpreted to meet the goals.

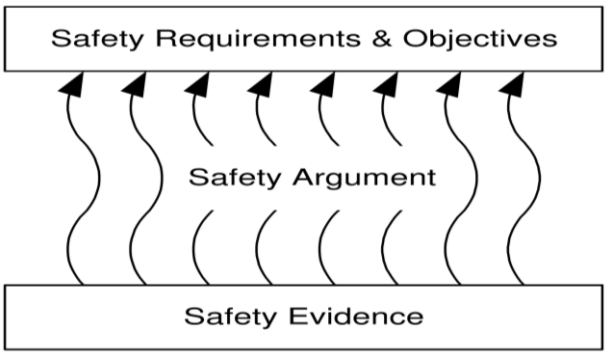

Figure 7: Argument – Spine of the SC

3.3. The Life Of The Safety Case

The safety case is remains live throughout the lifecycle of the system and should start as early as possible i.e. at the concept phase:
Preliminary/Initial (Concept Phase) SC.
This captures:

- The scope of the SC and definition of the system (and boundaries/interfaces to other systems or dependent SCs i.e. space vehicle to spaceport to range safety command and control etc.).
- Defines the SC approach; arguing functional attributes, product attributes, process attributes.
- Identifies the key safety requirements and applicable standards/means of compliance (and references the Safety Management Plan and Safety Program Plan)
- Identifies the key safety issues (from the associated hazard analysis) with high-level derived safety requirements for the subsystems and system level. So here we follow the Design For Minimum Risk (DMR) approach with fail-safe, damage tolerance requirements etc.
- The Preliminary Report (SCR) then sets out the argument (story) and provides the evidence to substantiate the Top Goal; hence it summarises the SC and should provide recommendations to continue work to gather the evidence detailed OR provides an early opportunity to find out if there are fundamental flaws in the design or intended operation. Hence the SC Statement should clearly detail whether the project is viable to continue to the next phase.

Interim (Detailed Design) SC.
This is an expansion of the Preliminary SC and should increase confidence that the initial SC can be supported i.e. based on the detailed design and further hazard analysis using appropriate safety tools & techniques.
The lower-level goals and supporting evidence 'nodes' can be populated with the design architecture, some modelling to provide validation of requirements, the Failure Mode Effect & Criticality Analysis and Fault Tree Analysis will have derived additional requirements for the design (interlocks, protection measures), including apportionment of risk (reliability) budgets etc.
The Interim SCR will state that the design is acceptable to now progress to Manufacture and then Test (or will detail flaws in the design which should either be re-designed or be accepted with operating limitations/procedures [if acceptable to the Authorities]).

Operational SC. This is the SC that demonstrates to the Regulator that the agreed requirements have been met, in accordance with the appropriate standards, and that where necessary the alternate acceptable means of compliance demonstrate the systems is safe for its intended use. This can therefore be seen as the Initial Operating Capability SC. Going forward throughout the operating life of the system, the Operational SC can be updated (where required due to modifications or changes in operation) or a more bespoke Operating SC could be developed focusing on operations, maintenance and modifications etc.
Back to the Operational SC, this covers:

- Sufficient assurance that the system <u>as constructed is</u> acceptably safe to be allowed to operate in its intended operational context for the first time.
- Completed arguments (story of the design, analysis, build, test) with associated assumptions and justifications where needed
- Completed evidence (solutions nodes) that substantiate the associated goals and hence the Top Goal. This includes compliance matrices for design, safety, testing etc. and hence verification of all requirements per the Preliminary SC (and additional requirements added throughout the project)
- Descriptions of any applied for concessions or 'work arounds' on specific issues. This will provide analysis of the problem and associated operating limitations or procedures.
- Conclusion that the system is acceptably safe with the list of limitations and operating procedures for any issues.

3.4. Maintenance of The Safety Case

Throughout the operating life of the system, the safety case should remain 'live' as an

important part of the Safety Management System (SMS). Part of an effective SMS is Change Management and changes to the design either due to mission requirements or safety issues needs to be managed effectively i.e. considering the effects to existing hazards (and does the change introduce new hazards) and impact to other subsystems etc.

4. SC PITFALLS (& TIPS TO AVOID THEM)

4.1. Proving the system is 'safe'

It is easy/straight-forward to develop a safety case to provide a positive 'story' (argument) with all evidence being present and correct. This is especially true when the author/ reviewer has a mindset (or cognitive bias) to favour information that confirms their preconceptions and hence are not looking to challenge the information.
The key (and added value) is to develop a structured argument that challenges the Top Goal and provides arguments and justification where required i.e. demonstrating an equivalent level of safety or design means of compliance.
At the start of the safety case construction, it is important to establish the requirements and standards as part of a team effort. The safety specialist should lead the workshop with the aim of developing the safety case argument (through the lower level goals and justification notes/assumptions).

4.2. Retrospective Safety Case

Starting a safety case after the design is completed is problematic. The safety rationale and argument will be less robust, trying to link the 'as designed' evidence (including probabilistic results) to meet some safety objective, as well as design standards. This could lead to a re-design of parts of the system with associated overrun in costs and schedule.
The Safety Case should begin at the concept phase, along with preliminary hazard analysis, such that appropriate safety requirements and safety objectives can be derive i.e. that are realistic and achievable. The Safety Case construct can be a useful tool in developing a strong argument and then detail the sort of evidence that should be sought i.e. the initial safety case 'solution's (evidence) will actually be requirements; for instance detailing appropriate standards (or regulatory requirements) that should be satisfied in order to substantiate the safety case goals. In relation to safety and reliability, the solutions can detail the activities that will need to be completed as the project develops.

4.3. Lack of SQEP and Independent Assurance

The SC author should be a safety specialist with knowledge of the system under scrutiny i.e. Suitably Qualified and Experienced Person (SQEP). Where this is not the case, then, as detailed above, confirmation bias will creep in as well as lack of understanding of appropriate requirements and standards.
The UK Ministry of Defence Nimrod aircraft SC was 'a lamentable job from start to finish ….. riddled with errors….tickbox exercise ….. open hazards…..' etc. [6].
With complex and safety critical systems that have severe consequences, it is advisable to employ an Independent Safety Advisor to provide assurance that the SC author (and those conducting the hazard analysis) are conforming to best practice and that the system has appropriate requirements and standards to follow.

4.4. Interfaces (Inter-system or between systems)

Interfaces present weak areas i.e. boundaries between subsystems, systems and external systems.
Check the assumptions and dependency statements.
Ensure the interface failure modes have been appropriately considered and derived safety requirements recorded (and properly transferred to suppliers or external stakeholders).

4.5. Arguments

Arguments without evidence are unfounded.
Construct arguments correctly – get independent checks

4.6. Evidence

Evidence without arguments are unsubstantiated (unexplained).

4.7. Shelf-bound SC

Once constructed and a SCR written (and a launch license granted for instance) then 'job done'. The SCR and diagram (GSN/CAE) then sits on the shelf gathering dust. Wrong!

5. SAFETY CASE FOR SPACE

The NASA Safety Center [7] provides further rationale in a system safety failure case on the UK's Piper Alpha disaster, as mentioned in the Introduction. The NASA 'Case for Safety' states:
Fortunately, the UK's movement toward Safety Cases after the Piper Alpha disaster finds a parallel in NASA system safety engineering and methodology as Risk-Informed Safety Cases (RISC). The RISC is developed beginning early in the systems development lifecycle and reviewed at each major milestone. Then it plays a key role in NASA's acceptance and possibly certification (if applicable) of the newly developed system.

There are different and novel space vehicles and hence it is clear that prescriptive requirements are not appropriate and that performance (and risk) based requirements are more suitable. This non-prescriptive approach is how the UK HSE manages safety and this is how the prospective UK Space Agency (and UK Commercial Spaceflight CAA team) intend to handle space launch risks. In the US, the FAA-AST regulations are also not too prescriptive and require an applicant to submit a Safety Review Document to cover the key regulatory requirements. The document's main headings relate to relevant Code of Federal Regulations Part 400 requirements and therefore the applicant's descriptions and 'solutions' to each requirement are essentially the compliance statements (or evidence). The document could therefore be described as the 'safety case'; or can it? On the one hand, requirements have been identified, but on the other hand, to what standards and to which alternate acceptable means of compliance?

5.1. Benefits of Safety Case for Space

Space systems are complex and novel; hence how does an operator substantiate their launch license application without justifying and arguing their evidence (and where required, arguing an equivalence or alternate acceptable means of compliance – to the regulator's requirements)?
A well-constructed safety case, based on expert knowledge of the system provides the operator with an opportunity to tell the regulator the story of the design, including what requirements were identified and how these have been met – and where issues were identified, how these were mitigated to an equivalent or alternate means of compliance i.e. by further analysis and testing and demonstrating the system functions safely. Rockets are risky and consequences of failures are generally severe resulting in Loss of Vehicle on the launch pad or during the ascent. The SC provides an opportunity to challenge the design and operation in order to influence the design.

5.2. Operators Safety Case

Whether a spaceport operator or space launch vehicle designer/operator a safety case will assist in providing the 'glue' between your system, subsystems and externally to interfacing systems. It will help drive the design by compiling a structured argument based on the agreed requirements and complying to the agreed standards and means of compliance.
The operator's SC safety engineer has a chance to challenge the design and operations. An example would be to challenge why pre-launch chill-down times are reduced (procedural change); here the SC author could quote best practice and then raise a recommendation that the procedure is changed to reflect best practice or that additional mitigation is introduced to monitor the component temperatures to ensure the shorter chill-down times actually provide the desired component operating temperatures.

5.3. Regulators 'Assurance' Case

One could argue that, for an operator to submit a safety case as part of their launch license application, the Regulators should have their own assurance case – which would essentially be a structured framework (the argument) based on the legislation (requirements) that, if followed, would provide confidence that the applicant's 'case' would meet the regulations for launch.
In essence, this is where the regulators can define the credible bounds of an acceptable safety argument and provide guidance on the level of evidence required to meet the individual goals and hence overall safety case (top goal).
Taking the FAA-AST CFR Part 415 Appendix B, the list of required Safety Review Documents in theory could be the evidence (that the FAA-AST are looking for i.e. they

have defined the boundary for the applicant with these headings). This SRD outline should include:

1.0. Launch Description (§415.109)
2.0. Launch Operator Organization (§415.111)
3.0. Launch Personnel Certification Program (§415.113 and §417.105 of this chapter)
4.0. Flight Safety (§415.115 & §417 Subpart C)
5.0. Ground Safety (§415.117)
6.0. Launch Plans (§415.119 and §417.111 of this chapter)
7.0. Launch Schedule (§415.121)
8.0. Computing Systems and Software (§415.123)
9.0. Unique Safety Policies, Requirements and Practices (§415.125)
10.0. Flight Safety System Design and Operation Data (§415.127)
11.0. Flight Safety System Test Data (§415.129)
12.0. Flight Safety System Crew Data (§415.131)
13.0. Safety at End of Launch (§415.133)

Hence the operator should provide descriptions and justifications and supporting analysis for each of the Chapters above.

Perhaps a future exercise, for the Regulators, would be to compile their own assurance case to evaluate whether the above list of 'evidence' is sufficient/complete. Additionally this approach may assist them (the US FAA-AST) in expanding their regulations to include safety of those on board and then the airworthiness/spaceworthiness of the launch vehicles.

6. CONCLUSIONS

Safety Cases should add value to your business whether a space launch vehicle designer/operator or spaceport operator. If constructed properly, by safety SQEP (and checked with Independence) the SC will provide the story (the argument) that the 'system' is acceptably safe to operate in the defined environment. This argument, based on deterministic, qualitative and quantitative claims/goals will be supported by the evidence – these should be true/false statements that summarise the documented evidence (design reports, safety analysis, test results etc.) to provide a level of confidence in the associated goals i.e. the evidence should be substantiated. Where this is not the case, then this will be partially substantiated (or at worst unsubstantiated) and a level of confidence assigned; in this instance additional measures should be provided to allow the system to operate i.e. operating limitations, operating procedures etc.
The SC will then be presented as a SC Report as part of a launch license application with the aim of assisting the Regulators understand the 'story' of your system's conception, design, build, testing and how it will operate.
The next step will be for Regulators to be aware of Safety Cases and to know how to 'read' and 'interrogate' the robustness of the SC to enable them to approve the system. Regulators should use recognised tools to aid in the SC review and provide guidance to operators in compiling safety cases (defined boundaries and guidance on depth of evidence required).

7. REFERENCES

[1] United Kingdom Ministry of Defence, Defence Standard 00-56, Issue 4

[2] National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, Deepwater: The Gulf Oil Disaster and the Future of Offshore Drilling, p252, January 2011

[3] The Hon. Lord Cullen, The Public Inquiry into the Piper Alpha Disaster, Vols 1 and 2 (Report to Parliament by Secretary of State for Energy by Command of Her Majesty, 1990)

[4] National Aeronautics and Space Administration, Independent Assessment of X-37 Safety & Mission Assurance Processes and Design Feature, Headquarters Office of Safety & Mission Assurance June 18, 2001

[5] Adelard, Assurance and Safety Case Environemnt (ASCE) tool, Available at: Https://www.Adelard.com

[6] Charles Haddon-Cave, The Nimrod Review, HC 1025, London: The Stationery Office Limited, 2009

[7] National Aeronautics and Space Administration, NASA Safety Centre, The Case for Safety, May 2013 Volume 7 Issue 4

8. ACRONYMS/ABBREVIATIONS

Abbreviation	Meaning
AC	Advisory Circular
ALARP	As Low As Reasonably Practicable
ASCE	Assurance & Safety Case Environment
CAE	Claims Argument Evidence
CFR	Code of Federal Regulations
DMR	Design for Minimum Risk
FAA-AST	Federal Aviation Administration – Office for Commercial Space Transportation
FMECA	Failure Modes Effects & Criticality Analysis
FTA	Fault Tree Analysis
GSN	Goal Structuring Notation
HSE	Health & Safety Executive
NASA	National Aeronautics and Space Administration
SC	Safety Case
SCR	Safety Case Report
SMP	Safety Management Plan
SMS	Safety Management System
SOP	Standard Operating Procedure
SPP	Safety Program Plan
SQEP	Suitably Qualified Experienced Personnel