73rd International Astronautical Congress (IAC), Paris, France, 18-22 September 2022.

IAC-22-A1.6.6.x70640

Adopting an Objectives-Driven Assurance Case Approach for Achieving Space Flight Mission Planetary Protection Objectives

Elaine Seasly[a]*, J. Nick Benardini[b]

[a] *Office of Planetary Protection, National Aeronautics and Space Administration (NASA) Headquarters, 300 E Street SW, Washington, District of Columbia, United States, 20546-0001,* elaine.e.seasly@nasa.gov
[b] *NASA Headquarters, Mary W. Jackson NASA Headquarters Building 300 Hidden Figures Way SW, Washington, DC 20546-0001, James.N.Benardini@nasa.gov*
* Corresponding Author

Abstract

Traditionally, the National Aeronautics and Space Administration (NASA) has utilized prescriptive technical and process requirements to ensure safety and mission assurance performance objectives for planetary protection are achieved during space flight missions. While prescriptive requirements may be easier to communicate and manage throughout the systems engineering process, the highly constrained nature of prescriptive requirements can limit the ability to take advantage of cost-saving opportunities and offer limited ability to explore other options or alternative designs, processes, and methods. It can also be difficult to develop prescriptive requirements for objectives that are probabilistic in nature or that cannot be satisfied by direct verification. In contrast, the development of an assurance case allows for a compelling, comprehensible, and valid argument to be developed with supporting evidence that shows safety and mission assurance objectives have been satisfied. Analogous to how patent applications are constructed for inventions, an assurance case has a high-level claim of meeting a safety and mission assurance objective, followed by a more specific set of sub-claims and technical evidence which supports the claims. The objectives-driven assurance case approach allows for a better understanding and exploration of the trade space, more flexibility to balance trades, and the ability to realize and implement technical and process innovations for resource, time, and cost savings. The assurance case is a living case that evolves over the entire program life cycle. Recently, NASA's Office of Planetary Protection (OPP) has adopted the assurance case approach as an acceptable methodology for demonstrating avoidance of contamination of target solar system bodies explored by NASA space flight missions. This methodology has been incorporated into NASA's new technical standard for planetary protection and is currently being utilized by the Mars Sample Return campaign for safe sample containment during sample return.
Keywords: assurance case, safety case, planetary protection, requirements, claims, evidence

Acronyms/Abbreviations

ALARP	As Low As Reasonably Practicable
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MPEP	Manual of Patent Examination Procedure
MSR	Mars Sample Return
MSL	Mars Science Laboratory
MOPS	Minimum Operating Performance Standards
NASA	National Aeronautics and Space Administration
NPD	NASA Policy Directive
NASA-STD	NASA Standard
OPP	Office of Planetary Protection
OSMA	Office of Safety and Mission Assurance
SMD	Science Mission Directorate
USC	United States Code
USPTO	U.S. Patent and Trademark Office
VLC	Viking Lander Capsule

1. Introduction

In 2017, the National Aeronautics and Space Administration (NASA) transitioned the administration of the Office of Planetary Protection (OPP) from the Science Mission Directorate (SMD) to the Office of Safety and Mission Assurance (OSMA) [1]. As a result of this transition, OPP has benefitted from the processes and procedures inherent to the OSMA discipline including concepts, guidelines, and implementation approaches for system safety [2]. One such concept, the safety assurance case, has recently been adopted by OPP to support space flight missions in demonstrating compliance with planetary protection requirements. An assurance case provides an argument and supporting evidence to demonstrate claims of safety or mission assurance are valid [3]. As the OPP shifts from strictly prescriptive-based requirements to the inclusion of performance-based requirements, techniques such as the assurance case approach provide space flight missions the flexibility to perform system trades, capitalize on opportunities for efficiency and improvement, and consider potential risks in a broader context.

While the assurance case approach has been utilized by high-risk industries such as rail service, nuclear, and defense systems [4], the assurance case approach is new to the discipline of planetary protection. To aid in communicating the goals, generation, and evaluation of an assurance case, the patent application process is presented as an analogy. The construction of an assurance case is similar to construction of a legal case, and many scientists and engineers have some familiarity of the patent application process as inventors.

2. Prescriptive Requirements

Prescriptive requirements are explicit requirements that state exactly "what to do" and "how to do it [5]." These types of requirements are highly specific and leave very little room for interpretation. Prescriptive requirements can be a benefit when definiteness is required, such as when the conformity of a product or process is necessary. Prescriptive requirements can be highly limiting and constraining by nature. From a systems engineering standpoint, prescriptive requirements may be easier to communicate and flow down through the layers of a supply chain, and provide a touchpoint in the process that is easy to point to for traceability and verification. Prescriptive requirements do have a proper place in certain products and processes, but are not the only type of requirement that can be utilized in defining a system or the safety of a system. Some systems use a combination of prescriptive requirements and performance-based requirements. For example, "…civil aviation uses a combination of highly prescriptive normative regulations, which mandate concrete product requirements and compliance processes, and so-called performance-based regulations specifying minimum operating performance standards (MOPS) [6]."

To effectively utilize prescriptive requirements, detailed knowledge of the system must be known, as unknowns or unpredictable behaviors can be difficult or impossible to identify. Any changes to prescriptive requirements carry a risk of increasing cost, especially if changes affect suppliers and require modifications to existing contracts. Changes can also cause a ripple effect and disrupt linked requirements in the systems engineering process. Subsequently, design or process efficiencies that are discovered after requirements are flowed down cannot be easily adopted.

Incorporating overly prescriptive requirements can encumber creative thinking and effective decision-making [7]. The consideration of alternative designs, approaches, and processes by engineering teams may be limited. Envisioning the future state and what "could be" of the system and potential risks may be reduced. And some may assume a false sense of safety, reliability, and control over future performance for a system or process that utilizes prescriptive requirements. As stated by the NASA Safety Center, "Such prescriptive processes are assumed to ensure safety and do not necessarily require corresponding evidence to validate a safety measure's effectiveness at ensuring that risks are kept As Low As Reasonably Practicable (ALARP) [8]." Over-reliance on prescriptive requirements may cause some to decrease validation tests of system safety or delete them altogether.

2.1. Use of Prescriptive Requirements in Planetary Protection

Planetary protection is the practice of protecting solar system bodies from harmful contamination by terrestrial materials to enable scientific exploration and protecting the Earth-Moon system from possible harmful extraterrestrial contamination that may be returned from other solar system bodies [9]. Perhaps some of the most well-known prescriptive and stringent requirements in planetary protection were those of the Viking mission. Comprised of two orbiters and two landers, the Viking mission to Mars was launched with two launches in 1975. The Viking landers contained experiments to search for signs of life on Mars, so planetary protection requirements were developed to prevent contamination of the onboard life detection experiments and to prevent biological contamination of Mars during the mission. Prescriptive requirements dictated the process to sterilize Viking hardware. For example, the biology package probability of contamination had to be kept below $1 \times 10–6$, which required sterilization at 120°C (248°F) in a dry-nitrogen atmosphere environment for 54 hours [10]. Each fully integrated Viking Lander Capsule (VLC) underwent terminal sterilization at 111.7°C for 30 hours [10]. Such requirements became the "gold standard" for sterilization of hardware destined for Mars, but became impractical and costly to apply to subsequent missions such as Mars Science Laboratory (MSL) and Mars 2020. As stated by the National Academies of Sciences, Engineering, and Medicine, "…applying certain very prescriptive Viking era requirements (bake subsystem Z for X hours at temperature Y) into level-1 performance requirements that could require a new Mars 2020 design was a major hurdle. Such standard prescriptions do not translate well as new missions emerge with differing designs and objectives, and thus more innovative approaches to planetary protection goals are needed [1]."

Innovative approaches to planetary protection will be needed for the Mars Sample Return (MSR) campaign, which will bring the first samples of Mars material back to Earth for detailed study to determine if life ever existed on Mars [11]. This will be the first restricted Earth-return mission since the Apollo missions to Earth's moon. As such, backward planetary protection to ensure Earth is protected from potential hazards posed by extraterrestrial matter will be key to mission success. As stated in the US Federal Register notice of intent:

> *There is no current evidence that the samples collected by the Mars 2020 mission from the first few inches of the Martian surface could contain microorganisms that would be harmful to Earth's environment. Nevertheless, out of an abundance of caution and in accordance with NASA policy and regulations, NASA would implement measures to ensure that the Mars samples are contained (with redundant layers of containment) so that they could not impact humans or Earth's environment, and the samples would remain contained until they are examined and confirmed safe for distribution to terrestrial science laboratories [12].*

The assurance case approach will be used to build a case of arguments and evidence to show no negative impact to humans or Earth's environment will result from returning samples from Mars. This will allow the MSR team to think creatively and consider a broader trade space and potential risks than what could be accomplished with prescriptive requirements. MSR will be able to "…select and/or develop implementations most suitable to meet their PP requirements from a systems standpoint [13]" through the assurance case approach.

3. The Assurance Case Approach

The industry standard ISO/IEC 15026 describes an assurance case to include "…a top-level claim for a property of a system or product (or set of claims), systematic argumentation regarding this claim, and the evidence and explicit assumptions that underlie this argumentation. Arguing through multiple levels of subordinate claims, this structured argumentation connects the top-level claim to the evidence and assumptions [14]." Tim Kelley at York University has created a six-step process to support developers of assurance cases [15]. The six steps are:

1) Identify a claim,
2) Define information needed to clarify the claim,
3) Identify strategy to support the claim,
4) Identify context, justification and assumptions needed to understand strategy,
5) Elaborate strategy (if new claims are identified, return to step 1), or
6) Identify basic solution [15].

Following the steps above, one can systematically develop an assurance case for any desired system. As stated by Denney, "Creating and submitting a safety case is both an accepted best practice and a regulatory requirement in many safety-critical industries [6]." For example, the medical device industry has adopted the assurance case approach for review and approval of medical device safety by the U.S. Food and Drug Administration (FDA) because the existing process that relied upon industry standards was "time consuming, complex, and potentially inconsistent [3]." Weinstock further elaborates, "The complexity of medical devices is growing and standards don't cover all of the relevant aspects. FDA reviewers (and the manufacturers themselves) have difficulty identifying all of the important technological risks [3]."

The construction of the assurance case begins with a claim, or a "statement of something to be true including associated conditions and limitations [14]." Claims can be further divided into greater detail through sub-claims. Claims and sub-claims are supported by evidence, which is "any artifact or tangible asset that can be used to substantiate claims/goals. It can take the form of verification and validation reports, design review records, human factors studies, manufacturing process validation records, etc. [15]." Together, the claims and evidence are supported by an argument conveying the "why" the evidence support the claim. Arguments can be deterministic, which demonstrates the truth of the claim by logic, quantitative, which justifies the claim to be true through probability analysis, or qualitative, through use of accepted best practices or expert judgement [15]. The argument is a critical part of the assurance case development, as arguments make it easier to comprehend and critically review a safety case [6]. As stated by Weinstock, "Instead of having to work through piles of evidence with little to no guidance, an assurance case provides the examiner with a structure that is easier to follow [3]." This can be especially important for systems that affect public safety, as the assurance case brings forth the entire story and reasoning why the system is safe in a cohesive and transparent manner. However, issues can arise if the story or the arguments for the case are not explained well. To support the development of assurance cases for disciplines new to the approach, such as the discipline of planetary protection, an analogy to the U.S. patent application process is presented.

4. Patent Application Analogy

Construction of an assurance case is similar to construction of a legal case. The construction and evaluation of a U.S patent application will be presented as an analogy to the construction and evaluation of an assurance case. The patent application process provides a more positive example than a legal defense case, and as many scientists and engineers have experience in applying for patents, provides a relatable example to the technical community.

A patent for an invention is the grant of a property right to the inventor, and in the United States, is issued by the U.S. Patent and Trademark Office (USPTO) [16]. Patents are valuable because they grant the patentee the right to "exclude others from making, using, offering for sale, or selling the invention throughout the United States

(35 United States Code (USC) §154). An inventor files a patent application with the USPTO, and a USPTO examiner reviews the application to determine if the invention is patentable subject matter, novel, and non-obvious. The examiner also evaluates the application for proper disclosure and detail of the invention. If the application passes all evaluation criteria, a patent is granted. If the application is lacking in detail or does not meet the requirements of patentability, the application may be rejected by the examiner with notification of the inventor for future actions.

Patent applications begin with the drafting of claims to define the invention. Sub-claims further define the main claim of the invention, offering additional details on the characteristics of the invention. A common visualization for claim drafting is the "claim drafting funnel," where the broadest claim is represented at the top and additional details of the invention are represented in the layers of the funnel as it necks down, creating higher specificity (Fig. 1). Assurance case claims are crafted in a similar manner, with a top-level claim followed by supporting sub-claims. The argument for the case is built on this support structure. As stated by Weinstock, "The argument consists of one or more subsidiary claims that, taken together, make the top-level claim believable. These lower level claims are themselves supported by additional claims until finally a sub-claim is to be believed because evidence exists that clearly shows the sub-claim to be true [3]."

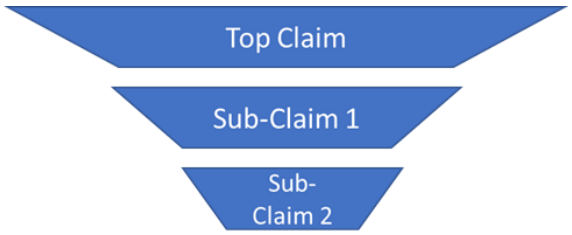

Fig. 1.Claim Drafting Funnel

Claims of an assurance case are supported by evidence, which demonstrates that the claim is credible and takes the form of "verification and validation reports, design review records, human factors studies, manufacturing process validation records, etc. [15]." The evidence to support the claims of a patent application are presented in the specification of the application and show the inventor invented what was claimed. The specification provides the written description to disclose the invention including drawings, the methods and processes to enable one to make and use it, and the best mode to carry out the invention (35 USC §112). The specification provides the evidence to teach the invention, communicate why the invention is novel and an improvement over the current state of the art, and can include supporting laboratory experimentation results or prototypes demonstrating the function of the invention.

Once a patent application or an assurance case has been constructed, the resulting product is evaluated. An independent reviewer reviews the assurance case to determine if it is understandable, that the arguments are sound and supported by evidence in a convincing manner, and all relevant assurance issues are addressed [3]. The reviewer determines if the case is structurally complete, the claims are phrased correctly and logically, and if the overall argument is persuasive [3]. Similarly, a patent application is evaluated by a USPTO examiner, who is an independent reviewer. The examiner reviews the application against patent laws to determine if the application contains patentable subject matter with utility (35 USC §101), is novel (35 USC §102), and nonobvious (35 USC §103). Together with the previously described invention disclosure and claims (35 USC §112), the examiner determines if the invention is patentable [17]. The review process for a patent application can be quite detailed and complicated, especially when making the determination that arguments provided are persuasive. USPTO examiners utilize the Manual of Patent Examination Procedure (MPEP), an extensive document that provides guidance as a manual for USPTO examiners [18].

It is important for both a patent application and an assurance case to convey the arguments in a clear and understandable manner for the independent reviewer. "It will almost always be the case that the persons responsible for reviewing the assurance case will have less knowledge of the system under scrutiny than the developers [19]," as stated by Kelly in a step-by-step approach for reviewing assurance cases. Similarly, patentability is evaluated by patent examiners from the standpoint of a person having ordinary skill in the art (PHOSITA), meaning the claimed invention must be clearly described to be understood by a PHOSITA and should not have been obvious to a PHOSITA to demonstrate novelty [17]. Both a patent application and an assurance case must not burden the reviewer in tracing the arguments through the claims and evidence, but rather should provide a clear and comprehensive narrative to guide the reviewer through the logical flow of information to illustrate the strength of the case and enhance the persuasiveness of the argument.

As described, an assurance case and a patent application are both constructed of claims, required to provide supporting evidence, make arguments of persuasiveness, and are evaluated by independent reviewers. Both an assurance case and patent application have to be clearly communicated to convince the independent reviewer the argument is persuasive. The goal is that the presented patent application analogy provides an initial basis for understanding for those

planetary protection practitioners that are unfamiliar with assurance case development.

5. Adoption of the Assurance Case Approach for Planetary Protection of NASA Missions

NASA's OSMA policy reflects adoption of the assurance case approach by OSMA disciplines. In NASA Policy Directive (NPD) 8700.1, it is the role of OSMA technical authorities to, "Concur or non-concur with the adequacy of assurance cases for safety and mission success in support of relevant decision authorities [20]." The background leading to this updated policy to align with evolving acquisition strategies and NASA systems engineering practices is further described in an OSMA white paper [21]. As part of OSMA's technical authority, the OPP has updated its policy documents to incorporate the assurance case approach for satisfying planetary protection objectives of NASA space flight missions [9][22].

It is important to note that all prescriptive requirements are not being removed or replaced by the assurance case approach. Rather, the assurance case is offered as an additional methodology for space flight missions to consider in meeting planetary protection objectives. Prescriptive requirements may be used in cases such as critical processes or test procedures where the result provides evidence to support the claim of an assurance case.

Mars Sample Return is currently developing an assurance case for satisfying backward planetary protection objectives. Since the assurance case approach is still new to the planetary protection discipline, workshops with the science, engineering, and communications teams are currently being held to increase understanding in the approach. While the planetary protection examples discussed previously focused specifically on missions to Mars, the assurance case approach may be applied to any mission with planetary protection objectives. The end goal is for the assurance case approach to eventually be a familiar method used within the planetary protection discipline.

6. Conclusions

An assurance case provides a persuasive argument for a claim to be true with supporting evidence. Developing an assurance case provides the ability to think creatively about the design and performance of the future state of a system and the ability to identify risks in a broader context. It is also a communication tool that provides transparency into the decision-making process throughout the project lifecycle, which in turn, increases confidence in the approach.

NASA's OPP has adopted the assurance case approach in the latest updated agency policies for planetary protection, and is currently supporting the development of the assurance case for backward planetary protection for the Mars Sample Return campaign. The assurance case is still a new approach for the discipline of planetary protection, and a patent application analogy has been presented to support scientists and engineers in understanding the approach. OPP will continue to hold workshops, communication events, and publish lessons learned as use of the assurance case approach increases in the planetary protection discipline.

References

[1] National Academies of Sciences, Engineering, and Medicine, Review and Assessment of Planetary Protection Policy Development Processes. Washington, D.C.: The National Academies Press, 2018.

[2] NASA, "NASA System Safety Handbook Volume 2: System Safety Concepts, Guidelines, and Implementation Examples," 2014.

[3] C. B. Weinstock and J. B. Goodenough, "Towards an Assurance Case Practice for Medical Devices," 2009, http://www.sei.cmu.edu, (accessed 27 August 2022).

[4] NASA Office of Safety and Mission Assurance, "OSMA Introduces New Objectives-Based Strategies," https://sma.nasa.gov/news/articles/newsitem/2014/12/04/osma-introduces-new-objectives-based-strategies (accessed 27 August 2022).

[5] American Institute of Chemical Engineers, "Center for Chemical Process Safety (CCPS) Process Safety Glossary," https://www.aiche.org/ccps/resources/glossary/process-safety-glossary/prescriptive-requirement, (accessed Aug. 27, 2022).

[6] Denney, E. and G. Pai, "A Methodology for the Development of Assurance Arguments for Unmanned Aircraft Systems," 2015.

[7] NASA Office of Safety and Mission Assurance, "OSMA Introduces New Objectives-Based Strategies." https://sma.nasa.gov/news/articles/newsitem/2014/12/04/osma-introduces-new-objectives-based-strategies (accessed 27 August 2022).

[8] NASA, "The Case for Safety: The North Sea Piper Alpha Disaster," NASA Safety Center, 2013, https://sma.nasa.gov/docs/default-source/system-failure-case-studies/sfcs-2013-05-06-piperalpha.pdf?sfvrsn=f7a2eff8_3 (accessed 27 August 2022).

[9] NASA, "NASA Procedural Requirement (NPR) 8715.24: Planetary Protection Provisions for Robotic Extraterrestrial Missions," https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8715&s=24 (accessed 27 August 2022).

[10] Meltzer, M., When Biospheres Collide: A History of NASA's Planetary Protection Programs. 2010.
[11] NASA, "Mars Sample Return Mission," https://mars.nasa.gov/msr/, (accessed 28 August 2022).
[12] United States Federal Register, "National Environmental Policy Act; Mars Sample Return Campaign," Doc. Number NASA–22–024; Docket Number–NASA–2022–0002, vol. 87, no. 73, pp. 22578–22581, 2022, https://www.govinfo.gov/content/pkg/FR-2022-04-15/pdf/2022-08088.pdf (accessed 28 August 2022).
[13] NASA Planetary Protection Independent Review Board, "NASA Planetary Protection Independent Review Board (PPIRB) Report," 2019. https://www.nasa.gov/sites/default/files/atoms/files/planetary_protection_board_report_20191018.pdf (accessed 28 August 2022).
[14] International Organization for Standardization, ISO 15026, Part 2, Safety and software assurance case, 2011.
[15] Association for the Advancement of Medical Instrumentation, "AAMI Technical Information Report 38: 2014 Medical device safety assurance case report guidance."
[16] United States Patent and Trademark Office, "General information concerning patents." https://www.uspto.gov/patents/basics/general-information-patents (accessed 28 August 2022).
[17] Mueller, J.M., Patent Law, 4th ed,. New York: Wolters Kluwer Law & Business, 2013.
[18] United States Patent and Trademark Office (USPTO), "Manual of Patent Examining Procedure (MPEP," https://www.uspto.gov/web/offices/pac/mpep/index.html, (accessed 28 August 2022).
[19] Kelly, T.P., "Reviewing Assurance Arguments-A Step-By-Step Approach."
[20] NASA, "NASA Policy Directive (NPD) 8700.1F, 'NASA Policy for Safety and Mission Success,'" https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=8700&s=1F, (accessed 01 September 2022).
[21] Dezfuli, H., C. Everett, R. Youngblood, and C. Everline, "Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework In Line With Evolving Acquisition Strategies and Systems Engineering Practices," 2021, https://ntrs.nasa.gov/citations/20220003490 (accessed 01 September 2022).
[22] NASA, "NASA Technical Standard (NASA-STD) 8719.27, 'Implementing Planetary Protection Requirements for Space Flight,'" 2022, https://standards.nasa.gov/standard/NASA/NASA-STD-871927, (accessed 01 September 2022).