Modeling Risk Dynamics in e-Operations Transitions

Eliot Rich
Department of Information Technology Management
School of Business
University at Albany
1400 Washington Avenue
Albany, NY 12222
e.rich@albany.edu

ABSTRACT

Migrations to new modes of operation are perilous times for most organizations. For firms that routinely work in high-threat, high-reward situations, the risks of innovation are particularly challenging. This paper presents a systems-based approach to understanding these risks, drawing examples from one firm migrating to e-Operations for offshore oil platforms to increase profitability. The firm recently participated in two facilitated group model building exercises to examine the effects of the migration on the organization and resources needed to safely implement multiple changes over time. Based on these exercises, a simulation model of the timing and relative levels of risk, was developed. The results of the workshop and simulation demonstrate the effect of a combined qualitative and quantitative modeling approach to understanding complex problems.[1]

Keywords

Simulation, Risk, System Dynamics, Oil Platforms, Knowledge Management, e-Operations

INTRODUCTION

The presence of operational risk is integral to power production, airline safety, chemical plants, and other areas where potential vulnerabilities must be mitigated. Management of this risk requires recognizing the presence of the uncertain, the effects of both random events and intentional acts, and understanding the trade-offs that create superior or inferior outcomes.

Operational risks are likely magnified during times of process change. Implementing innovative operating models, technologies, and procedures introduces additional vulnerability during transitions as staff adapt their existing expertise to new working modalities. Change may also introduce personal stress during transitions because of uncertainty of the effect of change on outcomes, beliefs about personal efficacy and control, and modification of relationships.

These effects are particularly important in a high-threat, high-risk environment. Accelerated change without appropriate mitigation may result in catastrophic loss of life and economic disaster. Before implementing any new system, companies working in such high-threat areas must be quite careful to evaluate the effects and possible outcomes of their innovation. The protracted effects of ongoing change on operational risk, the *risk dynamics*, bear special examination. An organization's ability to manage and absorb complex changes over an extended period might well limit the timing and success of the adaptation.

This article reports on the initial steps towards developing a risk dynamics model for operational changes in an offshore oil production facility. The techniques of system dynamics and group modeling building were employed to develop a proactive analysis of the timing of the emergence of risk during a decade-long transition to remote

[1] The group model-building workshops described herein are part of the AMBASEC (A Model-based Approach to Security Culture) and the IRMA (Incident Response Management) projects funded by the Research Council of Norway (project nos. 164384 & 164372). AMBASEC is anchored at Agder University College, while IRMA is based at SINTEF, the Foundation for Scientific and Industrial Research, Norwegian Institute of Technology (NTH). Our thanks to both institutions, the collaborators in the Security Dynamics Network (http://www.securitydynamics.org) and our industry partners for their assistance.

operations. The focus is on the overall risks inherent in the transition, rather than on the particulars of the innovation and technology.

The next section presents the background of the study and the particular concerns that were raised by managers and operations personnel at the facility. This is followed by a description of the structure of the simulation and the causal model that underlies it. Next are two simulation model runs, followed by a section that interprets the findings, the strengths and weaknesses of this approach, and expectations for future work.

E-OPERATIONS, ORGANIZATIONAL TRANSITION, AND EMERGENT RISK

The e-Operations model, an application of advanced technology to offshore oil and gas production, brings together the best parts of remote operations and automated production.[2] It uses information and communications technology to monitor and control manufacturing facilities at a distance, combining real-time data collection, visualization and data integration. It also enables access to previously unavailable expertise from multiple facilities and sources. While the remote operations concept is not new, the emergence of inexpensive bandwidth and computing power makes e-Operations an attractive option for many firms. This is particularly true for high-threat operations, where remote sensing can reduce human exposure to hazardous environments.

The introduction of computer-enabled e-Operations adds risks as well. Operational sensors, control systems, and communications channels must be absolutely reliable to ensure constant control and contact with the now-remote operators. Platforms must remain secure, even in the face of concerted computer-enabled efforts to sabotage production or inadvertent error.

When approaching the transition to e-Operations, security-conscious organizations face two changes in their modus operandi. First, they have to manage the change and adoption of an e-based operations model, with the modifications to work procedures, staff knowledge, and structural capacity that go along with radical redesign. Second, they need to consider what steps are needed when moving to a computer-based environment where hackers, disgruntled insiders, and criminals may see e-Operations as an opportunity to exploit new vulnerabilities.

Moving to e-Operations for offshore oil platforms

The firm in question has a number of oil platforms working in hazardous conditions. Under traditional operating models, offshore engineers and operators control virtually all of the platform's activities. The daily hazards of this operation are quite real: the firm's annual report explicitly describes the number of accidents and fatalities in their facilities, and the steps being taken to improve the operating conditions.

Some of the work is amenable to moving to safer conditions. Not all skills are needed all the time on every platform. It is envisioned that an improved and robust communications infrastructure will enable the movement of some experts to onshore sites. Such a communications scheme would also create synergies between sites, allow more rapid access to expertise away from the operating areas, provide real-time access to operational data, and reduce operating costs. There is an element of increased risk, however, as having fewer people at the remote site means that the tactile element of analysis and fault detection may be missing.

Moving from traditional offshore operations to e-Operations requires adapting existing knowledge to the new environment. Each platform crew currently attempts to solve problems on its own, an approach that conflicts with the desired goal of centralized communications and knowledge sharing. In the new model, offshore operators need to know more about how to operate and respond to the new supervisory control and data acquisition (SCADA) systems. Onshore engineers will need to interpret the data they are receiving from the various sensors and visualizations, rather than what they directly observe on the platform.

There are clear financial incentives to adoption of e-Operations. The firm often faces decreasing returns to capital investment. Operating costs are increasing as platforms age and oil becomes more difficult to extract. Rather than abandon these oil fields and the many millions of investment, the firm is interested in shifting to a more automated operating model to extend the life of old facilities, and make new facilities more profitable. These incentives create great pressure within the organization to move to integrated e-Operations. It is anticipated that when this move is completed, platform operation costs will decrease by 20-30%, and extend current oil reserve utilization by 5-10%. In

[2] For more on e-Operations, see http://www.sintef.no/.

the current environment the development of new facilities is highly regulated and quite expensive. Thus, any movement to keep existing investments productive is quite attractive.

In high-threat environments, even controlled and managed events carry a severe economic cost. In one recent event, a contractor unintentionally introduced a computer virus into a control system for an offshore oil platform. Isolating and repairing the affected systems forced a one-day shutdown at a cost of $1M, but with no damage to the site or the environment. This was a controlled response to the threat.

There is a constant threat of severe disruption. The oil industry is very conscious of this threat, and works quite diligently to train its staff in procedures to ameliorate and mitigate these threats. One concern raised in implementing e-Operations and remote control is the possibility that removing people from the platforms increases risk, and that the human safety features, which are highly effective but expensive (in terms of staff effort), would become somewhat less effective when fewer people are in place.

The Modeling Workshops

A group model-building workshop was held under the direction of the Security and Quality in Organizations Research Cell, Agder University College, Norway, in September 2005 to consider this problem. This two-day event brought together experts in the offshore oil industry, computer security, psychology, and system dynamics. It followed a similar exercise conducted in May 2005, which has been reported elsewhere (Rich and Gonzalez, 2006). A facilitation team from the University of Albany, USA led the sessions. This team has developed several protocols for organizing and running such sessions over the last decade (Andersen and Richardson, 1997, Vennix, 1996, Luna-Reyes and Andersen, 2003, Richardson and Andersen, 1995).

The September workshop had four outcomes:

- Establishing the role of transition risk in the context of e-Operations. At the May workshop the gradual transformation of the firm from traditional operations to e-Operations was identified as one of several dynamics that were affecting risks and risk mitigation in the firm. In this workshop the participants decided to focus on this transition, and leave issues such as mitigation through communications and incident response teams for another time.
- Identification of reference modes. In proactive modeling, there is often little formal data available for integration into the model. A strength of the system dynamics approach is its ability to use expert judgment and intuition as part of a formal model (Sterman, 2000, Richardson and Pugh, 1981). In this case, the participants were asked to consider what the likely timing and transitions for the integration of the work processes might be. As part of a small team exercise three parallel estimates of the process transition were created. All of these transitions had characteristics of "s-shaped" growth: Innovations that built over time, then tapering off as the dissemination of change was completed. In this case, the estimates for completion of the project were based on a multi-year plan already in place (Figure 1).

Figure 1 – Sample reference mode from expert knowledge elicitation

- Articulation of dynamic hypotheses. Once the reference modes were presented, the group worked to collectively identify what assumptions were in play that underlay these reference modes. In the system dynamics literature these assumptions are characterized as "dynamic hypotheses", statements about the problem that may be described in the form of changes over time. The hypotheses extracted from the discussions and subsequent modeling are presented in the next section.
- Building a structural foundation for understanding risk dynamics. The final outcome for the workshop was the identification of system structure that was thought to generate the dynamics. This was done in the form of a causal loop diagram with the group, and then extended into a formal simulation model for experimentation and discussion for the weeks and months after the meeting ended. The results of the initial experimentation are presented below.

DYNAMIC HYPOTHESES AFFECTING RISK

Hypothesis 1. A Knowledge Gap Drives Vulnerability

Migration from existing operating approaches to newer ones carries with it some degree of uncertainty. In a high-risk environment, this uncertainty is a major concern, as failures can cast a pall on the entire firm. Engineering models and operating experience provide a sound basis for the transition, but there is always some unforeseen change or element that needs to be managed as it occurs during the change. Thus, the transition from existing paradigms can be modeled as a move from traditional work processes to a stage where new processes are developed and in place, followed by a period of time where changes are integrated and debugged. The result of this integration is a set of mature work processes.

The knowledge needed to become competent in the new techniques takes time to develop. Traditional operations are the basis for their knowledge in the new operation, but this knowledge needs to be reframed for the new operating environment, and in turn practiced and disseminated. This structure parallels that of the process development itself, with a transition from traditional knowledge to new knowledge, followed by integration and maturation.[3]

Using the stock-and-flow notation of system dynamics, the transitions are represented by two parallel aging chains (Figure 2). Resources devoted to developing new work processes move these processes forward; resources for

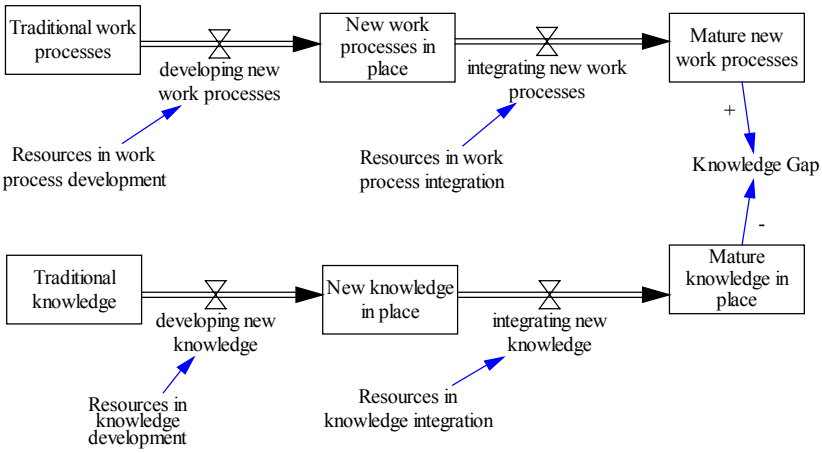

Figure 2 Knowledge Gap from e-Operations Transitions

[3] Alternatives to this model that would emphasize the knowledge needs of new employees, or ones where the existing base of knowledge was made obsolete in the face of environmental change. In this case turnover was excluded from the scope of the model and the knowledge change limited to the application of existing domain knowledge in a new process context. This assumption eliminates the complexities of knowledge obsolescence.

knowledge development help adapt the existing skills of platform staff to work with the e-Operations techniques. Resources on integration are applied to modify and mature the newly developed procedures and knowledge. The productivity of these resources will be added to the model later.

Pressure to adopt a potentially profitable change quickly increases the knowledge needed for safe operation, creating a "knowledge gap" between what is needed and what is currently known. A large knowledge gap increases the firm's vulnerability to operational threats, and the greater the damage if the threat comes to pass.

Hypothesis 2. A Knowledge gap and relative newness of processes and knowledge contributes to vulnerability

The presence of a knowledge gap in the transition to e-Operations indicates a potential vulnerability: the project teams may not be prepared to understand how the new changes will affect their routine and exceptional operations. On the other hand, training and knowledge in advance of the transition - a "knowledge surplus" – would be expected to mitigate some of the risks associated with change. For the purpose of the simulation we estimated that a well-prepared platform team with adequate knowledge might be able to reduce their vulnerability by 80% of normal, while a team facing a knowledge gap would not be able to reduce their vulnerability at all.

In addition, the vulnerability of the platform is believed to increase temporarily when new processes are put into place. This hypothesis recognizes the inevitable conflicts that emerge when multiple new techniques are applied in parallel to an existing situation. In this context there are many individual processes that are being migrated to e-Operations, grouped into clusters of about 20 major processing cycles. Each is expected to require some weeks or months to integrate. During this interim period, an increase in the "average newness" of the entire e-Operations transition would be expected to increase vulnerability. Similarly, an increase in the "average newness of knowledge" contributes to an increase in vulnerability. These three factors are combined in the model to estimate a relative vulnerability index (Figure 3).

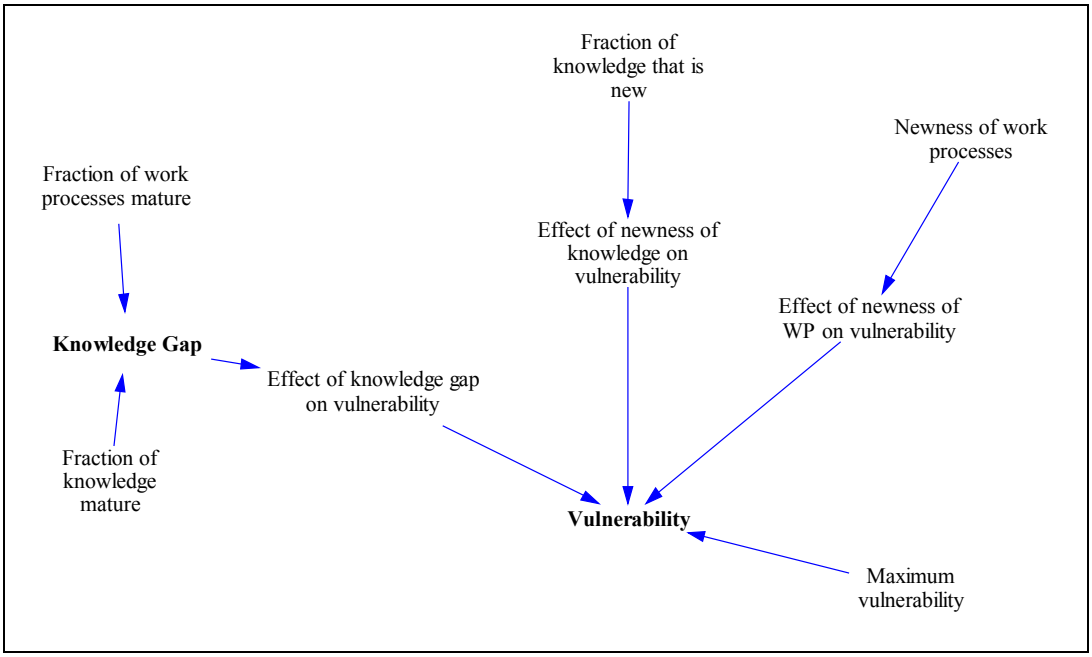

Figure 3 Knowledge gaps, newness, and vulnerability

Hypothesis 3a. Development of work processes and knowledge reduces the effort required for subsequent development

Hypothesis 3b. Integration of work processes and knowledge reduces the effort required for subsequent integration

Hypothesis 3c. Parallel development of multiple new processes increases the coordination burden and decreases development productivity

These related hypotheses define how the resources devoted to implementing change are affected by workload and the experience gained from the early stages of innovation. As new processes are developed, subsequent processes will be easier to codify; while there may be some desire to reap low-hanging fruit by selecting easier steps, the substantial investment in infrastructure required to enable e-Operations – remote sensing and high-bandwidth telecommunications – indicates that increasing productivity as more new processes emerge within some bounds is reasonable. This is modeled with two feedback loops, a positive loop drawing new work processes forward, and a negative loop that slows the transition rate as the number of unmodified processes is depleted.

At the same time there is recognition that a large number of ongoing development processes puts a communication and coordination burden on those tasked to complete the task. This exerts a balancing pressure on the drive to move traditional processes forward (Figure 4). A similar structure exists for the development of new knowledge, but is not depicted in this paper.

A feedback structure is also in place for the maturation of processes and knowledge. As the first few work processes mature, the productivity of the persons responsible for this work is assumed to increase, drawing processes through the aging chain more quickly, a reinforcing loop. When the bulk of processes have been matured, there is a balancing effect that slows the final transition (Figure 5). Again, a similar structure exists for knowledge maturation, but is not shown.

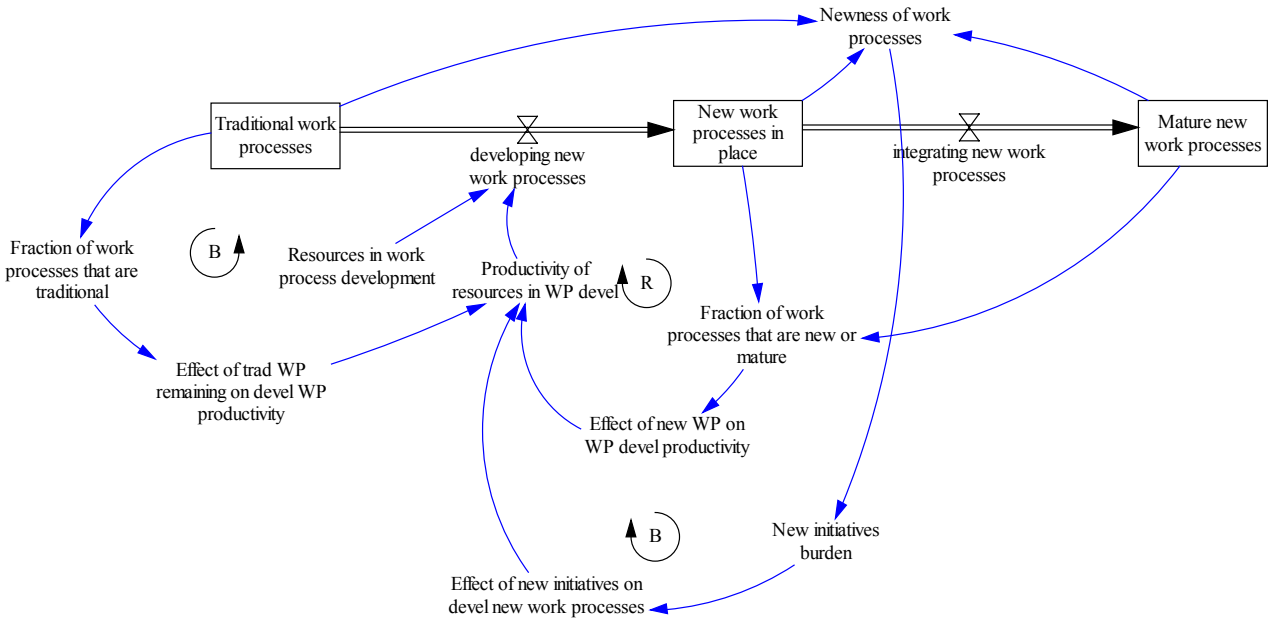

Figure 4 Effects of accumulating experience and workload burden on development of new work processes

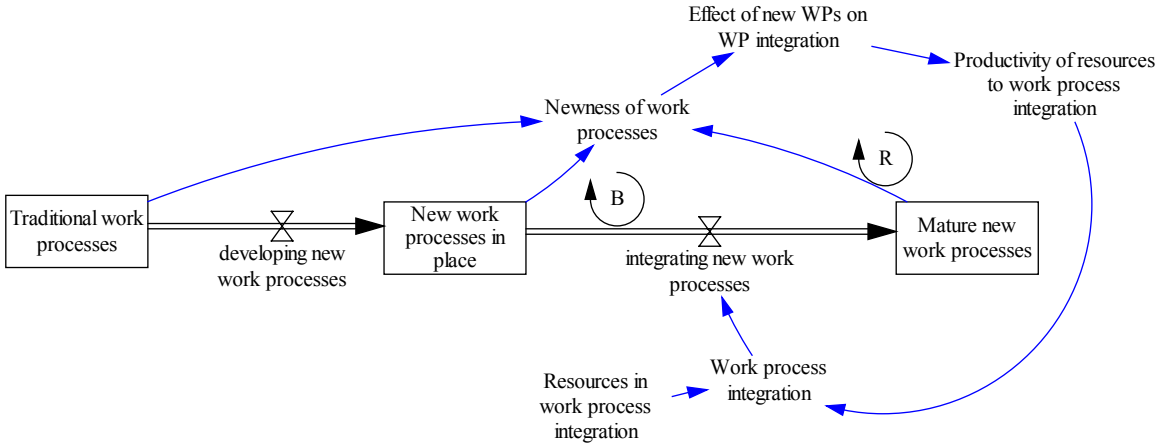

Figure 5 Maturation of processes and productivity

Hypothesis 4. Increased vulnerability increases the frequency of incidents.

For this work it is important to distinguish between *events* and *incidents*. In the high-threat world of oil platforms there is a constant stream of problematic events. Some of these events occur so frequently that they seem routine: a particularly recalcitrant piece of equipment requires adjustment or tuning on a regular basis. Some events, such as widespread systems failures, are uncommon but very challenging. Endogenous events, such as insider threats, are particularly difficult to predict, as their causes and precursors are not often monitored or even well-understood (Randazzo et al., 2004).

An event becomes an incident when it is no longer routine: when it falls outside the anticipated activities of the platform, generating a loss of revenue or increase in operating costs. In this model, the increase in vulnerability from a knowledge gap increases the likelihood that an event will turn into an incident. If process knowledge is adequate for the current state of the e-Operations transition then the number of events that turn into incidents will decrease but not disappear.

Hypothesis 5a. Incidents improve learning and reduce the severity of future incidents.

Hypothesis 5b. Mature processes and knowledge improve resilience and reduce the severity of incidents

One of the positive effects of incidents is their effect on the knowledge base of the organization. When properly analyzed, incidents provide insight and direction for protection against future incidents. Increased knowledge about incidents will increase the number of incidents that are detected and reduce their severity, the effect that they have on the site (Figure 6).

Severity is also affected by the relative resilience of the procedures in place at the platform. A mature set of processes and knowledge will be more resilient than newly introduced ones, with the effect of reducing the severity of incidents that occur. In the next section severity will also factor into the cost of incidents, where detection and mitigation reduces the cost of an incident.

The learning loop itself is balancing: An increase in accumulated knowledge will make subsequent incidents easier to detect and mitigate, reducing the severity of subsequent incidents. As the severity of incidents decreases, the incremental learning they provide will also decrease, closing the learning loop.

Earlier research from this project speculated about the presence of knowledge and detection traps that might limit the effectiveness of incident response teams in the presence of constrained resources (Rich and Gonzalez, 2006). We have included these structures but they are not active in the simulation.

SIMULATIONS

In this section we summarize the results from experimenting with a simulation that illustrates how operational risk changes during the transition to e-Operations. The causal model was advanced to a formal simulation after the group modeling effort was completed, and is based largely on the interpretations of the problem by the modeling team. The parameters in the runs are modeler estimates, reflecting the current understanding of the domain.

Several simulation runs were conducted using the Vensim modeling environment.[4] In the base run, the simulation models a 10-year transition with a constant event rate, and balanced resources between development and integration for both processes and knowledge. For comparison a second run is presented where resources are reallocated towards knowledge integration.

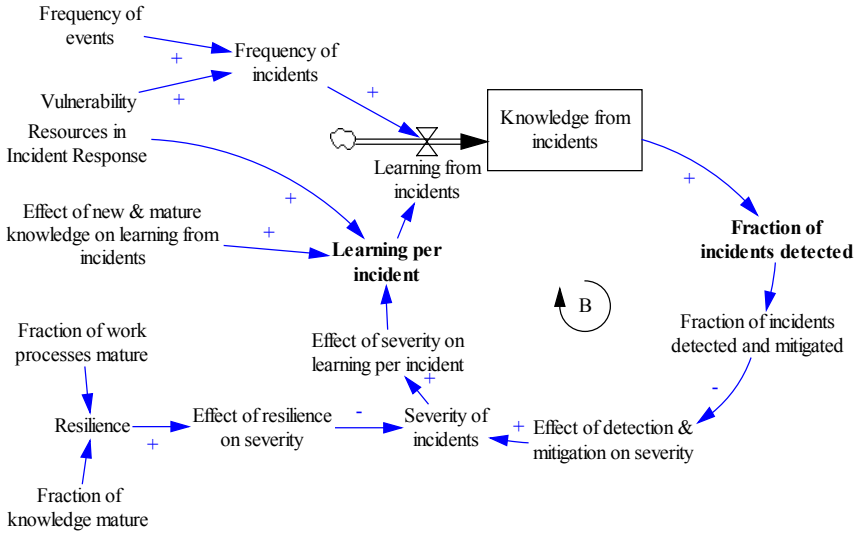

Figure 6 Frequency, Severity and Learning from Incidents

[4] The simulation model is available from the author upon request

Base Run

In the initial runs of the simulation the anticipated s-shaped transition of processes and knowledge is present. By 10 years most of the work processes have been matured, and the remaining are under review. The required process knowledge has a similar dynamic, but maturation takes longer as the need to coordinate several parallel process development activities increases the workload burden and slows knowledge development (Figure 7).

The difference in the process and knowledge development rates creates a knowledge gap (Figure 8, left graph), indexed based on the relative completion of mature process and knowledge. The gap starts at zero and increases for the first 80 months of the project, as knowledge maturation falls behind the development of processes. The presence of immature processes and knowledge quickly drives up the number of incidents, that is, the number of events that are not routine (Figure 8, right graph). For six years the firm is attempting to manage an increasing number of incidents due to the knowledge transition. As incidents occur, the immature processes are modified and the severity drops from better understanding of the new processes. More immature processes are arriving each day, generating even more incidents.

Incident costs peak sooner than the number of incidents because of the influence on decreasing severity of incidents. In essence, the staff are learning from painful experience – as the number of incidents rises, the average severity decreases. The combined effect of frequency and severity drives incident cost to a peak at around time 36. Incident costs start to fall even though the number of incidents continues to rise. Only towards the end of the simulation does the incident cost per month approach the baseline level. Even then the number of incidents is much higher than at the beginning of the simulation, with disruptions of daily routines much more likely.

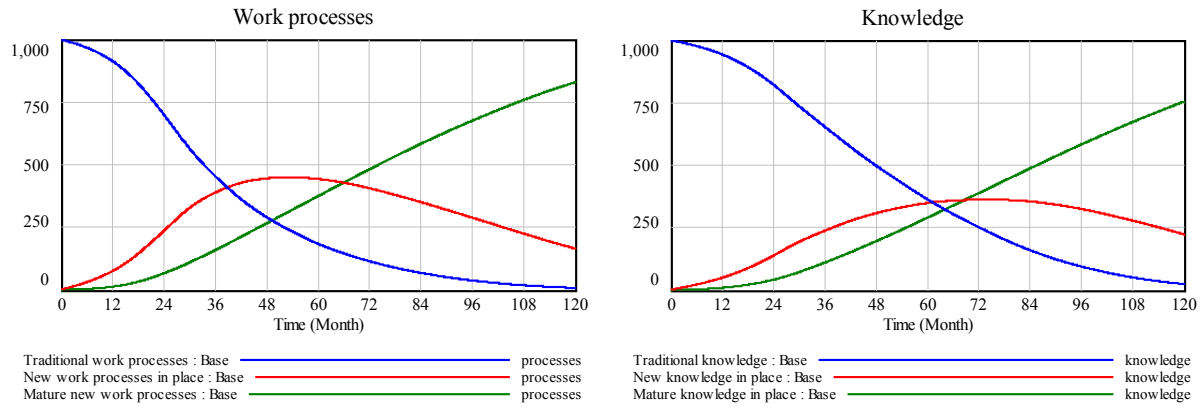

Figure 7 Base Run: Processes and Knowledge

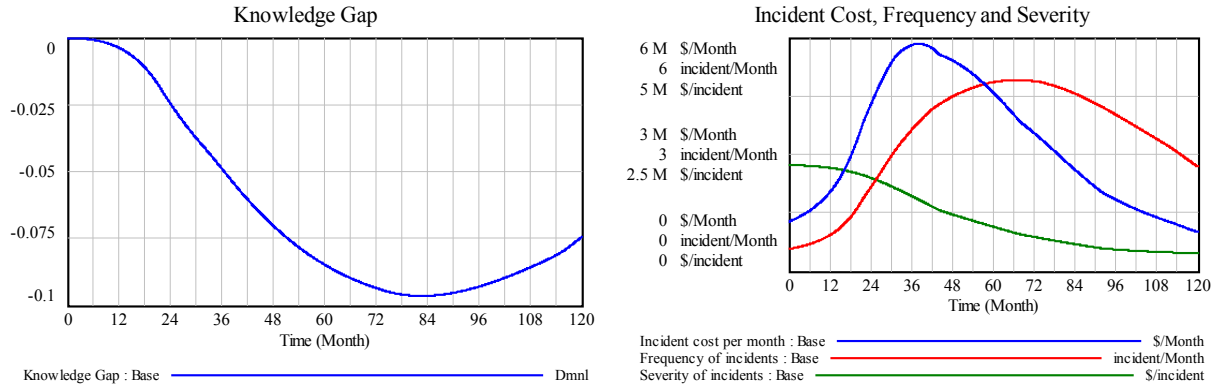

Figure 8 Base Run: Risk Dynamics

The presence of a knowledge gap is probably hard to establish in the field, as the gap might not be manifest until an incident occurs. In the absence of problems the operating risk is just a probability, not reality. The accumulation of multiple processes in flux adds to the size of the gap, and the increasing costs of change. A manager looking at the increasing costs of incidents in the first few years of the project might not recognize the "worse before better" scenario, and conclude that incident costs might continue to escalate indefinitely, putting the project's future in doubt.

Increasing efforts to integrate knowledge

Another simulation was executed with application of resources shifted towards the integration of knowledge. If risk is being driven by a knowledge gap, then applying resources to explicitly monitor and apply the field experience with new processes should reduce the costs and ongoing threats. To examine this scenario, the resources applied to knowledge integration were increased by 25%. These resources were drawn from staff that had originally been assigned to process integration.

The shift of resources towards knowledge integration results in an increase in mature knowledge, reaching 83% of the goal as compared to 75% in the base run. On the other hand, only 69% of the total processes reached maturity by the end of the run, as compared to 83% in the base run. This is a direct result of the "zero-sum" nature of the resource change – applying resources to knowledge integration will allow knowledge to mature faster, and removing resources from process integration will slow the transition of new processes (Figure 9).

The effects of this change on incidents are more telling. Shifting resources towards knowledge integration changes the knowledge gap from a deficit to a surplus: the staff are well-prepared for the ongoing process change (Figure

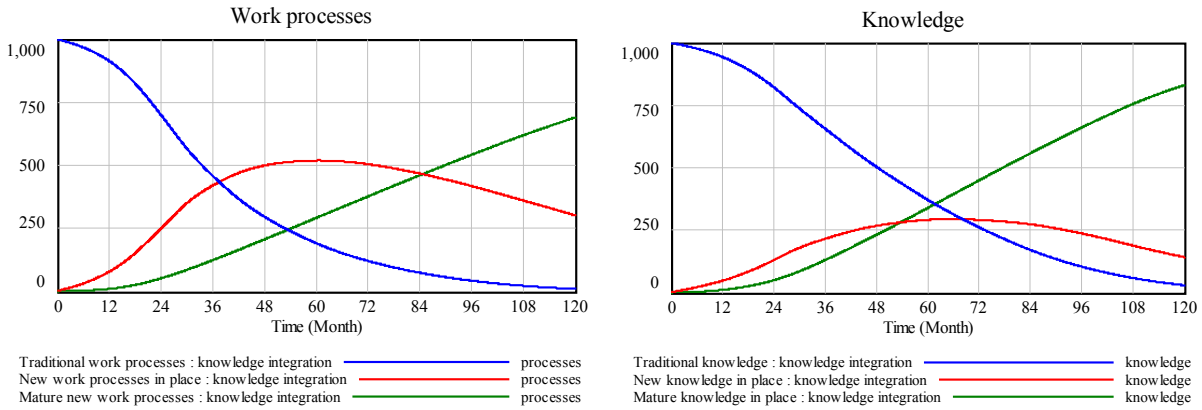

Figure 9 Increased Knowledge Integration Run: Work Processes and Knowledge

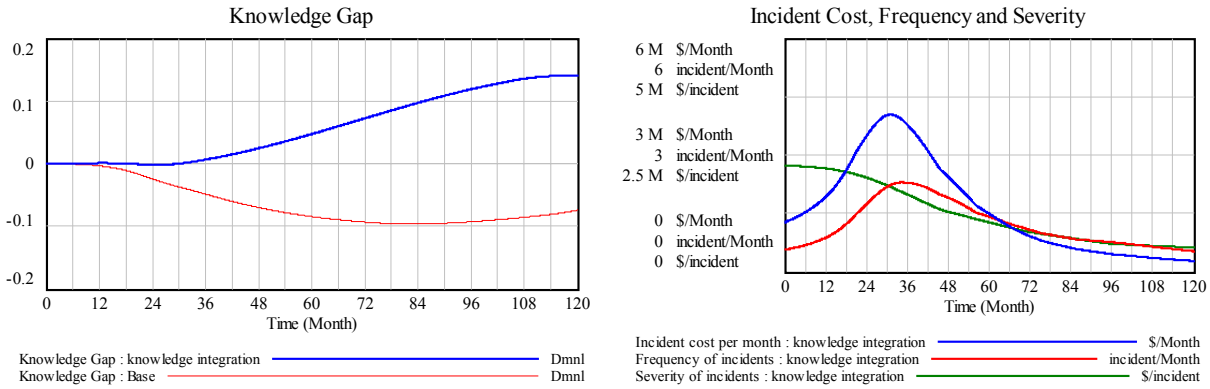

Figure 10 Increased Work Process Pressure Run: Risk Dynamics

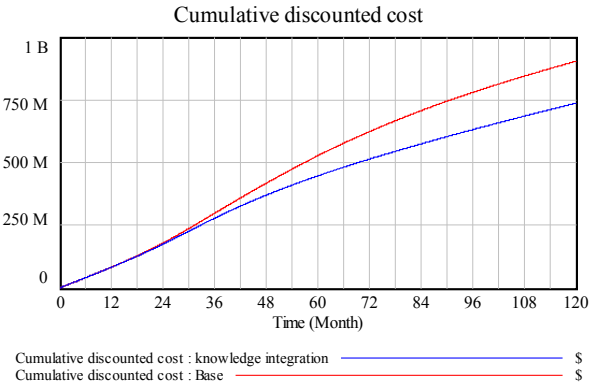

Figure 11 Cumulative Discounted Operating Costs

10, left graph). The frequency of incidents still increases during the first 36 months to about 2.3 / month, and then falls off. While incident costs still rise during the transition, they peak a bit sooner and reach only $4M / month as compared to $5.7M/Month around 36 months into the process.

Shifting resources to knowledge integration reduces operating costs, and the cumulative cost difference continues throughout the simulation (Figure 11). In these runs the resources available to enact change are constant, so that costs vary from the effects on the frequency and severity of incidents.

OBSERVATIONS AND FUTURE RESEARCH

While this work is still ongoing, the group model building process and the modeling activities provided insight into the problem of process transitions in high-risk environments.

- Group model building engaged and focused a diverse set of experts to develop a holistic, systems view of a problem. Through the feedback models, a wide set of interrelationships emerged that influence the success or failure of the e-Operations initiative was identified.
- Though little hard data was available, the participants' knowledge of the general structures and behaviors in their environment was sufficient for credible and understandable causal modeling. This is a crucial finding in high-threat environments, as little data is ever made available outside the secure environment of the firm.

The qualitative models identified several problematic areas in the transition, and the simulation models reinforced and expanded on several of them.

- Accumulating Risk. The simulation demonstrates how operational risks accumulate as multiple processes are developed and matured in parallel. In this model, the increased risk comes from the nature of transitions and learning, rather than a shift to an inherently riskier approach to business. If the firm was moving to a somewhat riskier operating model in the search for greater profit margins, the problem might well be exacerbated.
- Learning under fire or learning by design? Relying on field experience to refine and mature innovations can increase the costs and risks of transition. When learning support in the field is limited, the task of process and knowledge refinement becomes an exercise in fire-fighting. Learning occurs when problems occur. Providing explicit support for review and refinement of processes reduces the number of incidents, which in turn reduces the disruptive effects of change.
- Effects of change on staff. While the model does not explicitly address the effects of change load on turnover, it is not hard to imagine that a sharp increase in incidents might increase turnover and resistance to future changes. Both of these would slow the transition to new operating approaches.

Future plans for this model includes a detailed parameter review, endogenous adjustments of staffing levels, and addition of stochastic risks and events. In addition, explicit market dynamics for oil pricing may be useful as this model currently assumes a constant production and revenue stream throughout the period in question.

The simulation stimulates interesting questions about the dynamics of risk and operational transition. If a project manager sees that the cost of incidents is increasing, what might their reaction be? Would a re-thinking of the project be in order? Would resources might be shifted towards knowledge maturation and mitigation. or would the pressure to keep existing production online limit the ability of the organization to adapt? Often these questions arise during project post-mortems – where did we go wrong? Simulation permits the examination of issues critical to the success of change initiatives before the problems arise, as well as the development of critical indicators of success before the project becomes a problem.

REFERENCES

1. Andersen, D. F. and Richardson, G. P. (1997) Scripts for group model building, *System Dynamics Review,* **13,** pp. 107-129.
2. Luna-Reyes, L. F. and Andersen, D. L. (2003) Collecting and analyzing qualitative data for system dynamics: Methods and models, *System Dynamics Review,* **19,** pp. 271-296.
3. Randazzo, M. R., Keeney, M. M., Kowalski, E. F., Cappelli, D. M. and Moore, A. P. (2004), Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector**,** U.S. Secret Service and CERT Coordination Center / Software Engineering Institute, Pittsburgh, PA.
4. Rich, E. and Gonzalez, J. J. (2006) Maintaining Security and Safety in High-threat e-Operations Transitions In *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39)*Ed, Sprague, J., Ralph H.) IEEE Computer Society, Kauai, Hawaii.
5. Richardson, G. and Andersen, D. F. (1995) Teamwork in group model building, *System Dynamics Review,* **11,** pp. 113-138.
6. Richardson, G. and Pugh, A. (1981) *Introduction to system dynamics modeling with DYNAMO,* MIT Press, Cambridge, MA.
7. Sterman, J. D. (2000) *Business dynamics: Systems thinking and modeling for a complex world,* Irwin McGraw-Hill, Boston.
8. Vennix, J. A. M. (1996) *Group model building: Facilitating team learning using system dynamics,* John Wiley & Sons, Chicester.