January 2022

Bob Youngblood

Directorate Fellow
Nuclear Science and Technology Directorate
Idaho National Laboratory

Application of Objectives-Driven Assurance Cases to System Development in an Evolving Acquisition Model

R. W. Youngblood,[1] H. C. Everett,[1] H. Dezfuli [2]

[1]Idaho National Laboratory
[2]US National Aeronautics and Space Administration

INL is managed by Battelle Energy Alliance for the US Department of Energy

Idaho National Laboratory

Acknowledgments

- Work at Idaho National Laboratory was performed under Department of Energy Idaho Operations Office Contract DE-AC07-05ID14517, with funding to Idaho National Laboratory provided through a NASA Interagency Purchase Request.
- The present emphasis on the need to focus on management was informed by the large body of literature bearing on the application of safety cases. Of particular significance were the reviews of Piper Alpha and Nimrod, and the treatments found in the UK's Defence Standard 00-56 and MASSC. The present work has not relied on details of these sources, not least because of specific NASA circumstances, but rather has tried to reflect the high-level insights from Piper Alpha and Nimrod, as reflected in the latter documents.
- The authors acknowledge many useful conversations with Chester Everline.

Key Points

- Some aspects of licensing novel reactor designs correspond in part to aspects of the decisions made by the United States National Aeronautics and Space Administration (NASA) in managing the risks of novel space systems. Recent work at NASA in this area contains ideas that may be useful in the reactor arena.
- By promoting a particular kind of focused discussion between acquirers and providers, the use of assurance cases should be particularly valuable, especially under the new acquisition model, in which NASA sometimes obtains systems from outside suppliers rather than developing them in-house.
- In principle, objectives-driven (including “performance-based”) approaches to assurance of performance have significant advantages in cases where they are applicable.
- For truly novel systems, completeness of the safety analysis is a significant issue; it is important for the assurance case to include a commitment by the provider (or applicant) to seriously pursue analysis of operating experience, so that previously unrecognized hazards can be identified and addressed.
- Inquiries into major accidents often point to deficiencies in management oversight in all parts of the life cycle; management processes need to be addressed in the formulation and in the implementation of an assurance case.

Accidents that (among others) have shaped the development of safety case regimes 1: Piper Alpha

- Piper Alpha
  - Piper Alpha was an offshore oil rig in the North Sea that suffered a catastrophic explosion and fire in 1988 with a large loss of life. At the time of the accident, Piper Alpha was not under a safety-case regime.
  - The Cullen inquiry into the accident described numerous deficiencies in design and operation, and recommended a safety-case approach. Subsequent legislation imposed a safety-case approach.
  - Cullen, speaking 25 years later:
    - "And as I dug down to the background of what happened, I discovered it was not just a matter of technical or human failure. As is often the case, such failures are indicators of underlying weaknesses in management of safety."

Accidents that (among others) have shaped the development of safety case regimes 2: Nimrod

Nimrod XV230 was a Royal Air Force aircraft that suffered a fire during a mission in Afghanistan in 2006, leading to the deaths of all aboard (14 lives lost). Nimrod had a safety case, but according to the Haddon-Cave inquiry:

Loss of XV230 avoidable

9. The Nimrod Safety Case was drawn up between 2001 and 2005 by BAE Systems (Phases 1 and 2) and the MOD Nimrod Integrated Project Team (Third Phase), with QinetiQ acting as independent advisor. The Nimrod Safety Case represented the best opportunity to capture the serious design flaws in the Nimrod which had lain dormant for years. If the Nimrod Safety Case had been drawn up with proper skill, care and attention, the catastrophic fire risks to the Nimrod MR2 fleet presented by the Cross-Feed/SCP duct and the Air-to-Air Refuelling modification would have been identified and dealt with, and the loss of XV230 in September 2006 would have been avoided.

Lamentable job

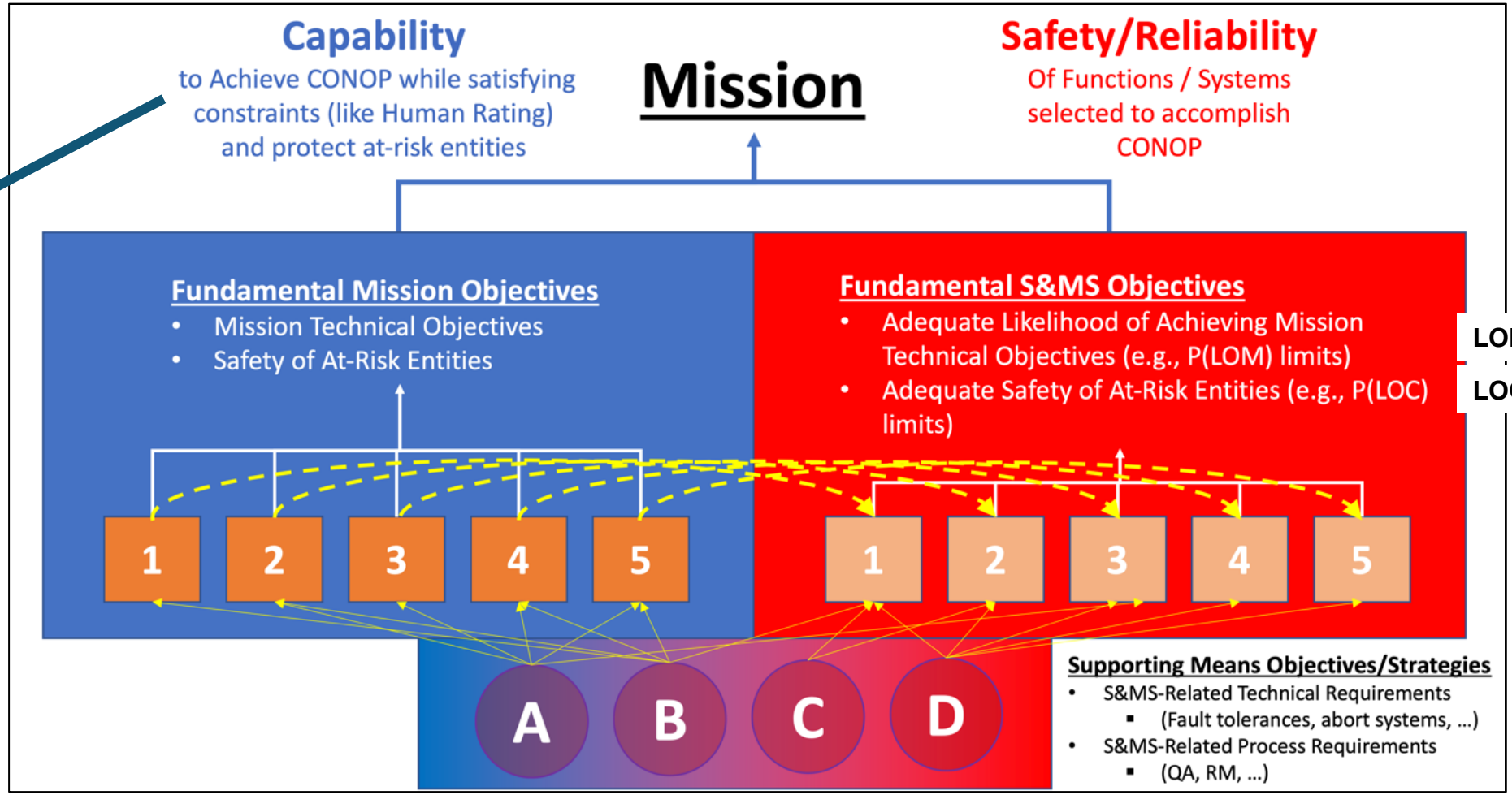
10. Unfortunately, the Nimrod Safety Case was a lamentable job from start to finish. It was riddled with errors. It missed the key dangers. Its production is a story of incompetence, complacency, and cynicism. The best opportunity to prevent the accident to XV230 was, tragically, lost. (Chapters 10A and 10B)

General malaise

11. The Nimrod Safety Case process was fatally undermined by a general malaise: a widespread assumption by those involved that the Nimrod was 'safe anyway' (because it had successfully flown for 30 years) and the task of drawing up the Safety Case became essentially a paperwork and 'tickbox' exercise. (Chapter 11)

Relationship between Fundamental NASA Mission Objectives and Fundamental Safety and Mission Success (S&MS) Objectives

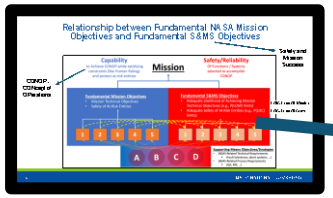
CONOP: CONcept of OPerations



LOM: Loss Of Mission

LOC: Loss Of Crew

The "W-Engine" for S&MS assurance in a given life cycle phase.



Technical Authorities (TAs) for Engineering, Safety and Mission Assurance, and Health and Medical interests independently oversee technical aspects of programs and projects; they are appointed and funded separately from programs and projects to assure their independence.

From Program/Project Initialization

Fundamental S&MS Objectives, Levied S&MS-Related Technical and Process Requirements, S&MS Success Criteria

Planning the Phase

Execution of the Phase

LCR of the Phase

Life Cycle Review

1 Acquirer/Provider Review/Adjust S&MS Success Criteria as Needed Given Development to Date (with TA involvement)

2A Develop a detailed S&MS Plan for the Phase

2B Develop an S&MS Argument for the Validity of the S&MS Plan

3 TAs Evaluate S&MS Argument

4 Acquirer/Provider Negotiate Audit Support & Reporting Requirements (with TA involvement)

5 Evaluate S&MS Argument, Grant Authority to Proceed to Execution, Accept Risk

6A Execute Phase & Produce S&MS Evidence for the Phase

6B Acquirer, TA Oversee Provider Processes

7 Update the Phase's S&MS Argument in Light of Execution and Incorporate the Argument & Evidence into the S&MS Assurance Case

8 TAs Evaluate S&MS Case

9 Evaluate S&MS Assurance Case, Mandate Corrective Actions, Grant Authority to Proceed to Next Phase, Accept Risk

alidation*

erification**

From the Previous Phase

To the Next Phase

* Executing the right plan

** Executing the plan right

Acquirer | TAs | Provider

Iterations / feedbacks are not shown in this process diagram

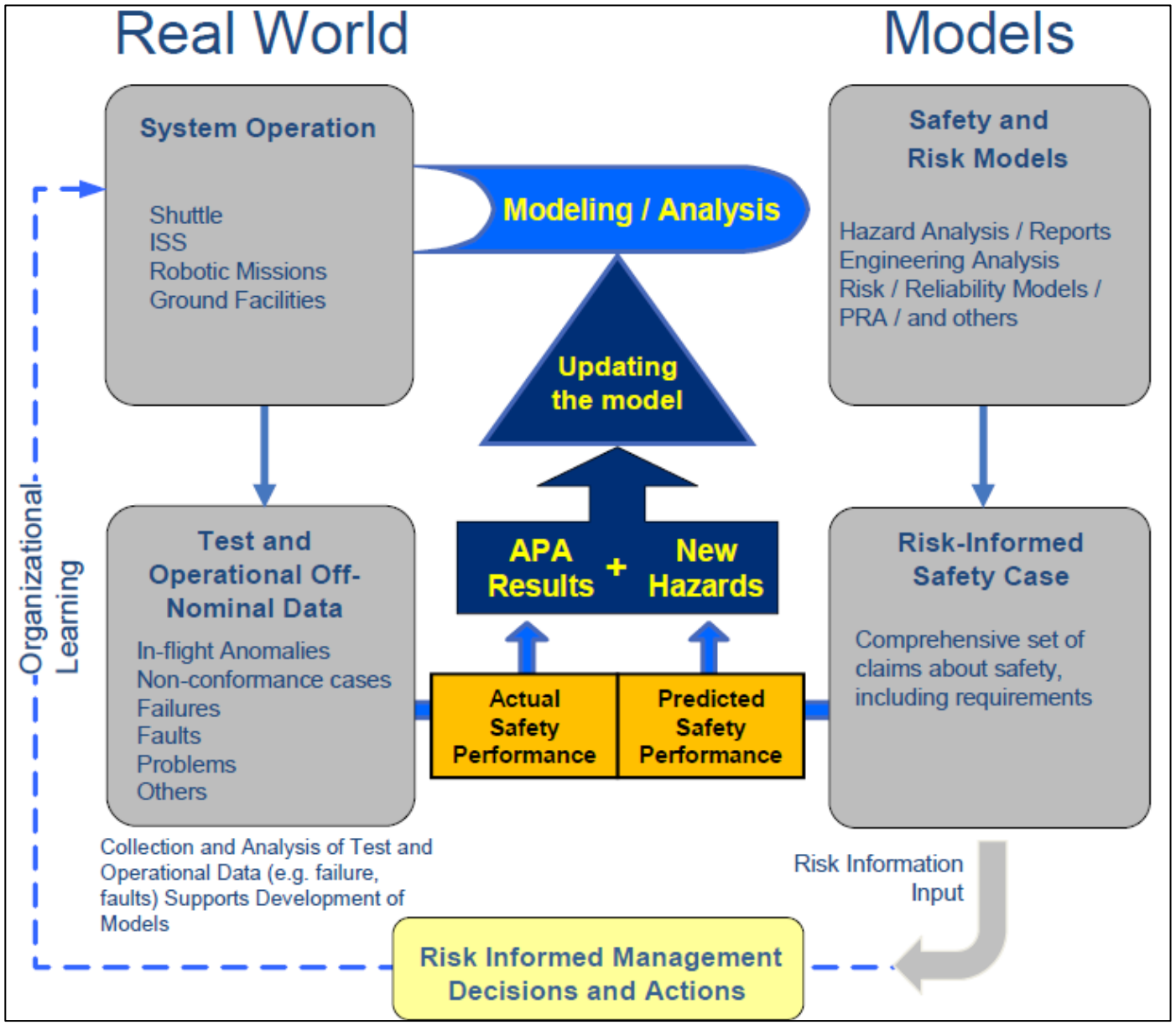
What the Assurance Case Should Include in order to support that decision:

S&MS Assurance Element	Comments
Mission S&MS performance is adequately understood.	Mission hazards are well understood; the response of the system to hazardous events/faults/failures is well characterized; and mishap consequences and likelihoods are adequately defined, at a level of detail commensurate with the current level of mission/system definition. Risk-significant uncertainties in any of the above are identified and characterized.
The boundaries and assumptions within which S&MS performance is evaluated are understood.	The boundaries and assumptions within which acceptable mission S&MS performance is to be achieved are defined, including the concept of operations, system definition, environmental stress limits, operational limits, system condition, extent of personnel training, etc.
Effective S&MS-related management processes and controls are in place.	The Provider's S&MS-related management processes and controls (e.g., risk management, quality, software assurance, configuration management) are compliant with all levied and agreed-upon S&MS-related process standards; S&MS is managed holistically as an integrated part of a management system that includes other mission execution domains (e.g., cost, schedule); audits and reports indicate a robust safety culture; systems are in place to effectively identify and manage emerging risks (e.g., precursors); processes for post-flight data review and lessons learned are effective; risk acceptance procedures are adequately formalized and technically sound; etc.
Mission S&MS performance meets (or is forecasted to meet) minimum tolerable levels of mission S&MS performance	Assessed S&MS performance provides adequate confidence that minimum tolerable levels of S&MS performance will be met, considering the work to be done (e.g., S&MS-related technology maturation, hazard control development) and accounting for all hazards, including those not yet identified.
Mission safety performance is (or will be) As Safe as Reasonably Practicable (ASARP)	System/mission definition decisions have been risk-informed, involving adequate trade studies and the prioritization of safety in decision-making, with documented rationales; plans and processes are in place to ensure future decisions are ASARP.
Mission complies with all Acquirer-levied S&MS-related requirements	Per defined verification protocols.

S&MS: Safety and Mission Success
ASARP: As Safe as Reasonably Practicable

Real World vs. Models:

Information Flow in the APA [Accident Precursor Analysis] Context



Summary (1 of 2)

- NASA's Office of Safety and Mission Assurance is working to develop and implement an approach to assurance of Safety and Mission Success (S&MS) that makes essential use of Assurance Cases and of management processes intended to provide greater assurance of success in the development process itself.
- This has been occasioned in part by fundamental changes in NASA's acquisition model, in which major developments that would have been carried out in-house will now be carried out by commercial providers.
- Under these conditions, real effort is needed to assure that Providers and Acquirers have a detailed common understanding of what will be done, based on a considered objectives hierarchy, a carefully formulated plan of work in each phase, and assurance at the end of the phase that the work has successfully followed the plan.
- The objectives-driven framework discussed here is meant to promote successful development and deployment with more assurance than is to be had from applying the existing piecemeal prescriptive requirements.

Summary (2 of 2)

- Within this framework, certain topics suggest themselves for consideration in the context of licensing novel reactor technologies:
  1. The “Assurance Case” idea:
     - Some countries have long since made extensive use of the Assurance Case idea in many areas; it has been applied less widely in the US but is presently emerging in the context of reactor licensing (e.g., the Licensing Modernization Project*). The concept of an objectives-driven assurance case is very relevant to development and permitting of a truly novel technology.
     - Completeness of our technical understanding is a real issue for a truly novel technology, and the assurance case framework promotes thoughtful consideration by all parties involved.
  2. Having the “case” artifact is not enough.
  3. Learning from experience: Another important consideration for truly novel technologies is a considered and ongoing process for learning from experience. Some form of this has been ongoing for many years, but not necessarily with an optimal emphasis.

* NEI 18-04 Rev. 1

References (1 of 3)

[1] NUCLEAR ENERGY INSTITUTE, Risk-Informed Performance-Based Technology Inclusive Guidance for Non-Light Water Reactor Licensing Basis Development, Report Revision 1, August 2019, Nuclear Energy Institute, Washington DC, 2019.

[2] AFZALI, A., Technology Inclusive Guidance for Non-Light Water Reactor Safety Analysis Report: Content for a Licensing Modernization Project-Based Affirmative Safety Case, internal report, Southern Company, Washington, DC, 2021.

[3] NRC, PART 53—RISK-INFORMED, TECHNOLOGY-INCLUSIVE REGULATORY FRAMEWORK FOR COMMERCIAL NUCLEAR PLANTS, Consolidated Part 53 Preliminary Proposed Rule Language, February 2022 (ADAMS Accession Number ML22024A066).

[4] DEZFULI, H., et al., Modernizing NASA's Space Flight Safety and Mission Success (S&MS) Assurance Framework in Line with Evolving Acquisition Strategies and Systems Engineering Practices, Office of Safety and Mission Assurance, National Aeronautics and Space Administration, NASA Headquarters, Washington, D.C. (June 2021). Available at https://ntrs.nasa.gov/citations/20220003490. This site not only contains a link to the white paper, but also addresses copyright, stating "Public Use Permitted."

[5] APOSTOLAKIS, G., How Useful Is Quantitative Risk Assessment?, Risk Analysis 24, No. 3, pp 515-520 (Society for Risk Analysis, 2004)

[6] ISO/IEC/IEEE 15026, Parts 1, 2, 3, 4, Systems and software engineering -, Systems and software assurance –, ISO, the International Organization for Standardization and IEC, the International Electrotechnical Commission (Switzerland, 2019).

References (2 of 3)

[7] CULLEN W. D., The Public Inquiry into the Piper Alpha Disaster, Her Majesty's Stationery Office (London, 1990).

[8] HADDON-CAVE, C., An Independent Review into the Broader Issues Surrounding the Loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, The Stationery House Limited (London, 2009).

[9] Defence Standard 00-56, Safety Management Requirements for Defence Systems, Part 1: Requirements ([UK] Ministry of Defence, 2017).

[10] Defence Standard 00-56, Safety Management Requirements for Defence Systems, Part 2: Guidance on Establishing a Means of Complying with Part 1 ([UK] Ministry of Defence, 2017).

[11] Manual of Air System Safety Cases, Military Aviation Authority ([UK] Defence Safety Authority, 2019)

[12] [US] NRC INSPECTION MANUAL, Part 9900: Technical Guidance, Operation - Safety and Compliance (Reactivation of identical TG inadvertently deleted from the Inspection Manual on March 9, 2007, ML003753992, USNRC, 2007).

[13] ROGERS W. P. et al., Report to the President by the PRESIDENTIAL COMMISSION On the Space Shuttle Challenger Accident, National Aeronautics and Space Administration (Washington, DC, 1986).

[14] Columbia Accident Investigation Board Report (NASA, 2003)

[15] GROEN F. et al., Nasa Accident Precursor Analysis Handbook, NASA/SP-2011-3423 (NASA, 2011). Note that the web site for download of this document (ntrs.nasa.gov/citations/20120003292) states "public use permitted."

References (3 of 3)

[16] Accident Sequence Precursor (ASP) Program page on the NRC Web Site, https://www.nrc.gov/about-nrc/regulatory/research/asp.html .

[17] NUCLEAR REGULATION / NRC Needs to More Aggressively and Comprehensively Resolve Issues Related to the Davis-Besse Nuclear Power Plant's Shutdown, GAO-04-415 (US Government Accountability Office, 2004).

[18] International Space Station (ISS) EVA Suit Water Intrusion / High Visibility Close Call, IRIS Case Number: S–2013–199–00005 (NASA, 2013).

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.