REPORT ON THE SAFETY MANAGEMENT SYSTEM IMPLEMENTATION

AT THE CALIFORNIA PUBLIC UTILITIES COMMISSION

Paul Schulman and Karlene Roberts

Center for Catastrophic Risk Management
University of California, Berkeley

March 16, 2016

Agenda

- Properties of an Effective Safety Management Systems
- Observations and Concerns in the Internal Efforts to Develop an SMS
- External Challenges in the developing of an SMS
- A Model for the CPUC as a leading Safety Institution

Agenda

- **Properties of an Effective Safety Management Systems**
- Observations and Concerns in the Internal Efforts to Develop a SMS
- External Challenges in the developing of an SMS
- A Model for the CPUC as a leading Safety Institution

Elements of Effective Safety Management Systems

- a clear and consensus-based conception of "safety" within an organization and regulated organizations.
- safety is treated as a *prospective* property, a *systems* process that produces successful outcomes.
- safety is defined and organized at the start around what specific ("never") events are to be prevented at the highest priority.
- events or operating conditions are then identified that could be *precursors* to never events -- make them more likely or reduce confidence that they can be avoided.

SMS elements (Cont'd)

- a resistance to trade-off time and money spent on the highest priority safety threats ("never" events) and their precursors with other values – e.g. increased output (including service), speed, efficiency or cost reduction.

- there is public and political support for resisting these trade-offs.

- a commitment throughout the organization to ongoing analysis of risks and their precursors and to the possibilities of error and incompleteness in the analysis and understanding of these.

SMS elements (Cont'd)

- safety analysis is an ongoing activity widely distributed throughout the organization at all levels

- many individuals play the role of "safety professionals" and "partisans of the neglected perspective".

- "reliability" includes these error-management elements. It is *not* defined only in terms of the constancy or surety of production output, capacity or service.

- in its process focus, reliability *includes* safety -- there cannot be safety without reliability.

SMS elements (Cont'd)

- Rules and procedures are modified and updated to reflect a shifting knowledge base covering "better practice" and an *upgrading of safety goals* as a result of new knowledge and technology.

- there is careful risk assessment -- the likelihood and severity of failures and accidents are analyzed and the risks are prioritized.

- human and organizational factors are also included as risk or risk mitigation variables.

SMS elements (Cont'd)

- effective safety management systems are also attentive to uncertainty itself as a special type of risk.
  - they manage against *possibilities* when probabilities cannot be formally computed
  - they weigh uncertainty in consequences flowing from an error or failure and often manage to worst-case scenarios because of this.

SMS elements (Cont'd)

- Clear and consistent signals of commitment and support for safety are sent from top and higher-level personnel in the organization to all members and also to organizations in its environment -- vendors, clients, regulated organizations, overseers and the public.

- Institutional incentives support the safety management system (training and career advancement in safety)

- effective safety management systems will be founded on a recognition that accidents and failures can happen and therefore safety management will also include strategies of emergency response, resilience and recovery

SMS elements (Cont'd)

Finally, effective safety management systems are embedded in what has come to be termed a "safety culture":

- an encouragement of the reporting of mistakes and error.
- a prospective focus on risks.
- a respect for expertise over hierarchy on safety issues.
- resistance to simplification and a widespread sensitivity to the possibility of representational error.
- a continual search for improvement.

Agenda

- Properties of an Effective Safety Management Systems
- **Observations and Concerns in the Internal Efforts to Develop a SMS**
- External Challenges in the developing of an SMS
- A Model for the CPUC as a leading Safety Institution

Some observations on CPUC Safety Management System Development

- A number of positive developments in moving the CPUC toward its SMS
  - a recognition by many of the ongoing nature of safety management as an organizational project and the need for constant monitoring, questioning and commitment to improvement necessary for safety management regimes if they are to be successful.

Observations II

- a restructuring of general rate case proceedings to include a risk assessment of specific risk issues associated with utility investment proposals (Safety Mitigation Assessment Proceeding and Risk Assessment Mitigation Phase)

- work on the development of an agency emergency response plan, with an Incident Command Structure

- development of the Safety Flag program to encourage reports from many individuals within the CPUC

Observations III

- the end of year safety en banc session (a beginning in raising safety discussions to include utility and Commission officials in a public forum)

- monthly performance metrics proposed in the Safety Management Strategy Action Plan and now implemented by SED in its monthly reports

Selected concerns, questions and suggestions

Clarity and depth of understanding of SMS concepts and objectives throughout the CPUC

- A clear and consistent concept or definition of "safety"?

  -- focus of the SMS itself – in-house or external (to the regulated utilities)?

  -- individual event-focused (slips, trips and falls)or *system* safety?

  -- utility "safety" as rule compliance, or more?

  -- safety measures – lagging vs leading (precursor)indicators?

- A general issue in the understanding of “reliability” in relation to safety
  -- "reliability" defined by the Commission and by its regulated utilities is only *service* reliability: output and capacity
  -- this leads to the idea that reliability and safety are different and potentially conflicting values
  -- but for effective SMS’s reliability *includes* safety – both are founded on the management of error:
  errors in estimation, description, attention and understanding of operations and processes

Suggestions

- the proposed CPUC advanced safety seminar brown-bag lunch meetings is a good idea
- a safety en banc might be used to lay public groundwork for merging safety and reliability perspectives
- could renaming the CPCN (something like: Certificate of Public Service and Safety) establish a stronger legal overlap between reliability and safety?

Need for wider distribution of SMS roles, responsibilities and incentives

- risks of a single safety officer or a single safety committee
- need for the safety flag system to penetrate down to the lowest level across all divisions
- need for supports and incentives for safety monitoring and actions
- Need for clarity in roles of advisor, advocate and enforcer
  - confusion in specific differences in role content
  - possible advantages in some role overlap

Suggestions

- assign “risk owners” to safety projects and safety flag issues
- include staff in a safety advisory council
- attach the safety flag system to subgroups of this council
- awards, bonuses or other recognition for safety-related suggestions and actions
- investigate changing legal restrictions on advisor, advocate and enforcement roles

Suggestions (Cont'd)

- a Commission philosophy about regulation beyond rules?
- promote an association of auditors and inspectors across the branches and programs that would allow them to meet and share experiences, ideas and tips with one another. This might add to the promotion of professional identity among these personnel.

Enhancing risk assessment in the SMS

- Good progress in enterprise risk audit and in creation of RA group in the SED.
- Safety risk assessments now are a required part of rate cases
- But a great need to add granularity to risk factors assessed
- Human and organizational factors in safety and risk are often neglected
- So too is uncertainty neglected in risk calculation

Suggestions

- CPUC in its SMS can drive improvement in risk assessment methodologies, its own as well as the risk assessment methods employed in the utilities
- It can push for Process Safety (human and organizational) variables in R.A.s
- CPUC can also encourage incorporation of uncertainty in risk assessments

Need to improve safety metrics

- Monitoring and measurement are key functions for an SMS
- Metrics widely used for safety (incidents and accidents) are lagging and not leading indicators

Suggestions

- Safety is not simply about accidents, it's about conditions that preclude accidents. The Commission could help develop a set of precursor indicators that signal the strengthening or fraying of those conditions:
  - projects to develop these precursor indicators for each of the major industries and organizations it regulates. This should be done in close consultation with those organizations.
  - the discipline of Process Safety analysis has identified and developed metrics for many precursor variables. Consult such specialists.

Agenda

- Properties of an Effective Safety Management Systems
- Observations and Concerns in the Internal Efforts to Develop a SMS
- **External Challenges in the developing of an SMS**
- A Model for the CPUC as a leading Safety Institution

The External Environment for a Safety Management System for the CPUC

- an effective safety management system in the CPUC depends in no small measure on the presence of effective safety management systems, including safety cultures, in the organizations it is regulating.

- it also depends on support from governmental overseers in its environment and from the public

A note from observations

- it has been impossible for us in our interviews and observations not to be aware of the political conditions surrounding the Commission -- particularly the post-San Bruno political environment.

- attacks on the Commission by political leaders, by groups and in the media have focused on its regulatory competence as well as the relations it has with its regulated organizations, particularly PG&E. These attacks appear to have affected employee morale at all levels.

- It is evident to us that many people we have talked to at all levels are looking over their shoulders at their political exposure in relation to their tasks.

- Regulatory actions, ranging from rule-making, rate case decisions or settlements, inspection and audit observations and reports, incident investigations, findings and subsequent enforcements are all subject to legal and political push-back.

- In addition, new policy objectives are given to the CPUC by legislative action or pressure without consideration, it seems to us, of the institutional capacity of the CPUC, given current staffing and budgetary limits, to effectively carry them out.

- From our perspective a large issue in relation to the Commission's development of an effective safety management system is its need *to achieve some increased measure of institutional and political security and independence*.

Agenda

- Properties of an Effective Safety Management Systems
- Observations and Concerns in the Internal Efforts to Develop a SMS
- External Challenges in the developing of an SMS
- **A Model for the CPUC as a leading Safety Institution**

The CPUC as a Leading Safety Institution

- The CPUC , we believe, with the development of its safety management system should also be transforming itself more fully into an institution -- widely respected for its skill and its values with respect to safety

- "Institutions" (as opposed to simply "organizations") have significant stability and weight in relation to their environment.

The CPUC as a leading institution:

- The CPUC could become a clearinghouse for information and expertise regarding safety
  - make the CPUC a preeminent institution in the state, and possibly beyond, in the development, sharing and application of expertise in safety management, particularly in the area of process safety

-- It is likely that utility executives and operators will know more than inspectors, auditors and policy-makers within the Commission about specific engineering designs and operational requirements of their technical systems, **but**

-- it is not certain the utilities will know or follow industry "best" practice standards in managing these systems

-- it is even less likely they will see or understand the full picture in managing for safety and for interconnected infrastructure risk, or the current state-of the art in process safety management, or the latest developments in risk assessment

The CPUC could potentially be a leading institution in relation to all of these

A leading institution: Suggestions

- The CPUC could devote safety en bancs, sponsored workshops or public meetings with invited industry leaders, trade association officers and representatives of standards organizations such as the ISO to discussions of standards covering better safety practices in specific industries.
- Similar workshops could be sponsored to review latest research findings and better practices in process safety management

- The CPUC could also work with California Universities to support applied research projects in industrial engineering and other fields related to improving its safety regulation.
- It could also contract out to faculty in these universities for technical advice.
- The CPUC could, as suggested earlier, sponsor symposia and research projects on risk assessment and its improvement, particularly to incorporate more human and organizational variables.
- Perhaps a Public Purpose Fund might be created to support this research.

- Also, The CPUC could invite academic researchers or post-docs working in safety management, risk assessment or policy analysis to be visiting fellows for a year at the Commission, advising Commissioners and other staff members, and perhaps conducting seminars in their areas of expertise.

- another need the Commission could address is that of process safety training not only for its own staff but for the utilities also.

- Why not develop a course in process safety management taught within the CPUC that would be offered not only to its own staff at all levels but also to personnel in the utilities? A certificate of completion (not a certification) could be given to all who complete the course.

- This could be a way to help promote shared safety perspectives between the Commission and its regulated organizations.

- It could also contribute to the self-identification among personnel in both settings that they can indeed play a role as "safety professionals" in whatever job they occupy, in whatever organization, with a reference group of other individuals who adopt the same perspective.

A Note on Staffing Adequacy

- It seems obvious to us, and is forcefully stated in the Independent Review Panel Report on the San Bruno accident, that more staff are needed for both analysis and inspections to support the Commission's objectives in safety management and to provide for an effective SMS

- a safety management capacity model with respect to staff size and needed skills could be developed to more clearly identify, as well as support needed improvements in staffing. We believe the CPUC should consider as part of its capacity model, the use of resident inspectors on a rotating basis at the largest of the utilities it regulates

Changes in formal adversarialism?

- Consider ways to relax adversarialism to:
  - pursue joint R&D projects with regulated organizations that could lead to new improvements in their safety management systems
  - engage in joint root cause analyses of incidents and accidents outside of the official ALJ proceeding
  - engage in periodic long-term safety planning sessions with utilities outside of the rate case framework

Paul Schulman and Karlene Roberts

Center for Catastrophic Risk Management
University of California, Berkeley

CONFIDENTIAL

Report on the Safety Management System Implementation

At the California Public Utilities Commission

Paul Schulman and Karlene Roberts

Center for Catastrophic Risk Management
University of California, Berkeley

February 17, 2016

In this project at the CPUC we were asked to provide advice to the Commissioners and CPUC executive management that might help in preparing to implement an effective, state-of-the-art safety management system. We conducted interviews, made observations and reviewed relevant documents to identify current practice within the CPUC and to analyze strengths, as well to suggest as constructively and practically as possible, where current management and governance practices differ from what are considered to be better practices in safety management. Our analysis is placed within the context of over 50 years of combined experience observing and analyzing "high reliability organizations" in a variety of settings including including nuclear aircraft carriers, commercial nuclear power plants as well as infrastructures in electricity, gas, telecoms, rail, water, levee maintenance and marine ports and transport. We have also observed organizations with regulatory functions -- the FAA, NRC, Institute of Nuclear Power Operators (INPO) and the Atomic Energy Control Board of Canada (now the Canadian Nuclear Safety Commission).

At the same time we took account of the fact that the CPUC has an unusually diverse set of regulatory missions, involving quite different utilities and infrastructures, with different technologies and some with different legal and regulatory relationships with federal agencies. Where our analysis identifies conditions or practices that fall short of strong positive examples we have seen, we describe why we believe these differences might raise difficulties for effective safety management. We also identify alternate practices and suggestions for changes that might help to achieve a stronger safety management system within the Commission.

For this report we conducted, as part of our research and observations, 40 interviews and reviewed many documents, including the Safety Action Plan (and its recent February 2016 Update), Safety and Enforcement Division monthly reports, the safety flag proposal (and attended two Executive Safety Council meetings about this), the safety intervenor proposal, and earlier reports from the Crowe Horwath Group on SED operations, the Independent Review Panel on the San Bruno Accident, as well as the "Report on Key Findings From the CPUC Modernization and Reform Project," written by Edward O"Neill. We also attended a planning session in the ESC for the safety en banc (and watched the online video of the actual meeting).

As we undertook our observations and interviews we kept in mind the following questions (adapted from the safety management framework of the FAA) related to successful operation of safety management systems:

1. Safety Policy
   Is there an overall philosophy of safety?

    a. Are explicit and agreed-upon definitions of "safety" and "risk" present?

-- What is the balance between internal personnel safety and external infrastructure safety?
-- Is safety both individually based (slips, trips and falls) and system focused?
-- Is there a concept of system safety that connects system reliability to safety?
-- Does a safety focus extend to the environment? To successive generations?

b. Is "safety" only retrospectively defined (intervals without accidents) or prospectively understood (through leading and not lagging indicators)?

2. Safety Risk Management

Are systematic and ongoing risk assessment and risk management processes in place to cover regulated organizations?

a. Is there an assessment of probabilities and consequences?
b. Is there a prioritizing of risks (the most significant events to prevent)?
c. Is there an identification of precursor conditions with respect to risk?
d. Is there identification and analysis of interconnected risks across infrastructures?
e. Is there recognition of the differences between states of risk, uncertainty, ambiguity and ignorance?
f. Are there strategies and structures for ongoing learning, revisions and improvements in risk management at the CPUC?

3. Safety Assurance

Are there commitments and strategies to measure and improve Safety Management itself?

a. Are there multiple indicators of safety management performance at the CPUC?
-- Are there precursor indicators for detecting lapses in effectiveness? (e.g. loss of consensus on safety goals; lapses in communication, etc.)
-- Are corrective action (safety flag) reports circulated? Are they speedily investigated and closed?
-- Are root-cause investigations of accidents undertaken? What's the time lag between events and final reports?

b. Are regulated organizations at least meeting all industry safety and reliability standards?
-- Are non-compliance reports from regulated organizations investigated?
-- Are frequency and number tracked for a trajectory of improvement?
-- Are they making investments to exceed some industry standards?
-- Is there a commitment and strategy in place to encourage implementation and continuing development of reciprocal safety management systems within the CPUC's regulated organizations?

c. Does the CPUC and its regulated organizations have in place emergency response and crisis management frameworks to handle critical events should they occur?

4. Safety Promotion
   Is there an ongoing promotion and development of the safety management system?

   a. Who "owns" the emerging safety management system at the CPUC? What are the organizational incentives that support it's promotion and development?
   b. Do safety management goals and practices penetrate down to all levels and across all units?
   c. Are ongoing learning, revisions and improvements to the SMS likely?

While at this point in the Commission's SMS development there are few answers to these questions, CPUC members at many levels may want to refer to them as a reference point to guide and mark progress in SMS development. At the same time many of the same questions should also be asked in relation to the CPUC's regulated organizations because research and emerging better practice now recognize that a reciprocal dependency is likely to exist between the success of a regulator's SMS and the existence of complimentary and effective SMS's in its regulated organizations. As we will argue, formal adversarial relationships alone cannot promote this dual effectiveness. We do not believe the CPUC, despite its own safety management system, will be able simply to audit, inspect, fine and punish its way to fulfillment of its regulatory goals and public expectations regarding safety.

Our Observations, Findings and Suggestions

This report focuses on foundational preconditions for the development of an SMS and where we believe the CPUC is at the moment with respect to them. We also highlight some strengths and weaknesses we've observed in our observations and interviews bearing on prospects for the future development of an SMS at the CPUC. Finally, we discuss some changes we believe are going to be necessary in agency culture, practice and support if a first-class and effective SMS is eventually to be achieved. Some of these changes will not be rapid or easy. Some of them it seems to us are within the ability of CPUC leaders and members to effect, but some of them will require acceptance and support from authorities outside the CPUC. Many of our suggestions will be posed as questions for members of the CPUC itself to consider. CPUC leaders and staff know far better than we do whether and how our suggestions could be implemented and what their likely impacts might be.

We start with a description of some specific organizational conditions which, from our prior research and experience with what we term "high reliability" organizations (HROs), we believe are important for a safety management system to be effective.

I. Elements of effective safety management systems

1. The first element is a clear and consensus-based conception of "safety" within an organization -- what constitute design-based safe conditions for operations. But the management of safety is organized at the start around what specific ("never") events are to be prevented at the highest priority. Then through careful analysis events or operating conditions are identified that could be precursors to never events, that is, make them more likely or reduce confidence that they can be avoided. A great deal of managerial attention is directed to staying out of precursor zones carefully defined in relation to these precipitating conditions or events. The definition of safety dominant in HROs therefore is not simply the absence of harmful events and the failure of things to go wrong. It is not identified retrospectively as events that didn't happen. Safety is understood to be things going right -- the design-based outcome of operations conducted and bounded as planned. Effective safety management systems consider safety to be a *prospective* property, a *systems* process that produces successful outcomes. It is monitored by leading indicators of the integrity of these system processes, not simply a retrospective count of individualized events like slips, trips and falls[1]. The modern conception of safety embraces system safety -- strategies to protect against errors, failures and events that can ramify outward from one point to include a wider set of interconnected elements with larger and more adverse consequences.

2. There is also a resistance in these organizations to trade-offs between time and money spent on the highest priority safety threats ("never" events) and their precursors even if they are of relatively low likelihood, and other competing values such as increased output (including service), efficiency and cost savings. There is public and political support for resisting these trade-offs.

3. In addition there is a commitment throughout the organization to ongoing analysis of risks and their precursors and to the possibilities of error and incompleteness in the analysis and understanding of these. The valuation of safety includes an aversion to representational error -- errors in estimation, specification, attention and understanding of operations and processes that may have connections to safety[2]. Safety analysis is an ongoing activity widely distributed within the organization at all levels, with different degrees of formality. With respect to safety many individuals play the role of "partisans of the neglected perspective".

---

[1] For recent literature that elaborates these two perspectives and supports the "system process" focused approach to safety see: Eric Hollnagel, *Safety I and II: The Past and Future of Safety Management* (Ashgate Publishing, 2014) and Sidney Dekker, *Safety Differently* (CRC Press, 2014).

[2] For a classic work on representational errors and their impact on safety see James Reason, *Human Error* (Cambridge University Press, 1990) and more recently Daniel Kahneman, T*hinking Fast and Slow* (Princeton University Press, 2013).

4. In the organizations with the best safety management systems, "reliability" includes the error-management regime described above. It is *not* defined simply in terms of the constancy or surety of production output or service. In this respect and in its process focus, reliability *includes* safety and there cannot be safety without reliability.

5. In HROs rules and procedures are of major importance but they are not static. They are frequently modified and updated to reflect a shifting knowledge base covering "better practice" in operations and an *upgrading of safety goals* as a result of new knowledge and technology.

6. Careful risk assessment (including "bow tie" analysis[3]) is also part of effective safety management systems. The likelihood and severity of failures and accidents are analyzed and the highest risks are ranked in a risk register. But this assessment is not founded solely on technical failure scenarios. Human and organizational factors are also included as risk or risk mitigation variables. Further, risk assessment does not mean attending only to formal risk scores of probability and consequence. It is also founded on experiential knowledge among operators and maintenance personnel. Effective safety management systems are also attentive to uncertainty itself as a special type of risk and consider *possibilities* even when formal probabilities cannot be computed. They also weigh the ambiguity that might surround understanding the full consequences flowing from an error or failure[4] and often operate under worst-case scenarios because of this. Being in unstudied or unmeasurable conditions is seen as risky in its own right and operating under these conditions has been prohibited by some regulatory organizations as a strategy of safety management[5].

7. An effective safety management system will be founded on a recognition that accidents will happen and therefore safety management must also include strategies of emergency response, resilience and recovery. Procedures for declaring an emergency are clear. A special incident response group may be provided for in these procedures with distinct roles described for individuals to play in case of an emergency[6]. There are also provisions for learning from accidents, failures and lapses -- such as root cause analysis.

8. Additionally an effective safety management system is one which would periodically measure and monitor itself -- taking its own temperature concerning fluctuations in mindfulness, mutual trust, cooperation, shared perceptions, and communication across sections, divisions and hierarchical levels. These can be measured by surveys as well as by behaviors. The Institute of Nuclear Power Operators, for instance, looks at the cleanliness of work spaces in its nuclear plant inspections as a proxy for attentiveness and attitudes of care among maintenance workers.

---

[3] An analysis which elaborates multiple causes of a single undesirable event followed by an elaboration of multiple consequences.

[4] A very useful distinction between risk, uncertainty, ambiguity and ignorance has been offered by U.K. risk analyst Andrew Stirling in "Keep It Complex" Nature, n. 468 (20/30 December 2010).

[5] It is a violation of federal regulations (10CFR50) to operate U.S. nuclear power plants "outside of analysis" a regulation enforced by the NRC.

[6] There are now formal federal and state protocols for planning and organizing emergency response activities in the National Incident Management Systems (NIMS) developed by the Department of Homeland Security and the State of California's State Emergency Management System (SEMS).

Who is sent to represent units at safety meetings and how many employees attend general meetings concerning safety are additional proxy measures of interest and commitment to an SMS. A safety management system, like safety itself, is not a once and for all solution or achievement for any organization. It must be continually worked on, renewed and restored against inevitable entropy and decay in the face of other pressures and priorities in the organization.

9. Another element in effective safety management systems consists of institutional roles related to safety management and clear institutional incentives in support of the SMS. Clear and consistent signals of commitment and support for safety are sent from top and higher-level personnel in the organization to all its members but also to organizations in its environment -- vendors, clients, regulated organizations, overseers and the public. Safety as a mission is surrounded with institutional incentives and that means career incentives. Safety analysis, assessment and improvement are taken up as part of the professional identity of employees at many levels. Safety management system roles and responsibilities are also connected to performance assessment and career advancement. In too many organizations with weak commitments to safety, safety jobs are career dead ends.

10. Finally, effective safety management systems are embedded in an overall set of assumptions, values and attitudes widely shared throughout an organization: what has come to be termed: a "safety culture". In our observation of strong safety-focused organizations the following have been present:

-- a widespread valuation of safety as a dominant objective throughout the organization

-- an encouragement of the reporting of mistakes and error

-- a prospective focus on risks[7]

-- a respect for expertise over hierarchy on safety issues

-- a resistance to simplification and a widespread sensitivity to the possibility of representational error

-- a continual search for improvement.

II. Observations of and suggestions to the CPUC relative to the above SMS elements in its initial period of SMS development

In our interviews and observations conducted at the CPUC we observed a number of positive developments regarding its formulation of a safety management system relative to the 10 elements noted above. There is excellent recognition, in many places, of the ongoing nature of

[7] This has been termed by two analysts: "a preoccupation with failure" (K. Weick and K. Sutcliffe, *Managing the Unexpected*, Jossey-Bass, 2015.)

safety as an organizational project and the need for constant monitoring, questioning and commitment to improvement necessary for safety management regimes if they are to be successful. Also recognition of the need for continual data gathering and analysis -- the monthly performance reporting metrics proposed in the Safety Management Strategy and Action Plan and now implemented by SED is an excellent start, particularly if some of these metrics are normalized for factors such as time of year, federal pre-emption, staff turnover and then analyzed for trends over multiple years. Some of these and more prospective precursor metrics might ultimately serve as a foundation for the development of enhanced safety indicators not only within the CPUC but throughout its regulated industries.

The restructuring of rate case proceedings to include a risk assessment of specific safety issues associated with utility investment proposals is also an important step and should signal the Commission's commitment to emphasizing safety especially if the Commission is committed to the enhancement of risk assessment methods used internally and by regulated utilities. The commitment in the action plan to develop an agency emergency response plan, with an Incident Command Structure is also an important step on the road to an effective SMS. Also the initial development of the "safety flag" system lays a foundation for improved communication about risks across sections, divisions and hierarchical levels. The proposed creation of an external Safety Intervenor to place safety advocacy squarely within the formal legal proceedings of a rate case also testifies to the Commission's rethinking of the role of safety advocacy in its adjudicary processes.

We also see as positive mention in the action plan of a career ladder associated with safety management, with promotion possibilities for staff in this organizational domain, and the commitment to ALJ and staff training in the Action Plan Update. Finally, the end of the year safety en banc session was also a beginning in raising safety discussions to include utility and Commission officials in a public forum. We will discuss each of these above developments and proposals in more detail in relation to other observations and suggestions we make in this report.

Our interviews, observations and review of documents also lead us, however, to raise the following concerns, questions and suggestions. We pose them in relation to the numbered SMS elements described above.

1, 2. A clear conception of "safety" and safety management systems? One striking finding we discovered in our interviews is that there doesn't seem to be a clear conception or definition of safety shared throughout the Commission or across divisions or even across branches within the SED. We have heard the call for "more safety" but it's not clear that there's an underlying understanding of what that means. In addition to this ambiguity, there was also a lack of clarity on the objectives of or on what constitutes a safety management system. Some interviewees thought the SMS was to be focused only on workplace safety within the CPUC itself. Others thought an SMS was only appropriate for operators of the utilities the Commission regulates.

A number of interviewees also cited uncertainties in how to measure safety as well as disagreements about how to approach safety as a regulated property (we were told by an

inspector in one branch of SED: "From my perspective if an organization is following rules and is in compliance that's safety" and yet by an inspector in another branch: "We have to look beyond the regulations in our work.").

It is one thing to expect that strategies of safety enforcement might differ somewhat across different industries and also depending upon federal pre-emption of some CPSU regulatory responsibilities. But it is another if the concept of safety itself does not have clear content or agreed-upon meaning within an organization. From the standpoint of the development of a safety management system this would seem to be a weak foundation. The good news side of this is that this stage in the development of the SMS would seem to be a great time to initiate some Commission-wide discussions leading to a statement about safety that can be a useful reference point, while still recognizing some diversity in management and regulatory approaches appropriate to different Divisions and different branches within SED. The safety seminar brown-bag lunch sessions proposed in the Safety Action Plan Update (February, 2016) would seem to be a great venue for the promotion of this. Possibly a retreat (a suggestion of Commissioner Picker) could help spread the word about the goals and purposes of an SMS and solicit ideas and suggestions about strategies for its design and implementation.

We would suggest that part of Commission discussions be devoted to identifying major safety events to be avoided, and their precursors, both in the Commission itself and in its various regulated industries. We were told by one of our interviewees that this search for the highest priority events to be avoided might cause problems, given the diversity of CPUC missions. But within the different divisions and the diverse branches of SED, if highest priority events are identified, in both internal operations (say through the enterprise risk audit undertaken by Carl Danner) and in regulated organizations (through both agency and utility risk assessments) the same process can occur. In so doing these units will be discovering a variety of additional enterprise and safety-related risk precursors, some of which might well require Commission-wide policy attention. Without the starting focus on the worst and/or most consequential "never" events, the search for safety can become a disconnected set of efforts whose focus would not be guided by clear principles of inclusion or exclusion.

Related to this another important topic for Commission-wide discussion is the recognition of system safety as an important focus, beyond individualized events such as slips, trips and falls. For example, increasingly the Commission may well find itself confronted with the likelihood that failure in one of its regulated infrastructures has the potential to induce failure in others. The infrastructures, due to their preoccupation with their own operations as well as proprietary safeguards against sharing information, in our view are not tending to these growing mutual interconnections and their ramifications for public safety[8]. The CPUC is in a position to have information about each of the infrastructures under its jurisdiction, information which they do not readily share with one another. Because of this, we believe one function of its SMS should

[8] For an analysis of growing interconnected infrastructure risk see E. Roe and P. Schulman, *Reliability and Risk: The Challenge of Managing Interconnected Infrastructures*, Stanford University Press, 2016.

become "connecting the dots" regarding interconnected infrastructure vulnerability and risk and, ultimately, the development of interconnected system safety regulation.

2, 3, 4. Resistance to safety trade-offs and the understanding of "reliability".

Another problem we see in current understanding of safety in the Commission concerns the relation between safety and reliability as concepts and as regulatory objectives. Currently the Commission preserves and operates on a distinction between these two. This distinction is recognized both at top levels in rate cases, and all the way down to the inspection level (as one inspector described it: "reliability is about the output of a plant; safety affects people" and another: "I don't worry about reliability at all."). It is a distinction, we have observed, that is made in many utilities as well.

But in our view this distinction rests upon a fundamental misperception. The "reliability" defined by the Commission and by its regulated utilities is only *service* reliability -- pertaining to the output of an organization. This is an extremely narrow definition. In accepting it the Commission unintendedly helps to preserve a situation where service reliability has been allowed to trump safety, when these are treated as distinctive, and in fact, oppositional values that must be traded-off in operational attention and decision-making, in the allocation of resources and in longer-term investment decisions. These presumed oppositional relationships between service reliability and safety are reinforced, but not resolved, by public and regulatory pressure and punishments for lapses in either.

At the same time, this presumed distinction has blurred a necessary overlap between managing for reliability and managing for safety. This overlap is well understood in the high reliability organizations we have researched. For them reliability includes safety. Both reliability and safety must be founded upon the management of error. Even service reliability requires the same aversion to representational error -- errors in estimation, specification, attention and understanding of operations and processes -- that we described earlier as associated with effective safety management systems. The same error or failure that kills people is also likely to shut down service. Also, in an era of great social dependency on infrastructure service, service interruptions can be hazardous, even life-threatening, events. (As we were told by more than one operator managing the California high voltage grid in the control room at CAISO "when there's a blackout people die.")

There cannot be safety without reliability in this larger sense. But reliability must be founded on risk assessments that to be accurate and complete must also include system safety hazards. Without this shared analytic foundation any presumed trade-offs between service reliability and safety will be managed under conditions of uncertainty, ambiguity and even ignorance and as such these trade-offs in themselves will not be reliable.

We believe a major foundational requirement for an effective safety management system at the CPUC is the recognition of the error in believing reliability and safety to be two separable strategies founded on differing analytic approaches to two conflicting values. Recognition of this

error should be promoted not only within CPUC activities from rate cases to inspections, but also in the utilities the Commission regulates.

It might be argued that the separation between service reliability and safety is embodied in law and thus will require major legal action to change. But in the California Public Utilities Code, in Section 451 it is stated that

> Every public utility shall furnish and maintain such adequate, efficient, just, and reasonable service, instrumentalities, equipment, and facilities, including telephone facilities, as defined in Section 54.1 the Civil Code, as are necessary to promote the safety, health, comfort, and convenience of its patrons, employees, and the public.[9]

This would seem to be a recognition in law that a major *purpose* of service is to promote public safety. It is hardly within the logical meaning of "service" then *to operate in ways that endanger the public*. This section of the Public Utilities Code it would seem provides a legal foundation for the indivisibility of service reliability and safety in the responsibilities of utilities. They should be indivisible in reliability and safety analysis, in rate cases and in utility management as well. But apart from legal arguments, it will be important for the CPUC to gain public and political support for this blending. This may well be a difficult, complex and long-term process and we return to this issue later in our recommendations.

2. Support for safety management perspectives within the CPUC. Relative to encouraging widespread support and involvement with the SMS the recent development of the safety flag system, as mentioned earlier, is a promising development. But it will work only if employees take it seriously, which requires that they believe safety issues they raise will in turn be taken seriously -- heard, evaluated and acted upon expeditiously at higher levels.

We expressed concern at the idea of an ombudsman whose responsibility it would be to review these flagged issues or a chief safety officer (CSO) as the primary advocate and person accountable for the performance of the SMS overall. Placing responsibility for this system in a single individual at the Executive Level, while it might appear to give authority and weight to the role, also runs the risk of reinforcing an impression of the reporting system as a process controlled by higher management. Should this happen the link between the ombudsman at the executive level and the rest of the organization could become quite attenuated.

Relative to a CSO, investing many functions -- triaging issues, following up on individual cases, providing a liaison to regulated firms, policy advocacy at the Commissioner level -- within a single person or office raises to us real reliability questions. Will one person or office be able to tend to each of these sufficiently? Will the functions be sustained across different individuals who will occupy the role -- individuals who may have different talents, interests, energy and attention and degrees of respect from Commissioners, Executives, Program Managers and other employees? Will the existence of a perceived "chief safety officer" mean that others in the

[9] For further legal analysis see Peter W. Hanschen and Gordon P. Erspamer ([2004]. A Public Utility's Obligation to Serve: Saber or Double-Edged Sword? Electricity Journal (December, 2004), 32-49.

Commission including program managers will think safety doesn't have to be their concern, that someone else is "on that job"? This has certainly happened in other organizations with chief safety officers.

Given the diversity of responsibilities and functions associated with the SMS, we believe it would it be worth thinking about investing many safety flag, advocacy and oversight functions in a larger group, such the Staff Advisory Committee proposed in the Safety Management Action Plan or possibly the Executive Safety Council (ESC) itself -- with sub-groups handing different aspects of these functions and its membership augmented by additional representatives across divisions and units, including lower-level staff. In similar programs we've observed in other organizations (often called Corrective Action Programs) each flagged issue is assigned a "risk owner", who assumes responsibility for pushing the evaluation and response to the flagged issue along and following through with reports to safety groups on the progress. Risk owners need not be restricted to those at higher executive levels. Some compensation could be offered for this activity.

5. The rule basis for safety. Clearly the Commission has rule-making processes already in effect covering both reliability and safety issues as it sees them. It has general orders that cover a great deal of its regulatory activity. It enforces rules on behalf of other agencies in gas (PHMSA) and rail (FRA) industries. As we indicated earlier in our interviews we discovered different conceptions at the inspection level concerning compliance and safety. For some inspectors compliance is safety. Others look beyond the rules to identify safety issues. One rail inspector noted an untied boot lace on a railyard worker and identified this as a potential issue. "What does that say about the safety culture there?" he asked. As important as rules and procedures and their enforcement are to promoting safety, from the standpoint of effective safety management it is also important for individuals to look beyond the rules and procedures. Formal rules may be incomplete insofar as addressing all issues important to ensuring safety. Further rules need to be updated to reflect shifts in knowledge.

One role for a safety management system is to continually scan for possible rule-based error, rules that fail to promote safety because they are ambiguous, impractical to follow or contradictory to other rules. When the scanning for rule-based error is turned to rules imposed on external organizations it can allow an SMS to play a key role in the promotion of regulatory reliability.

We see a difference between regulating for reliability and regulatory reliability. Regulatory reliability means a continuing reappraisal with respect to questions such as: To what extent do regulatory rules promote and enhance error management in regulated organizations and industries? To what degree might elaborated regulatory rules push organizations away from independent safety management on their own toward a formal and too narrow compliance definition of safety and reliability? To what degree might adversarial relations between regulators and organizations lead to the rigidification of safety management systems in both regulatory and regulated organizations?

We do not see evidence of clear or consistent Commission-wide philosophy of regulatory enforcement with respect to rules, nor on the role of inspector discretion beyond rules or on appropriate variation in this discretion in individual regulatory programs across industries. Nor do we see a strategy for the promotion of regulatory reliability within the safety management system evolving at the CPUC. We suggest that attention be paid to more uniform training among inspectors and auditors across branches and programs. We think it could also be helpful to promote an association of auditors and inspectors across the branches and programs that would allow them to meet and share experiences, ideas and tips with one another. This might add to the promotion of professional identity among these personnel.

3, 6. The CPUC SMS and Risk Assessment. A key element of any SMS is a strategy and method of risk assessment. The CPUC has moved ahead on this front. It has done an "enterprise risk" audit that has identified a variety of enterprise risks -- issues that could keep the Commission from reaching its objectives. In addition, Arthur O'Donnell and his group in the new Risk Assessment and Enforcement Section for SED's gas and electric programs, has begun to do risk assessments for the Energy Division and different branches of the SED. The rail programs also have some personnel specializing in risk assessment. The CPUC has additionally required utilities to present risk assessments in order to support rate cases brought before the Commission and these must now include safety risk assessments.

A current problem with risk assessment methodologies employed by many utilities is that they are conducted at such a high level of generality that they are more an analytic exercise than a managerial one. Often risk assessments often do not incorporate the knowledge gained by operators and lower line staff.

Further, as was described to us: "The utilities give us their methodology and show how it connects to their rate case filing. Their biggest problem at present is they can't connect the mitigation of risk with their budget and investments. This effort to have an economic approach to risk is new." This problem stems at least partly from the generality and small number of risk elements (sometimes called "risk drivers") employed in many risk analyses and calculations. This does not lead to much granularity in parsing out the variables and their individual contributions to risk or to changes they can make in risk year-over-year. As we were told by one utility analyst: "Trying to resolve year-to-year changes in risk is like trying to measure the thickness of a human hair with a yardstick."

Most of the risk drivers in these analyses are physical elements. There is a great need to expand the number of risk variables to include human and organizational factors that can contribute to or mitigate risks. These are likely to be precursor variables that can affect the likelihood of major catastrophic failures. The discipline known as "process safety" analysis has been developed, starting in the chemical processing industry, which focuses strongly on human factors and organizational conditions that affect risk.[10] It remains for risk assessment methodology to

[10] Center for Chemical Process Safety of the American Institute of Chemical Engineers, *Guidelines for implementing process safety management systems* (1994).

integrate indicators and metrics of these factors with overall risk assessments.[11] Then it might well be possible for utilities to analyze how specific investments in improving these can lead to measurable risk reductions with shorter time frames more appropriate to budget and rate case decision-making.

Another important issue in risk assessment is the need to account for uncertainty in knowledge about likelihoods and consequences. A number of risk assessment exercises in their demand for single numerical values associated with probabilities as well as consequences and their costs can themselves create risk by disguising uncertainty. This can lead to the representation errors of misspecification and misunderstanding mentioned earlier as threats to the reliability of safety analysis and management.

We discuss these issues because here, we believe, is an important role for the CPUC and its safety management system. A safety management system for a regulatory agency must support its own regulatory reliability and guard against representational error, not only in its own regulatory rules and processes but also in those of its regulated organizations. We believe the CPUC should in its SMS embrace the objective of improving risk assessment methodologies, its own as well as the risk assessment methods employed in the utilities. One approach to this is contracting research in California universities, sponsoring workshops, public symposia with recognized leaders in the field of risk assessment and, we would suggest, even jointly sponsored applied research programs with industry associations and some of its own regulated utilities. Perhaps a Public Purpose fund could be established to support this research. A safety en banc could be a useful format for discussions across utilities of risk assessment challenges and potential improvements.

7. Emergency response capabilities. The safety action plan notes existing safety rules (both General Order 166 and Section 768.6 of the Public Utilities Code) covering emergency preparedness. Both of these are focused on emergency preparedness in the regulated utilities, not in the CPUC itself. The enterprise risk audit describes both natural disaster and agency emergency preparedness risks and safeguards. Planning and communication connections with local disaster management organizations and law enforcement agencies are mentioned as "controls" and "safeguards". We didn't ask specifically about emergency response preparations in the Commission, but would simply note here that defined emergency roles and responsibilities are part of disaster preparation. They should be included in the purview of the SMS.

An important feature of an emergency management capacity is the ability to learn from emergencies and from failures in general. Many high reliability organizations have elaborate root- cause analysis provisions, including special a root-cause analysis group formed after each incident or accident to review and report. The Commission has authority to do incident investigations for events at utilities, both informal analyses and/or through formal proceedings

[11] Process Hazards Assessments (PHAs) are proposed in many process safety protocols as a way to bring the experiential knowledge of operators and maintenance staff to bear in identifying and assessing specific risks.

by an ALJ. But it's not clear that any review of Commission-level regulatory performance in issuing orders, rulings, inspections and audits are part of these investigations. The adversarial nature of the ALJ review may make it more difficult for learning and root-cause level analysis to occur in formal investigations. Perhaps a different format could be developed for root-cause analysis as part of the regulatory reliability function of the SMS.

Another approach taken by regulatory agencies such as the NRC is to require case histories to be written about events or problems at nuclear power plants. These case studies are then distributed to other plants to allow for the development of shared background information. Case history write-ups could be a useful learning strategy for the CPUC.

One additional issue we were made aware of by more than one interviewee concerns crisis management at the Commission. Utility crises can become political crises for the CPUC. It was suggested that during a political crisis -- media and legislative criticism that arises over an event such as the San Bruno explosion or a charge made pertaining to the Commission -- decision processes can be buffeted by the political winds. Anxiety can lead to hasty statements and changes in policy. We address the political foundations underlying Commission crisis management and its safety management system in general in a later section.

8. A self-monitoring safety system. A safety management system must be founded on indicators and metrics. We have discussed already the metrics associated with risk assessment. For an SMS two other sets of measurements are important: the safety performance of the system in terms of outcomes and the functional integrity of the management system itself. Regarding safety outcomes, we noted that the SED is now, as part of its monthly reports, including safety metrics for its regulated utilities. These are primarily incidents and accidents. As useful as metrics such as these are to track improvement it is important to recognize that these are lagging and not leading indicators. Safety is not simply about accidents, it's about conditions that preclude accidents. The Commission needs to develop a set of indicators that signal the strengthening or fraying of those conditions. We suggest the Commission should, as part of its SMS, have projects in place to develop these precursor indicators for each of the major industries and organizations it regulates. This should be done in close consultation with those organizations.

The second set of measures concerns the health of the SMS itself -- monitoring the fluctuations that might occur in attention, trust, communication, cooperation and motivation of Commission members in relation to safety. As we noted earlier there is no once-and-for-all solution to the problem of safety or to the effectiveness of a safety management system. These internal indicators should also be part of the SMS development process in the CPUC. Suggestions concerning their development could be solicited from a variety of groups at all levels in the Commission.

9. Safety roles and incentives. One of the striking things we discovered in our interviews and discussions within the CPUC was the confusion in understanding of the roles of advisor, advocate and enforcer among a surprising number of people. While everyone seems to think these roles have distinctive and different legal content, there were few clear definitions of the

differences and also disagreements into which category similar roles fell. It seems to us from our interviews that the confusion leads to an overly protective and overly-rigid functional separation in order to avoid any legal violations. Some inspectors argued that enforcers (inspectors and auditors) shouldn't be advocates. One suggested: "enforcement puts a limit on creativity." Others argued that inspectors "should be advocates for safety". Many argued that advisors can't be advocates. Perhaps regular meetings of enforcement staff across industries in the association we suggested could help advance the clarity of safety roles at the enforcement levels of Commission operation. The Staff Advisory Committee could address this need at other levels of the Commission.

Much of this role confusion seems to stem from the legal and adversarial framework surrounding incident investigation proceedings and to some extent rate cases. Edward O'Neill's "Report on Key Findings From the CPUC Modernization and Reform Project" also raises this as an issue and the dampening effect it can have on communication within the Commission. He attributes much of the formalization and adversarialism to the Bagley/Keene Act. The Act, he contends, constrains Commissioners from collectively discussing policies and deliberating with one another and with staff unless its done in a public meeting with a prior fixed agenda that does not allow any items to be discussed that are not on the agenda. The Report recommends the Commission push for revisions to Bagley/Keene to allow more informal collective conversations among Commissions and among Commissioners and staff. His report also suggests that the heavy reliance by Commissioners on private *ex parte* communication with outside stakeholders, allowed in rate case proceedings and in quasi-legislative rule-making processes has "tended to drive a wedge between Commissioners and working level staff." [12]

Apart from the legal issues, from a safety management perspective it seems to us desirable that there be some overlap between the roles: that inspectors and auditors should be seen and see themselves as potential advocates as well as advisors for safety and the improvement of the rules they are supposed to enforce, and that opportunities for less formal means of information sharing outside of adjudicatory proceedings be enlarged among Commissioners and encouraged between Commissioners and staff.

As we have indicated, incentives are also important elements in supporting the roles associated with a safety management system. It is not clear to us that at present either Commission managers or staff see major institutional incentives attached to roles closely connected with safety. In many organizations participation in safety management is not a career enhancing role. There does not seem to be a plausible career track for safety specialists in the Commission. An effective SMS for the Commission will require that there be a variety of career advancement opportunities as well as other incentives associated with the SMS.

What are safety role incentives? One potentially powerful one is professional identity as individuals internalize the values of reliability and safety. In many high reliability organizations

[12] Edward O'Neill, "Report on Key Findings From the CPUC Modernization and Reform Project" (June, 2015).

we have analyzed we found selected individuals whom we came to call "reliability professionals"(and in these organizations reliability included safety).[13] We found them in a variety of positions, some top-level but also some among department heads, program managers, shift supervisors, and on down to control operators and maintenance engineers. They need not be holders of particular professional degrees or even of any higher degrees at all. But they internalize a commitment to things going right in their organizations, and with this they are extremely sensitive to the development of precursor conditions and to the possibilities of representational error in their units and beyond.

Reliability professionals concern themselves with safety issues beyond their individual job responsibilities. It is important that the CPUC recognize, encourage and support the role of "safety professional" as part of the professionalism of its managers and staff. This is especially true at the enforcement level where safety requires that attention is paid to precursor issues that may well not be covered in formal rules and procedures. A safety professional must see beyond procedures in whatever role they occupy.

Another incentive is peer recognition for the safety commitment of individuals. In effective safety management systems awards (plaques, cash or vacation days) may be given for safety suggestions, corrective action issues noted by employees or the successful implementation of safety measures. These can be awarded by safety committees that have significant staff representation from all levels. The safety flag system in the Commission could incorporate these award strategies.

An important incentive recognized and supported by high reliability organizations is reinforcement and not punishment for employees who report error, even their own, in analytic exercises, in following internal procedures, or in enforcement. As has been demonstrated in a variety of settings, the punishment of error is not likely to be a significant factor in reducing error, but is likely instead to reduce the reporting of error, a negative factor in the search for reliability and safety.

As one program manager told us: "Individuals need to learn how to use their voice to raise issues. This should be a part of their training. But people who do raise issues don't always get support from higher management." All of these motivational issues are important for the Commission to consider as part of its safety management system development.

10. A safety culture at the CPUC? We have described elements of a "safety culture" earlier. We have been told that currently there is a conflict between "vigilance" and "compliance" cultures dominant in different divisions, branches and units at the Commission. But clearly both vigilance and compliance are important aspects of an effective SMS.

It is not easy to specify how to develop an overall "safety culture" within an organization. Research on organizational culture strongly suggests it cannot be done overnight. Organizational

[13] A detailed description of these "reliability professionals" can be found in E. Roe and P. Schulman, *High Reliability Management* (Stanford University Press, 2008).

culture has been defined as a set of assumptions, values and artifacts that has worked well enough to be transmitted to new generations of organizational members[14]. But it is likely to take more than one managerial and staff generation to establish a sustainable safety culture in place.

The concept of a safety culture has been increasingly popular in many organizations, including some regulatory organizations. The European Aviation Safety Agency (EASA) has been working on a framework for assessing safety culture in its regulated organizations. As the EASA notes (with some ambiguity), "While no requirements regarding Safety Culture are included in the EASA rules on organization and accountabilities within a Safety Management System … or in the Acceptable Means of Compliance, the concept of 'culture of safety' is promoted in … the Basic Regulation of EASA."[15] Also the Canadian Nuclear Safety Commission (CCNS) has added safety culture to its list of inspected variables in its nuclear power plant regulation. One danger in monitoring and measuring a safety culture is that a formal "check-the-box" framework would be imposed on what is still in essence a somewhat ambiguous concept.

We believe that to promote clarity and accuracy in thinking within the Commission about its monitoring and measuring, a safety culture should be more about what the Commission *does* than about what it *has*. In particular, the CPUC's safety culture should be defined by specific:

-- attitudes concerning tasks (about priorities in work, responsibilities, appropriate behavior)
-- behaviors (actions taken on behalf of safety; open communication)
-- incentives (rewards and sanctions concerning safety related behavior), and
-- inter-generational persistence ("person-proofing" the above so they survive changes in leaders and role occupants).

However it may be assessed, an important principle to remember is that an effective safety culture, and indeed an effective safety management system in the CPUC depends in no small measure on the presence of effective safety management systems, including safety cultures, in the organizations it is regulating. It is to this issue -- the relation of the Commission's SMS to organizations and political forces in its environment -- that we turn next.

III. Additional Suggestions Pertaining to the external environment of a safety management system within the CPUC

In a recent conference on industrial safety management held in Europe a number of safety officers from diverse industrial organizations all agreed that the effectiveness of safety management in their home organizations depended on their primary regulatory agencies also having strong and effective safety management systems[16]. We would also argue the reverse: the effectiveness of a regulatory agency's safety management system depends on the existence of effective reciprocal systems in the organizations it seeks to regulate. In short, in the development

[14] Edgar Schein, "Defining Organizational Culture."
[15] European Aviation Safety Agency, "Safety Management and Safety Culture" (January, 2011).
[16] For the findings of this conference see Swiss Re, *Safety Management in Context* (June 19-21, 2013), Zurich.

of its SMS the CPUC cannot ignore external forces and organizations that are integral to its safety objectives.

To start, it has been impossible for us in our interviews and observations not to be aware of the political conditions surrounding the Commission -- particularly the post- San Bruno political environment. Attacks on the Commission by political leaders, by groups and in the media have focused on its regulatory competence as well as the relations it has with its regulated organizations, particularly PG&E. These attacks appear to have affected employee morale at all levels. From our perspective they reflect a larger issue in relation to the Commission's safety management system -- the need of the agency to achieve some increased measure of institutional and political security and independence.

It is evident to us that many people we have talked to at all levels are looking over their shoulders at their political exposure in relation to their tasks. Regulatory actions, ranging from rule-making, rate case decisions or settlements, inspection and audit observations and reports, incident investigations, findings and subsequent enforcements are all subject to political push-back. In addition, new policy objectives are given to the CPUC by legislative action and/or pressure without consideration, it seems to us, of the institutional capacity of the CPUC, given current staffing and budgetary limits, to effectively carry them out. As one of our interviewees put it: "we are in a wash of policies".

A classic work in organization theory describes the transformation of "organizations" into "institutions". Organizations are valued for instrumental uses only, are in a constant battle to sustain themselves in competitive or hostile environments, and are buffeted by these environments and the need to respond and react quickly to them. Institutionalization is a process by which an organization acquires social value in itself, takes on a distinctive social character based on acceptance of its mission, and respect for its competence and capacity.[17]

Institutions have achieved significant stability and weight in shaping their environment. They are respected, even cherished, by communities in which they operate based on the widespread acceptance of their skills and values. The CPUC , we believe, with the development of its safety management system should also be transforming itself more fully into an institution -- widely respected for its skill and its values with respect to safety. We offer the following suggestions about how this might be promoted.

1. <u>The CPUC as a clearinghouse for information and expertise regarding safety</u>. From our standpoint it seems that one element in advancing the CPUC in its institutional missions as well as stabilizing its relations with outside organizations, including its own regulated organizations, would be to make it a preeminent institution in the state, and possibly beyond, in the development, sharing and application of expertise in safety management, particularly process safety. Currently CPUC expertise in relation to its regulatory missions is questioned publicly and also doubted in some of its regulated organizations. We heard from some of our interviewees that

[17] Philip Selznick, Leadership in Administration (1957).

they themselves did not feel qualified to challenge utility engineers about technical designs or operational strategy. A number of interviewees also said that there were not enough engineering staff who understood the technical arguments made by utilities in rate cases or the assertions of utility managers concerning technical foundations of operating practices.

Regarding safety management itself there does not seem, as we have noted, to be widespread in-house understanding of the analysis or even meaning of safety. One interviewee asserted in this respect: "We need to do better in having the skill to see safety issues." Further, the Crowe Horwath report on the Gas Safety and Reliability Branch noted: "the mix of staff experience and training does not provide a balance of regulatory, policy or industry expertise to best support GSRB activities"[18] (Crowe Horwath)

While it is likely that utility executives and operators will know more than inspectors, auditors and policy-makers within the Commission about specific engineering designs and operational requirements of their technical systems, it is not inevitable the utilities will know or follow industry better practice standards with respect to these systems. It is even less likely they will see or understand the full picture in managing for safety and for interconnected infrastructure risk, or the current state-of the art in process safety management, or the latest developments in risk assessment. The CPUC could potentially be a leading institution for all of these.

A number of strategies could help achieve this. The CPUC could devote safety en bancs, sponsored workshops or public meetings with invited industry leaders, trade association officers and representatives of standards organizations such as the ISO to discussions of standards covering better safety practices in specific industries. CPUC staff and utility personnel would attend. Similar workshops could be sponsored to review latest research findings and better practices in process safety management. The CPUC could also send its program managers and enforcement personnel to conferences elsewhere on specific industry practices including safety management. The CPUC could also work with California Universities to support applied research projects in industrial engineering and other fields related to improving its safety regulation. It could also contract out to faculty in these universities for technical advice. The CPUC could also sponsor symposia and research projects on risk assessment and its improvement, particularly to incorporate more human and organizational variables. As we've suggested, a Public Purpose Fund might be created to support this research.

Also, the CPUC could invite academic researchers in safety management, risk assessment or policy analysis to be visiting fellows for a year at the Commission, advising Commissioners and other staff members, and perhaps conducting seminars in their areas of expertise. It could in addition develop a paid internship program for masters level engineering, economics and management students to work for a period at the CPUC. These internships could be located in several divisions in both analytic and enforcement units.

[18] Crowe Horwath, "Gas Safety and Reliability Branch Management and Operations Review" (2015).

2. Career Development Strategy. Another area of Commission action could be enhanced programs in staff career development and training. We have heard from our interviewees concern that there has been an erosion of engineering skills among staff as more policy analysts have been hired at the Commission. At the same time we have heard concern expressed that more policy analytic skills need to be developed to support advisory roles throughout the Commission. One way to get the productive "balance" of expertise, argued for in the Crowe Horwath Report is to have more trained personnel in each field. It might be useful to provide opportunities for staff to attend classes or enroll in programs to enhance their skills in either field and to provide some training in risk assessment for all staff. It might be cost effective for the Commission to offer its own in-house training for staff in some of these areas.

In relation to in-house training, another need the Commission could address is that of process safety training not only for its own staff but for the utilities themselves. Why not develop a course in process safety management taught within the CPUC that would be offered not only to its own staff at all levels but also to personnel in the utilities. A certificate of completion (not a certification) could be given to all who complete the course. This could be a way to help promote shared safety perspectives between the Commission and its regulated organizations. It could also contribute to the self-identification among personnel in both settings that they can indeed play a role as "safety professionals" in whatever job they occupy, in whatever organization, with a reference group of other individuals who adopt the same perspective.

3. A Note on Staffing Adequacy. We have heard throughout the Commission in our interviews about the inadequacy of staff to handle the work load at all levels. This has also been noted in outside assessments we have seen. The Independent Review Panel on the San Bruno accident concluded that among other issues, "the CPUC did not have the resources to monitor PG&E's performance in pipeline integrity management adequately." It seems obvious to us, and is forcefully stated in the Independent Review Panel Report, that more staff are needed to support the Commission's objectives in safety management and to provide for an effective SMS.

The question is how to determine staffing adequacy with respect to safety. While the Commission certainly has other objectives, it seems to us important to promote inside and outside of the agency a recognition that safety is a base level requirement not simply one among many competing objectives. There should be some understanding of a threshold level of regulatory capacity needed to monitor, enforce and promote safe operations in the utilities. From all that we have read in earlier reviews, observed and been told, the CPUC is currently below that threshold with respect to staff and skills. Some areas are more critically in need of upgrade than others. It seems to us obvious, for example, that in the Gas Safety and Reliability Branch the audit and inspection force is simply too small to do necessary pipeline monitoring and enforce PHMSA pipeline integrity regulations.

We recommend that a safety management capacity model with respect to staff size and needed skills be developed to more sharply identify, as well as justify, needed improvements in staffing. We believe the CPUC should consider as part of its capacity model, the need for resident

inspectors on a rotating basis at the largest of the utilities it regulates. The NRC currently has a force of 150 resident inspectors onsite at the nuclear power plants it regulates. Audit and inspection staff members could rotate (perhaps on a year or two-year basis) between different utilities and between the utilities and CPUC headquarters. This analysis we believe should be part of the SMS development process. The commitment to a first-class SMS should include adequate staffing for safety, and such a case can and should be made, we believe, to funding authorities.

4. Changes in Adversarialism. An additional strategy which could advance the institutionalization of the CPUC is the development of new relationships to reduce formal adversarialism in its regulatory relationships. As we noted, the success of an SMS in the Commission depends on effective safety management systems in its regulated organizations. Just as the suggestions in the O'Neill Report on CPUC Modernization and Reform for revising the Bagley/Keene Act to reduce formal separations between advocacy and advisory roles might improve intra-Commission communication, so relaxing adversarialism to pursue joint R&D projects could lead to new improvements in external infrastructure safety management. One way to achieve this and pursue the research and training processes described above could be the development of a Safety Institute either within SED or perhaps detached in some ways from the enforcement and rule-making processes of the CPUC.

5. A New Role for the CPCN? Another strategy to advance the safety focus of the CPUC might be to re-examine the Certification of Public Convenience and Necessity (CPCN). The CPCN is the legal foundation placed under a utility's operation by a public regulatory body. First, we suggest the Commission consider trying to alter the archaic title of this certificate. Its title does not include safety and even implies that service reliability is the most important aspect of utility regulation. Might the Commission consider pushing for a change in title to something like: "Certification of Public Necessity and Safety"?

At present for the CPUC, a CPCN seems to be a once and for all award to a utility. In other states there are renewal periods specified for some CPCNs. In the academic and healthcare world, accreditation organizations offer accreditation as a renewable certification, subject to compliance with standards and operating requirements as well as inspections and site visits. Could the CPUC also initiate periodic reviews, if not renewals, for at least some of its newly issued CPNCs in 7 or 10 year intervals? This could occasion careful evaluation of safety records and practices as well as the effectiveness of a safety management system in each of the regulated organizations.

Apart from a renewal requirement (which would probably be seen as a "nuclear option" as far as the utilities are concerned) another possibility might be considered. Why not periodic 5 to 7 year CPCN "assessments" between the CPUC and utilities which are conducted with a view to long-term safety planning. We know the Commission currently conducts triennial audits, but these "assessments" would be of a prospective nature with a longer-time frame and a larger scope. These assessments could be opportunities to examine the latest findings and better practices for enhancing safety in the management of individual utilities. They could be exercises in assessing

current levels of safety and planning for improvements over a 5 to 7 year period. If cooperatively conducted with the regulated organizations, these safety assessment and planning sessions could possibly supplement the rate case as an alternate, less adversarial format for developing utility investment strategies for long-term safety improvements.

We believe actions such as these, supported by the commitment of the Commission to be a leading safety institution, not only in California but in the nation and beyond, could give it both political and institutional weight in resisting pressures that dilute its mission and destabilize its regulatory priorities and agenda.

Safety Management and Rate Cases. Our final thoughts concern safety issues and their presentation in rate cases. We have read the Commission's Solicitation for Input regarding proposed external safety intervenors in rate cases and other proceedings. We are not enthusiastic about this proposal for two reasons. First, it puts the treatment of safety issues primarily within the context of formal adversarial relationships. This, we believe, will undermine not advance the analytic foundations of a safety management system. Many of the issues in safety analysis and management require, as we have tried to demonstrate, careful thinking as well as protections against representational error. Neither side in an adversarial proceeding has a major stake in these protections, other than what might advance its own position.

In adversarial proceedings there is a tendency, not toward seeing the larger picture, but in focusing on smaller issues that might convey adversarial advantage.[19] In fact, it is very unlikely that an external intervenor for safety will have access to enough information about technology, procedures, practices and problems in regulated organizations to raise effectively a full range of safety issues. Further, in adversarial proceedings there is likely to be an overstatement of claims on both sides. Safety management is a process of learning and discovery -- not simply winning arguments, nor is it simply about "doing the right thing", it is also about *learning* the right thing.

The second and more important reason we do not support the external intervenor proposal is because we have been arguing that safety advocacy should be within the competence and scope of the CPUC itself. The CPUC should be the intervenor for safety in all its proceedings, based on its knowledge, access to information and competency as well as its institutional values and mission. The heightening of all of these is what a safety management system should be about. The safety intervenor proposal suggests that the CPUC will instead be a neutral bystander in debates concerning safety. This cannot it seems to us be a position from which the Commission can make itself a leading institution in the promotion of safety in its regulated industries.

Conclusion. As we noted at the outset, we offer this report and our analysis under the caution that CCRM is not a typical consulting agency. We are a group mostly of academics who offer perspectives and analysis based on our research experience with many organizations attempting to achieve high levels of safety and reliability. We do our work with practitioner organizations

[19] An interesting analysis of the character of adversarial proceedings, both strengths and weaknesses, has been written by philosopher Arthur Isak Applbaum, *Ethics for Adversaries* (Princeton University Press, 2000).

primarily to increase our learning and experience and to promote understanding and improvements in safety and reliability that might reach beyond the boundary of any single organization. We do not intend, nor are we able, to prescribe ready-made answers to any organizations relative to their problems. Nor do we offer any validation or certification of specific organizational practices. One of our main functions is to ask questions of individuals in organizations that they might not be asking themselves. But the people who work and have vast experiences in an organization are far better equipped to answer these questions than we are.

It is in this spirit that we offer our findings to the CPUC. The usefulness and practicality of our suggestions is best determined by the members of the CPUC itself. We have been highly impressed by the commitment, skill and professional integrity of those Commission members at all levels whom we interviewed. We are also well aware of the difficulties faced by the Commission as it attempts to fulfull its policy and regulatory missions, given the budgetary and personnel restrictions under which it is forced to operate and the difficult political environment it occupies. It has been a privilege for us to have been allowed access to the Commission to talk to its personnel and observe some of its operations. All of our interviewees have given very generously of their time to provide us with thoughtful and greatly instructive answers to our many questions. We are very grateful to everyone in the Commission for their assistance in this project.