A Sociotechnical Systems Design for High Reliability Nuclear Power Plant Teams: The Organized Search for Potential Failures

Eli Berniker PhD[1]
Pacific Lutheran University- Emeritus
berniker@gmail.com

Authors note: *This paper has been revised as a result of the author's attendance at the November, 2013 American Nuclear Society meeting. The author has not previously studied Nuclear Power Plants (NPPs). Therefore, the original paper was a projection of sociotechnical system analysis and design based on a theoretical understanding of the relevant challenges. The ANS provided a rich, concrete, context for the paper, which is incorporated in what follows. In particular, Probabilistic Risk Assessment and its potential failure scenarios will become a basis for operationalizing mindfulness and the design of organizational roles applied to the "search for potential failures."*

1. ABSTRACT

The paper will integrate a very diverse set of perspectives into a coherent and tentative organization design. Normal Accident Theory (NAT) will be discussed in terms of the Second Law of Thermodynamics along with an ecological concept of Complex Chance Events (CCE) as a theoretical perspective on the complexities of NPP operations. Probabilistic Risk Assessment (PRA) frames complexity by simulating potential failure scenarios, making those complexities explicit. High Reliability Organizing (HRO) suggests the cognitive mindsets necessary in groups or teams faced with such levels of uncertainty; a view mirrored in the call for an *ethos* of searching for potential failures. Sociotechnical Systems Design (STSD) is an approach to integrating these various perspectives into a model for a functioning organization.

A multidisciplinary approach necessarily questions the definitions of concepts ventured by constituent disciplines as they are tested by alternative perspectives. *Failures* will be disassociated from errors and will be defined as a gap in operational understanding of the NPP technical system. Such technological gaps become agendas for learning and research. "Extra-procedural activities" by NPP crews will be translated into *Procedural Failures* understood as key events in the search for potential failures. The respective roles of the Nuclear Regulatory Commission (NRC), nuclear power industry and their representative institutions will be compared to signal the need for a neutral body to organize and disseminate information about procedural failures and suggest agendas for research. We might tentatively label that organization the Nuclear Power Risk Management System (NPRMS)

The result will be a tentative design for high reliability NPP organizations with the role and the necessary capacity to systematically "search for potential failures." The design must be tentative because such an organization can no more be designed remotely than an NPP can be managed remotely. Organization design requires the active participation of those who operate a nuclear power plant.

2. INTRODUCTION

The purpose of this paper is to identify the critical challenges in achieving high reliability operation of complex high consequence sociotechnical systems and to propose guidelines for the design of organizations that operate such systems. STSD refers to a specific body of knowledge and design practice that is an approach to creating team based organizations. This paper is an exercise in STSD.

Understanding the challenges of complex STS requires that we integrate between the disciplines of physics, engineering, ecology, and the organizational sciences. Complexity is a measure of the number of potential paths to failure. A quantitative test of Normal Accident Theory[i,ii] demonstrates that technical systems failures occur as a direct result of their complexity independent of human error. Uncertainty is demonstrated by the preponderance of CCEs, events so unique that they have zero probability of being repeated. Complex STS failures in NPP are likely examples of such events.

Human organizations are expected to detect, prevent, control, and mitigate the effects of technical system failures. In response to these challenges, HRO calls for *mindfulness* as the sense-making logic required of operators[iii]. A core characteristic of *mindfulness* is a focus on failure. At the 2013 ANS embedded topical meeting on risk management, Dr. N. Sui suggested a similar focus as the "search for potential failures" based on PRA simulations of failure scenarios. These perspectives suggest a

critical design insight: *Complex Sociotechnical Systems cannot be managed remotely.*

Reliability depends on reducing uncertainty by creating knowledge. STSD suggests designing two overlapping sets of teams with the same members in different roles: Operating/Maintenance Teams (OMT) and Process Reliability Teams (PRT). The OMT is charged with operating and maintaining the technical system; the PRT is charged with developing *mindfulness* as a practice and codifying knowledge.

To facilitate the creation of knowledge, failures are redefined as any process variations that are not understood; i.e. a failure of knowledge. In effect, "searching for potential failures" is equivalent to identifying gaps in knowledge. The PRT will focus on a particular form of failure, Procedural Failures, which are signaled by the need to take "extra-procedural actions." When such actions are related to potential failure scenarios, a learning agenda is defined and those scenarios become real in the sense that events have confirmed them.

While the PRT can develop considerable operational knowledge, we cannot expect them to have the research capability to completely codify that knowledge. The role of the NRC as regulator is in conflict with learning processes that must be exploratory. Therefore, an intermediate NPRMS is required as the locus of industry wide research agendas independent of the both the NRC and the industry. The NPRMS would not have authority in its role of generalizing information and knowledge.

Parallel sets of teams in a NPP call for an integrating team, a Recovery Management Team (RMT), which functions in the event of major failures. The role of the RMT is to manage, contain and recover from such failures. For example, a gap in knowledge and understanding could lead to potentially catastrophic consequences.

Two kinds of information system support are suggested to support *mindfulness* and recovery from significant failures: A Decision Support System to enable convergence on failure diagnoses and a Dialectical Inquiry System (DIS) to maintain the status of alternative potential failure scenarios. These systems should be linked but independent.

This paper will propose design guidelines for these teams. It should be evident that no design can be specified in advance given the nature of complex systems. Remote over specification would be maladaptive.

3. SYSTEMS COMPLEXITY, UNCERTAINTY, AND FAILURES

To appreciate the extent of uncertainty associated with sociotechnical systems as complex as an NPP, we can access two relevant models, NAT and an ecological model of CCE.

3.1 Normal Accident Theory

NAT was proposed by Perrow[iv] in his study of the Three Mile Island nuclear power plant failure. He postulated two qualitative factors that explained the failures of complex technical systems: *Complexity* and *Coupling*. Fred Wolf[v] tested NAT quantitatively and demonstrated its validity in classifying petroleum refineries with respect to Reportable Quantities (RQ's) of hazardous emissions and Total Case Incident Reports (TCIR). RQ's are representative of refinery "accidents."

Complexity, intuitively, measures the number of paths to failure of a technical system. Wolf measured complexity by applying the Second Law of Thermodynamics, *entropy* = *k* log D. D, an estimate of the number of possible states, was computed as an index of refinery complexity, C_{plant} based on the number of possible states at each control node, Q_i.

$$C_{iplant} = \sum_{i=1}^{n} C_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} \left(Q_{ij} \right) \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \left(\sum_{k=1}^{x} Q_{ijk} \right)$$

(*Note the similarity between this computation and PRA's many millions of failure scenarios*.)

Coupling was partitioned as tighter continuous processing, or looser batch processing. Coupling is a measure of the potential recovery modes in the system. For example, coupling can be loosened by storage tanks, which buffer processes, dampen transient fluctuations, and allow for maintenance without interrupting product flow to customers. Tighter coupling results from time dependent invariant sequences. A continuous processing refinery pumps directly into delivery pipelines. A batch processing refinery pumps into storage tanks that can maintain deliveries for many hours. Loose coupling supports multiple flexible recovery processes; tight coupling supports fewer recovery options.

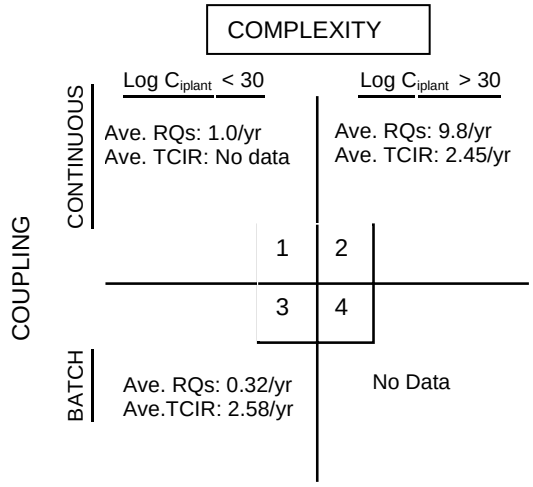

Figure 1. Research Results by Quadrant

The data indicates an RQ ratio between quadrant 2 and quadrant 3 of 30:1. Of particular significance is the partition between low and high complexity, $Log_{10} = 30$. No organization has the cognitive capacity to monitor 10^{30} possible states or millions of possible failure scenarios. We can learn of leaks only when they have happened.

NAT and Wolf's validating research lead to the following conclusion:

> *Complex technical system failures can be the result of physical laws independent of human organizations and error.*

This conclusion should not be surprising as it is the necessary implication of the Second Law; all systems that expend energy must increase entropy, wear out and fail. NPPs have no exemption from the Second Law.

3.2. Complex Chance Events

NAT suggests that many failures result from multiple unrelated failures that interact to create unanticipated paths to systems failure. Such events may be absolutely unique, i.e. non-repetitive.

A CCE has an extremely low probability of ever repeating over the lifetime of the universe. The physicist Walter Elsasser[vi] computed 10^{106} as the largest number of events possible in the known universe assuming that there are 10^{81} particles and the shortest event time was a nanosecond. Thus, no probabilities lower than 10^{-106} can be real. 75! approximates 10^{106}. Therefore, "whenever more than 75 distinguishable events co-occur by chance, one can be certain that they will never randomly do so again."

Every person reading this paper is a CCE. Work the numbers. Each human being is the result of 40,000 binary choices between two sets of genes. In effect, the universe is not old enough for any of us to occur more than once. CCEs are ubiquitous. Uniqueness overwhelms order in the universe.

NPPs are equally unique. Each NPP will be a unique product of its site-specific construction and operational history. PRA failure scenarios must be validated for each plant. We should, therefore, expect technical system failures to often be CCEs.

To be sure, particular failures, when analyzed, will result from much smaller sets of events. If the goal is increased reliability, ubiquitous CCEs call for skepticism with regard to expectations, procedures, and analytical models. That is the essence of High Reliability *mindfulness.*

What kind of world is dominated by pervasive uniqueness? "The fabric of causality is porous." And near the holes are countless "adjacent possibilities." Ulanowicz postulates that: *The operation of any system is vulnerable to disruption by chance events.*[vii]

Wolf's research suggests a magnitude of petroleum refinery complexity that can exhibit many CCEs, and similarly, NPPs are extremely complex.

The Three Mile Island NPP accident exemplifies a CCE. The accident was precipitated by a moisture leak that "got into the instrument air system of the plant."[viii] It was an "adjacent possibility" in the proximity of control nodes. Such events are not unusual. Thankfully, few result in systems failures.

3.3. Implications of NAT and CCE

We have demonstrated that systems failures are normal Second Law phenomena; they are natural physical phenomena. Therefore:

> *We should not confound failures with errors, a pervasive practice across organizations, industry, and much organizational research*.

Metaphorically, operating a nuclear power plant is akin to *Tiger Taming.* The tiger is NEVER tame. We must always be wary of "failure."

4. PROBABILITY RISK ANALYSIS

PRA is a method for dealing with the complexity of NPP and the fortunate rarity of major failures in the nuclear power industry. Essentially, it is a technique that simulates potential failure paths by assuming that any element of an NPP can fail and multiple failures are also possible. The result is many millions of potential paths to failure.

The number of potential failure scenarios produced by PRA confirms the cognitive conclusions

drawn from NAT and CCE, i.e. that so many potential states are beyond the possible comprehension of any organization and, as the author suspects, any computerized information system. Information systems would impose specific models on the data or simulations in an effort to make sense of so great a range of possibilities. Implicitly, such models assume a "tame tiger" or, at least, a relatively predictable tiger.

Rauzy argued that 75% of the theoretical failure paths are meaningless.[ix] In effect, the large number of potential failure scenarios is little more than a 'hunting license.' PRA's, as a method, are difficult to operationalize in practice. Hence, Sui's appeal for an "Ethos" of searching for potential failures.

5. PROCEDURAL FAILURES

Perhaps the most effective path towards a rich understanding of each NPP may be instances of "extra-procedural" responses. This is an anodyne label for what is generally called "workarounds;" that is, local unauthorized *ad hoc* procedures utilized to correct or maintain technical system functioning when approved methods do not work. They demonstrate the need for discretionary actions to deal with emerging events. These were studied by Massaiu and Holmgren of the Norwegian Halden Reactor Project.[x] The authors conducted a simulation of crew responses to simulated nuclear power plant failures and evaluated the readiness of crews to engage in "extra-procedural" actions. Their discussion is instructive.

> Two emergencies were made complex by creating situations where extraprocedural diagnoses and decisions were required for limiting plant degradation and minimizing release of contaminated substances outside the plant.…There are different philosophies regarding the ideal level of operator adherence to the emergency guidelines. One view maintains that extra-procedural activities (i.e., operator's autonomous initiatives, innovative actions) add a random risk element to the system and should be avoided. A different view argues that operators' initiatives "right the procedures with the world", which is the true reason to keep human operators in the system.[xi]

From their discussion, it is apparent that such activities may be common and have been well studied. The second view expressing the need for human operators is an apt summation of the STSD perspective; *People are the solution, not the problem.*

We may label "extra-procedural actions" Extra-Procedural Fixes (EPF). EPFs, better known as workarounds, abound in all industries, services, and systems. There are plenty of examples in the aircraft industry, software programming, and almost every form of organized human work. They are necessary because authorized procedures never completely cover all eventualities or, alternatively are simply means to assign blame to employees. British rail workers, forbidden to strike, invented the work-to-rule strike. They followed all required procedures and no train left the yard. An American postal executive once labeled this "malicious obedience."

What does an EPF mean? How should it be interpreted? Let us define such events as *Procedural Failures* signifying situations when the set of authorized and available procedures is ineffective in resolving a problem, variation, or disruption in a process. They are *ad hoc* insofar as they are unauthorized but might become a regular part of the response repertoire of the operating crews.

EPFs are necessary when there is no procedural response to a particular set of circumstances; the procedural response is inadequate or simply does not work. They are the result of necessarily incomplete understandings of potential failure scenarios.

If we consider EPF's in the context of PRA failure scenarios, much valuable information is generated. First, each instance requiring an EPF validates a subset of failure scenarios insofar as particular failures have been confirmed. To the extent that such EPFs are repeated, statistical data can suggest probabilities of particular failures.

The PRA failure scenario serves as a frame of reference when applying the EPF. What potential failure paths require attention? Weak signals relevant to other systems elements in the failure scenario become important. The operating team can integrate what had appeared to be isolated process variations into potential failure scenarios.

More worrisome is the universal tendency to suppress EPFs from management and authoritative decision-makers. EPFs are often seen as violations of procedures and can lead to punishments. This type of failure scenario is not considered by PRA. For example, a technical system failure occurs and management, unknowingly, calls upon the crews to follow procedures that do not work. Precious time may be wasted and additional malfunctions may result.

Finally, the EPF, as a process, has not been properly tested. We do not know under what conditions EPF will fail. To use the Challenger disaster as an example, in 1988, Starbuck and Milliken wrote, "the most important lesson to learn from the Challenger disaster is not that some managers made the wrong decisions or how o-rings worked: the most important lesson is that fine-tuning

makes failures very likely"[xii]. Fine-tuning is "experimentation in the face of uncertainty" in the "context of very complex sociotechnical systems so its outcomes appear partially random".

The identification, documentation, and analysis of Procedural Failures that necessitate EPFs is an excellent way to operationalize the "search for potential failures" and will be the basis for developing the *mindfulness* necessary in HRO and a core design element in the proposed STS design. Instead of suppressing EPFs, the discovery of Procedural Failures should be a most valued contribution of operating teams in achieving higher reliability.

As we proceed, the EPF is defined as a local, unauthorized, response to technical systems deviations and malfunctions for which there are no accepted effective procedural responses. Alternatively, the Procedural Failure (PF) is defined as a gap in technological understanding indicating the lack of an effective authorized response to those deviations and malfunctions. The distinction is important because the PF signals a need for research, learning, and testing. The EPF signals an organizational problem. As long as we focus on the latter, the technological challenges will not be explored.

6. HIGH RELIABILITY ORGANIZING IN COMPLEX SOCIOTECHNICAL SYSTEMS

HRO deals with the sensemaking of groups of people operating complex, potentially dangerous technical systems. The HRO construct, *mindfulness*, is central to the proposed design of reliability teams. HRO represents an "ethos" of searching for potential failures, and is difficult to incorporate into operating organizations. The literature is rich in discovering and observing *mindfulness* but not in its implementation as an organizational practice.

6.1. Characteristics of Group Mindfulness[xiii]

Within the limits of this paper, HRO cannot be fully explored. The characteristics listed below are cited in order to link them to the challenges presented in reliably operating an NPP and to provide a basis for defining the objectives of a STS design of a NPP operating organization.

- A preoccupation with failure, suspicion of success, and acceptance of uncertainty.
- A reluctance to simplify interpretations – The world they face is "complex, unstable, unknowable, and unpredictable."
- Sensitivity to operations and a focus on the front line where the work gets done. Attention to weak signals.
- A commitment to resilience; keeping "errors" small, improvising workarounds to maintain system functioning.
- Deference to expertise instead of authority. Push decision making to people with most expertise.

The essence of *mindfulness* is captured well in a study of the Diablo Canyon NPP. "Chronic worries" are described as the "widespread recognition that all of the potential failure modes into which complex technical systems could resolve themselves have yet to be experienced. Nor have they been exhaustively deduced."[xiv] The hallmark of a high reliability organization is that it never believes that it has achieved high reliability. If it did, it would lose its edge, because *the tiger is never tame.*

The *mindfulness* construct suggests skepticism about authority, plans, policies, and procedures that filter perceptions and assume more is known than is the case. *Standard operating procedures assume that the tiger IS tame.* More generally, the limitations of specified procedures are recognized.

Two limitations of HRO should be noted. First, the tendency to confound failures with "errors" suggests that we can, somehow, organize to prevent systems failures. In general, organizational science has not recognized that the Second Law of Thermodynamics obtains for all forms of human activity and whatever technical systems we create. All organizations are necessarily entropic.

Second, HRO lacks a design perspective. If mindfulness is to become the primary cognitive approach to the operations of complex systems such as an NPP, it must be embedded in an organization that can develop mindfulness, function effectively in the face of the challenges of uncertainty, and create a structure for responding to failures with catastrophic potential. The search for potential failures must be more than an "ethos." As noted above, a focus on EPFs provides a structural link between HRO and PRA failure scenarios. That link will be explored in the discussion of STS design.

Integrating NAT, HRO, PRA, and STSD, the following tentative conclusion emerges:

> *Complex sociotechnical systems with potentially catastrophic consequences of failures should not be remotely managed.*

Uncertainties preclude the communication of adequate data to convey the potential complexity of major failures. The technological models that frame

data collection are simplifications and always suspect. Furthermore, the suppression of procedural failures threatens the effectiveness of remote decision-making.

7. SOCIOTECHNICAL DESIGN CHALLENGE: RISK MANAGEMENT

This paper began by demonstrating the scale of uncertainty that is characteristic of highly complex technical system operations. We can partition the concept of technology into two classes of phenomena: (1) the *artifacts* that are technical systems and methods of operation and (2) the *knowledge* that informs those artifacts. We can define *technology* as a body of knowledge about the causes and effects of human actions. Technologies inform how we do work. Uncertainty is a sign of gaps in technological understanding. *Mindfulness*, in this case, is attending to knowledge gaps. Therefore, managing risk, understood as a "search for potential failures," requires gaining knowledge relevant to the gaps in a particular technology. This concept suggests a redefinition of failure.

Failure can be any variation, disruption, or anomaly in a technical system functioning that is not understood.

Failures may be transient and of little consequence, and can still signal technological gaps and result in potentially major failures. PRA defines failure as a malfunction in the NPP operating system; potential *failure scenarios* are sets of such malfunctions.

The STS challenge is to design an organization or set of organizations with the capacity to identify technological gaps in nuclear power technology, document these gaps in terms of the relevant failure scenarios, and support research into methods and procedures that manage the risks suggested by those technological gaps.

8. SOCIOTECHNICAL SYSTEMS DESIGN

Sociotechnical Systems Design (STSD) has roots in a natural occurring experiment in English coal mines, some 60 years ago, when a group miners got together to ask for a "common pay chit," self-organized into self-managing teams, and reintegrated their fragmented jobs into shared team effort. It was the first demonstration that there were more effective and efficient alternatives to fragmenting work into jobs, the basic unit of modern organizations. [xv,xvi]

The logic of jobs is to fragment skilled work into narrow tasks so that wages may be reduced and less skilled workers employed. That works in simple manufacturing with well defined tasks and requirements. The complexities and uncertainties of a coal mine limited the utility of pre-specified jobs. This group, or team, succeeded in driving down the coal getting cycle time from 36 hours to 24 hours. As skilled and experienced miners, they knew how to deal with the uncertainties of underground coal mining. *People were not the "problem" but the solution.* That has been an STSD fundamental premise throughout its history.

The focus of STSD is on organizational and technical systems factors rather than human factors. The question STSD poses is: *How do we design work for teams?* Reintegrating work into teams is relatively straightforward when all of the necessary tasks and challenges are reasonably well known. "Searching for potential failures" is an entirely different challenge.

8.1. NPP Operating Teams

Envision two teams consisting of the same members acting in two different roles. One team may be labeled the OMT with the task of operating a particular unit or subsystem at a NPP. Given functional limits on team size, there would be several parallel OMTs each assigned to particular units or subsystems. The design principle is to form teams around subsystems so bounded that each team has the capacity to solve the majority of problems within its unit[xvii]. Problem solving that requires boundary crossing is fraught with risk.

Each of these teams will also act as a PRT with the role of developing *mindfulness* by systematically searching for potential failures. The PRT's will meet periodically (i.e. weekly), to pursue their task. Membership may include engineers who are either local or remote. The role of the PRT's is to document EPF events, relate them to particular sets of failure scenarios, and identify areas where further research and testing may be useful. In effect, PRT's codify the experiences of the OMT so that they are available to the organization.

There is a need for a third team. In the event of a failure with potentially catastrophic consequences, a RMT will be necessary. They, too, will have to operate *mindfully* and tap into the experience developed by the OMTs and PRTs. The RMT will consist of representatives of the PRTs and auxiliary expertise from across the NPP. There follows a proposed design model for these teams. The primary focus will be on the OMT and the PRT and their roles with respect to managing risk.

8.2. Operating/Maintenance Team (OMT)

The OMT is a traditional STSD process industry challenge. STSD has been particularly successful in processing plants. Without developing that design, a few principles will be suggested. First, teams replace jobs as the basic unit of design. Jobs are fragments of work, simple tasks, turned into full time activities for employees. It is a way of deskilling the work force. Teams, or crews, are necessary because of the range of activities that must be coordinated in a variable work context. That was also true of the coal mine.

The integration and cross-training of operations and maintenance serves multiple purposes. It supports rapid response to emergent conditions, develops a shared understanding of the technical system and its default states, and supports preventive maintenance. Paper mills suffer from random breakdowns and the recovery window is short because of limited storage between pulping and the paper machines. The fastest recoveries are achieved with cross-trained integrated teams. Handoffs between maintenance and operations degrade information quality. For example, a successful repair does not always mean that the device has been left in the proper default state.

The training of submariners for the US nuclear fleet illustrates the expectations of team member competence.

> *Every submariner must pass a qualification program unique to each submarine that at a minimum takes nine months to complete above and beyond all previous training. The submariner must know each system and every valve aboard the vessel. The logic for this requirement is all individuals serving aboard a submarine must understand how to control its systems in an emergency.* [xviii]

There is a theoretical basis for the above training. Ross Ashby formulated a Law of Requisite Variety demonstrating that only variety can destroy variety. The response variety of an organism (or organization) must be greater than the variety of challenges it faces if it is to respond to contingencies effectively[xix]. A team of submariners so trained can respond to contingencies in many more ways than a similar number of people each limited to their individual jobs. Such multi-skilling is a core STS design principle.

STSD calls for participative design as an adaptive principle. Given uncertainties, corrective actions will have to be adapted to emergent events; EPFs. Participative design develops the needed adaptive capacities in the OMT.

Salary systems should be designed to support learning objectives. That suggests "pay for knowledge" rather than pay for performance. Salaries are a function of earned certifications leading to increasing competence, professionalization of work roles, and long career paths[xx] all in support of increased reliability and *mindfulness*. Certification does not exempt team members from particular tasks. All members are available for all tasks they are competent to execute. That was the principle that Rickover applied to his submariners.

Objections may be raised about the cost of such training and the increased wages earned at higher competence levels. The problem is not cost but cost accounting. Cost accounting treats labor as a variable cost that should be controlled as a function of output and markets. NPPs do not operate as variable output systems. The concern with variable costs is only an artifact of accounting practice misapplied to NPPs. A professionalized work force is a critical element in improving reliability.

9. THE PROCESS RELIABILITY TEAM

The concept of parallel teams with shared membership is new to STSD. The PRT incorporates the OMT in a different role, the development of mindfulness as a practice of searching for potential failures based on PRA scenarios. This cannot be left to individuals because team processes are necessary to make sense of events in the face of significant uncertainty. Nor can this role be divorced from the OMT as if mindfulness can be a remote function. The practice of mindfulness must be available when consequential failures occur.

Traditional organization design, based on the principles of "scientific management" promoted by F.W. Taylor, separates thinking from doing, i.e. fragmented mindless jobs. Mindfulness is assigned to management. Incorporating the OMT into the PRT creates a basis for teams to practice mindfulness and integrate the search for potential failures into operational work roles.

The search for potential failures based on failure scenarios is developed by codifying operating experience in the PRT. Team training in the utilization, verification, and documentation of PRA scenarios is not simply an addition to operational skills and tasks. It calls for a different "ethos" which can only emerge from a separate discourse.

The PRT is a part time team meeting regularly to review events and actions. It may require additional outside expertise especially when they are learning to consider risk-informed approaches, and develop a set of failure scenarios. The group's essential role is to learn, create knowledge, and prepare itself for crisis

management. Those capacities will be crucial in the event of potential consequential failures.

The work of the PRT is organized around two separate, but linked, foci. The first is risk-informing its decision making and developing potential failure scenarios, and the second is developing Extra Procedural Fixes (EPF) when the need arises. Each of these presents unique opportunities and organizational challenges.

9.1. The Process Reliability Team – PRA Failure Scenarios

PRA scenarios are created by simulating all possible elementary failure combinations into millions of potential failure scenarios, 75% of which may not be important.[xxi] Presumably, a majority of these are, in principle, impossible combinations. The utility of the remaining scenarios is an empirical question to be answered in NPPs. Evidence of particular failures and combinations of failures must come from operating practice.

One role of the PRT is to validate failure scenarios. A small set of failure scenarios are assigned to the PRT. The set should include diverse paths and include all of the significant elements of the PRT's assigned unit or subsystem. The PRT will review, document, and log all variations, discrepancies, repairs, corrective actions and knowledge gaps in a database that organizes the data in terms of the selected failure scenarios. These may not be failures in the technical sense but are evidence of the need for human intervention.

As data and history accumulates, particular scenarios will be validated in terms of observed events while others may never surface. If each scenario describes a rare, or unique, sequence of events, we might assume a Pareto type distribution would emerge; a small subset of scenarios will exhibit the major part of potential failures. The selection of scenarios may shift accordingly as the PRT sets its agendas.

The above process is achieved by *attention to weak signals*, an important characteristic of the practice of mindfulness. The validation of particular failure scenarios provides a strong basis for improving reliability. When malfunctions occur that evoke known failure scenarios, the OMT may focus on the relevant failure scenario until anomalous events suggest a different scenario. Such anomalies will only be obvious if the more salient scenarios are well studied and understood. *Mindfulness requires a shift in perspective and skepticism about what is known when anomalies are identified. They cannot be ignored.* Over time, the PRT and, therefore, the OMT should develop a keen capacity for mindfulness.

The data accumulated by the PRTs should be transmitted to the NRC or a designated central organization so as to improve the utilization of PRA scenarios across the industry. As data on particular failure scenarios is collected, particular scenarios will become more salient as characteristic of different types of NPP. Actual technical system failures may be rare. However, the amount of human action required to maintain the reliability of system elements will be known and associated with potential failure scenarios.

9.2. The Process Reliability Team – Extra-Procedural Fixes … Procedural Failures

The two labels, EPF and PF convey the problematic issues that emerge when considering such phenomena. EPFs, or workarounds as they are known elsewhere, are always suppressed. They are never recognized as failures of procedures, designs, or organizational policies and practices, even if safety or reliability issues are not involved.

There are good reasons for the above suppression. All of the stakeholders, nuclear power generators, equipment builders, and the NRC, have a shared interest in that suppression. For private entities, it is a concern about liability. That was evident in BP's handling of the Deepwater Horizon catastrophe. There is ample evidence of similar concerns in the chemical, airline, and marine transportation industry.[xxii] At local levels, operators suppress workarounds because they "own" such "tribal knowledge" and they are not paid to create such knowledge. Early in my industrial engineering career, a machine operator explained to me "You are paid to think. I am paid to work. Do not ask me questions."

EPFs are suppressed because "Operator Error" is the default explanation of major failures. There is no reward for their success and considerable risk if they do not work. By explaining failures as operator errors, the discipline and industry deny important opportunities for discovery and technological improvements offered by understanding EPFs as PFs.

This is not a question of culture or "ethos." The above stakeholder concerns suggest the need for an intermediary organization configured to neutralize those concerns and enable technological progress. Without such an organization, the PRTs cannot engage in the exploration of EPFs. Suppression will prevent more effective study and learning.

9.2.1. Nuclear Power Risk Management System (NPRMS)

There is a need for a government agency that is independent of all of the present stakeholders involved in nuclear power generation: the NRC, the Department of Energy, power companies, equipment manufacturers, and research institutions. The design of that agency is beyond the scope of this paper. The Aviation Safety Reporting System (ASRS) operated under NASA provides an example of such an agency and its operation. It is a system where pilots and others can safely report problems, anomalies, and mistakes. The NPRMS would not have authority over any aspect of nuclear power nor should it be a research granting agency. NASA and the ASRS do not fly commercial aircraft, build them, or regulate those activities. As such, they are not industry stakeholders. The NPRMS should operate in a similar fashion.

The role of the NPRMS is to be the vehicle for collecting EPF and PF information from across the industry, relating that information to failure scenarios, and identify technological gaps as subjects for systematic research.

The reason that the NRC cannot serve this purpose is because of its regulatory role. There is a conflict between regulation and learning. The NRC asks a NPP to incorporate PRA into their operations but cannot impose that requirement via regulation. The NRC would have to authorize all of the EPF procedures. In effect, adhering to NRC's role and procedures would shut down the industry.

PFs indicate technological knowledge gaps. The PRTs identify those gaps and characterize them, making it possible to study when they should or should not be applied.

The primary role of the NPRMS is to facilitate and integrate the use of PRAs in the nuclear power operations. The NPRMS would be a vehicle for the exploration of PFs and disseminating information across the industry and research institutions. Second, by indentifying technological gaps, potential research agendas are established.

Assuming the existence of such an agency fulfilling the specified roles, we can return to the PRTs and propose how they might integrate EPFs into their role.

9.2.2 Process Reliability Teams, Extra Procedural Fixes, and Procedural Failures

With respect to EPFs, the role of the PRT is to document them, check across the NPP for similar responses, and anchor them in particular failure scenario. They may explore the logic of the fix, the peculiar conditions that require the procedure, and any events that precede the response. In addition, they may raise questions about the inadequacy of the authorized responses. The result is a rich description of the EPF and of the PF that it signals.

After summarizing the information, it should be submitted to the NPRMS under a procedure that protects the PRT and organization. The NPRMS can then proceed to investigate the EPF and the implied PF across similar NPPs in the industry.

As PRT's become increasingly sophisticated in their roles, we would expect them to request or develop particular PRA scenarios. As EPFs become salient, the PRT might develop scenarios that involve specific malfunctions, authorized responses, and EPFs in various combinations. In effect, a technological space will be defined with rich insights. The frequency of EPFs suggests that this may be a risky space with major uncertainties. The NPRMS could then assess the significance of this space and suggest research issues.

When PRT's have reached this level of sophistication and collaboration with the NPRMS, the "ethos" of "search for potential failures" will have become a systematic professional activity within NPP organizations. Attaining such proficiency would be a goal of an STS organization design.

9.3. Process Reliability Team – Design

The above discussion establishes the functional purposes of the PRT and some guidelines for its design. The PRT is the locus where operating mindfulness evolves and paths to increased reliability will emerge. In addition, PRT collaboration with some form of NPRMS will contribute to improved practices industry wide.

There are many ways to design such teams and design principles to guide design.[xxiii,xxiv] To be relevant to actual operational challenges, the design process should include the members of the PRT. There are many reasons for their participation. If we understand their work as professional, their input in the design process would be self-evident. In addition,

for the PRT to be effective, its members must "own" their design. Most critical, the response to contingent events must always be developed and elaborated in real time. In effect, the teams must redesign their actions and deployment regularly. They cannot look to management. As a soccer coach once put it, "If the team is looking at the coach, it is too late."

The best way to learn how to design team actions is to design their original configurations. They must understand the logic of their roles and the conditions to which that logic refers; hence, participative design. We can teach the tools and techniques and guide their processes but they must, ultimately, make their own design decisions.

The process of design involves team members, management, and ultimately the NRC, guided by organization design consultants. The "search for potential failures" as the platform for mindfulness can become effective practice at the subunit level in NPPs. Collaboration can achieve what regulation cannot.

10. MAJOR FAILURES – THE RECOVERY MANAGEMENT TEAM (RMT)

As noted above, multiple parallel OMTs and PRTs will require a higher level team to integrate NPP wide actions in the event of potentially catastrophic events. This team would include members of local PRTs, members of management, and outside expertise as needed. They, too, will have to practice mindfulness in the face of uncertainty. The design of the RMT will emerge from the structure and functioning of the OMTs and PRTs.

Major failures are those with evident catastrophic potential. The definition of a *major failure* is a gap in knowledge or understanding amplified with the question "*Could the change in the process result in catastrophic outcomes?*" Major failures trigger an active role for the Recovery Management Team (RMT). The threshold for alerting the RMT should be low. Most incidents will be corrected. Activation becomes a test of RMT *mindfulness.*

If a major failure is not readily controlled, the RMT becomes the organizational body with the authority over all operations and corrective actions. They are not a remote managerial team. Having developed a rich capacity for mindfulness, they will be the most experienced and qualified team to manage recovery from major failures for each NPP.

Will they succeed? Perhaps the best trained, most highly professional, and experienced teams have been the crews of US nuclear submarines. They are superbly trained and organized. There have been accidents and the loss of two nuclear submarines, but there has never been a nuclear accident in the submarine fleet.

The record of the nuclear power industry has been excellent given the complexities of the NPPs. This record has been achieved primarily because of a defense in depth philosophy and massive engineering efforts. The purpose of this proposed design is to marshal the organization and its work force in support of increased reliability.

11. RISK MANAGEMENT INFORMATION SUPPORT SYSTEMS

Every NPP should include a pair of computerized analytical systems that function on the basis of PRA failure scenarios. These systems will operate in opposition to support mindfulness in the face of potentially significant contingent events.

The Decision Support System (DSS) applies known models to help the PRT and RMT converge on valid diagnoses of failures and identify necessary containment and corrective actions. In practice, whatever diagnoses emerge will reflect one or more failure scenario. Such systems tend to undermine mindfulness by producing an "anticipated reality" and suggesting greater levels of certainty than are justified. A corrective system is needed.

The PRTs and the RMT will require an additional independent but linked information support system. Independence is necessary because the essence of mindfulness is inconsistency and the recognition of multiple untested diagnoses of system states.

11.1 Dialectical Inquiry Systems (DIS)[xxv]

As the RMT converges on a diagnosis, it is crucial that alternative models and diagnoses be preserved and updated. The Dialectical Inquiry System (DIS) would maintain a list of relevant PRA scenarios and documented failure scenarios, including the data that supports them, and data on any conflicting logic. As actions are taken and more information about the states of the system is accumulated, the DIS would update the relevant scenarios. Therefore, the RMT can readily reconsider failure scenarios and their validity.

This is an information system version of what the Sandia labs call their Blue and Red teams. The function of the Blue team is to model and create nuclear weapon scenarios that are fail safe while the function of the Red team is to "crash" the work of the Blue team.

Dialectical logic insists that for any set of data at least two valid antithetical theses may be ventured

and supported (one can often find three). Data, alone, does not resolve the conflict, therefore, learning must shift to the models and assumptions underpinning these alternative theses.[xxvi] Further support for a DIS comes from Feyerabend's insight that the relationship between theory and data is "incestuous." Theory defines what shall be seen as data and data, in turn confirms the theory. He recommends testing theories with radically antithetical models, i.e. models that do not share all of their primitives.[xxvii]

The quality of RMT reasoning should always be tested by a set of available alternative models. This is not a prescription for inaction but for effective mindfulness. Given the complexity of a NPP, we cannot expect individual minds or teams to track all of the relevant possibilities.

12. CODA

The title of this paper suggests that it will present a design for high reliability teams. The logic of the paper should have made clear that such a design cannot be developed remotely for a specific complex system in its unique setting. Complex high consequence sociotechnical systems can no more be designed remotely than they can be so managed. Faced with complex technical systems that are characterized with a great number of possible states, many paths to failure and significant potential for high consequence failures, both remote design and centralized remote management cannot assure reliability.

High reliability is possible through improved risk management. The industry has an excellent platform for mindfulness, PRA and its associated failure scenarios. In addition, there is concrete evidence of procedural failures, which indicate gaps in technological understanding. Based on these tools, many possible sociotechnical systems designs may be developed.

The proposed combination of Operating/Maintenance Teams OMT) and Process Reliability Teams (PRT), and a Recovery Management Team (RMT), and a separate Nuclear Power Risk Management System (NPMS, is intended to create conditions for the integration of PRA failure scenarios into nuclear power plant operational practices as a path towards improved reliability.

The paper is intended to extend the horizons of possible sociotechnical systems organization designs. In doing so, a rich variety of potential designs become available. Developing specific organization designs is a professional activity that engages local participants in a collaborative design process with organization design consultants. The design of a sociotechnical system is a continuing process as challenges emerge, technological knowledge increases, and teams gain increasing competence in risk management.

REFERENCES

[i] PERROW, CHARLES *Normal Accidents: Living with High risk Technologies* 2nd (Princeton, N.J.: Princeton University Press, (1999)

[ii] WOLF, FREDERICK, ELI BERNIKER, MITCHEL F. BLOOM, and ALFRED MARCUS, "Complexity and Tight Coupling: A Test of Perrow's Taxonomy in the Petroleum Industry" *Journal of Operations Management* (1999)

[iii] WEICK, KARL E and KATHLEEN M. SUTCLIFFE, *Managing the Unexpected: Assuring High Performance in the Age of Complexity* San Francisco: Jossey-Bass, (2001)

[iv] PERROW *ibid*.

[v] WOLF, FREDERICK *ibid*

[vi] ULANOWICZ, ROBERT E *A Third Window: Natural Life beyond Newton and Darwin* , p43, West Conshohocken, PA: Temple Foundation Press (2009)

[vii] *Ibid.* p45.

[viii] PERROW *ibid* p17

[ix] RAUZY, ANTOINE PRA/PSA Can the engineering models be improved? ANS meeting November 11, 2013

[x] MASSAIU, SALVATORE and HOMGREN, LARS "An empirical investigation of team decision-making with emergency procedures" ANS November 12, 2013

[xi] Massaiu *ibid* p2023

[xii] STARBUCK, W. AND MILLIKEN, F. "Challenger: Fine-Tuning the Odds Until Something Breaks" Journal of Management Studies, 25 (4), 1988 319-340.

[xiii] WEICK *ibid* p3.

[xiv] Weick, K., Sutcliffe, K. and Obstfeld, D. (1999). Organizing for High Reliability:Processes of Collective Mindfulness in Research in Organizational Behavior, 21 (1), 81-123. *p92*

[xv] TRIST, ERIC L. and BAMFORTH, K. "Some social and psychological consequences of the long-wall method of coal getting." Human Relations 4, 1951, pp. 3-39.

[xvi] TRIST, E. L.; HIGGIN, G. W.; MURRAY, H.; and POLLOCK, A. B. *Organizational Choice*. London: Tavistock, (1963).

[xvii] BERNIKER, ELI "Some Principles of Sociotechnical Systems Design" (1992) Unpublished paper available at:

https://dl.dropboxusercontent.com/u/12564505/Princriples%20of%20STS%20Design.doc

[xviii] LACROIX, F *Answering the challenges* United States Naval Institute Proceedings 127 (7) 29 (2001)

[xix] ASHBY, W. ROSS. "Self-regulation and Requisite Variety." Ch. 11: Introduction to Cybernetics. New York: Wiley, 1956; rpt. in systems Thinking. Middlesex, England: F. E. Emery, (1969)

[xx]BERNIKER, ELI , *The Agency Model of Work: Personal Causation in the Workplace,* Dissertation UCLA (1985)

[xxi] RAUZY *ibid*

[xxii] PERROW, CHARLES *ibid*

[xxiii] CHERNS, A.E "Principles of sociotechnical design" Human Relations 29,(8) 783-792.(1976)

[xxiv] BERNIKER, Eli *ibid*

[xxv] CHURCHMAN, C. WEST *The Design of Inquiring Systems,* New York: Basic Books, (1971)

[xxvi] MASON, R.O. "A dialectical approach to strategic planning" *Management Science,* 15(8): B403-B414. (1969).

[xxvii] FEYERABEND, PAUL K. "How to Be a Good Empiricist - A Plea for Tolerance in Matters Epistemoloqical." The Philosophy -of Science, pp. 12-39; edited by P.A. Nidditch. London: Oxford University Press, (1968)

NOMENCLATURE

Complexity is a measure of the number of paths to failure

Complex Chance Events are unique with zero probability of repetition

Complex STS are sociotechnical systems with many paths to failure.

Extra-Procedural Fixes are *ad hoc* improvised responses to malfunctions or process variations.

Failure is defined as any change in a technical system process that is not understood.

High Reliability Organizing (HRO) calls for *mindfulness* as a requirement to achieve reliability.

Mindfulness suggests skepticism about what is known about complex STS functioning, the acceptance of uncertainties, and a focus on failure.

Major Failures are technical systems events whose potential outcomes may be catastrophic.

Normal Accidents are expected failures due to technical systems complexity.

Nuclear Power Risk Management System (NPRMS) is a tentative label for an independent government agency that collects risk management data from Nuclear Power Plants.

Operating/Maintenance Team (OMT) refers to an integrated group charged with operating and maintaining a particular unit or subsystem of a nuclear power plant.

Probabilistic Risk Assessment (PRA) is a method of simulating all of the possible failure scenarios of a nuclear power plant.

Process Reliability Team (PRT) consists of the OMT in the role of developing mindfulness and risk management capacities.

Procedural Failures are gaps in technological understanding signaled by the need for Extra-Procedural Fixes.

Reliability refers to the capacity to prevent, to control outcomes, and recover from major technical system and technological failures.

Recovery Management Team (RMT) is a higher level team that integrates the work of the PRTs and coordinates the entire NPP in the event of major failures.

Sociotechnical Systems (STS) are human work activities that utilize tools or technical systems.

Sociotechnical Systems Design (STSD) is a body of knowledge about the design of work organizations that operate technical systems with a particular focus on teams as the unit of organization.

Technical Systems Failures are variations, disruptions, or states in technical systems that require corrective responses.

Technological Failures are gaps in knowledge with respect to the functioning of technical systems. *Historically, we do not need to understand a technology in order to use it.*