Long-Term Viability of Underground Natural Gas Storage in California

An Independent Review of Scientific and Technical Information

Chapter 1, Section 1.6
Risk mitigation and management

Robert J. Budnitz[1], Giorgia Bettin[2], Tom Tomastik[3], and Curtis M. Oldenburg[4]

[1] Robert J. Budnitz Scientific Consulting, Berkeley, CA; [2]Sandia National Laboratories, Albuquerque, NM; [3]ALL Consulting, LLC, Galena, OH; [4]Energy Geosciences Division Lawrence Berkeley National Laboratory, Berkeley, CA

California Council on Science and Technology

December 2017

Long-Term Viability of Underground Natural Gas Storage in California

An Independent Review of Scientific and Technical Information

Jane C.S. Long, PhD, Independent Consultant
Steering Committee Co-Chair

Jens T. Birkholzer, PhD, Lawrence Berkeley National Laboratory
Steering Committee Co-Chair

Amber J. Mace, PhD, California Council on Science and Technology
Project Director

Sarah E. Brady, PhD, California Council on Science and Technology
Project Manager

Steering Committee Members
J. Daniel Arthur, P.E., SPEC, ALL Consulting L.L.C
Riley M. Duren, P.E., NASA Jet Propulsion Laboratory
Karen Edson, retired California Independent System Operator
Robert B. Jackson, PhD, Stanford University
Michael L.B. Jerrett, PhD, University of California, Los Angeles
Najmedin Meshkati, PhD, University of Southern California
Scott A. Perfect, PhD, Lawrence Livermore National Laboratory
Terence Thorn, JKM Energy and Environmental Consulting
Samuel J. Traina, PhD, University of California, Merced
Michael W. Wara, PhD, Stanford Law School

Non-Voting Ex Officio Steering Committee Members
Catherine M. Elder, M.P.P; Aspen Environmental Group (Technical Expert)
Jeffery Greenblatt, PhD; Lawrence Berkeley National Laboratory (Author)
Curtis M. Oldenburg, PhD; Lawrence Berkeley National Laboratory (Author)

Acknowledgments

This report has been prepared by the California Council on Science and Technology (CCST) with funding from the California Public Utilities Commission.

Copyright

 ISBN Number: 978-1-930117-86-0 Long-Term Viability of Underground Natural Gas Storage in California: An Independent Review of Scientific and Technical Information

About CCST

The California Council on Science and Technology is a nonpartisan, nonprofit organization established via the California State Legislature in 1988. CCST engages leading experts in science and technology to advise state policymakers- ensuring that California policy is strengthened and informed by scientific knowledge, research, and innovation. CCST responds to the Governor, the Legislature, and other State entities who request independent assessment of public policy issues affecting the State of California relating to science and technology.

Note

The California Council on Science and Technology (CCST) has made every reasonable effort to assure the accuracy of the information in this publication. However, the contents of this publication are subject to changes, omissions, and errors, and CCST does not accept responsibility for any inaccuracies that may occur.

For questions or comments on this publication contact: California Council on Science and Technology 1130 K Street, Suite 280 Sacramento, CA 95814

916-492-0996

ccst@ccst.us www.ccst.us

Layout by a Graphic Advantage! 3901 Carter Street #2, Riverside, CA 92501

www.agraphicadvantage.com

1.6 RISK MITIGATION AND MANAGEMENT

1.6.1 Abstract

This section reviews (1) key elements that must be included in an effective risk management plan (RMP) for a UGS facility; (2) potential additional practices that could improve UGS integrity; and (3) regulatory changes under way by DOGGR covering UGS integrity, with comments on the new CARB methane monitoring regulations for context. We outline the elements of a well-conceived site-specific RMP that must be based on a formal quantitative risk assessment (QRA), and we provide guidance on methodologies to perform rigorous risk assessment. We also provide guidance on a range of other attributes that an RMP must contain. Underlying effective risk management is the idea that there are risk targets or goals, the attainment of which guides risk mitigation activities. Our analysis includes a critique, with recommendations, of the draft DOGGR UGS regulation published May 19, 2017 that is under consideration at the time of writing this section. Some of the specific recommendations relate to the requirements for a site-specific RMP at a UGS site, including the need for each UGS facility to perform a quantitative risk analysis, to perform regular training of the operational staff using written procedures, and to collect failure data and off-normal event data to be compiled in a publicly available database. The current DOGGR draft regulation should explicitly address the importance and role of human and organizational factors, as well as safety culture. Another recommendation relates to the need for DOGGR or the industry to develop risk targets or goals to guide decision-making, while still other recommendations relate to specific sections of the draft regulations that require various monitoring and measurement activities to assess and mitigate well integrity issues.

1.6.2 Introduction and High-Level Conclusions/Recommendations

1.6.2.1 Introduction

In California, the subsurface portions of UGS facilities have been regulated on the state level by DOGGR, both prior to and since the Aliso Canyon incident. DOGGR considers the subsurface portion as including the reservoir used for storage, the confining caprock, gas storage wells and wellheads, observation wells, and any other wells approved for use in the project. The California Public Utilities Commission (CPUC) regulates the surface infrastructure at UGS facilities. The California Air Resources Board (CARB) regulates greenhouse gas (GHG) emissions from UGS facilities as of October 1, 2017 (CARB 2017c). Until early 2017, federal regulation did not provide operational, safety, or environmental standards for the subsurface portions of UGS. Although the Natural Gas Pipeline Safety Act of 1968 has been found by a U.S. District Court to provide authority to PHMSA (the U.S. Pipeline and Hazardous Materials Safety Administration) over such facilities, until 2017 the agency declined to develop regulations around them, stating in a 1997 Advisory Bulletin that operators should consult industry guidelines and state regulations on the subject. Meanwhile, underground gas storage has been excluded from the U.S. EPA's Underground Injection Control program which regulates various types of fluid injection into the subsurface under the Safe Drinking Water Act (e.g., liquid waste, oil and gas waste water, CO_2, etc.).

In the immediate aftermath of the 2015 Aliso Canyon incident, DOGGR moved ahead to develop emergency regulations (California Natural Resources Agency, 2016) for the existing UGS facilities in the State. These emergency regulations were intended to quickly and efficiently reduce the LOC risk of these facilities, focusing mainly on the subsurface portion of UGS as described above. These emergency regulations will be superseded in January 2018 by permanent regulations now under development. DOGGR published on May 19, 2017 a draft of these new permanent regulations (California Natural Resources Agency, 2017), which we reviewed in this study. In addition to various new technical and administrative requirements, the emergency regulations and the proposed new permanent regulations require that each UGS facility in California must develop and implement a Risk Management Plan (RMP) with certain specified features.

Meanwhile, in December 2016, PHMSA introduced an Interim Final Rule (IFR) that incorporated two American Petroleum Institute (API) Recommended Practices (RP) (API RP 1170, "Design and Operation of Solution- mined Salt Caverns used for Natural Gas Storage," issued in July 2015 (17), and API RP 1171, "Functional Integrity of Natural Gas Storage in Depleted Hydrocarbon Reservoirs and Aquifer Reservoirs," issued in September 2015). The IFR became effective as of January 18, 2017. States are now required to adopt the federal standards but they may certify, as did California, to act as PHMSA's agent and impose their own rules that go beyond the federal standard. DOGGR's interim and proposed final rules go beyond PHMSA's IFR recommended practices. These are the rules that we have reviewed in this study, results of which are given below.

The five prior sections of this report (Sections 1.1-1.5) document and review the state of UGS in California and its attendant risks to workers, the public, the environment (e.g., via GHG emissions), and to gas supply reliability. In the section below (Section 1.6.2), we evaluate and discuss the risk management plans (RMPs) as they are specified and described by DOGGR in its draft regulations. Following that discussion, we present (in Section 1.6.3) additional elements of risk management that should be included in the required RMPs. Finally (in Section 1.6.4), we present some notes and recommendations regarding the regulation of UGS and the requirements of the proposed new DOGGR regulations (California Natural Resources Agency, 2017) in particular, along with comment on the new CARB regulations (CARB, 2017c).

1.6.2.2 High Level Conclusions and Recommendations

This section (Section 1.6) contains a number of conclusions and recommendations on various topics, some of which are highly specific and, although important, do not rise to the level of having policy implications. However, some of these conclusions and recommendations are judged to be of greater importance than the others, and they are presented in full here at the beginning of Section 1.6, with the understanding that the remaining text of Section 1.6 provides the basis and support of the following high-level conclusions recommendations.

Overall Assessment of DOGGR's New Emergency and Proposed Draft Regulations

Finding: The draft DOGGR regulations that will govern subsurface operations at UGS facilities in California contain numerous important provisions that will make UGS safer, and that will also allow for a better understanding of the levels of safety achieved at any specific UGS facility.

Conclusion: The existence of both the emergency DOGGR regulations now in place (California Natural Resources Agency, 2016) and the draft permanent regulations still under development (California Natural Resources Agency, 2017) represents a major step to reduce risk of LOC, particularly the requirement for each facility to provide a risk management plan; the requirement of the use of two barriers in wells, e.g., use of tubing and packer; and the requirements for well testing and monitoring. We conclude that the new regulations should profoundly improve well integrity at UGS facilities in California. (See Conclusion 1.14 in the Summary Report.)

Evaluating Risk Management Plans as a Major Element of UGS Integrity

Finding: One of the major and most important elements of both the emergency regulations and the draft permanent regulations is that each UGS facility in California must develop and implement a Risk Management Plan (RMP) with certain specified features as follows: "RMPs shall include a description of the methodology employed to conduct the risk assessment and identify prevention protocols, with references to any third-party guidance followed in developing the methodology. The methodology shall include at least the following: (1) Identification of potential threats and hazards associated with operation of the underground gas storage project; (2) Evaluation of probability of threats, hazards, and consequences related to the events."

Conclusion: Requiring risk management plans and risk assessment studies for each facility is an important step in ensuring UGS integrity, but the draft permanent regulations do not contain enough guidance as to what the risk assessment methodology needs to provide. (See Conclusion 1.15 in the Summary Report.)

Recommendation: We suggest that DOGGR make further clarifications and specifications in the risk management plan requirements as follows: (1) the need for each UGS facility to develop a formal quantitative risk assessment (QRA), to understand the risks that the facility poses to various risk endpoints (such as worker safety, health of the offsite population, release of methane, property damage, etc.), and (2) the need to develop a risk target or goal for each risk endpoint that each facility should stay below and that is agreed to by the regulator (DOGGR), rather than written into an enforceable government regulation. These two needs, if satisfied, will provide the basis for rational and defensible risk-management decision-making that would not be possible without results from a formal risk assessment and defined risk targets and goals. We also provide guidance on a range of other attributes that an RMP must contain, including (1) consideration of human and organizational factors as well as traits of a healthy safety culture, and (2) recommendations regarding intervention and emergency response planning. (See Recommendation 1.15 in the Summary Report.)

As the text in this section explains, the development of the site-specific risk analyses can be accomplished in stages, the first stage being a scoping analysis to provide a short-term understanding at each UGS facility of the various risks and the issues that give rise to those risks. These risks can arise from natural hazards, from equipment failures either below or above ground, from human errors and organizational problems, or from a variety of other sources. These short-term scoping studies, to be supplemented later by more detailed analyses, can provide early guidance to decision-makers about what interventions may be needed, if it is concluded that some of the risks require early intervention to reduce either their likelihood of occurring or their consequences. We emphasize that the QRA recommended here need not be an exhaustive probabilistic risk assessment requiring multiple man-years of effort for every conceivable failure scenario, although it is always important to support any such analysis with relevant data that have an adequate pedigree in terms of quality. Instead, we recommend that a formal and practical risk assessment be carried out for the most important risk categories and failure scenarios. The state-of-the-art QRAs currently offered by several engineering consulting companies can provide the adequate rigor. In parallel, an activity needs to begin promptly to develop the risk targets or goals that will ultimately guide risk-mitigation decision-making. Whether this process should be led by the industry or by a government agency is a decision that is beyond the remit of this CCST study; however, the development process definitely requires broad stakeholder input.

Recommendations Regarding Specific Well Integrity Requirements

Finding: The proposed regulations contain various technical requirements for (1) well construction, (2) mechanical integrity testing, (3) monitoring, (4) inspection, testing, and maintenance of wellheads and valves, (5) well decommissioning, and (6) data and reporting. Overall, the Steering Committee finds these requirements a major step forward to improve well integrity in UGS facilities. In terms of the detailed specifications, the committee has several suggestions for revision, e.g., to clarify ambiguous language, provide additional specification, ensure consistency with industry standards, and balance the benefit of frequent testing with the risk to aging wells from installing instrumentation. These detailed suggestions are given in Section 1.6.4 of the report.

Conclusion: The technical requirements for wells provided in the draft DOGGR regulations contain many provisions that are expected to enhance the safety of well operations at the UGS facilities in California. As with any new regulation, application in the practice over time will be an ultimate test, with an “effective” regulatory framework being one that enhances safety to the point that risks are acceptable, while not placing unnecessary burden on operators. (See Conclusion 1.16 in the Summary Report.)

Recommendation: We recommend that DOGGR considers several detailed suggestions made in this Section 1.6 to improve the specific well integrity requirements in the draft regulations. Also, we recommend that the finalized regulations be reevaluated after perhaps five years of application. (See Recommendation 1.16 in the Summary Report.)

Need for Regular Peer Review or Auditing of New DOGGR Regulations

Finding: It is a common practice in many fields to evaluate the effectiveness of regulations, in particular those that may have been newly developed, on a regular basis by peer-review teams or auditing teams. For example, the Groundwater Protection Council (GWPC) organizes peer reviews of the Class II Underground Injection Control Program in certain states to which the U.S. EPA has delegated regulatory authority. (Class II wells are used only to inject fluids associated with oil and natural gas production—not gas storage.) The peer reviews typically include regulators from other states that are involved in those same programs, but may also involve stakeholders from academia and environmental organizations. Although many different approaches have been used and models for organizing them are widespread, one possible suggestion is to use the Interstate Oil and Gas Compact Commission (IOGCC) to help with this review.

Conclusion: Conducting a peer review or audit of the new DOGGR regulations after a few years of implementation would ensure that (1) the latest science, engineering, and policy knowledge is reflected to provide the highest level of safety, (2) these regulations are consistently applied and enforced across all storage facilities and are thoroughly reviewed for compliance, (3) an appropriate safety culture has been fully embraced by operators and regulators, and finally (4) the regulator has the necessary expert knowledge to conduct a rigorous review of the regulatory requirements. (See Conclusion 1.17 in the Summary Report.)

In contrast to purely prescriptive regulations, the risk management planning and analysis to be conducted as part of DOGGR's new regulations requires judgment-based decisions by the risk "assessor" where expert knowledge comes into play. A risk analysis, for example, requires decisions about which risk scenarios to consider (or not), the probability associated with a certain accident scenario, or what the uncertainties are about probabilities and impacts. It follows that regulatory review of such risk analysis requires expert knowledge in order to agree or disagree with the assumptions going into the analysis.

Recommendation: The Governor should ensure that the effectiveness of the DOGGR regulations and the rigor of their application in practice be evaluated by a mandatory, independent, and transparent review program. Reviews should be conducted at regular intervals (e.g., every five years) following a consistent set of audit protocols, to be applied across all storage facilities. Review teams would ideally be selected from a broad set of experts and stakeholders, such as regulators from related fields in other states, academia, consultants, and environmental groups. Results from the mandatory review should be published in a publicly available report, with an opportunity for public comment.

Responsibility for the design and execution of the review program should either be with a lead agency designated by the Governor, or alternatively could be assigned to an independent safety review board appointed by the Governor. (See Recommendation 1.17 in the Summary Report.)

1.6.3 Risk Management Plans related to UGS integrity -- review and evaluation of key RMP elements and of DOGGR's proposed RMP regulations

1.6.3.1 Introduction and Objectives

The handling of high-pressure natural gas during UGS operations entails risk, i.e., the possibility (non-zero likelihood) of failure with consequences (e.g., injury, death, environmental contamination, and property damage). Risk at UGS facilities can be managed and reduced, but never driven to zero. Risks need to be managed by careful assessment, including the analysis of what UGS components or operations entail the most risk and how these risks can be reduced, and by proactively monitoring the operations to detect and address potential failures of various components before they fail, causing a potentially catastrophic incident.

Risk is an expression of the likelihood that an event leading to a loss or to other undesired consequences may occur, and the magnitude of those potential consequences if it does occur. Risk can therefore be lowered by reducing the likelihood of occurrence or the severity of consequences, or both. Preventing any initial failure from occurring is arguably the most effective way to reduce the risk of causing harm to people or to the environment. Risk assessment in the UGS industry focuses primarily on the estimation of risk to the public safety.

Risk assessment is both a design tool and a valuable tool for ranking potential risks during the operating lifetime of a storage facility, for prioritizing operational efforts to reduce the likelihood of leakage, and for guiding emergency planning. It can be used to assist decision-making on future land use in the vicinity of the pipelines and facility.

The first objective of this section (and of Task 1.6.3) is to provide *recommendations* as to what should be the scope and level of detail of a Risk Management Plan (RMP) to be used by the operator of a UGS facility, so as to assure its integrity against both catastrophic incidents and less serious loss-of-containment (LOC) scenarios including long-term or chronic leakage scenarios. The second objective is to *evaluate the RMP requirements in the draft DOGGR regulation* now under consideration.

As an introduction, we note here that the draft DOGGR regulations that govern subsurface operations at UGS facilities (California Natural Resources Agency, 2016) contain numerous important provisions that will make UGS safer, and that will also allow for a better understanding of the levels of safety achieved at any specific UGS facility. The existence of both the emergency DOGGR regulations now in place and the newer (final) ones still under development (California Natural Resources Agency, 2017) definitely represents a major step to reduce the likelihood of another SS-25-type incident, particularly due to the requirement of the use of two barriers in wells, e.g., use of tubing and packer (see the discussion of DOGGR's proposed new regulatory requirement 1726.5 below in Section 1.6.4.3).

Below, the seven elements of an effective Risk Management Plan will be described. We will also provide below a review and evaluation of the RMP requirements in the draft final DOGGR regulations. Our evaluation concludes that in many areas, the RMP requirements are effective and adequate, e.g., in the areas of emergency preparedness, documentation, and updating of the RMP, but in some other areas *they fall short of what is necessary* to assure that each individual UGS facility in California has an effective RMP that its management can use to manage the facility's risk effectively.

1.6.3.2 Background

In the aftermath of the 2015 Aliso Canyon incident, emergency regulations were developed (California Natural Resources Agency, 2016) governing certain activities at the 12 existing UGS facilities in California. These emergency regulations were intended to quickly and efficiently reduce the LOC risk of these facilities. These emergency regulations will be superseded by permanent regulations that are now under development (California Natural Resources Agency, 2017).

One of the major elements of both the emergency regulations and the proposed new permanent regulations is that each UGS facility in California must develop and implement a Risk Management Plan (RMP) with certain specified features. In response to the emergency regulations, each of the UGS facilities in California developed such a plan, but these are currently only tentative, and updated RMPs will need to be developed and submitted when the final regulations come into force.

There are a number of different types of consequences related to LOC that a UGS facility poses, and each needs to be managed separately. For example, LOC can arise from hazards affecting the subsurface and lead to impacts to groundwater (underground sources of drinking water (USDW)), or LOC can be acute and above ground, with potential for fueling fires and explosions with resulting injury or death at the site, or LOC can be slow and chronic, leading to GHG emissions that affect climate. As these examples suggest, consequences and the risks associated with them fall into different categories, and we will use the term *"risk category"* to refer to them.

Risk category – a definition: Here the term *risk category* is important to understand. If there is an off-normal event, be it minor or major, there are different end-points of concern, each of which maps into a "category" of risk. The most important risk categories are risks to the *public health and safety*, to the facility's *workers*, to the *environment* and *natural resources*, and to the facility's *infrastructure*. Each must be "managed," and each must be kept below whatever "acceptable" level has been established. (See Section 1.6.3.3 below.)

A facility's Risk Management Plan may or may not address all of these categories, and if mandated by regulations, the level of concern for the different risk categories may vary.

1.6.3.3 Acceptability of the Various Risks: Risk Targets, Risk Goals, Risk Acceptability Criteria

For any facility, the need for a Risk Management Plan rests fundamentally on the notion that the facility poses non-zero risks in each of the various "risk categories," and that those risks must be managed. Hence, the notion that a facility can continue to operate rests, either implicitly or explicitly, on the acceptability of the risks that it poses.

For most industrial activities—indeed, for most human endeavors more generally—society has not established explicit risk criteria that are used in determining whether the risks involved with that activity are "acceptable." This is as true for UGS facilities as it is for most other similar facilities. Given the difficulty of defining acceptable risks, an alternative approach, sometimes used in other technical areas, is the use of *risk "targets" or "goals*,*"* which do not have the force of explicit (go-no-go) specified acceptability criteria, but which provide to the facility operators and the public a *notional expression of a goal or target*, expressing the range of risk levels that are judged to be acceptable.

It is important to understand the distinctions between these various ideas, so to be clear about what the words mean, they will be explained (as we use them here) as follows.

- A *risk criterion* would be a level of risk that is in a regulation, and which is enforced in the sense that if the risk posed by a facility exceeds the criterion, the facility is in violation.

- A *risk target* or *risk goal* (and these two words are effectively synonyms in our usage and in how the community of risk professionals uses them) would be a level of risk that is agreed to by an industry-wide consensus and to which the regulatory agency concurs, rather than something written into an enforceable government regulation.

- The words *"risk target"* or "risk goal" mean that the management at each facility would know that it is <u>expected</u> to try to do what it can, within sensible technical and financial constraints, to achieve the goal or target, but that if the facility does not succeed, operations can continue if a reasonable explanation can be provided to the regulator about why the goal or target cannot be achieved, and the regulator agrees to allow continued operation.

As will be explained below, decision-makers who are charged with managing risks should have some sort of risk target or goal for each risk category in order to provide a basis for deciding how to go about risk management in a rational, defensible, and transparent way.

Unfortunately, no risk targets, risk goals, or risk acceptability criteria now exist for UGS facilities, which means that considerable judgment is required to support the risk decisions made pursuant to any UGS Risk Management Plan (or the risk decisions pursuant to any specific government regulatory scheme that aims at regulating UGS risks). This is true even if a technically strong risk assessment has been performed, an issue to be discussed below. This shortcoming, this absence of any risk targets, goals, or acceptability criteria, makes both the development of USG Risk Management Plans and their use complicated and controversial.

There is, of course, always a danger that if strict risk criteria, or even risk targets or goals, become an overarching end-in-themselves, the result could be that a facility's managers and operators will come to believe that achieving them means that the facility if *safe enough* – that is, that *no further safety improvements are needed.* This is an incorrect interpretation of what is intended here. Another crucial element of an appropriate safety philosophy is that even if the risk goals or targets (or risk criteria) are met, one must always strive to do better, while still accounting for the costs and other burdens involved. This is the "ALARA" concept (as low as reasonably achievable), which is discussed below in a separate side bar at the end of this section.

Recommendation: It is recommended that either DOGGR (as part of its regulations or policies) or the industry (perhaps through an industry consortium) determine, for each category of risk, a threshold level of risk, and promulgate these threshold levels as risk targets or goals. There are many possible ways in which a risk target or goal might be formulated, and of course for every risk category, a different target or goal is necessary. An example or two may suffice to provide the general idea.

One possible way of formulating a risk target or goal might be along these lines.

> *It should be the target or goal for each UGS facility that any uncontrolled release of methane to the environment larger than XX kilograms over a 24-hour period should have a mean annual likelihood lower than 10^{-4} per year.*
>
> *It should be the target or goal for each UGS facility that any accident at the facility or any uncontrolled release of methane to the environment that causes severe injuries or deaths of more than XX workers should have a mean annual likelihood lower than 10^{-5} per year.*

The numbers (XX) in these targets or goals are left unwritten here, and likelihoods are provided just as placeholders, for a good reason. Without a public process to obtain inputs from both the general public and the affected facilities, there is no way to know what the numbers should be; that is a policy issue that is beyond the scope here. But the numerical levels should not be set except after the give-and-take of an open and transparent public process. Also, when these targets or goals are being developed, it is vital that one describe just how risk will be managed using the targets or goals through engineering design, through operations, through measurements of various parameters, through the collection of failure data and human-error data to support the risk models, and so on.

It is also important that the process of developing these targets or goals keep at the forefront that the principal users of them will be decision-makers who manage risk, regulatory agencies who oversee the facilities, and members of the public who rightly want to know how much risk there is and how it is being managed. All of them deserve these targets or goals as a crucial tool in supporting their own decisions. The basic requirement in the draft DOGGR regulations concerning this issue is in the following sentence, taken from 1726.3(a):

> *The Risk Management Plan shall demonstrate to the Division's satisfaction that stored gas will be confined to the approved zone(s) of injection and that the underground gas storage project will not cause damage to life, health, property, or natural resources.*

This speaks to risks of "damage" to "life, health, property, and natural resources." However, the fundamental problem with this requirement is that, in the absence of a promulgated or agreed upon acceptable risk level or risk goal or target, it is impossible to "demonstrate" that a facility "will not cause" the undesired endpoints. Because there is no such thing as zero risk—there is always some likelihood that damage will occur—meeting the requirement stated as "will not cause" is impossible.

This fundamental dilemma (or mismatch between expectations and reality) can only be resolved fully by the promulgation of risk targets or goals for each endpoint mentioned (life, health, property, and environment and natural resources). Risk "targets" or "goals" are mutually agreed upon by operator and regulator, but do not have the force of a requirement.

The formulation of a risk target or goal should deal with some combination of how large an impact or consequence is unacceptable, or how frequent is too frequent for a given impact, or some combination. For other complex engineering systems (commercial aircraft, nuclear power plants, offshore oil rigs), various government agencies have dealt with this acceptable-risk issue in different ways, and there is no set prescription for how acceptable-risk levels should be formulated. An excellent review of precedents from the regulation of other industries is provided by Abedinisohi (2014).

As an example of how the issue of lack of risk targets and goals pervades everything else, how can one decide how much monitoring is needed (what to measure, how frequently, to what required accuracy)? How can one decide which of several risk-mitigation activities is best, or sufficient? The DOGGR draft regulation in 1726.3(a) states, in the very next sentence after the one quoted just above, the following:

In accordance with subdivision (b), the Risk Management Plan shall evaluate threats and hazards associated with operation of the underground gas storage project and identify prevention protocols that effectively address those threats and hazards.

How can the facility RMP "evaluate" threats and hazards unless one knows to what extent a given threat or hazard matters? And how can the RMP "identify prevention protocols that effectively address those threats and hazards" unless one knows what the word "effectively" means? In common parlance, the word "effectively" should normally mean that the "prevention protocol" would cause the risk to drop below whatever risk level is targeted and/or acceptable. Without knowing what is acceptable, or what aspirational target or goal is to be used, we cannot determine which prevention protocols will be sufficient, and why. *The dilemma here is fundamental to all that follows.*

1.6.3.4 Risk Management Plans – Recommended Content and Level of Detail

Background

The study team's work on this topic began with a review of several RMPs recently submitted to DOGGR by UGS installations in California in response to the emergency UGS regulations. It was understood that these were hastily assembled, were tentative in character, and will be revised (perhaps extensively) after DOGGR's final regulations are adopted. The study team has had experience with RMPs currently used to assure the safety of other types of engineered systems. That experience has informed the work here. The study team also gained insights from the American Petroleum Institute's Recommended Practice 1173 (API, 2014) and various ISO (International Standards Organization) documents cited therein. Also, the emergency regulations and the draft final DOGGR regulations both include a discussion of the attributes that an RMP must contain. All of the above has informed the discussion below.

As a general matter, it is important to state that any organized approach to risk management through a "risk management plan," even if it does not meet all of the attributes described below, will be useful both in understanding risks and in reducing them.

Risk Management Plans—Recommended RMP elements

Below is a list of the seven recommended elements (scope, content) that an acceptable RMP for UGS facilities in California should have. A detailed discussion of each element follows in the subsequent sections.

- Element #1 of the RMP needs to establish activities to *understand the current "level" of risk* posed for each risk category. This is accomplished either by measurements, by analysis, by a comparison with other similar facilities, or by some combination.

- Element #2 of the RMP needs to describe activities to *compare* the current "level" of risk, category by category, against any risk *targets*, risk *goals*, or risk *acceptability criteria* that may apply.

- Element #3 of the RMP needs to describe activities to carry out *routine (or periodic) monitoring, data collection, and analysis*, to determine whether there is a change in the current "level" of risk for each risk category.

- Element #4 of the RMP needs to provide for *prevention and intervention activities* if the risk "level" (for any category) exceeds acceptable guidelines, or if there is a realistic concern based on monitoring or analysis that a problem could arise in the future—this is what the words "risk management" imply.

- Element #5 of the RMP needs to describe an *emergency response plan* that specifies various activities that are necessary while an accident scenario is developing and then afterward, and also specifies the roles and responsibilities of the several different government agencies, companies, and others in assuring that the emergency response is effective. The plan also needs to provide for regularly scheduled pre-planning drills against written procedures, for prepositioning of response equipment, for communications protocols, and the like.

- Element #6 of the RMP needs to establish the protocol(s) for documenting the results of the risk analyses, the periodic measurements, the intervention activities (if any), the results of the interventions, and any other information that the facility owner, the regulatory agency, and/or the public should know.

- Element #7 of the RMP needs to provide *guidelines for modifying the Plan* in response to new information, such as from the routine monitoring and analyses carried out within the Plan. Associated with this is the need for review and approval of the updated Plan.

The Risk Management Plan—Element-by-element discussion

<u>RMP Element #1—Methodology for understanding the current "level" of risk</u>

For UGS facilities, a useful understanding of the level of risk does not generally exist for each of the risk categories, *because no rigorous and quantitative facility-specific risk assessment has been completed at any California UGS facility, as best we can ascertain.* As will be discussed below, understanding the level of risk posed by a given UGS facility for each risk category, accomplished by completing a quantitative risk assessment (QRA), should be one major element of the Risk Management Plan, because it is an essential prerequisite to the execution of the rest of a useful Risk Management Plan.

The goal of this Element of the RMP is to provide guidance for understanding the current level of risk posed by the facility, risk category by risk category. This is accomplished by analysis, supported in part by measurements, failure data, a comparison with other similar facilities, or by some combination.

This RPM Element is the most critical of all, because unless the current “level” of “risk” can be understood, a firm technical basis does not exist to support any of the next three elements (comparison to risk guidelines, monitoring and analysis, and intervention).

The way risk analysts usually discuss their understanding of the risks posed by any activity is by using the term *“risk profile.”* The risk profile must be facility-specific, and furthermore it needs to be specific to each category of risk. For any risk category, the risk profile includes not only the quantified likelihoods of different “amounts” of risk (such as numbers of health impacts, or dollar values of different types of property damage), but also the likelihoods of the various risks, an understanding of each specific accident scenario that contributes to the risk, and then the principal contributors to each accident scenario. The hierarchy for a risk profile is therefore as follows, starting at the highest level and working down into more detail:

- The risk profile for the facility as a whole

- The risk profile differentiated by risk category (for example, risks to public health and safety, to the facility’s workers, to the environment and natural resources, to the facility’s infrastructure, etc.)

- For each risk category, the risk from each important off-normal scenario (that could lead to a large accident under some circumstances)

- For each off-normal scenario, the principal contributors to that scenario (for example, failure of an item of equipment, corrosion of a pipe, a human error including those due to human and/or organizational factors, etc.).

Note that in the above, the words *important* and *principal* are used, even though the determination of which scenarios are important and which contributors matter most is always fraught with uncertainty and analyst judgment. The obligation of the analyst, as always, includes explaining where judgments play a role and to what extent.

The risk profile inevitably involves numerical values, which need support from facility-specific data, including the sort of data discussed below in Section 1.6.4.3:

- For the facility as a whole, the risk profile needs to be presented in terms of the *annual frequency* of different accidental scenarios characterized by different “risk endpoints” and different “sizes” of the impacts. However, this facility-level information is of less use to decision-makers unless the risk has been differentiated among the various risk categories.

- Within each risk category, the risk needs to be presented so that it differentiates among the various off-normal scenario types that contribute to the risk. For *each scenario type*, the risk needs to be presented in terms of the annual frequency of that scenario, and also in terms of which "risk endpoints" are involved and the "size" of the risk impact.

- For each scenario of importance, the contribution arising from *each contributing factor* (for example, failure of an item of equipment, corrosion of a pipe, a human or organizational error, etc.) needs to be presented in terms of the likelihood of failure or error expressed in that likelihood's natural units (per test, per trial, per year, and so on).

A discussion of the uncertainties in the numbers is also important, and no risk profile is complete without such a discussion, so that users of the risk-profile information can understand the uncertainties: their origin, their character, how reducible or irreducible they are, and why. The analyst should also attempt to identify, if feasible, where collecting additional data can reduce the uncertainties.

The principal contributors will always be highly scenario-specific. As examples, for one scenario, contributors could be the failure of a pump, followed by an overpressure failure of piping close to the surface; for another, they could be the failure due to corrosion of a well casing followed by a human error in failing to secure a valve; for yet another, an earthquake could cause damage to two or three different components.

Unless the scenario-specific failures that contribute to each serious accident scenario are understood, in terms of both "what" and "why," there will not be enough insight to understand how the risks posed by that scenario can be managed. That is, *intervention (either for prevention or mitigation) can only be confidently recommended if it is guided by an understanding of "what" and "why,"* leading to an understanding of why a proposed intervention makes sense.

A scenario-specific analysis: Note that in the above, the emphasis is on performing scenario-specific analysis. The community of risk analysis experts has long recognized that the appropriate way to understand risks from a given engineered facility must be by examining them *one scenario at a time* (Kaplan and Garrick, 1981). Furthermore, because each scenario has, almost by definition, a different likelihood per year of coming to pass, the analysis described here is by its nature *intrinsically probabilistic.* It is probabilistic in its basic building blocks (the likelihood of a given equipment failure, or of a degraded process such as corrosion, or of a human error), and it is probabilistic in how these basic building blocks are combined to develop the annual likelihood of the scenario.

Still further, given a scenario, there are different likelihoods of the various potential consequences, such as ranges of releases of an undesired chemical, or ranges of impacts on human health and safety (either to workers or to off-site individuals), or ranges of damage to the off-site environment.

One important factor that is sometimes overlooked is the contribution of human and organizational factors (HOFs) to the evolution of the off-normal scenarios of interest. Human errors, be they errors of commission or errors of omission, have been found to play a prominent role in the risk profiles of most complex engineered systems (Frank, 2008). It is therefore imperative that they be modeled in any UGS risk analysis. Some human errors can initiate a sequence that would otherwise not begin; others can exacerbate a sequence that would otherwise evolve toward a safe state; still others can cause a sequence involving modest consequences to produce much more important consequences instead. Fortunately, the risk-analysis community has been working on methods for addressing human and organizational factors in the analysis, including approaches for quantifying the likelihood of various human reliability issues (Reason, 1990; Reason, 1998; Barriere et al., 2000; Bley et al., 2005; Gertman et al., 2005; Forester et al., 2007). Work has also been under way to account for how humans can intervene positively to help stop a developing sequence or to mitigate its consequences (Reason, 1998; Reason, 2016; Meshkati and Khashe, 2015).

The relevant risk-analysis methodologies exist: For engineered systems like UGS facilities, a well-developed methodology exists and is widely used. It is commonly called "probabilistic risk assessment" (PRA) and can take many different forms. It is well beyond the scope here to present details of the various PRA methodologies—the relevant literature is extensive (Vesely et al., 1981; Hickman et al., 1983; Frank, 2008; Garrick, 2009; ASME/ANS, 2013). However, every PRA methodology must answer the following three questions (Kaplan and Garrick, 1981), which cover what has been written just above, although in different words. These three questions have become known in the community of probabilistic risk analysts as the "risk triplet":

What can go wrong? *[These are the scenarios.]*

How likely is each important scenario? *[These are the annual frequencies.]*

What are the consequences? *[These are the endpoint impacts.]*

One major insight from experience with PRA analysis of complex engineered systems is that delineating the various scenarios provides the bulk of the insights—albeit the insights are typically most useful when some understanding has been developed as to which ones are the most "important," and why. Whether the word "important" in the previous sentence is attached to the annual frequency of a scenario, or to its consequences, or both, or to the fact that major uncertainties exist, is of course something that is highly specific to each individual analysis.

Another major insight, as noted above, is that various human and organizational issues are often found to be among the important factors in affecting whether a given scenario develops into a serious accident, or not.

Recommendation: To complete Element #1 successfully, a facility-specific quantitative risk analysis must be undertaken. The risk analysis must provide a quantified estimate for each analysis "result," including an estimate of the uncertainties in the numbers, and must describe each important contributor in a way that supports later Risk Management Plan Elements (see below), such as comparisons with acceptable risk levels, decisions on further monitoring or analysis, decisions on intervention, and so on. Therefore, it is recommended that the proposed new DOGGR regulations should describe what must be accomplished by an acceptable risk assessment approach and methodology, along with information about how DOGGR will review a given approach and methodology to assure that it is adequate. Although each facility can select its own approach and methodology, this is necessary in the DOGGR regulations to ensure that sufficient rigor and thoroughness are used across all facilities in California. The methodology must address each risk category considered in the Risk Management Plan.

The relevant language in the DOGGR draft regulation states:

[from 1726.3(b)] The Risk Management Plan shall include a description of the methodology employed to conduct the risk assessment and identify prevention protocols, with references to any third-party guidance followed in developing the methodology. The methodology shall include at least the following:

1. *Identification of potential threats and hazards associated with operation of the underground gas storage project;*

2. *Evaluation of probability of threats, hazards, and consequences related to the events.*

This language speaks of "threats," "hazards," and "consequences" in a way that provides only the most minimal guidance as to what the risk assessment methodology needs to provide. The last word, "events," presumably refers to the threats and hazards, but it is not clear.

As discussed above, the approach generally taken by the community of risk-analysis experts, when dealing with an engineered facility, is to concentrate on identifying the major off-normal accident scenarios, one-by-one. This is because it is the various accident scenarios that need to be prevented (one-by-one) from occurring either with too high a frequency or associated with too large a set of end-point consequences, or some combination.

Fortunately, the DOGGR draft language does use the crucial word "probabilities," indicating that the methodology contemplated by DOGGR must be probabilistic in its formulation.

Recommendation: To address the issue raised here, we propose the following draft language capturing the concerns described above:

[proposed for 1726.3(b)] The methodology shall include at least the following:

1. *Identification of the most important potential accident scenarios associated with operation of the underground gas storage project, based on a detailed description of the characteristics of each facility (number of wells, age, operating scheme, etc.);*

2. *Evaluation of the frequency (for example, the annual probability) of each such accident scenario, and the range of consequences associated with it, including estimates of the uncertainties in the numerical values;*

3. *For each important accident scenario, identification of the principal equipment failures, the principal external initiating events if any (earthquakes, flooding, aboveground industrial accidents, etc.), the principal operational errors, and other aspects that contribute to each accident scenario, and for each a description and quantification of its role relative to other contributors in the evolution of the scenario;*

4. *For each scenario leading to an accidental release, identification of the important engineered or natural features that affect the extent of the various end-point consequences, and a quantification of their relative roles, including an estimate of the uncertainties in the quantification.*

The above proposed requirement, although specific in its detail, is crafted carefully to establish *what* type of analysis is required, and with what scope, but without specifying *how* that analysis is to be performed. Notice, however, that the requirement to evaluate scenario probabilities in (2) and the words "extent of the various end-point consequences" in (4) mean that the analysis must be intrinsically probabilistic—reflecting the fact that the various important scenarios have different annual probabilities of occurring and a range of possible consequences were they to occur.

The above approach is also predicated on an *a priori* identification of the various risk categories of interest—be they public health and safety, risk to workers, risk to the environment and natural resources, risk to the facility's infrastructure, or others. The analysis must be structured to concentrate (one by one) on whichever of these risks are deemed to be within the scope of the risk analysis.

One final comment is important. The approach outlined above uses the concept of *individual accident scenarios* as its *organizing principle.* This organizing principle can then become the focus of each subsequent activity in the Risk Management Plan. That is, it is how comparisons can be made between the existing risk profile and what is acceptable. It is how to determine which specific monitoring, data collection, and analysis activities are needed, and why. It is how to identify and then to evaluate the efficacy of various proposed intervention proposals, be they proposals to make an actual change, or proposals to add or intensify a monitoring activity. A variety of analysis approaches are in wide use to gain an understanding of how the various scenarios could develop, and in how the underlying failures or errors contribute. Methods such as Failure Modes and Effects Analysis (FMEA) can be important tools in this regard (Rausand and Hoylan, 2004).

An additional concern (and associated recommendation) deals with the topic of the role of humans (and especially of human errors) in risk assessments of UGS facilities. Specifically, in most complex engineered systems, and UGS facilities should not be an exception, an important fraction of all of the off-normal scenarios of interest are caused by human errors or are influenced by safety-culture considerations. This is due both to the difficulty in designing against such errors, and the pervading influence of a poor safety culture, if it exists, in affecting everything related to the safety of such complex systems.

Some examples of issues related to this topic (the role of humans in off-normal scenarios and the broader role of safety culture in achieving the facility's overall safety objectives) include (1) the possible reluctance of an operator or maintenance worker to report his/her own error for fear of recriminations, thereby depriving the rest of the organization with the opportunity to improve the operation by learning lessons from the error; (2) confusion in the chain-of-command during the response to an off-normal event; (3) short-cuts taken by a member of the operating crew that compromise safety in the interest of efficiency, and that are self-justified because "the risk of a problem is very low"; (4) failures in operating equipment arising from the disregard of maintenance procedures or standard protocols; and (5) cover-ups by one worker of the errors of another in the interest of short-term camaraderie. A host of other examples exists. This leads to the following "Concern and Recommendation":

One of the concerns with the specific technical details of the RMP guidance in the current DOGGR draft regulation is that the regulation emphasizes certain specific hardware failure issues (and corresponding monitoring activities) without the benefit of insights from a proper analysis of human and organizational factors in the risk profile for any given facility. There is also an emphasis almost exclusively on the "hardware" side of UGS facilities, without adequate consideration of various organizational factors and of whether certain human actions and errors, as well as safety culture, could be important contributors. To address this concern, a sensible Risk Management Plan must give appropriate emphasis to both categories (hardware/equipment problems and human errors including organizational factors) in a way guided by risk-profile insights.

Moreover, the importance of safety culture to promote safety in high-hazard industries, such as UGS, and the ones regulated by the Pipeline and Hazardous Materials Safety Administration (PHMSA), has been strongly emphasized in a recent study by the National Academy of Sciences Transportation Research Board [*Designing Safety Regulations for High-Hazard Industries* (NAS/TRB, 2017)]. This study has analyzed the use of management systems to promote safety in high-hazard industries and has recommended adopting "management-based" regulations to "infuse a greater sense of responsibility and accountability (i.e., safety culture) into the regulated firms" (parenthetical statement in the original, p. 32). According to this study, the underlying rationale for utilizing "management systems to promote safety in high-hazard industries" is that "safety risks, especially catastrophic risks, can arise from interactions among conditions and activities that are difficult to anticipate and may be specific to each firm or work site. Such context specific risks will be unknown to the regulator, especially in view of the diverse and complex operations characteristic of high-hazard industries… [such] regulations may be advantageous in situations where the sources of risk are complex and context specific, as is characteristic of low-frequency, high- consequence events.” (p. 3)

Conclusion: The draft DOGGR regulations ignores how human and organizational factors, as well as a healthy safety culture, drive safety outcomes and performance. (See Conclusion 1.18 in Executive Summary.)

Recommendation: The final DOGGR regulations for UGS facilities should explicitly address the importance and role of human and organizational factors as well as safety culture, commensurate with their impact. DOGGR could follow the State of California’s Department of Industrial Relations’ (DIR) Occupational Safety and Health Standards Board and at least adopt the two new “Human Factors” and “Safety Culture” elements in the recently revised and updated CalOSHA Process Safety Management for Petroleum Refineries regulation, which became effective on October 1, 2017 (CalOSHA, 2017). In this context, DOGGR should also consider applying other related and applicable elements of the new CalOSHA regulation to UGS safety, such as “Management of Organizational Change.” (See Recommendation 1.18 in Executive Summary.)

RMP Element #2—Comparison of the current “level” of risk against the any risk targets, goals, or acceptability criteria that may exist

The goal of this element of the Risk Management Plan is to provide guidance for performing a comparison of the current level of risk, as developed in Element #1, against any risk guidelines (targets, goals, or acceptance criteria) that may exist, be they established by the facility owner or by the regulatory agency. This comparison helps in answering the question as to *whether the current risk level is acceptable*, and if not, why not. As noted above, this comparison needs to be done for each risk category separately.

To perform Element #2, Element #1 must have been completed, so that there is an understanding of the facility’s current risk profile, and in particular the level of risk for each category of risk.

The work in Element #2 then becomes one of comparing (category by category) the current level of risk posed by the facility with any risk targets, goals, or acceptability criteria that may exist. Here, one key issue is that there will inevitably be uncertainties in the understanding of the current risk level posed by the facility. Absent uncertainties, the risk comparison is not difficult. Given the uncertainties, some of which can be large but (more importantly) some of which may not be completely quantifiable, considerable judgment will often be necessary in making the comparison(s) required in Element #2.

RMP Element #3—Routine (or periodic) monitoring, data collection, and analysis

In the absence of risk management plans, past monitoring, data collection, and analysis at UGS facilities have not been guided by nor integrated with rigorous scenario-based risk assessment and risk mitigation approaches. This disconnect or lack of formal integration of monitoring, data collection, and data analysis activities with scenario-by-scenario risk assessment insights can lead to neglect of needed monitoring and/or unnecessary monitoring activities.

The goal of this Element of the Risk Management Plan is to provide guidance for performing monitoring, data collection, and analysis, so as to determine whether there is a change in the current "level" of risk for each risk category.

The execution of RMP Element #3, as for Element #2, depends on the completion of Element #1, so that there is an understanding of the current risk profile, leading to an understanding of the level of risk for each risk category and of the individual contributors, scenario by scenario. Understanding the uncertainties is also important. Only then can a sensible program be established to monitor and analyze the risk level, because only then will there be the knowledge to support a decision about *what to monitor*, *what to analyze*, and why. Specifically, which potential equipment failures, and which potential human errors, are in need of monitoring, data collection, and analysis to improve our understanding or to reduce our uncertainty? And equally important, which interventions might be feasibly undertaken if the monitoring and analysis activity reveals a problem?

Besides understanding which aspects of the facility and its safety culture and operation currently contribute most to the risk profile, additional items may be added to the list of those needing monitoring and/or analysis. Specifically, there is the need to supplement the information derived from the current risk profile with engineering judgment, because certain aspects of any engineered facility that contribute very little to the current risk profile (but could be major contributors under different circumstances) only have such modest impacts, because their failures are known to be currently very rare, or the effects of the failures are known to be modest under current conditions. But things can change over time. Therefore, if there is a major concern about the impacts of a failure, and if change over time is a concern, then a monitoring program is necessary despite that specific item's not contributing much to the current facility risk profile.

Recommendation: It is recommended that DOGGR require that monitoring, data collection, and analysis must be informed using the insights from a scenario-by-scenario risk analysis to assist decision-makers in determining what to monitor, what data to collect, what to analyze, and why. Especially for scenarios characterized by a low probability of occurrence but a potential for high consequences, only a risk analysis that identifies and characterizes them can reveal the optimal intervention(s) to reduce their potential consequences.

The relevant language in the DOGGR draft regulation is found in several different places in 1726.3. For example, 1726.3(c)(3) calls for the Risk Management Plan to incorporate mechanical-integrity testing; 1726.3(c)(4) calls for corrosion monitoring; 1726.3(c)(5) calls for monitoring of casing pressure and several other parameters; 1726.3(c)(7) deals with reservoir integrity; 1726.3(c)(8) deals with formation of hydrates; etc.

The RMP requirements, however, lack an explicit link to an underlying risk analysis that can describe the extent to which each issue requiring monitoring, data collection, and/or analysis is linked to a specific accident scenario, and if so how. For each monitoring or data-collection activity described in the RMP, one should have a technical basis for deciding (1) how often, (2) with how much detail or accuracy, and (3) how much uncertainty in the measurements is tolerable, and why.

Recommendation: Throughout the new DOGGR draft regulation are requirements for monitoring, data collection, and analysis. Each of these requirements must be linked directly to an underlying risk analysis that can support a determination of the technical basis for deciding, for that activity, (1) how often, (2) with how much detail or accuracy, and (3) how much uncertainty in the measurements is tolerable, and why. An explicit linkage in the language of the requirements to the specific accident scenarios at issue can help provide the technical basis for these decisions.

RMP Element #4—Intervention activities

As background, the word *intervention* here covers both activities that would prevent a safety issue from arising and activities undertaken to reduce the likelihood or mitigate the consequences arising from an existing safety issue once identified.

The description in the proposed DOGGR regulations of the elements required in the RMP does not specify the need for general criteria for when and how to decide what changes or interventions are needed to mitigate risks that are deemed too high. But before intervention activities are decided upon, clear decision criteria need to be developed and used, based in part on the acceptability of the risk. These criteria need to be described in the facility's Risk Management Plan.

The goal of this element is that the Risk Management Plan should describe those intervention activities that must be undertaken if the risk "level" (for any risk category) exceeds risk targets or goals or risk acceptable guidelines, or if there is a realistic concern based on monitoring or analysis that a problem could arise in the future. This is what the words "risk management" imply.

Element #4 follows logically after #2 and #3, because intervention is called for only when the risk-management decision-makers conclude either (i) that a risk is "too high" (from Element #2); or (ii) that, based on monitoring and analysis (Element #3), a change in the risk profile either has occurred or is in danger of occurring; or (iii) that reducing uncertainties is sufficiently important.

Intervention, in turn, can mean either an actual change (to a piece of hardware, or to a procedure guiding operator actions or maintenance activities), or an intensified monitoring activity. That is, using colloquial language, *intervention can mean either "fixing something" or "watching something more carefully."* Furthermore, although intervention is usually called for because an actual problem has arisen, it is not uncommon for intervention to occur because new information has told the decision-makers that there is too much uncertainty.

Recommendation: A Risk Management Plan must include a description of the decision-making process including criteria for undertaking interventions of various types. This is needed even though many of the details cannot be provided in the RMP, because each intervention is by its nature highly situation specific.

The proposed new DOGGR regulations do not contain language linking the intervention protocols directly to the various accident scenarios being addressed. In the proposed new DOGGR regulations, language is needed requiring this link. This must be part of the facility's Risk Management Plan.

The relevant language in the DOGGR draft regulation states:

[from 1726.3(b)] The Risk Management Plan shall include a description of the methodology employed to conduct the risk assessment and identify prevention protocols. .… The methodology shall include at least the following:

(1) .…

(2) .…

(3) Identification of possible prevention protocols to reduce or monitor risks, including evaluation of the efficacy and cost-effectiveness of the prevention protocols;

(4) Selection and implementation of prevention protocols.

This text is acceptable as far as it goes, but lacks a direct link to the organizing principle of the various accident scenarios. To accomplish this, the regulatory language should provide that direct link.

Recommendation: A change must be made to replace the words "prevention protocols" with "intervention protocols" everywhere in regulatory subsection 1726.3(b).

In the regulatory language of 1726.3(b) above, a change must be made so that (3) and (4) read as follows, where the proposed additional new language is in *italics:*

(3) Identification of possible intervention prevention protocols to monitor the facility's safety culture to reduce or monitor risks, including evaluation of the efficacy and

cost-effectiveness of the intervention prevention protocols, *linked to the specific accident scenario(s) affected by each proposed protocol*

(4) Selection and implementation of intervention prevention protocols, *linked to the specific accident scenario(s) affected by each proposed protocol.*

RMP Element #5—Emergency response plan

The goal of Element #5 of the Risk Management Plan is to provide guidance for the UGS facility's emergency response plan. As noted above, this plan must specify various activities that are necessary while an accident scenario is developing and then later, and also specify the roles and responsibilities of the several different government agencies, companies, and others in making the emergency response effective. The plan also needs to provide for regularly scheduled pre-planning drills against written procedures, for prepositioning of response equipment, for protocols concerning communications, and the like.

Emergency response plans are in place dealing with many other dangerous processes and industries, and there is vast experience with how they should be formulated, exercised, and kept up-to-date. Both the Federal Emergency Management Agency and agencies is each of the several states (including California) have general guidance and specific guidelines concerning standard practices (FEMA, 2010; FEMA, 2014; California Governor's Office of Emergency Services, 2012).

For UGS facilities in California, their emergency response plans, as contained in the current Risk Management Plans, are not now generally based on a careful understanding of a given facility's risk profile. This omission should be remedied.

Recommendation: A Risk Management Plan must include an emergency response plan that establishes both requirements and expectations, and that is based on a careful understanding of the given facility's risk profile.

RMP Element #6—Documenting the results

The goal of this element of the Risk Management Plan is to provide guidance for documenting the results of the risk analyses (the "risk profile"), the measurements, the analyses, the intervention activities (if any), the results of the interventions, and any other information that the facility owner, the regulatory agency, and/or the public should know.

Recommendation: A Risk Management Plan must include a description of what documentation is required, or desirable, and why. Depending on the circumstances, certain documentation requirements may be specified, and others suggested.

RMP Element #7—Guidelines for modifying the Plan

The goal of this element is to provide guidelines for the modification of the Risk Management Plan itself in response to the routine monitoring and analyses carried out within the Plan, or in response to information gathered during installation, startup, operation, maintenance of new or modified equipment, or arising from the introduction of new procedures. Associated with this is the need for review and approval of the updated Plan. Placing the guidelines for the Plan's own modification within the Plan itself provides pre-determined markers concerning the thresholds for modifications and the frequencies for considering them.

One final comment should be made about Risk Management Plans and their use in a regulatory environment. If DOGGR is to use the facility-specific RMPs to inform its regulatory decisions, it is likely that some training may be necessary so that the regulatory staff can obtain the full benefit of the insights that can be derived from these RMPs.

1.6.4 Potential Additional Practices That Could Improve UGS Integrity

The study team has identified the following three "additional practices," each of which has specific benefits but also entails certain costs and burdens. These are termed "additional" because they are not described in the proposed DOGGR regulations. Each of these will be discussed in turn:

- Training of the operating crew at each UGS facility to assure more effective response to off-normal conditions that could lead to large accidental releases

- In the event of a release of gas from a UGS facility, development at each facility of an ability to predict the site-specific and release-specific transport and fate of released gas in the environment and its effect on local populations and infrastructure

- Development of a system for routine reporting on safety issues as they arise at any UGS facility and the sharing of that information with other facilities and with the public.

1.6.4.1 Operating Crew Training

Regular training of operators and maintenance personnel can be a significant factor in decreasing the likelihood and also the severity of large accidents. This is true even if the training, which consists of written material or lectures, is offered only sporadically. When this training is linked to the use of written procedures to help the personnel to respond to off-normal conditions, and when the training involves regular periodic updates, the benefits are enhanced.

The use of training like this has been a hallmark of industries (such as nuclear power plants, commercial aviation, and refineries) for which an accident can involve very major consequences. It is why, for example, commercial aircraft pilots undergo extensive training, both before assuming their responsibilities and then on a continuing basis afterward.

In the discussion here, the word *training* will encompass both the use of procedures and the development of “teaching modules” that allow each individual to understand the phenomena, the timing, and the issues involved with the evolution of each class of off-normal event. This also implies that an analysis exists that has identified the major types of “accident scenarios” that threaten the facility, so that training and procedures can be targeted specifically to those one-by-one.

Indeed, a major benefit of this entire approach is that, for each accident scenario at issue, the analysis work done to support the training provides to the operating and maintenance personnel the benefit of the insights, experience, and careful analysis of engineers who have thought through appropriate response actions in advance. (See American Nuclear Society, 2014.)

One of the important findings is that, in general, training in conjunction with written procedures does not mean that the operators or maintenance personnel need to follow the procedures by rote. In part, this is because not all accident scenarios can be anticipated in detail. It is always imperative that personnel who are on-the-spot at the time when an off-normal event occurs must think through what to do and why, aided by the written procedures and the prior training, but not necessarily completely governed by them. Experience shows that the personnel present at the time are in a better position than anybody else to understand the context and the details of the events as they occur, and to think carefully about what best to do (United States Nuclear Regulatory Commission (U.S. NRC), 1980).

Therefore, the procedures, and the training in their use, are to be thought of as providing important guidance, but not binding requirements. See (GWPC and IOGCC, 2017) for further insights specifically tailored to the operation of UGS facilities.

Also, although this training should be mandatory, this does not imply that an operator or maintenance worker cannot work until the training has been completed. A flexible approach is needed, especially given that new employees typically do best if they use on-the-job learning in conjunction with the initial training (American Nuclear Society, 2014).

One key prerequisite must be accomplished. That is, an effort needs to be expended to *perform an analysis of the major potential accident scenarios*, one-by-one, so as to support the training and the written procedures. In the course of this analysis work, insights will reveal which potential accident scenarios must be emphasized in the training and supported by the written procedures (and why), and which don’t (and why). The expense to perform this analysis, while significant, will pay major dividends, and not only in helping to avert the major accident scenarios of concern. Experience in other industries has shown that training with procedures increases the reliability of the operations, thereby reducing the frequency of modest incidents that have lesser safety significance but can have important financial consequences, such as improvements in equipment problems, operational downtime, worker safety, and other areas (Frank, 2008).

The situation in California is probably typical. There is no California requirement at today's operating UGS facilities for the regular training of the operating and maintenance crew, nor for the use of written procedures to assist the crew in its response to off-normal conditions and events that might lead to a severe accident. (These procedures are sometimes referred to as "emergency response procedures.") Nor are there any ANSI standards or other similar documents that can provide a basis. Regular training and written procedures have been demonstrated in other industries to improve safety around off-normal conditions and events, and, as noted above with the observation that an important fraction of off-normal scenarios in most complex engineered systems can arise from human errors and safety-culture concerns, it is likely that UGS could benefit similarly from analogous training and procedures.

The importance of this issue calls for either an industry-wide collaboration or a government-mandated requirement. Perhaps the recommended training and procedures could best be brought into existence by an industry consortium that would voluntarily agree to undertake the work to develop the technical basis. Alternatively, perhaps the best approach is through a government (DOGGR) requirement. Either approach can work, but the decision is highly situation-specific, and beyond the ken of the authors of this report.

Conclusion: There is no California requirement at today's operating UGS facilities for the regular training of the operating and maintenance crew, nor for the use of written procedures to assist the crew in its response to off-normal conditions and events that might lead to a severe accident. Regular training and written procedures have been demonstrated in other industries to improve safety around off-normal conditions and events. It is likely that UGS could benefit similarly from analogous training and procedures. (See Conclusion 1.19 in Executive Summary)

Recommendation: It is recommended that at each operating UGS facility in California, a requirement be put in place for the regular training of the operating and maintenance crew using written procedures. This could be either a requirement developed and implemented voluntarily by the industry itself, or a requirement embodied in a government regulation. It is further recommended that the requirement above be placed in the Risk Management Plan section of the draft California UGS regulations. (See Recommendation 1.19 in Executive Summary.)

1.6.4.2 Capability to Predict the Site-specific and Release-specific Transport and Fate of Releases

In the unlikely event that an accident unfolds with the potential to produce a major accidental release of natural gas, there would be a clear benefit if the capability existed to predict in near real time the transport and fate of a large release to the environment of natural gas, and also to predict its impact on workers, the local population, property, and the broader environment. This is borne out of experience with almost every major disaster involving potential or actual releases of dangerous substances from a facility to the environment (Broughton, 2005; Perrow, 1984; U.S. NRC, 1980).

Ideally, each facility would possess this type of analysis capability, so that, in the event of an accidental release, the analysis in near-real-time of the releases and their likely fate could be available to allow for the protection of lives, property and the environment. The analysis capability should possess the following features:

1. It should be site-specific.

2. It should account for local weather conditions and other relevant local conditions (traffic, etc.) in real time.

3. It should be able to provide the desired analysis is close to real time, so as to assist local decision-makers in maximizing the protection of workers, the local environment, the local population, property, and the environment.

4. The analysis and its implications should be capable of being made broadly available to the public.

There is significant experience with analysis of this type, although most of it is for facilities that are somewhat different (Hanna et al., 2006; Lisbona et al., 2014; Mahgerefteh et al., 2006; McGillivray et al., 2014). The adaptation to UGS facilities is, however, straightforward. The U.S. Department of Energy maintains a capability to perform these analyses on an emergency basis that provides an excellent model for the capability needed here (Sugiyama and Nasstrom, 2015).

The analytical capability need not be in-house at each facility, and indeed it is probably less efficient to do it that way. More promising might be an arrangement in which a central analysis team or company, under contract to the various facilities, would develop the analysis capability, receive all of the relevant data from wherever they are developed, and maintain its expertise over the years by interacting with similar existing capabilities in similar industries.

Once developed, the analysis capability needs to be kept up to date, not only in terms of data inputs but in terms of advances in the state of the art. There would need to be periodic training of on-site personnel at each facility as to how to use and interpret the analysis outputs.

Of course, off-site emergency-responder organizations need to be tied in: police, fire, security, environmental and agricultural protection agencies, and so on. These entities would also need to be trained and to take part in periodic drills.

At today's operating UGS facilities in California, there is no requirement that each facility possess the capability (through analysis) to predict in near real time the transport and fate of a large release to the environment of natural gas, and also to predict its impact on workers, the local population, and the broader environment, despite the clear benefit to safety if this capability were to exist. Though not a requirement, it is clear that the ability to predict off-site and downwind impacts of major LOC incidents at UGS facilities would improve emergency response and increase safety of both on-site and off-site populations.

If a shared approach is chosen for developing and maintaining the analysis capability, much of the development cost could be shared among the many different UGS facilities. The cost of the capability's upkeep would also need to be shared among facilities.

The capability could also either be maintained within each operating company or be provided by contractual arrangements off-site.

The importance of this issue calls for either an industry-wide collaboration or a government-mandated requirement. That is, perhaps the recommended analysis capability could best be brought into being by an industry consortium that would voluntarily agree to undertake the work to develop the technical basis. Alternatively, perhaps the best approach is through a government (DOGGR) regulatory requirement.

Conclusion: Although a range of practical and sophisticated models are readily available for predicting the impacts of off-normal LOC events, there is currently no requirement for UGS facilities to possess, or have access to, atmospheric dispersion models that can predict the fate of natural gas emitted from a facility. Also, the lack of temporal and spatially varying emission data from each facility, as well as the past lack of reliable local meteorological data (now addressed by the new CARB regulations for methane emissions from natural gas facilities) (CARB, 2017c), make it difficult to accurately simulate the atmospheric dispersion and concentrations of gas leakage from UGS facilities. (See Conclusion 1.20 in Executive Summary.)

Recommendation: Each operating facility in California should arrange to develop a capability to predict the atmospheric dispersion and fate of a large release of natural gas to the environment in near-real-time, and the impact of such a release on workers, the local population, and the broader environment. The simulation capability should be developed by an independent (ideally single) institution with the technical capacity (i.e., modeling skills) and transparency that meet the public's demand for trust. (See Recommendation 1.20 in Executive Summary.)

One example of an institution with this skillset is the National Atmospheric Release Advisory Center at Lawrence Livermore National Laboratory in Livermore, CA, a national support and resource center for emergency planning, real-time assessment, emergency response, and detailed studies of atmospheric releases.

1.6.4.3 Database for Routine Reporting of Off-normal Events Relevant to Safety

Industries such as commercial aviation and the nuclear-power plant industry, always put safety as the first priority. These industries established a mandatory system for reporting all off-normal failures and errors, no matter how small. Actual "events" comprising a series of one or more failures in sequence are also reported. These are then compiled into a publicly available database (U.S. NRC, 2017b; Den Braven and Schade, 2003; Browder et al., 2010). This database, used by all, enables continuous improvements to be implemented.

The most important categories in which the improvements are realized are in equipment reliability and in human performance. The documentation of failure modes of equipment, for example, enables others with similar equipment (industry-wide) to learn how to avoid those failure modes or to mitigate their consequences. The documentation of human errors, either in operating the plant or in its maintenance, again enables others to learn from experience. And the documentation of events (sequences comprised of a series of failures) enables them to be studied to reduce their frequency or their consequences (Frank, 2008).

Although the insights derived from collecting and documenting these categories of errors, failures, and events accrue mostly toward improving the individual items or actions, less obvious are the benefits in reducing the likelihoods and consequences of potential major accident scenarios. Experience in other industries shows, however, that perhaps the most important benefit of the gathering and analysis of this information is that it occasionally leads to the identification of a previously poorly understood accident scenario; this scenario can subsequently be designed against or protected against by training and procedures (Garrick, 2009). This identification of a new or unsuspected possible scenario can then be shared industry-wide, something not possible without both the existence of a broad database and its careful analysis.

In short, this learning-by-experience approach is made possible by the existence of an industry-wide database that gathers data on equipment failures (major and minor), human errors (major and minor), and unusual events, including events characterized by dependent failures (in which a failure in item A directly leads to a failure in item B or to a human error affecting item B.)

When proposals for such an industry-wide database were first broached in the nuclear-power industry (after the Three Mile Island nuclear accident in 1979), three concerns were raised: (1) the *cost* to every facility from reporting everything and then the cost of its analysis, done by a central group; (2) the issue of *liability*—if you report it, somebody will be identified as liable and perhaps somebody will sue in court; and (3) *proprietary* and intellectual-property concerns would stand in the way of publicly reporting that, say, a specific company's pumps seemed to be failing more often than those of its competitors.

All of these concerns, raised at the time, needed to be addressed, but in the end, each of them was overcome by an industry-wide agreement, with regulatory concurrence, as to the urgent need and major value of the endeavor (U.S. NRC, 1979; Nuclear Energy Institute, 2014).

The specific features of such a system would need to be worked out by the industry in collaboration with the regulatory agency. However, the features of the system can be outlined without working out the details. Specifically, the "safety issues" within the scope would need to include not only major events or their precursor events but also data on failures of individual safety equipment items and data on operational and maintenance errors. The reporting would need to be mandatory and performed according to a specific guidance document. The system would also need to provide guidance on standardized methods for reporting the information and analyzing its significance. The database should include root cause evaluations, and a requirement for full disclosure and reporting of them, independent auditing, and a continuous-improvement process. The scope should also include management-system deficiencies. Finally, a central analysis group must be established to compile the database and also to analyze it, categorize it, and disseminate it. The cost of maintaining this central group would need to be borne by the various operating facilities, whose complaints about the cost can be rebutted mainly by the prospect (sure to be realized over time) of large operational improvements in reliability to be derived from the use of the failure data.

A few studies in the literature (Evans, 2008; Evans, 2009; Folga et al., 2016) have compiled incidents and events at UGS facilities, and these have been very useful in providing a historical overview of the worldwide UGS industry's performance. However, even if studies like these were to be developed or updated on a regular basis, they would be no substitute for the database recommended here.

The development of a comprehensive database allows UGS operators and others to better understand the causes of off-normal events so that efforts to improve integrity management systems or other risk management programs will be more likely to reduce their number and severity. A comprehensive database can also be used to establish quantifiable performance measures by which the effectiveness of these plans may be evaluated.

There are good precedents for voluntarily reporting "safety-related" issues by industry professionals/individuals or companies to a central shared database. One analogous program is the Aviation Safety Reporting System (ASRS) in U.S. civil aviation, which allows airline pilots and other crew members to provide near-miss information on a confidential basis. ASRS, which is based on voluntary reporting and is administered by the National Aeronautics and Space Administration (NASA), analyzes the information and makes it available to the public and across the aviation industry worldwide for educational purposes to decrease the likelihood of aviation incidents and accidents.

At California's UGS facilities, as elsewhere, although modest off-normal conditions and events (equipment failures, human errors in operations or maintenance, and other failures that adversely affect or potentially can affect the safety, security, or environmental performance) can happen, there is no requirement that these situations or incidents be routinely reported and compiled into a database that would be shared broadly. Such a database should exist. Furthermore, the reporting of such events and failures should be mandatory and the data and any results of analyzing the data should be shared broadly. Absent such a database, opportunities are lost to learn from these off-normal events and failures, which would enhance safety, specifically by helping to reduce the likelihood and/or the consequences of less likely major accidents.

Conclusion: Experience from other industries shows that the reporting of minor off-normal events and failures can be very useful when shared and aggregated for the purposes of improving operations and learning from mistakes. (See Conclusion 1.23 in Executive Summary.)

Recommendation: It is therefore recommended that a database be developed for the reporting and analysis of all off-normal occurrences (including equipment failures, human errors in operations and maintenance, and modest off-normal events and maintenance problems) at all UGS facilities in California. An example of one kind of input to this database is the required reporting of leak detection and repair required under the new CARB regulation for methane emissions from natural gas facilities (§95673(a)(12) (CARB, 2017c)). The database should be made publicly available to enable others to derive lessons learned from it. (See Recommendation 1.23 in Executive Summary.)

The database should include root-cause evaluations, and a requirement for full disclosure and reporting of them, independent auditing, and a continuous-improvement process. The scope should also include management-system deficiencies. Once this publicly available database exists, the reporting of such events should become mandatory under a no-fault protocol. This requirement could either be embodied in a government regulation, or be a requirement developed and implemented voluntarily by the industry itself.

The recommended database and its custodian for the gas industry can follow the ASRS model, if a NASA-type research and development custodian can be found for the underground gas storage and pipeline industry. Alternatively, the entity could be modeled after the nuclear power industry's self-regulatory body, the Institute of Nuclear Power Operations (INPO). If it is to be in a California regulation, it is further recommended that the requirement above be placed in the Risk Management Plan section of the new draft of the California UGS regulations.

1.6.5 Regulatory Changes Under Way for UGS Integrity—Review and Evaluation

1.6.5.1 Background

Constructing and operating an underground gas storage facility in California requires that a Certificate of Public Convenience and Necessity be granted by either CPUC (or Federal Energy Regulatory Commission (FERC)), as described in more detail in Chapter 2 of this report. For the purposes of this section related to evaluating regulatory changes since the 2015 Aliso Canyon incident, we note the following:

1. UGS is explicitly excluded from the U.S. EPA's UIC program (see Section 1.2) so there is no oversight by U.S. EPA.

2. PHMSA had previously declined to exercise its authority to regulate UGS wells but began this year on January 18, 2017 through Interim Final Rule (IFR) to exercise its authority through the adoption of the recommendations in API 1171 (relevant to DHR storage) PHMSA (2016).

3. DOGGR regulates UGS wells in California, and in particular DOGGR grants permits to drill wells and sets well design standards.

4. CPUC regulates the surface infrastructure at UGS facilities, although DOGGR has an interest in this infrastructure to the extent that it interacts with DOGGR's own regulatory authority covering UGS wells.

5. The California Air Resources Board (CARB) and the various Air Quality Management Districts in the state collect information about emissions from all stationary sources in California, including UGS facilities. A discussion of this can be found in Section 1.4.5 earlier in this report.

6. CARB regulations on detection, reporting, and repairing natural gas leaks at UGS facilities went into effect October 1, 2017 (CARB, 2017c). We note that the measurements under these regulations are concentration measurements used to detect leakage rather than quantify emissions (leakage rates).

The context for the discussion in this section is that in the aftermath of the 2015 Aliso Canyon incident, emergency regulations were developed (California Natural Resources Agency, 2016) governing certain activities at the several UGS facilities in California. These were intended to decrease LOC risk and improve the safety of these facilities. These emergency regulations will be superseded by permanent regulations that are now under development (California Natural Resources Agency, 2017).

1.6.5.2 Scope of this Review

The proposed regulations contain both technical requirements and various administrative requirements. This review and evaluation will cover only the technical requirements. These technical requirements are grouped under the following section headings in the draft regulations. These will be reviewed below section-by-section.

1726.3	Risk Management Plans *[A review and evaluation of Section 1726.3 on RMPs can be found above in Section 1.6.3.]*
1726.4	Underground gas storage project data requirements
1726.5	Well construction requirements
1726.6	Mechanical integrity testing
1726.7	Monitoring requirements
1726.8	Inspection, testing, and maintenance of wellheads and valves
1726.9	Well leak reporting
1726.10	Requirements for decommissioning

1.6.5.3 Section-by-section Review

Underground Gas Storage Project Data Requirements (Section 1726.4)

The UGS regulations for project data require updated data to be submitted when changes to such data are available. Although a couple of examples are provided, the regulation is ambiguous in that it does not define what constitutes a change nor provide a timeframe for reporting such change.

The article (8)(b) in 1726.4 states, *"Updated data shall be provided to the Division if there are changes in operating conditions, such as gas plant or compressor changes, or if more accurate data become available, such as updated cross sections, new reservoir characteristics data, or new pressure flow modeling."* Changes in operating conditions can include a large number of elements which could or could not be relevant to the safety of the operations. To minimize misinterpretation and to achieve consistency in the data reported across all storage fields, we recommend a definition of relevant changes be included. Alternately, a list inclusive but not limited to, could be provided to aid operators with the task. It should be noted that, unlike the reporting for the Mechanical Integrity Test and well leaks, the regulations do not provide a timeline under which the operators are required to report the change.

Additionally, although operators of existing projects might have some or most of the data requested by the regulations, some might be old or difficult to retrieve. In light of the new regulations (and to aid the set-up of the record management program, if not in place) we would recommend an initial review of all existing data to date. This would help highlight gaps and discover inconsistencies, if any. There are many ways this could be achieved, either by on-site review, or submission of all data to the regulators. Other states' regulators have provided a checklist to assist operators in compiling all relevant data and identify gaps as relevant to the new regulations. A similar system could be utilized in California.
A checklist (or similar) would not necessarily be restrictive, but allow for flexibility in the options provided.

After a new site project has been approved (or an existing one reviewed under the new regulations) a periodic (every few years) review of all data should be applied. The scope of the periodic review is to maintain updated data, test the Record Management System and identify gaps or new needs.

The current UGS regulations also require the reporting of *'more accurate data if it becomes available'*.

Recommendation: To maintain consistency in reporting across the industry it is recommended that a definition of a change in the project data be provided. Additionally, a predefined timeframe for reporting such changes should be specified. Furthermore, we recommend a review of all data be done every few years.

Well Construction Requirements (Section 1726.5)

The UGS regulation (subsection (b)(1)(A)) seems to require the use of tubing with packer as a minimum to meet primary barrier requirements. That requirement seems inconsistent with other parts of the text. Additionally, the regulations do not address when or how often bond logs or alternative methods of cement evaluation are required. Inconsistencies were found in what is required as a primary barrier. Clarification is necessary on when and how often cement evaluation is needed.

As a general matter, the concept of more than one barrier between high-pressure gas and the environment is an excellent way to improve well integrity. The subsection 1726.5 (b)(1)(A) of the UGS regulations states that at minimum, the primary barrier should comprise production casing (i) and tubing with packer (ii). This statement suggests that both are required. Subsection b(11) states that *"For well equipped with tubing and packer […],"* suggesting that not all wells have a tubing with packer configuration. These two statements are inconsistent. According to the barrier definitions, if tubing alone is used for production and injection, then the tubing would be the primary barrier while the casing would be considered part of the secondary barrier. If production and injection are allowed in both then the casing would be considered the primary barrier.

Subsection (b)(1)(B)(i) requires that to meet the standard for the secondary barrier, the casing cement should overlap at least 100 ft between the concentric casing, with a good quality cement bond. What constitutes a good cement bond is not specified. Similarly, subsection (b)(7)(B)(10) requires that the cement bond log or evaluation show an adequate bond between the cement and the casing and the rock. A clarification on how and if these requirements are similar is suggested with an additional statement on district discretion on acceptable results as newer, more accurate logging tools became available.

Also, it is well known that cement bond quality will degrade within the well life cycle, especially if pressures are cycled periodically. The UGS regulations do not specify when, after curing and reaching appropriate compressive strength, the evaluation needs to be performed, nor if subsequent evaluations are required to gauge the aging of the cement.

Recommendation: Clarification of what qualifies as a primary barrier is recommended to avoid confusion. Because many of these wells are repurposed, i.e., conversions of existing, old oil and gas wells, we recommend that the evaluation of cement bond integrity be addressed throughout the lifetime of a well and not just at initial casing installation.

Mechanical Integrity Testing (Section 1726.6)

Demonstration of external and internal mechanical integrity is a critical aspect of maintaining well integrity in any UGS field. UGS regulations require annual temperature and noise logs to demonstrate external mechanical integrity and pressure testing for at least 30 minutes every two years for every active well to demonstrate internal mechanical integrity.

Subsection 1726.6 (a)(1) of the UGS regulations requires temperature and noise logs to ensure integrity. These logs are designed to evaluate the location of an external leak behind casing, if present. The reliance on cement, temperature, and noise logging evaluation to demonstrate external mechanical integrity requires that all logging operations are performed to industry standards.

Corrosion is a significant problem associated with well integrity in the UGS fields in California. Regulatory requirements address the need for corrosion logging and monitoring to evaluate corrosion effects on well integrity. Corrosion logging and monitoring operations are a reactive approach to the problem of corrosion impacts on well integrity.

A Casing Wall Thickness Inspection log should be conducted on each gas storage well. The Casing Wall Thickness Inspection of the well measures the thickness of the external casing of a well, as well as the amount of any corrosion that has occurred to that casing. For this test to be conducted, the tubing is removed from entire depth of the well, and measurements are taken directly from the inside wall of the casing. If the inspection reveals thinning of the casing, the current strength of the casing will be calculated. If the current strength of the casing has diminished to the point that it cannot withstand authorized operating pressures for the well plus a built-in additional safety factor of pressure, the well has failed this test. A passing test for a Casing Wall Thickness Inspection would show no thinning of the casing that diminishes the casing's ability to contain at least 115% of the well's maximum allowable operating pressure.

Subsection 1726.6(a)(3) of the UGS regulations requires an internal well integrity demonstration by pressure testing of the production casing or of the tubing if injection is through the tubing with a packer system. Duration of the test is specified to be 30 minutes (or 60 minutes in special circumstances) with no more than a ten percent decline. If continuous pressure monitoring of the tubing and the production casing-tubing annulus using a SCADA system, is in fact implemented and is able to detect suspicious behavior, the frequency of these internal mechanical integrity tests could be decreased or even eliminated.

The UGS regulation requires notification prior to MIT testing and a report within 30 days of the test conclusion. Any well testing (and intervention) that is outside the normal operating procedure should also be reported irrespective of the reason for conducting it (yearly requirement) or the scope.

Recommendation: We recommend the following industry standards for logging to demonstrate external mechanical integrity:

(A) Temperature Survey. *A temperature survey performed to satisfy the requirements of external mechanical integrity testing shall adhere to the following:*

1. *The well must be taken off injection at least twenty-four hours but not more than forty-eight hours prior to performing the temperature log, unless an alternate duration has been approved by the DOGGR.*

2. *All casing and all internal annuli must be completely filled with fluid and allowed to stabilize prior to commencement of logging operations.*

3. *The logging tool shall be centralized, and calibrated to the extent feasible.*

4. *The well must be logged from the surface downward, lowering the tool at a rate of no more than thirty feet per minute.*

5. *If the well has not been taken off injection for at least twenty-four hours before the log is run, comparison with either a second log run six hours after the time the log of record is started or a log from another well at the same site showing no anomalies shall be available to demonstrate normal patterns of temperature change.*

6. *The log data shall be provided to the DOGGR electronically in either LAS or ASCII format.*

(B) <u>Noise Log</u>. A noise log performed to satisfy the requirements shall adhere to the following:

1. *Noise logging may not be carried out while injection is occurring.*
2. *All casing and all internal annuli must be completely filled with fluid and allowed to stabilize prior to commencement of logging operations.*
3. *Noise measurements must be taken at intervals of 100 feet to create a log on a coarse grid.*
4. *Noise logging shall occur upwards from the bottom of the well to the top of the well.*
5. *If any anomalies are evident on the coarse log, there must be a construction of a finer grid by making noise measurements at intervals of twenty feet within the coarse intervals containing high noise levels.*
6. *Noise measurements must be taken at intervals of ten feet through the first fifty feet above the injection interval and at intervals of twenty feet within the 100-foot intervals containing:*

   a. The base of the lowermost bleed-off zone above the injection interval;

   b. The base of the lowermost USDW; and

   c. In the case of varying water quality within the zone of USDW, the top and base of each interval with significantly different water quality from the next interval.
7. *Additional measurements must be made to pinpoint depths at which noise is produced.*
8. *A vertical scale of one or two inches per 100 feet shall be used.*

(C) <u>Cement Evaluation Logging</u>. A cement evaluation log performed to satisfy the requirements of this section shall adhere to the following:

1. *Cement evaluation tools shall be calibrated and centralized to the extent feasible.*
2. *Cement evaluation tools shall be run initially under surface pressure and then under pressure of at least 1,500 psi.*
3. *If gas is present within the casing where cement evaluation is being conducted, then a padded cement evaluation tool shall be run in lieu of an acoustic tool.*

(D) <u>Anomalies</u>. The operator shall take immediate action to investigate any anomalies, as compared to the historic record, encountered during testing as required. If there is any reason to

suspect fluid migration, the operator shall take immediate action to prevent damage to public health, safety, and the environment, and shall notify the DOGGR immediately.

A proactive approach to corrosion in UGS would be a more logical solution to addressing this problem, such as determining what is causing the corrosion of the wells and determining how to prevent it.

Monitoring Requirements (Section 1726.7)

The UGS regulations require real-time monitoring of all annuli. Mandatory reporting and follow up remediating actions are required for annuli that are found with pressure greater than 100 psi. These regulations have the potential to force operators to perform a large number of remedial actions with limited success rates. However, real-time pressure monitoring is a proactive approach in addressing and identifying potential incidents or releases and the benefits can sometimes outweigh the costs.

Currently, the majority of the existing wells are not set up to measure all annuli pressure, especially surface and intermediate. Although we agree that new wells should be required to be set up to monitor all annuli, retrofitting all existing wells in service would be a major undertaking.

Additionally, the UGS regulations require remediating action for any well that is found to have an annulus pressure greater than of 100 psi (for annuli that should not have any pressure). Although the presence of gas does indicate migration through the annulus, it does not necessarily reflect the severity of the breech. A remediating requirement, as it is currently stated, would result in an extremely large number of remedial actions. Remedial actions can vary considerably, but the potential for annular over-pressurization, which can result in a breakdown of the casing shoe and in a release at the surface, is a major concern for UGS wells.

Strategically placed observation wells in the vicinity of spill points, within an aquifer, and above the confining zones in porous and permeable formations should be installed and monitored to detect the presence or movement of gas from storage operations. Observation wells can be placed above, below, or laterally within the gas storage reservoir depending upon the geology of each gas storage project. These wells need to be placed within porous and permeable geologic formations capable of being monitored. The location and design of observation wells should take into consideration:

1. Observation wells located within the storage zone that are suitable for monitoring reservoir pressure, can be considered, but should be placed within the buffer zones in order to limit artificial penetrations within the gas storage field reservoir.

2. Potential migratory paths from the reservoir to another formation.

3. Fluid interface monitoring at the location of the reservoir spill point.

4. Permeable zones and stratigraphic traps above the storage zones.

5. Low-permeability zones, formations or fields adjacent to and in communication with the storage zones.

Observation wells should be constructed to the same standards and criteria established in the well construction guidelines for gas storage wells to ensure all safety considerations. Groundwater monitoring wells should also be considered for installation in an effort to monitor underground sources of drinking water (USDW).

Recommendation: We recommend the collection and recording of pressure data for all uncemented annuli and injection tubing. Additionally, observation wells should be utilized at all UGS sites, and installation of groundwater monitoring wells to evaluate USDW should be considered.

Inspection, Testing, and Maintenance of Wellheads and Valves (Section 1726.8)

On this topic, the proposed DOGGR regulatory language is fairly adequate, but additional details are lacking and are herein proposed. All wellheads and valves need to be function- and pressure-tested and capable of withstanding the maximum allowable operational pressures in the UGS field.

Recommendation: All wellheads and valving should be function-tested and pressure-tested at least annually, and should be rated to withstanding the maximum allowable operational pressures within the UGS field.

Well Leak Reporting (Section 1726.9)

This subsection of the new UGS regulations requires mandatory reporting of well leaks and provides the definition of what constitutes a “reportable leak.” No reporting of other events relating to subsurface and surface incidents or a missed accident is required. The reporting of leaks is adequate for the intended purpose, although the reporting of other events relating to subsurface and surface incidents or a missed accident should be required.

A lot can be learned by the collection and analysis of failures and missed accidents in wellbores, wellheads as well as surface facilities. Data of this kind are often used by a specific industry to improve the safety record and culture overall. In general, the incident doesn’t have to necessarily lead to a gas released to highlight a weakness in operating practices or structures.

In order to improve the safety culture across this industry, it is important to implement mandatory record keeping and reporting of all subsurface and above surface integrity issues, near-miss accident scenarios (irrespective of consequences), and any remediation and mitigation actions taken. This reporting, as opposed to the “reportable well leaks,” is not as time sensitive and could be integrated into a yearly reporting or as part of the 3-year UGS project review. This information would also, of course, be used directly in the risk assessments.

We also recommend that the division have a periodic review of all reported data and share lessons learned across the industry.

Recommendation: We recommend that a record of mandatory reporting of all integrity issues should be implemented independent of the size of the release. The time line and urgency of the reporting can be varied, depending on the gravity of the release according to the definition in this section of the regulations.

Requirements for Decommissioning (Section 1726.10)

The UGS regulations seem adequate for the decommissioning of a UGS project. However, the regulations do not define or require a pathway to reporting for the plugging and abandoning of a single (or multiple) wellbores.

Historically, a large number of incidents have happened in abandoned wells or fields (Evans, 2009; Folga et al., 2016). It is imperative that all safety precautions be taken prior to abandonment as detection of issues and interventions post abandonment is extremely difficult, costly, and intrusive.

We recommend that language to specify approved abandonment procedures, or to refer to industry standard practices (if deemed adequate), should be added to this section. For example, the abandonment procedure could require assessment of the integrity of the well casing and cement, followed by temporary plugging and abandonment with daily monitoring of annuli pressures for a time of at least a year before final approval to permanently abandon the well is granted. At the least, DOGGR needs to determine whether the current industry standards are adequate.

Recommendation: We recommend that the UGS regulations describe an adequate path to wellbore abandonment. Furthermore, DOGGR needs to determine whether the current industry standards are adequate.

Side bar: Safety Culture

NOTE: The following side bar was contributed by Professor Najmedin Meshkati, a member of the CCST Project's Steering Committee, who was also a member of the "Committee for Analysis of Causes of the Deepwater Horizon Explosion, Fire, and Oil Spill to Identify Measures to Prevent Similar Accidents to the Future," formed by the National Academy of Engineering/National Research Council. The following text is partially adopted from the published report of that same committee, entitled "Macondo Well Deepwater Horizon Blowout: Lessons for Improving Offshore Drilling Safety," (pp. 92-93 of Macondo Well-Deepwater Horizon Blowout: Lessons for Offshore Drilling Safety, National Research Council, 2012) and also updated and augmented by Professor Najmedin.

Although the emphasis in the text of this side bar is on the type of accidents similar to the Macondo Well blowout accident, the overall ideas concerning safety culture are broadly applicable, including to underground gas storage facilities.

The steps taken by the nuclear power and other safety-critical industries to improve system safety are reminiscent of the challenges presently confronting the offshore drilling industry. Although there are significant differences between the oil and gas industry and other industries (as discussed in this chapter), the safety framework and perspectives developed by those other industries can provide useful insights. According to the Swedish Radiation Safety Authority, an organization has good potential for safety when it has developed a safety culture that shows a willingness and an ability to understand risks and manage activities so that safety is taken into account (Oedewald et al., 2011). Other industries, regulatory agencies, trade associations, and professional associations have also addressed safety culture (for example, see Reason, 1998; U.S. NRC 2009; 2011; Nuclear Energy Institute, 2009; CCPS, 2005; IAEA, 1992).

The U.K. Health and Safety Executive defines safety culture as "the product of individual group values, attitudes and perceptions, competencies and patterns of behavior that determine the commitment to, and the style and proficiency of, an organization's health and safety management." Creating safety culture means instilling attitudes and procedures in individuals and organizations ensuring that safety issues are treated as high priority, too. A facility fostering strong safety culture would encourage employees to cultivate a questioning attitude and a rigorous and prudent approach to all aspects of their jobs, and to set up necessary open communication between line workers and middle and upper management (Meshkati, 1999).

A commonly accepted and widely used/cited definition of safety culture was jointly developed through an unprecedented collaboration of the government regulator, United States Nuclear Regulatory Commission (U.S. NRC), and the industry's created self-regulatory body, the Institute of Nuclear Power Operations (INPO). According to this definition, safety culture is "the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety over competing goals to ensure protection of people and the environment" (INPO, Traits of a Healthy Nuclear Safety Culture, INPO 12–012 April 2013).

An effective and healthy safety culture embodies the following generic traits [The traits are adapted from the U.S. Nuclear Regulatory Commission Safety Culture Policy Statement (U.S. NRC, 2011)]:

- Leadership safety values and actions: Safety is treated as a complex and systemic phenomenon. It is also a genuine value that is reflected in the decision-making and daily activities of an organization in managing risks and preventing accidents.

- Personal accountability: All individuals take personal responsibility for safety and contribute to overall safety.

- Problem identification and resolution: Issues potentially affecting safety are readily identified, fully evaluated, and promptly addressed and corrected.

- Work processes: The process of planning and controlling work activities is implemented so that system safety is maintained. The most serious safety issues get the greatest attention.

- Continuous learning: Opportunities to learn about ways to ensure safety are sought out and implemented by organizations and personnel. Hazards, procedures, and job responsibilities are thoroughly understood. Safety culture strives to be flexible and adjustable so that personnel are able to identify and react appropriately to various indications of hazard. These processes and approaches are embedded in management systems and processes that are widely used within the organization.

- Environment for raising concerns: A safety-conscious work environment is maintained, where personnel feel free to raise safety concerns without fear of retaliation, intimidation, harassment, or discrimination. They perceive their reporting as being meaningful to their organizations and thus avoid underreporting.

- Effective safety communication: Communications maintain a focus on safety. Knowledge and experience are shared across organizational boundaries, especially when different companies are involved in various phases of the same project. Knowledge and experience are also shared vertically within an organization.

- Respectful work environment: Trust and respect permeate the organization.

- Questioning attitude: Individuals avoid complacency and continuously challenge existing conditions and activities to identify discrepancies that might result in unsafe conditions. A subordinate does not hesitate to question a supervisor, and a contractor employee does not hesitate to question an employee of an operating company.

[It should be noted that the above definition and traits of healthy safety culture, which have been jointly developed by the U.S. NRC and INPO, have been adopted, almost exactly, by other federal regulatory and safety agencies, e.g., Bureau of Safety and Environmental Enforcement (U.S. BSEE, 2013).]

- Investigations of several large-scale accidents in recent years provide clear illustrations of the consequences of a deficient safety culture. A collision of two trains of the Washington Metropolitan Area Transit Authority (WMATA) Metrorail that occurred in June 2009 resulted in nine deaths and multiple passenger injuries. The National Transportation Safety Board (NTSB) found that WMATA failed to implement many significant attributes of a sound safety program (NTSB 2010).

- The NTSB, which, by quoting Professor James Reason, has called it an "organizational accident," stated that "the accident did not result from the actions of an individual but from the 'accumulation of latent conditions within the maintenance, managerial and organizational spheres' making it an example of a 'quintessential organizational accident'" (NTSB, 2011; Reason, 1998).

- The rupture of the natural gas transmission pipeline that was owned and operated by the Pacific Gas and Electric Company (PG&E), in a residential area in San Bruno, California, on September 9, 2010, is another example of catastrophic "organizational accident" ("Mismanagement Blamed for Bay Area Gas Disaster," *New York Times*, August 30, 2011, by Matthew L. Wald), which has been attributed to the safety culture of the company and lax regulatory oversight, according to the NTSB (2011). PG&E estimated that 47.6 million standard cubic feet of natural gas was released; the released natural gas ignited, resulting in a fire that destroyed 38 homes and damaged 70. Eight people were killed, many were injured, and many more were evacuated from the area.

- Explosions and fires at the BP Texas City Refinery in March 2005 killed 15 people and injured 180 others. The U.S. Chemical Safety and Hazard Investigation Board concluded that the disaster was caused by organizational and safety deficiencies at all levels of the BP Corporation. The U.S. Chemical Safety and Hazard Investigation Board has identified "safety culture" as one of the four "key issues" which caused this accident, along with regulatory oversight, process safety metrics, and human factors (CSB, 2007).

- According to three major seminal reports that investigated the BP Deepwater Horizon (DWH) blowout, inadequate management systems and poor safety culture were major underlying causes of that blowout [Deep Water: The Gulf Oil Disaster and the Future of Offshore Drilling, Report to the President - National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling - January 2011 (2011); the National Research Council's Macondo Well-Deepwater Horizon Blowout: Lessons for Offshore Drilling Safety (2011); and the U.S. Chemical Safety Board (CSB) (June 2016).]

- The American Petroleum Institute (API) Recommended Practice 1173, Pipeline Safety Management System Requirements (First Edition, June 2014, Draft Version 11.2; https://www.pipelinelaw.com/wp-content/uploads/sites/19/2014/09/API-RP-1173.pdf) entire section 10.6 is about "Evaluation of Safety Culture." It recommends that:

- "The pipeline operator shall establish methods to evaluate the safety culture of its organization. Operators shall assess the health of their safety culture using methods that assess employee perception of the safety culture. Methods to assess the perception of the culture include but are not limited to questionnaires, interviews, and focus groups. Policies, operating procedures, continuous vigilance and mindfulness, reporting processes, sharing of lessons learned and employee and contractor engagement support an operator's safety culture. Observations and audits of how each of these are being applied in the daily conduct of operations provide

> indications of the health of an organization's safety culture, including conformance with policies, adherence to operating procedures, practicing vigilance and mindfulness, utilizing reporting processes, integrating lessons learned and engagement of employees and contractors. Failure in application of these provides an indication of potential deterioration of the safety culture. Management shall review the results and findings of perception assessments, observations and audits and define how to improve application of the supporting attributes." (p. 17)

The U.S. Department of Transportation's Pipeline and Hazardous Materials Safety Administration's (PHMSA) "fully supports the implementation of RP 1173 and plans to promote vigorous conformance to this voluntary standard." Although PHMSA has not yet issued an official safety culture policy statement, it has adopted the Safety Management Systems (SMS) concept and contends that it has been "actively advancing implementation of SMS and a *strong safety culture* within the pipeline and hazardous materials sectors is the next step in continuous safety improvement for America's hazardous materials transportation system." (emphasis added, PHMSA Administrator the Honorable Marie Therese Dominguez's written statement before the U.S. House of Representatives, February 25, 2016).

The American Gas Association (AGA), which is a trade organization representing over 200 natural gas supply companies and others, has also echoed and endorsed the importance of safety culture and its AGA's Safety Culture Statement states, "The AGA and its member companies are committed to promoting positive safety cultures among their employees throughout the natural gas distribution industry" (AGA, 2011).

Most recently, on May 18, 2017, the State of California's Department of Industrial Relations' (DIR) Occupational Safety and Health Standards Board has announced that it has approved adding safety culture as one of new elements to its revamped/updated regulations on refinery safety. [In this regulation, which has been applauded by the industry's trade association, the Western States Petroleum Association (WSPA), and which became effective on October 1, 2017, the "Process Safety Culture," is defined as: "A combination of group values and behaviors that reflects whether there is a collective commitment by leaders and individuals to emphasize process safety over competing goals, in order to ensure protection of people and the environment."] This order is enforced by CalOSHA's Process Safety Management (PSM) Unit, adding section 5189.1 to Title 8 of the California Code of Regulations. This element outlined in the regulation requires refinery employers to: "Understand the attitudes, beliefs, perceptions and values that employees share in relation to safety and evaluate responses to reports of hazards by implementing and maintaining an effective Process Safety Culture Assessment program" (CalOSHA, 2017b).

Side bar: ALARA and ALARP

The acronyms ALARA and ALARP mean "as low as reasonably achievable" and "as low as reasonably practicable," respectively. While these words seem to be similar, they are not used identically in practice.

The concepts first arose in the field of radiation protection for occupational workers, in which health physicists and nuclear-medicine professionals struggled with how to explain the idea that, although there are strict regulatory limits to the amount of harmful lionizing radiation to which a worker can be exposed, *sometimes meeting those limits is not sufficient*, and *sometimes not meeting them is acceptable.* These concepts were later broadened to apply more generally to other technical areas, such as other fields of health and safety where exposures occur to workers or the general public, or where the release of harmful substances into the environment can cause harm to individuals or other receptors.

The ALARA (as low as reasonably achievable) concept

The U.S. Nuclear Regulatory Commission (U.S. NRC, 2017a) uses the following definition for radiation protection:

As defined in Title 10, Section 20.1003, of the Code of Federal Regulations, ALARA is an acronym for "as low as (is) reasonably achievable," which means making every reasonable effort to maintain exposures to ionizing radiation as far below the dose limits as practical, consistent with the purpose for which the licensed activity is undertaken, taking into account the state of technology, the economics of improvements in relation to state of technology, the economics of improvements in relation to benefits to the public health and safety, and other societal and socioeconomic considerations, and in relation to utilization of nuclear energy and licensed materials in the public interest.

The National Council on Radiation Protection (NCRP, 1999) explains ALARA this way, again for radiation protection:

In its presentation of dose limitations, the Council set specific upper limits of acceptable dose for occupationally exposed individuals, and the general public, with additional concern for the embryo/fetus. Through the inclusion of the ALARA principle, the NCRP wished to emphasize that adherence only to dose limits was not sufficient. Additionally, the specification in the ALARA principle that economic and social factors be considered has at times been overlooked, resulting in excessive monetary costs with little benefit. The ALARA principle should not be misinterpreted as simply a requirement for dose reductions irrespective of the dose level; sound judgment is essential in its proper application. Nevertheless, even at very low exposure levels, if simple and low-cost means would result in still lower exposures while retaining the beneficial outcome, sound judgment would indicate that such means should be encouraged.

The International Commission on Radiological Protection (ICRP) defines ALARA very succinctly (ICRP, 2007):

ALARA means "as low as readily achievable [with] economic and social considerations being taken into account."

To paraphrase the ALARA idea, it is not sufficient simply to meet the regulatory limits. Even if these limits are met, one must make "every reasonable effort" to do better, accounting for various factors, of which the most important are usually the state of technology and the costs in relation to the benefits. *In sum, broadly speaking, the ALARA concept comes into play when the regulations have already been met but when doing better is feasible.*

The ALARP (as low as reasonably practicable) concept

The ALARP concept is similar, but in practice it is usually brought into play when it is difficult to meet the strict regulatory limits.

The UK Health and Safety at Work Act (UK HSE, 1974; 2009) explains this idea as follows. Note that this explanation is not limited to radiation exposures:

ALARP stands for "as low as reasonably practicable," and is a term often used in the regulation and management of safety-critical and safety-involved systems. The ALARP principle is that the residual risk shall be reduced as far as reasonably practicable. … For a risk to be ALARP, it must be possible to demonstrate *that the cost involved in reducing the risk further would be grossly disproportionate to the benefit gained. The ALARP principle arises from the fact that infinite time, effort and money could be spent in the attempt of reducing a risk to zero. It should not be understood as simply a quantitative measure of benefit against detriment. It is more a best common practice of judgment of the balance of risk and societal benefit.*

To paraphrase the idea, ALARP is often brought into play when a regulatory limit has not been met, but the cost of doing so "would be grossly disproportionate to the benefit gained." That is, at a certain point a judgment is made that meeting the limits is not "reasonably practicable," accounting for various factors, of which the most important are usually the state of technology and the costs in relation to the benefits. *In sum, broadly speaking, the ALARP concept comes into play when the regulations cannot be met in a "reasonably practicable" way because the benefits to be gained from doing so are disproportionately larger than the costs required.*