WHITE PAPER

BUILDING THE HIGH-RELIABILITY ORGANIZATION (HRO)

Measuring and managing the four critical disciplines that produce consistent safety outcomes

MIKE SNYDER

Four years before BP’s Deepwater Horizon became global news, ExxonMobil walked away from a $187 million investment in a similar deep sea well. The well had yet to produce a single drop of oil when engineers detected geologic instability in the seabed. After consulting with geologists and drillers on the project, leaders decided that the best course of action was to cap the well and move on. Industry analysts at the time accused the organization of being too risk averse; after all, no incident had actually occurred.¹

That narrative changed in 2010, when operators of the Deepwater Horizon lost control of a wellhead that had been experiencing similar disturbances. This time there was no speculation of whether the risk was “real” or not. The resulting explosion and fire killed 11 workers and created an environmental and public relations nightmare. For leaders across industry, the tragedy of the Deepwater Horizon was compounded by the fact that many of the lessons it had to offer had already been “learned” before. So why did only one organization seem to heed them?

¹ For additional reading on the Blackbeard well and industry’s reaction to ExxonMobil’s decision, see “Exxon: Juggernaut or Dinosaur?” BusinessWeek, February 5, 2009 and “New Culture of Caution at Exxon After Valdez” by Jay Mouawad, New York Times, July 12, 2010.

©2015 DEKRA Insight. All rights reserved. All trademarks are owned by DEKRA Insight, reg. U.S. Pat. & Tm. Off.; reg. OHIM and other countries as listed on our website.
THE EMERGENCE OF THE HIGH-RELIABILITY ORGANIZATION (HRO)

Throughout the industrial age, human-made complex systems have advanced to provide the world with materials, clothing, fuel, food, and resources. However, these systems are susceptible to catastrophic events that result in multiple fatalities and major property damage. Since the 1980s, academics have worked to define what they call the High-Reliability Organization (HRO). The high-reliability organization is here defined as an enterprise that executes consistent and sustainable operations by creating a culture that anticipates and minimizes variation and implements high-quality decision making and controls.

The HRO paradigm seeks to categorize the characteristics of organizations that stay safe despite operating in high-risk conditions [Figure 1]. Think U.S. submarine groups, wildfire incident management teams, and nuclear plant operations. In theory, a high-reliability organization would routinely make the same same kinds of decisions that ExxonMobil did back in 2006 — and simultaneously avoid the mistakes made by operators of the Deepwater Horizon in 2010.

The challenge for leaders is that while there have been helpful descriptions of HRO practices\(^2\), defining HRO performance has largely been an academic exercise rather than a practical one. Leaders have struggled to translate anecdotal examples and feel-good “habits” into actionable and — more importantly — measurable practices.

Our firm sought to approach the HRO problem from a different angle. Rather than focus on individual behaviors found in HROs, which are helpful but hard to operation-

---

alize, we have sought to identify organizational practices that systemically mitigate risk. The result of this work is the definition of four measurable disciplines that together support the technical and operational aspects of process safety.

THE 4 DISCIPLINES OF HIGH-RELIABILITY ORGANIZATIONS

Through study of theoretical models of high performing safety organizations and study of incident investigations of actual process safety events we have recognized that there are four aspects of organizational performance that are key to safe operations (Figure 2). An organizational culture that supports these areas of performance will have fewer process safety incidents.

ANTICIPATION
Fostering systems and behaviors that are sensitive to “weak signals” that may be indicative of increased risk of catastrophic events.

Anticipation is about recognizing the early warning signs that help you head off incidents. An organization strong in Anticipation will have mechanisms to capture information from a variety of sources that may be meaningful early indicators of change to exposure. Examples could include process deviations, unusual maintenance requests, and even front line workers detecting differences in sounds.

We recently worked with a company that had defined the normal operating range of key process parameters, and had also defined a broader range for these parameters, which they called “safe operating limits”, where the operators could get the process “back into control”. Excursions outside of the safe operating limits were reported and studied, but excursions outside the normal operating range limits were not. This is an example of weak Anticipation – if the process gets outside its normal operating range, that’s an early indication that it didn’t function as designed. If the organisation asks why, they are likely to discover ways to reduce risk.

To have strong Anticipation we need a culture that supports it. This means:

- People are encouraged to report and the value of reporting is reinforced
- Data is acted on and people know that. They won’t bother if they perceive that information disappears into a black hole and nothing ever happens
- Leaders understand and accept that there will be lots of information that is not important but it’s worth sorting through to be sure we don’t miss the information that is critical
- We can identify key leadership behaviors that help create this culture. When those behaviors are practiced we build an organization with strong Anticipation

Organizations with strong cultures have leaders who visibly value the search for early warnings and reinforce the analysis of these indicators, even when this does not result in identification of serious risk. These leaders understand that supporting the detection and investigation of many false positives is worth it if it results in just one catastrophic event avoided.

Figure 2. The AIER Model
INQUIRY
Making effective use of information to analyze, understand, and plan mitigation of risks, while making a conscious effort to overcome bias.

The Inquiry discipline is about preserving the integrity of decision-making and action, specifically by protecting teams from the natural biases innate in all humans and groups. Traditional process safety management (PSM) includes a number of elements (such as process hazard analysis, pre-startup safety review, management of change) designed to evaluate and plan for control of hazards and risks. However, there are common (but often undetected) cultural characteristics that can undermine the effectiveness of these efforts and leave the organization vulnerable.

Cognitive bias refers to the tendency we all have to rely on intuitive, rather than analytical, thinking in order to process information efficiently. Our knowledge and experience allow us to reach conclusions and make decisions quickly and efficiently in many circumstances. However, this can also trap us in poor decisions. We saw the impact of cognitive bias in one incident where a crew of maintenance workers responded to the sound of leaking gas from pipelines in a trench. Everyone on the crew assumed the gas was nitrogen because there had been a previous nitrogen leak. But this time the leak was hydrogen, and when the trench cover was lifted a spark ignited the hydrogen and killed several people. Had the work crew applied appropriate Inquiry, it is likely that they would have overcome the bias that drove them to assume this was a nitrogen leak, and the dangerous situation could have been identified through the use of a 4-gas combustible gas indicator—typically used for screening hazards during pipeline leaks. Even if the leak was nitrogen, using the gas detector for Inquiry would have identified if an oxygen deficient environment was present.

Cognitive bias can also get us into trouble in formal hazard analysis—we can too readily accept what we think we know, e.g., that a particular condition or situation or deviation is not problematic. The tendency to go along with a group’s predominant opinion makes this worse. Biases can include:

- **Confirmation bias.** The tendency to search for or interpret information in a way that confirms one’s preconceptions.
- **Normalcy bias.** The refusal to plan for, or react to, a disaster that has never happened before.
- **Availability bias.** The tendency to predict based on how easily an example can be brought to mind.
- **Status quo bias.** The tendency for people to like things to stay relatively the same.
- **Groupthink.** The tendency to do (or believe) things because many other people do (or believe) the same.
- **Risk seeking/risk aversion.** The tendency to make risk-averse choices if the expected outcome is positive, but make risk-seeking choices to avoid negative outcome.

The only way to guard against the insidious effects of cognitive bias is through culture and leadership. There are specific leadership behaviors (for example, encouraging the voicing of dissenting opinions) that promote a culture that produces more accurate decisions. There are also specific skills involved in asking the right question in the right way to get the right data. Leaders must promote and measure the use of these leadership behaviors and skills.

EXECUTION
Monitoring, reinforcing, and verifying program execution, while staying true to the process.

The Execution discipline is about assuring consistent and reliable use of safety programs and processes. Even the most excellent hazard identification and control efforts are subject to failure or underperformance if the programs and practices are not followed as intended. While many organizations use periodic audits to provide a check on implementation, the key to assuring consistent and ongoing activity is developing leaders who monitor, reinforce, and verify effective program execution.

- **Monitoring** involves regularly acquiring information on what subordinates are doing, how they are progressing toward achievement of goals, and what issues or problems they may be encountering. This is not micromanaging; rather it is assuring that the leader has sufficient information to meaningfully recognize good performance, provide support when subordinates need it, and then providing corrective feedback on those (hopefully rare) occasions when subordinates fail to fulfill their responsibilities. A leader’s monitoring behavior may take many forms. Depending on the situation and the leader, these may include walking around and observing, informal conversations at the front line, periodic meetings with subordinates to review progress, use of written progress reports, review of appropriate metrics, etc.
• **Reinforcement** involves providing feedback that recognizes good performance. This communicates the importance and priority of the catastrophic event prevention activities and maintains focus on consistent execution. Effective reinforcement is based on effective monitoring, which provides the leader with specific data on which to base reinforcement, avoiding the vague and ineffective “good job” type of feedback to subordinates.

• **Verification** is similar to monitoring, but where monitoring is focused on the performance of subordinates, verification is focused on activities and programs. Assuring that audit findings are resolved in a timely manner is an example of verification, and leaders who do this effectively are more likely to have organizations in which consistent execution is valued as part of the culture.

**RESILIENCE**

Developing and exercising the ability to react in ways that prevent upset conditions from becoming catastrophic events — and then learning from the experience.

The Resilience discipline is about developing the agility to recognize and quickly respond to exposures in real time. Upset conditions occur from time to time in any system. A resilient organization is able to react in ways that prevent upset conditions from becoming catastrophic events, and then learning from the experience. This has a major influence on ultimate results. Even where automated control systems are designed to handle upset conditions, it is important that workers understand when and how to intervene, and are not only able but also willing to make appropriate interventions early. An organization that is strong in Resilience is more likely to prevent a small process disruption from becoming a major incident. There are three main requirements for Resilience:

• **Knowledge.** Do people at various levels have a broad enough understanding of the operation so that they can make good judgments in case of emergency? Some organizations approach this through use of extensive sets of rules and procedures. That approach is intended to assure consistency and avoid having to rely on technical knowledge at the operating level. However two problems arise with that approach. First, the range of possibilities that must be planned for results in a proliferation of procedures and rules that become impractical for anyone to know. Second, this approach assumes that all possibilities (with all variations in every scenario) can be identified in advance — something that is unlikely to be true. The alternative is to develop an organization in which people are knowledgeable and are taught to make good judgments based on their knowledge and the information at hand.

• **Willingness.** Are people more or less likely to take action on their own initiative? The answer is directly related to culture. People are less likely to act if they are not confident that the organization will support them. Perceptions of the culture’s support for resilience are formed over a long period and are based on many small actions taken and not taken by leaders. An organization desiring strong catastrophic event prevention will be sensitive to this and intentionally create the culture that supports resilience.

• **Continuous Learning.** Do leaders establish both the expectation that learning is an ongoing process that never stops — as well as the systems and processes to support such continuous learning? Resilient organizations make learning routine rather than waiting for an incident to trigger learning mode. They create formal mechanisms (e.g., cross-functional teams, advanced training in incident investigation) to continually capture and respond to risk data. They put the focus on generating new knowledge, not finding fault. Great learning organizations are also characteristically self-aware. They make sure that even the newest employee knows the story of where they came from and where they’re going. They’re vigilant about preserving organizational memory and assuring that hard lessons are never forgotten — or repeated.

**BUILDING A HIGH-RELIABILITY ORGANIZATION**

How can leaders develop a high-reliability organization? Fundamentally, high reliability is a blended cultural and technical process driven by leaders. Leaders must establish the expectation that attention to exposure is an ongoing learning process that never stops. At the same time, they must also assure that organizational and technical systems, as well as enabling systems, support such continuous learning. There are several practices that can help your organization move toward high-reliability:

• **Cultural Assessment.** The first step is identifying how your organization is performing now. Rather than look at incident rates (which are poor indicators of actual exposure). The AIER scales identified above
are readily measured (Table 1), alongside culture indicators shown to predict general safety outcomes (OCDI reference).

- **Technical Assessment.** Cultural assessments can be immensely powerful and have been demonstrated to predict safety outcomes. To provide a more holistic picture of organizational reliability, it is advisable to also conduct a technical assessment that evaluates the effectiveness of process safety systems, including the identification of risk, robustness of protective barriers, and capability of personnel responsible for system operations.

- **Develop a process safety improvement roadmap.** Based on the findings from the Cultural and Technical assessments, an organization’s capability can be assessed against one of several internationally recognized Process Safety Management models. Improvement plans can be developed and paced to meet organizational risk resolution timelines and resource capacity.

- **Adopt a learning orientation.** High reliability organizations are characteristically self-aware. They make sure that even the newest employee knows the story of where they came from and where they’re going. They’re also vigilant about preserving organizational memory, look outside their organization for learning opportunities, and assuring that hard lessons are never forgotten — or repeated.

<table>
<thead>
<tr>
<th>ANTICIPATION</th>
<th>INQUIRY</th>
<th>EXECUTION</th>
<th>RESILIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Always seeking</td>
<td>Always questioning:</td>
<td>Maintaining control while staying</td>
<td>Preparation, response,</td>
</tr>
<tr>
<td></td>
<td>Avoiding bias</td>
<td>ing true to process</td>
<td>and learning</td>
</tr>
<tr>
<td>Priority is given to</td>
<td>Rigorous analysis systems are</td>
<td>Leaders set clear expectations</td>
<td>Teams have rehearsed responding to</td>
</tr>
<tr>
<td>measures and weak</td>
<td>in place and used</td>
<td>Roles and responsibilities are</td>
<td>a variety of upset conditions</td>
</tr>
<tr>
<td>Data and hunches are</td>
<td>consistently</td>
<td>well defined and understood</td>
<td>Leadership supports and reinforces</td>
</tr>
<tr>
<td>valued</td>
<td>The organization actively</td>
<td>The risk acceptance process is</td>
<td>employee intervention to minimize</td>
</tr>
<tr>
<td>Systems and culture</td>
<td>to overcome bias</td>
<td>clearly defined and followed</td>
<td>impact</td>
</tr>
<tr>
<td>support problem</td>
<td></td>
<td>Recommendations are applied</td>
<td>Post upset activity focuses on</td>
</tr>
<tr>
<td>seeking</td>
<td></td>
<td>widely</td>
<td>learning and putting lessons into</td>
</tr>
<tr>
<td>Input from the</td>
<td></td>
<td></td>
<td>action widely</td>
</tr>
<tr>
<td>frontline is given</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>high value</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High sensitivity to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>change</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reinforcement of</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>reporting</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Sample criteria to evaluate AIER scales

**MOVING TOWARD HRO PERFORMANCE**

Expectations of what safety is and could be have exceeded far beyond the early charter of reducing costs and injuries simply. The promise of high-reliability organizations is that they define a path to consistent safe performance, even at the frontiers of industry and technology. As with all innovation, the key to adoption is being able to replicate the conditions and factors that create the phenomenon reliably and predictably. The practical and measureable nature of the AIER scales opens a new way to leaders wishing to create high-reliability organizations of their own.