Eli Berniker Canterbury STS RT Presentation

Complex Systems Failure: Designing Reliability Teams

Introduction

My purpose is to integrate several critical areas of theory, systems understood in terms of ecological science, Normal Accident Theory focused on technical system failures, High Reliability Organizing from social psychology, and Sociotechnical System design principles as a basis for creating Reliability Teams to manage failures in high consequence technical systems.

In simpler terms, how should we design organizations to reliably operate nuclear power plants, BP deepwater drilling rigs in the Gulf of Mexico, air traffic control systems and any systems whose failure can have catastrophic consequences?

Note, we are not discussing safety. That is an individual personnel issue. We are talking about reliability which is a system level phenomena.

This is a literature which may be unfamiliar to some of you. The presentation will be available, in full, on line including the references.

Core Theory

Ecological science – Complex Chance Events (CCE) – Ulanowicz

CCE = events that have zero probability of repetition in the life of the universe. *Nature does not optimize for efficiency. It optimizes for variety and complexity.*

We, each, are a CCE. ***Given the number of possible versions of each of from our particular parents, there is not enough time in the life of the universe for another one of us to occur.***

New Window on science: Unique events overwhelm repetitive events in the universe. U.. suggests an ecological systems model of how collections of organisms form complex stable ecological ensembles. Stability is achieved by virtue of ensembles of organisms rather than at molecular or cellular levels. The organisms pass through; the organized ensemble survives, evolves, and adapts.

This will become the dominant model and metaphor for the social and organizational sciences with a profound, non reductionist bridge, to the natural sciences. Ulanowicz demonstrates systems causality that cannot be derived from the elements passing through the system.

I discussed our work with him. He is an ecologist. Ecologist and biologists have, as he put it, physics envy. Social scientists have natural science envy. He demonstrates empirically in ensembles of living systems, the Everglades or Chesapeake Bay, exactly the higher level control exerted by systems that we all see in social entities and organizations.

Normal Accidents – Charles Perrow; Fred Wolf

Complex technical systems failures are complex chance events. The probability of failures is very high simply because there are so many to paths to failure. That is the nature of complexity. The systems are entropic and, therefore, incorporate major uncertainties.

They are commonplace events but we only hear about the catastrophic failures: BP TransOcean Gulf, Three Mile Island, Chernobyl, Exxon Valdez, etc. etc. These are all *High Consequence Systems. The term "High Consequence System" is a euphemism for the most dangerous of all man-made systems, the US Nuclear Arsenal.*

Failures are endemic. Fortunately, few appear to be catastrophic. Yet, once we incorporate ecological concerns into our reckoning, the present frequencies will prove to be intolerable.

Bottom Line: *Complex technical system failures are the result of physical laws independent of human organizations and human error. They are high uncertainty systems.*

Challenge: Sociotechncial Systems and High Reliability Organizing (HRO)

> ***How do we design work organizations that can achieve high reliability operations and respond effectively when failures occur? How do we push back the walls of uncertainty?***

This is not simply a problem of organizing to eliminate human error. Nor can we engineer our way to a solutions. Many failures originate in engineered safety subsystems. That was the case at Three Mile island. At its core, this is an STS challenge. The BP Gulf catastrophe seemed like a failure of a safety system. But we still do not know how the drilling failed in the ground several miles below the surface.

The purpose of this paper is to integrate two approaches that deal with organizational technical reliability, STS and High Reliability Organizing (HRO). Time does not permit expanding on the rich description of HRO developed by Karl Weick and Kathleen Sutcliffe. In every case, they are dealing with the interaction between groups of people dealing with complex, risky, potentially dangerous technical systems. Their work is superb but it ignores Normal Accident Theory or the design issues that are central to STS. (I will further develop the integration in an expansion of this paper.)

Their work is excellent save for two problems:

1. Failures are confounded with human error. Makes sense. Social psychology is all about people, not technical systems.

   Normal Accident Theory and CCE both demonstrate that the set of potential failures vastly exceeds those that can be attributed to human error AND is so large as to exceed the cognitive capabilities of any organization.

2. There is a complete absence of an organization design perspective as if *mindfulness* can be developed and supported in any organization structure.

Weick and Sutcliffe have addressed this challenge in their work on High Reliability Organizing and call for *mindfulness* as the key to increased reliability. The characteristics of mindfulness are:

- **Preoccupation with failure** – Large and small
  Very suspicious of success. System has yet to unfold all of its challenges.
- **Reluctance to simplify interpretations**
  They know that the world they face is "complex, unstable, unknowable, and unpredictable."
- **Sensitivity to operations** –
  Attentive to the front line where the work gets done. Attendant to weak signals.
- **Commitment to resilience**
  Resilience is a combination of keeping errors small and of improvising workarounds that keep the system functioning. That is STS common sense
- **Deference to expertise *instead of authority.***
  Push decision making and around down to people with most expertise.

The parallels with STS should be clear to everyone. Yet the HRO approach is completely devoid of the need to design organizations to support mindfulness.

Mindfulness calls for organizational cognitive practices that are the opposite of the rules, policies, and procedures that are at the heart of organizational functioning and stability. One oil company did not see a way to integrate its requirements into their normal operations.

Mindfulness requires the group autonomy that is at the heart of STS team design. STS has long understood the need for such autonomy but, usually, with respect to less challenging technical systems.

We can never assure complete reliability in the face of the great complexity and uncertainty of such high consequence systems. However, reliability can be systematically improved over time. That is the design challenge.

STS RELIABILITY TEAM DESIGN

Note: *Given the time limitations, I'll present a conceptual design as a basis for discussion. I will assume that participants are well versed in STS design principles and practices. Nor will I discuss design processes. In short, an idealization is proposed as a target for deliberation rather than as a practical application in a particular setting. A real design process is likely to result in a great variety of designs.*

Assume a complex technical system as distinct from complex administrative or financial systems. Technical systems are governed by natural laws; administrative and financial systems are governed by social and behavioral laws. They share similar entropic conditions and modes of failure. However, the nature of the uncertainties is very different when operating technical systems such as, for example, nuclear power plants, chemical plants, deep water oil drilling, energy distribution, or transportation systems, etc. The processes that increase entropy, or disorder, are universal to all systems. The order that appears to be stable in social systems is always tenuous.

Reliability Team Roles

The primary role of the Reliability Team is to develop the *mindfulness* with respect to a particular complex system that will enable it to achieve high reliability operations on a regular basis and to manage control, containment, and recovery in the event of major failures.

The **Reliability Team** has two roles:

A. Learning – the creation of knowledge during normal operating periods. *That is how we fathom and map uncertainties and practice mindfulness.*
B. To assume authority and management in the event of major failures. *They should evolve as the most experienced and tested group with specific knowledge of the site and its challenges.*

Given the above purpose, the Reliability Team cannot be limited to operating and maintenance professionals. It must be a multi-disciplinary team incorporating those additional professionals that would be necessary in the event of potential catastrophic failures.

It follows that this will be a part time team distinct from the Operating/Maintenance Team although it will include those teams.

Why?

The additional disciplinary expertise may not be local and could include members from external organizations. Potential major failures may require the involvement of many agencies, organizations, local and distant, and a variety of competencies. If the Reliability Team is to manage the failure, they will have to develop the trust of those agencies and organizations.

More critical, we cannot expect effective *mindfulness* to emerge from an ad hoc grouping of individuals in a short term.

A note on the Operating/Maintenance Team. These two functions must be closely knit together. Knowledge of default system states and operating conditions must be known to Maintenance lest they inadvertently create additional paths to failure. Maintenance histories must be available to Operators as a context for process variations. This is a single team although some maintenance work may be performed by support services.

Uncertainty and Mindfulness

The acceptance of uncertainty is a necessary condition for multi-disciplinary collaboration and learning on a multi-disciplinary Reliability Team. No single discipline can encompass all the uncertainties. Most of them will occur at the boundaries between domains and require both technical and organizational responses.

The acceptance of uncertainty implies that the complexities, unknowns, and potential outcomes **cannot** be captured as data to support remote management. *Mindfulness cannot be a remote function.* HRO suggests as much in its *Sensitivity to Operations.*

That is why a Reliability Team must develop local experience necessary to mindfully assume authority in the event of major failures.

Major failures are those with evident catastrophic potential and, therefore, trigger an active role for the Reliability Team.

Failures and Learning

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

This is implicit in *mindfulness* although it is not defined that way by Weick and Sutcliffe.

"Failure" is not human error. It is the acceptance of uncertainty and an agenda for learning. It is the assumption that all of the potential states of a technical system will not be recognized or understood.

This is also departure from STS and Quality Control practice. There is no zone of indifference to variation, control limits, and assumptions of random variation. All variations are opportunities for learning.

Reliability Team Learning

A condition for multi-disciplinary learning spanning various agencies and authorities is that the Reliability Team does not have administrative authority under ordinary operating conditions. *That is a condition for collaborative learning. The choice is learning OR administrative punishment. Both are not possible.* In effect, rank and authority are checked at the door. This has been a practice in after action reviews in the US Coast Guard.

What does authority mean in the face of major uncertainty and complexity? Clearly, there is no knowledge basis for authority. The BP Gulf catastrophe demonstrates the effects of exercising remote authority in the face of poorly understood complex events.

Without authority, the Operating/Maintenance Team (OMT) and the Reliability Team (RT) operate in dialog. The former present issues for consideration by the Reliability Team. The OMT, which is full time and local, is a subset of the RT which is part time and may be virtual.

The Learning Agenda – Normal Operating Conditions

The Reliability Team develops shared *mindfulness* via their learning agenda during *normal operating conditions.* The agenda includes:

- Defining conditions and processes to be studied via tests and experiments. *The technical system should be designed to be robust with respect to such experiments. If robustness is suspect, those processes become topics for particular research, engineering, and concern. They signal instabilities.*
- After Action Reviews - Knowledge Failures - The RT will document the knowledge gaps and pose questions for exploration.

- After Action Reviews – Corrective Actions – All instances of control actions should be reviewed to identify anomalies, if any.
- Rich documentation – The RT should engage the OMT in rich descriptions of systems variations beyond the normally collected data. *The point is to practice mindfulness independent of the data collection system and explore alternative perspectives on process variations.*

The Reliability Team Design

The RT will be a part time virtual professional team including members who are unlikely to be co-located at a single site. The required range of disciplines and expertise to be tapped may not readily available locally. This would be especially the case if multiple agencies and organizations are involved. Aside from the OMT, other members will have regular work roles in other organizational settings.

Note: The roles in the Operating/Maintenance Team will also be professional in exactly the same sense as that term applies to other professionals. They operate on the basis of shared knowledge and further evolve that knowledge in their practice. *We cannot afford anything less if the goal is high operating reliability.*

The RT will probably confer for a defined period each week supported by a dedicated information system discussed below.

The Acceptance of Uncertainty is the unifying basis for collaboration on the team. While partial solutions and improvements may be the province of particular disciplines, they are all to be understood in the context of process complexity and uncertainties. The RT must be alert to the potential failure modes that derive from increased system complexity.

The RT is a *Community of Practice* associated with a particular complex operating system rather than a disciplinary area. The RT would be expected to study their system as "holistic anthropologists" considering a total system of artifacts, practices, organization, and the understandings that inform its operations.

Given that the role of the Reliability Team is to create knowledge and practice mindfulness, it would be designed as a *Community of Practice* rather than as an operating team based on STS design principles.

Major Failure Alerts

Major failures are those with evident catastrophic potential and, therefore, trigger an active role for the Reliability Team. The definition of *failure* remains the same, a gap in knowledge or understanding. The change is the addition of a question "*Could the change in the process result in catastrophic outcomes?"* At the BP Gulf Transocean drilling platform catastrophe that question was ignored when the first signs of something wrong in the well were evident. The remote managers, representing three different organizations, preferred to not imagine the potential scenarios when confronted with major uncertainties.

The threshold for alerting the Reliability Team should be low. There should be many "false alarms." In the majority of cases, processes will be brought under control, deficiencies corrected, and stability maintained.

Major Failures

In the event of a major failure not readily controlled, the Reliability Team becomes the organizational body with the authority over all operations and corrective actions. Note that they include the Operating/Maintenance Team actively engaged with the system. They are not a remote managerial team.

They become the *Mindful Operating Team.* The experience with the system resulted from their learning agendas becomes the basis for their *mindfulness.* As failure managers, their role is to contain, control, and recover from the failure. Failure would have resulted in profound physical deviations from expected processes. *They will have become the most experienced and qualified group to manage recovery from a failure.*

Their immediate tasks include making sense of the failure, executing whatever protective and safety procedures are needed and notifying the agencies and authorities relevant to the potential impacts of the failure.

Additional STS Design Principles

The following have been implicit in STS practice since its inception. They have to be made explicit when confronted with high consequence systems.

Trust: The organization must trust the Reliability Team. If it cannot trust its own people, they should not be operating high consequence complex systems. The risks are too great. Remote managerial control cannot substitute for local, immediate mindfulness. The effect of remote managerial control is to substitute organizational, economic and liability concerns for local success in controlling outcomes.

Ownership: Reliability Team ownership means that the team has an ongoing rich picture of the operations and processes under their responsibility, the authority to act, and the means to independently monitor their results real time. *They become the crisis organization.*

Mindful Information Systems

The *mindfulness* required by High Reliability Organizing should be supported by a computerized information system with unique functions called for by mindfulness. There follow some suggestions derived from the work of C. West Churchman in *The Design of Inquiring Systems.*

Dialectical Inquiry Systems (DIS) : As the RT converges towards an understanding of the nature of a major failure, it is critical that alternative models and hypotheses be preserved. The DIS would maintain a richly documented set of alternatives models including the data that supports them, the data in conflict, and the logic of their rejection. The team should always be able to reconsider any of the

alternatives and the validity of their rejection. The framework for the DIS should be developed over time during normal systems operations.

Eclectic Inquiry Systems- The key to Eclectic Inquiry is multi-disciplinarity. It derives from the work of E. J. Singer, an early systems theorist, whose approach framed Churchman's book. The system maintains a log of disciplines that have been found to impinge on the anomalies and variations in process operations. The effect is to link internally generated questions and issues to alternative disciplinary fields.

Mindfulness is all about alternative models beyond those encoded in experience and expectations. Both of these forms of IT support emphasize what might be ignored as the RT converges in its understandings.

The DIS and the EIS have to be developed as part of the learning agenda during normal operating conditions.

Major Challenges

The major challenges to achieving high reliability in the operation of high consequence systems will be legal rather than organizational. The consequences of major failures quickly activate multiple organizations, agencies, communities, and other stakeholders. The primary agendas of each of these participants are to limit their costs and liabilities. Given that legal setting, the trust and open collaboration required to prevent catastrophes and manage failures will be difficult to achieve. Catastrophic failures are rare events while liabilities and responsibilities are an ongoing concern.

The challenge will be to design an organizational framework that incorporates the concerns of many competing stakeholders with opposed agendas. It is most likely that Reliability Teams will be first developed in single organizations without external members of Reliability Teams.

Coda

The proposed Reliability Team design has focused almost exclusively on managing the operation of high consequence systems safely and reliably to the exclusion of consideration of the many competing economic, legal, organizational and political concerns. The challenges of shifting so much authority and responsibility to a single team are great.

The logic should be clear. Faced with highly complex technical systems that are characterized with a great number of possible states, many paths to failure and significant potential for high consequence failures, the present forms of centralized remote control and management cannot assure reliability.

A proposed Reliability Team design is just that, a proposal. Practical designs will have to be developed and tested to improve the practice of high reliability organizing.

References

Berniker, Eli "*Some Principles of Sociotechnical Systems Design"* (1992) Unpublished paper available at STS Roundtable website or from the author: berniker@gmail.com

Churchman, C. West *The Design of Inquiring Systems* (New York: Basic Books, 1971)

Perrow, Charles *Normal Accidents: Living with High risk Technologies* 2nd (Princeton, N.J.: Princeton University Press, 1999)

Ulanowicz, Robert E *A Third Window: Natural Life beyond Newton and Darwin* (West Conshohocken, PA: Templeton University Press, 2009)

Weick, Karl E and Kathleen M. Sutcliffe *Managing the Unexpected: Assuring High Performance in the Age of Complexity* (San Francisco: Jossey-Bass, 2001)

Wolf, Frederick, Eli Berniker, Mitchel F. Bloom, and Alfred Marcus (1999) "Complexity and Tight Coupling: A Test of Perrow's Taxonomy in the Petroleum Industry" *Journal of Operations Management*