

Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning

Eliot Rich
University at Albany, SUNY,
e.rich@albany.edu

Finn Olav Sveen
Agder University College,
Norway
finn.o.sveen@hia.no

Ying Qian
Agder University College,
Norway
ying.qian@hia.no

Stefanie A. Hillen
Agder University College,
Norway
stefanie.a.hillen@hia.no

Jaziar Radianti
Agder University College,
Norway
jaziar.radianti@hia.no

Jose J. Gonzalez
Agder University College,
Norway
jose.j.gonzalez@hia.no

Abstract

The implementation of Integrated Operations (IO) for oil and gas recovery – a real-time linkage among platform-based facilities, on-shore control centers and suppliers – is anticipated to reduce operating costs by 30%, extend the lifetime of current production fields by five years or longer and maintain Norwegian Continental Shelf production for 50-100 years. The changes in operating procedures require extensive training to ensure continued personal and environmental safety.

Vulnerabilities may emerge during the rollout of updated techniques and integration of IO technology with existing work practices. We focus on user knowledge as key to successful change. A system dynamics simulation is presented that defines work process and knowledge transition. Interviews and historical records assisted in parameterizing the model. The simulation suggests that great care should be taken to facilitate and monitor the rate of knowledge maturation, even in the face of expensive implementation delays, to reduce the risk of catastrophic failure from endemic incidents.¹

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, David F. Andersen and

1. Introduction

Integrated Operations (IO) in the Norwegian Continental Shelf – the use of advanced computer control and communications technology to optimize production and reduce costs is changing the Norwegian oil industry. In concert with the Norwegian Oil and Energy Ministry, the industry has started a 15-year transition to modernize and consolidate its oil and gas production resources. This effort may extend the productive life of the Norwegian Continental Shelf fields by as much as 50-100 years. Three enabling technologies, remote control of hardware, collaborative videoconferencing and real-time decision support, have been combined to link offshore teams and onshore expertise through high-capacity networks.

The redesign of work process and the redeployment of staff from offshore to onshore changes the nature of platform work and decision-making. Information that was not previously available to onshore experts is now readily accessible. Offshore teams now consult with onshore colleagues through real-time video and audio links. At the same time, there are some situational data that are difficult to capture, and the movement of staff off-platform reduces the skills available in the field, raising concerns about increased vulnerability to accidental or

George P. Richardson from the University at Albany, the collaborators in the Security Dynamics Network (<http://www.securitydynamics.org>) and our industry partners for their assistance.

intentional failures, possibly resulting in catastrophic outcomes, including loss of life.

This paper presents a simulation model of the effects of the multi-year transition of production tasks on vulnerability and risk. The simulation examines the effect of changes from an old to a new operating model on staff competence and platform vulnerability. The model demonstrates how ongoing change and disruption of established work processes can increase the vulnerability of the platform to failure, and the need to pay particular attention to how staff integrate their new process knowledge during the transition. The results from this model have stimulated new interest in the quality of communications and knowledge transfer that IO enables.

2. Background

2.1. Integrated Operations – a \$41,000,000,000 opportunity

Norway is the third largest producer of crude oil and gas in the world, generating the equivalent of 1.6 billion barrels in 2005. The estimated NPV of current and future exploration is 4.2 thousand billion NOK, or \$700 billion USD. The government has established the complete and prudent recovery of this important asset over a 50-100 year period as a policy goal. The controlled exploitation of Norway's oil and gas resource is considered crucial to the future of the country, as they form the basis of the country's largest industry [1, 2].

To realize this goal, the industry has defined Integrated Operations, a strategy to link the many vendors, suppliers, and operators working in the Norwegian Continental Shelf. IO has three major goals: first, maximize production from existing and new oil reserves; second, reduce operating costs, which are rising as fields mature; and third, preserve the health, safety and work environment for personnel in the field as well as the greater European community [1, 2].

Currently each offshore platform acts as an independent "factory" where on-platform personnel manage daily operations. A platform might generate \$2-30 million USD or more of oil and gas each day. Platform personnel are absolutely responsible for the safe operation of their machinery, yet have little access or information sharing with on-shore personnel or other platform operators in the face of malfunctioning equipment or of changes in production plans from onshore managers. In essence, each platform is an isolated island; all the skilled resources need to be on-

platform, at significant cost and some risk to personal safety.

This offshore-centric operation is quite expensive. As oil fields mature, the costs of raw production increase exponentially. Consequently, with current operating costs and technology, the bulk of a field's proven reserves have often stayed in the ground [3].

The IO strategy is a two-phased approach to reduce production costs while maintaining safety and security. The first phase is the development and implementation of remotely operated or monitored offshore platforms, using highly automated production and sensor equipment. High-speed fiber networks, and modern drilling equipment, and new control centers, are being put into play. In parallel, extensive redesign of work and procedures started in 2005, and will continue for the next 5-10 years.

The second phase is creating a virtual organization of platform operators and vendors that share resources, information and expertise across platforms. The strategy calls for the efficient exchange of slack production and monitoring capacity among platforms, use of outsourcing for flexible deployment, consistent data and process controls, as well as the aggressive deployment of new production technology [4].

This transition will allow a consolidation of skills and enable the cost-effective extraction of much of the remaining reserves. The value of the move to IO is staggering. OLF, the Norwegian Oil Industry Association, estimates that the program might generate an incremental 250 billion NOK (\$41 billion USD) of NPV if implemented immediately. Rather importantly, OLF also states that a three year delay in implementation would drastically reduce the value of the strategy to 94 billion NOK (\$16 billion USD) as changes in oil prices and use of current higher-cost production techniques reduce the value of near-term efforts [5]. There is therefore significant pressure to implement IO quickly.

The transition is difficult. Platform personnel and onshore staff have been quite active in the development and redesign of operating processes; this is an area where they have singular competence. In a recent paper, Johnsen et al. [4] noted that the transition to computer supported operations still has some major vulnerabilities. For example, these authors note that control room staff are not familiar with the particular risks associated with information technology, and that their skills in identifying potential computer-generated hazards (e.g., software bugs, viruses, intrusions) are limited. In turn, they also recognize that the information and communication technology teams do not always understand the demands of (near) real-time

production and support. There is a knowledge void that requires concerted communication and cooperation, something that may not be part of the existing operational culture. Filling this void will likely become more important as the operations move through the second, virtual organization, phase of the project.

2.2. Implementation Failure and Organizational Change

While a new concept in the offshore oil industry, IO is similar to Client / Server (C/S) and Enterprise Resource Planning (ERP) systems in many respects. C/S systems were characterized by the introduction of multiple levels of decentralized technology, and ERP systems added the additional complexity of tight coupling between computer systems and organizational performance. By looking at the history of these systems, we can recognize potential weaknesses in IO implementation proactively, and work to minimize their effects. IO also relies on a new technology paradigm, one that must be as reliable as possible in a difficult and changing operating environment. The introduction of remote control and information changes the nature of the work, the communications channels among key players, and distributes the responsibility

for ultimate successful operations to many more players.

Establishing consistent work processes across platforms requires examination and redesign of complex business processes, involving multiple organizations and roles. Moving expertise off platform changes work roles and patterns of communication among previously co-located employees. Extensive training and re-training in updated processes is needed to ensure the continued safety of operations as well as proper leverage of newly available expertise.

In addition, there is great financial pressure to initiate and continue the transition. While few systems implementations run over a 15-year span, the sensitivity of the financial gain to a rapid start-up puts great pressure on near-term success.

The clear parallel among IO, Client/Server and ERP identifies an opportunity to gather foresight into implementation challenges. Table 1 delineates some of the areas where researchers into these technologies have identified concerns. Duchessi and Chengalur-Smith's [6] survey of Client/Server implementations examined problems and obstacles as perceived by senior managers. The greatest concerns were an inadequate internal skill set, unanticipated extra costs, the support of multiple vendor products, continual troubleshooting, and performance degradation as the number of components increased. They found that many companies underestimate the cost of education, training and rollout of the technologies. In addition, re-engineering may disrupt established communication channels within an organization.

Scott and Vessey [7], in their study of failure and success in ERP implementations, provide another perspective. When contrasting successful and failed implementations, the authors find fault with pressure to implement the systems rapidly in the face of changes in requirements and interim obstacles, the absence of information sharing culture, and a lack of training resources, among other reasons, that moved projects towards failure even with solid commitment to the final outcome. They propose that with the presence of strong strategic leadership it is possible to weather tactical setbacks.

Umble et al. [8] concur strong commitment, project management, cost control, and technical support are crucial to ERP success, and that learning and communication were sensitive areas. They emphasize that special care must be taken to consider the effects of change on the organization. They add recommendations to ensure data accuracy, and the use

Table 1: C/S & ERP Implementation Concerns

Implementation Concerns	Duchessi et al. (1998) [C/S]	Scott et al. (2002) [ERP]	Umble et al. (2003) [ERP]
Senior Management Commitment	X	X	X
Unstable technical architecture	X		X
Inadequate planning / monitoring	X	X	X
Inadequate internal skills	X	X	X
Unanticipated extra costs	X	X	X
Multiple vendors	X		
Continual troubleshooting	X		X
Degradation with complexity	X		
Education, training and rollout	X	X	X
Communication Channel Disruption		X	X
Time Pressure		X	X
Data Accuracy			X
Absence of Performance Measures		X	X

of focused performance measures as a continual metric of success.

2.3. Applying the lessons of C/S and ERP to IO

The preceding review of C/S and ERP implementation concerns provides a starting point for looking at the future of IO. Managerial commitment to IO appears to be quite strong. The concept of a unified approach to exploiting the remaining resources is supported by legislation and government policy, as noted above, but also by the industry association and by individual oil companies. Most of the major players in the fields have already begun the transition to IO [3].

The technical architecture is also partially in place. Isolated fiber optic lines have been run among most of the platforms in the North Sea, with redundant linkages and capacity far exceeding planned demand [9]. On some platforms special rooms with sophisticated displays and dedicated conferencing facilities create an extended control space that gives instant and effortless access to onshore and off-shore participants [10]. The logical (but not physical) isolation of these networks reduces concerns about hacking and outside attacks. There is still concern about intentional or unintentional attacks from employees and vendors [11].

The remaining issues of change management and adaptation, present in the C/S and ERP implementation reviews, are likely to be quite important in IO. Our concern for this paper is the effects of the transition on the safety of operations and personnel. Unlike most C/S and ERP sites, oil platforms are extremely hazardous workplaces. A study of platform incidents shows that losses of production and injury occur fairly frequently, and that there is always a small but real chance of catastrophic failure, resulting in the loss of life and serious environmental damage [4]. The possibility that IO may introduce any change in the probability of failure is taken quite seriously. Most assessments in remote operations tend to focus on technical systems, excluding human issues [12]. But, as Reason stated: "the human factor plays the major part in both causing and preventing organizational accidents" [13, p. 61].

In addition, these systems are vulnerable to intentional or unintentional attack. These threats may come from external or internal agents. The motivation of these agents are also different, ranging from intended actions, such as challenge, game playing, financial gain, destruction of information and revenge, to unintended actions, such as unintentional errors caused by employees, programming errors and data entry errors [13]. Intentional and unintentional action

could have hazardous effects on the system. Therefore human factors can also become a source of vulnerability in the system, especially if they relate to the introduction of new work processes and new technology.

The desire for rapid deployment of technology is countered by concerns about the vulnerability of the platform. While it is possible to design new work processes fairly quickly, the testing, training, rollout, and revision of each process is expected to take many months. The complexity of platform operations does not permit a discrete cutover. Instead, the pilot implementation is expected to take most of a decade, with 20 different processes to be implemented during that time.

The role of events and incidents in IO. Along with routine activities in oil and gas production come *events*, unusual outcomes or potential disruptions of the status quo [14]. Minor events may occur several times a week, while major events are less frequent. Most events are identified and mitigated before they can disrupt work. Events that cause damage or otherwise proceed without interdiction are called *incidents*. The number of events that become incidents reflect the relative *vulnerability* of the platform, that is, presence of exploitable weaknesses [15]. As events are an ongoing side effect of production, and the platform's protection less than perfect, there is always some base level of vulnerability. Any change to the operating environment must be considered in terms of its effect on vulnerability, that is, how well the platform and onshore team can detect events before they become incidents.

Not all incidents are the same. Johnsen et al. [4] classify the *risk* of various incidents along two dimensions, frequency and consequence. In this paper we use the term *severity* to represent the financial magnitude of the consequence associated with an incident. Thus, there are incidents that may be frequent and not severe, or infrequent and severe, or other combinations. Johnsen et al. argue that organizations can use their classification scheme to direct resources towards redesign of processes that exhibit high risk, that is, high severity or frequency.

3. A Dynamic Model of the IO Transition

How can we evaluate the tradeoff between rapid deployment and emergent vulnerability of IO? In this section of the paper we present a model of this transition process. Through simulation we attempt to consider the dual role of learning and unlearning, with additional concerns about the time and efforts needed to both develop and internalize new processes.

To develop this simulation we use the techniques of System Dynamics. System Dynamics is a computer-aided approach to policy analysis and design that applies to problems arising in complex social, managerial, economic, or ecological systems [16-18]. System dynamics models rely on three sources of information: numerical data, the written database (reports, operations manuals, etc), and the expert knowledge of key participants in the system [17]. System dynamicists rely on all three sources, with particular attention paid to the expert knowledge of key participants. Through the use of available data and verbal descriptions provided by experts, the modeling process exposes new concepts and/or previously unknown but significant variables. System dynamics models are excellent tools to study problems that arise in closed-loop systems, such as safety systems, where conditions are converted into information that can be observed and acted upon in order to change the state of the system [19].

The process of combining numerical data, written data, and the knowledge of experts in mathematical form often identifies inconsistencies about how we think the system works. The model educates us by identifying these inconsistencies. As such, system dynamics models do not target numerical forecasts. Rather, system dynamics models are policy tools that examine the behavior of key variables over time.

The model definitions and structures described below were developed as part of a series of group modeling workshops conducted in 2005 with oil industry and incident security experts [20, 21]. The insights gained at the workshops were transferred to a formal system dynamics model by the research team. This model, described below, is the basis for simulation of the possible effects of the IO transition on platform risk and vulnerability.

3.1. Model Sectors

The model consists of four interconnected sectors, each of which is discussed below (Figure 1).

Work processes, Knowledge and Technology.

Each offshore platform relies on a series of routine operations to extract, monitor and control oil production, which we term the “Traditional” approach. As part of the preparation for Integration Operations, researchers at a pilot site identified twenty major processes, e.g., daily production optimization and maintenance, which require re-engineering under the new regime. These processes are quite complex, and the transition from the traditional approach to the integrated approach is taken with much caution and review to ensure the ongoing safety of the platform. Thus, it is appropriate to think about a process as a transition of maturity among three states: *Traditional Work Processes*, the pre-integration state, *Immature Work Processes*, where an integration-dependent process has been advanced but is being reviewed and modified in the field, and *Mature Work Processes*, where an integration-dependent process is stable and working at the desired level of production.

In parallel with process maturation is the development of new knowledge and skills needed to safely operate the platform. Again, this is modeled as a transition among three states, *Traditional Knowledge*, *Immature New Knowledge*, and *Mature Work Processes*. As platform teams are asked to implement a new process, the value of their knowledge of existing procedures and situations is critical to the success of the transition. At the same time, however, they do need to “unlearn” some of their accustomed approaches to problem detection and problem solving before they become fully comfortable with consulting onshore colleagues.

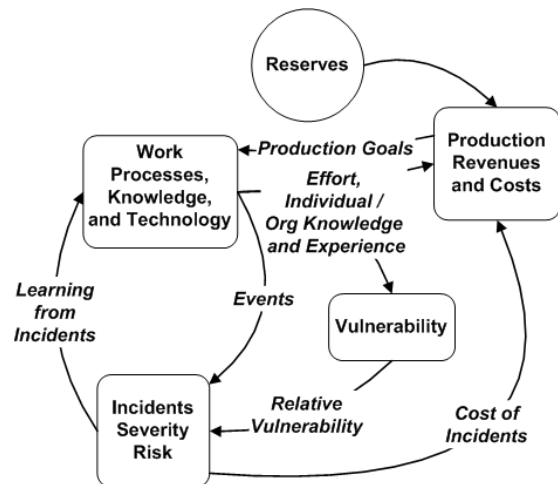


Figure 1: Sector Diagram

The experts at the group modeling sessions anticipated that the redesign and implementation of all twenty processes at the pilot site alone will take nearly 10 years, a long horizon for an IT implementation, but unremarkable for a major engineering project. In the case of the pilot site, creating new processes and identifying the requisite training is not nearly as time or resource intensive as maturation. Individual unlearning happens when dissonance and discomfort between previous experience and current reality exists [22]. At the organizational level, unlearning has been found to be quite challenging, as it may disrupt existing social structures [23]. In addition, the need to confront new processes and learning *in situ* rather than in a classroom slows change [24].

Incidents, Severity and Risk. This sector of the model includes the links between events, incidents and their outcomes. As defined earlier, incidents are unusual events, intentional or unintentional, that result in damage. Severity is the financial consequence of an incident, if the incident occurs. One of the results of incidents is pressure to improve work processes. Another is the individual and organizational learning gained from managing the incident and its outcomes. At the extremes, of course, catastrophic incidents are followed by major changes in process after some delay, while minor incidents often have little effect on work processes. Incident cost also feeds into the financial position of the firm.

Vulnerability. This sector establishes relationships about process knowledge and experience and the likelihood that an event may be mitigated. The production environment prior to IO has some level of vulnerability, even though current personnel are skilled and competent. The introduction of new processes and new knowledge reduces this competency and thereby increases the relative vulnerability of operations for some time until changes are assimilated and knowledge disseminated among work crews.

Production Revenues and Cost. In this sector falls the application of knowledge and skills to production. Here the pressure to meet plans creates pressure to change process and knowledge transition rates. As noted earlier, oil and gas reserves are becoming harder to extract, even with the advent of new technology, and this production sector is expected to be quite sensitive to market demand and changes in resource availability. This sector is not fully developed in the model at this time, as we focus here on risk and less on the economic viability of production.

3.2. Causal loops in process and knowledge transition

Identification of feedback structures is a crucial step in system dynamics analysis. For this paper we concentrate on the effects of feedback on the transition from traditional work processes to mature new work processes under IO and the development of the knowledge associated with this transition. Figure 2 shows some of the structure within the Work Processes, Knowledge and Technology sector. In this notation, rectangles are *stocks*, accumulations of material or information. Linking stocks are *flow* variables, which govern their rate of change. For example, at the bottom of the diagram, the rate *Developing New WP* (work processes) defines the speed at which *Traditional WP* moves to *Immature WP*. *Auxiliary* variables in the model represent other factors in the system. These auxiliaries affect rates, which in turn change stocks and the future values of the auxiliaries, closing feedback loops and the system. The signs at each arrowhead indicate the assumed polarity of the link, where “+” indicates that the variable at the arrowhead will respond to a change in the preceding variable by moving in the same direction, and an “-” sign indicates that the variables will change in opposite directions.

Over time, *Immature New WP* become *Mature New WP*. The transition rate is influenced by the resources available to support the transition and the productivity of transition. The transfer calculations are embedded in another section of the model, “transfer effectiveness”.² A similar structure is in place for knowledge transitions, with *Traditional Knowledge* developing into *Immature New Knowledge*, and in turn being integrated into *Mature New Knowledge*.

While this structure has many feedback loops, the most important loops concern the cumulative effect of change on the ability of the platform’s personnel to bring IO online: The first loop, B1 – Work Process Development, states that as *traditional work processes* are advanced to IO, it generates a *new initiatives burden* on staff; as this burden increases, the rate of knowledge transfer decreases, which slows the rate of subsequent work process development. This is an example of a balancing loop, where pressure to change is offset by the effort needed to enact the change.

² The complete simulation model, coded in Vensim 5.5c, is available from the first author on request.

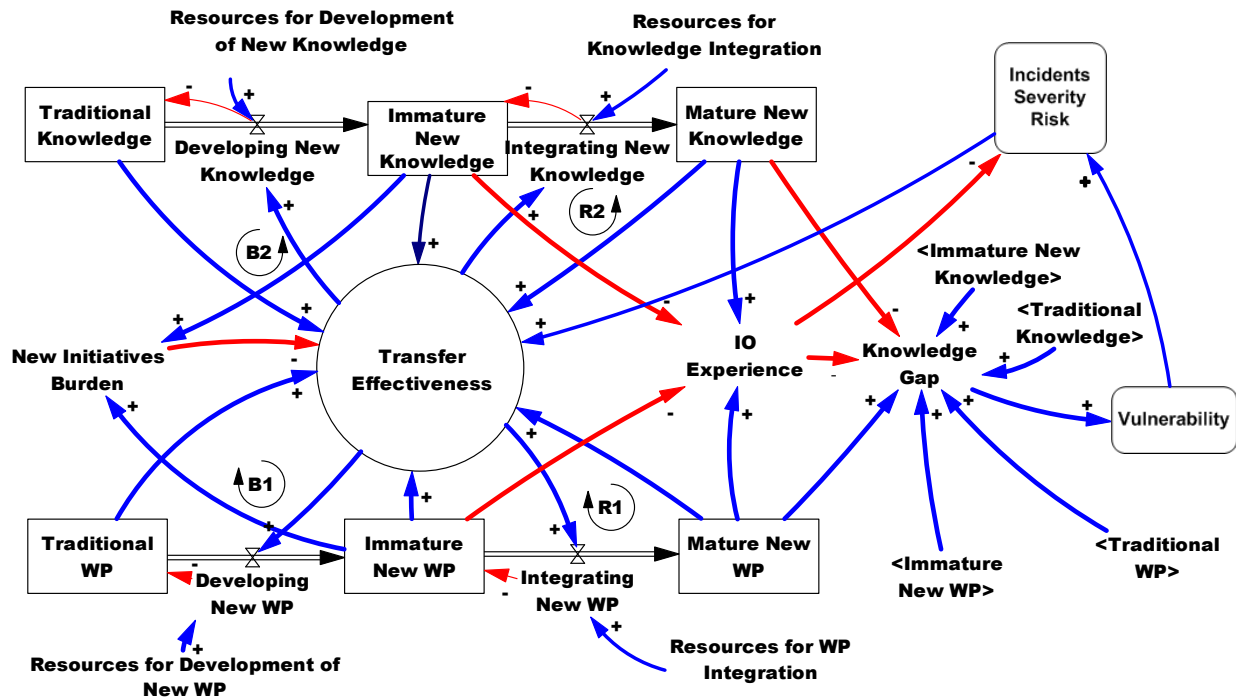


Figure 2. Work Process and Knowledge Stocks and Flows

The second loop, R1 – Work Process Integration, presents the concept that as processes mature, the rate of future process maturation will also increase. This is an example of a reinforcing loop, where an increase in the rate of integration accelerates the transition, assuming all other factors are equal. Through the same mechanism, a decrease in integration rate will also be reinforced,

The knowledge transition has two similar loops. Loop B2 depicts the effect of the development of new knowledge on the *new initiatives burden*, so that pressure to develop knowledge faster increases the *new initiatives burden*, and slows development. Loop R2 shows how an increase in the stock of *mature knowledge* increases the rate of integration, thereby reinforcing growth.

There are interesting interactions among these loops. An increase in efforts towards knowledge integration, for example, will indirectly affect knowledge development. This occurs because a reduction in immature knowledge reduces the *new initiatives burden*, which increases the effectiveness of knowledge transfer, and may accelerate the development of new knowledge.

The relationship between the implementation of IO and platform vulnerability spans several parts of the diagram. Based on the literature review and

discussions with the pilot team, it is expected that the introduction of new work processes and knowledge will have some disruptive effect on operations, which will resolve over time as more experience is gained with the new work techniques. The model includes a variable called *IO Experience*, which decreases as new processes and knowledge are developed, and increases with maturation.

There is no assumption that process development and integration proceeds at the same rate as knowledge development and integration. In fact, it is reasonable to expect that processes may be designed and advanced first, with knowledge changes trailing, as processes are field-tested. In this model, the difference between relative process and knowledge integration is called a *knowledge gap*. If processes are advanced faster than the knowledge needed to use them, a gap is created which in turn increases vulnerability. When an event occurs, the increase in vulnerability would make it more likely to turn into an incident. Incidents increase pressure to transfer knowledge and improve processes, which in turn affects vulnerability. This may increase or decrease the gap, depending on how the results of increased incident costs change the actions of decision-makers.

4. Dynamic Vulnerability Analysis

Development and integration of IO has multiple competing and reinforcing effects on platform vulnerability. To determine the relative strengths of these effects we implemented a simulation of the system. The simulation is based on the structures discussed above and several parametric assumptions, all derived from the group model building sessions and subsequent interviews with the pilot project team. The team plans to roll out the IO processes over 8-10 years, with 6 months needed to absorb and assimilate each change. For the costs of incidents historical data that looked at cost and frequency of incidents was obtained [4]. In addition, the authors assume that in a worst-case scenario with multiple failures the components of vulnerability may increase by as much as 600% during the transition, diminishing as experience is gained. This is a critical assumption, and one that requires extensive review in the future.

We use the model to explore the effects of incremental staff on the speed and safety of the transition. As noted earlier, a rapid implementation of IO represents a gain of many billions of dollars, but some unknown increase in vulnerability and incidents. We consider three alternatives.

- a **Base run**, (blue, line 1) where IO is virtually completed over 10 years,
- a **WP Development** run (red, line 2) policy where 50% more resources are applied to developing work processes than in the Base, all other values equal, and
- a **Knowledge Development** run (green, line 3), where 50% more resources are applied to developing new knowledge is emphasized.

Four metrics are used to evaluate the outcomes of the runs (Figure 3). The first two represent the progress towards completing IO. *Mature New Work Processes* and *Mature New Knowledge* indicate the number of IO processes and corresponding organizational knowledge in place over time. Each process is assumed to need one “knowledge unit” to be completely assimilated by the IO team. Fractional

units indicate partially accommodated processes or knowledge.

The third metric, *Knowledge Gap*, portrays the presence or absence of sufficient knowledge to manage a process with minimum vulnerability. A positive value means sufficient experience, and a negative value indicates insufficient experience, with corresponding changes in vulnerability. The fourth metric, *Incident cost per month* is the expected incident cost, rather than one driven by adverse events.

4.1. Base Run (blue, line 1)

In this run, equal resources are applied to both knowledge and work process development. The *Knowledge Gap* is zero, indicating that there is a balance between knowledge acquisition and the phasing in of new work process and knowledge development. *Incident cost per month* still increases slightly until about month 24 where the cost flattens out and eventually starts to fall because of a general improvement in severity through process review. At the end of the simulation the cost has decreased to approximately 5 million NOK/month from its initial value of 7.4 million, in large part because of anticipated safety improvements resulting from process changes in IO.

4.2. WP Development (red, line 2)

In this run, the attempt to speed the transition by adding resources to work process development has a major side effect. Work processes complete around month 84, 36 months earlier than the base, which would increase financial returns as discussed earlier in the paper. Pressure to develop work processes also generates a *Knowledge Gap*, which increases the vulnerability of the system, and incident cost. Incident costs start to rise about month 12, from about 7 million NOK/month to 11 million NOK/month. As knowledge development catches up with work processes, incident costs start to fall, becoming equal to the base around time 100.

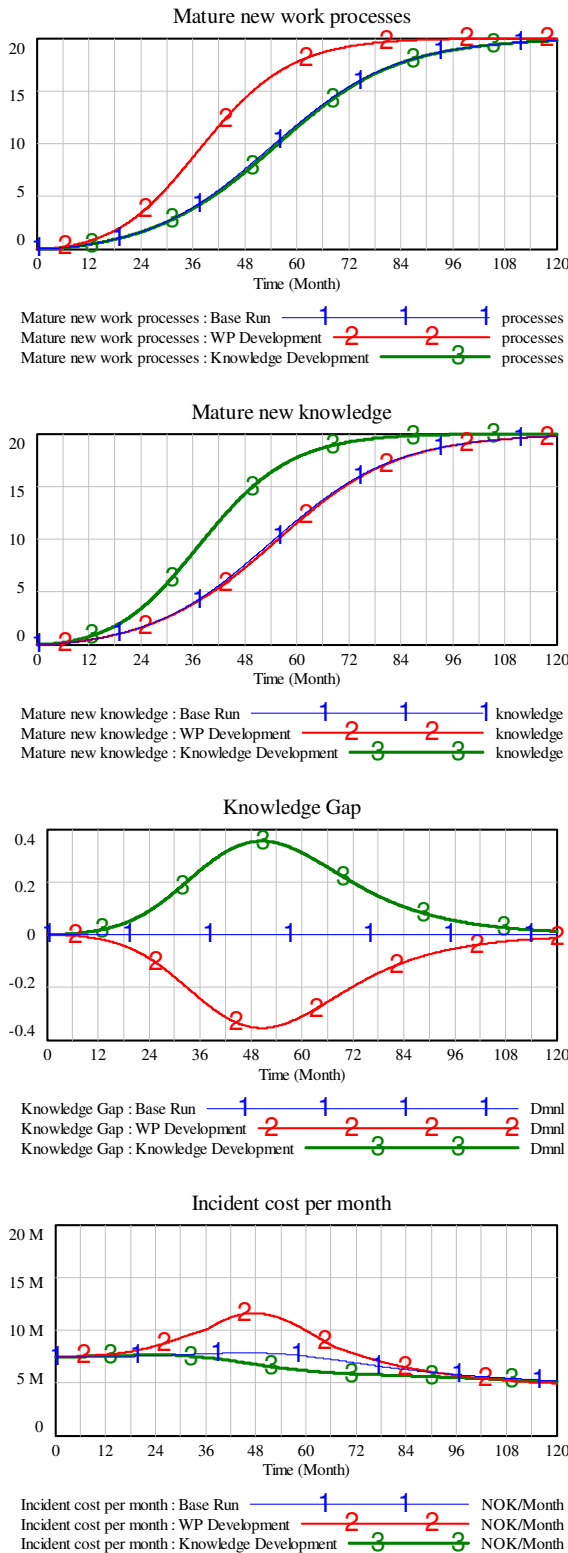


Figure 3. Simulation Results of IO

4.3. Knowledge Development (green, line 3)

As in the earlier cases, this run shows that work processes substantially complete within the 10-year timeframe. In addition, the new resources accelerate the integration and maturation of knowledge. This creates a knowledge surplus (depicted as a positive *Knowledge Gap*) that reduces vulnerability and incident costs somewhat during the critical transition at 36-84 months. This reduction in incident cost may be viewed as a safety margin to ensure successful completion of IO. By month 72 incident costs become consistent with the other runs.

5 Discussion and Conclusions

Based on existing research in C/S and ERP systems we theorized that moving projects forward faster than the knowledge needed to support them – a knowledge gap – creates vulnerabilities over time in IO transitions. Through a simulation model we quantify the potential risks associated with accelerating the transition to new work processes in an industry where costly incidents are endemic.

The results of the simulation show that the benefits of rapid development are offset by rapidly escalating vulnerability and incident costs, particularly in the first years. The dynamic theory centers on the effect of new initiatives on the competence of staff attempting to assimilate multiple immature changes. Efforts applied on ensuring knowledge development appear to be rewarded with fewer incidents attributable to the transition.

The import of this work is not in the numerical values of the runs. Rather, our results reinforce extant theory that hurrying an implementation can result in significant risks. The simulation model shows that risks are not linear – they first grow over time and later shrink, and an unprepared firm may find themselves with serious problems. In addition, the simulation identifies the asymmetric effect of resources change; adding resources to different parts of the system has different effects.

For the IO program, the findings argue for a careful investigation and review of the effectiveness of knowledge development during the rollout of this complex and expensive system. The problem may in fact be even more severe, as the model does not yet include secondary effects of a catastrophic incident on the future of IO and the exploitation of oil and gas in the Norwegian Continental Shelf. Future research is needed to examine how the effects of resources on process and knowledge integration affect the results.

A final comment about the methodology is important. The group modeling process used to develop the model has resulted in bilateral transfer of insight from experts to modelers and from modelers to experts – allowing the development of a low-cost model that can be simulated and allows to test different scenarios with potentially very costly consequences and to explain how unintended vulnerabilities and risks are caused as side-effect of managerial decisions.

References

- [1] Norwegian Ministry of Petroleum and Industry (Det kongelige Olje- og Energidepartementet), "Oil and gas activities," Oslo, Norway, White Paper. Unofficial English Translation available at <http://odin.dep.no/filarkiv/159874/Sreportno38.pdf> 38, 2002.
- [2] Norwegian Ministry of Petroleum and Industry (Det kongelige Olje- og Energidepartementet), "On the Petroleum Activity (Om Petroleumsvirksomheten)," Oslo, Norway, White Paper. Unofficial English Translation available at http://odin.dep.no/filarkiv/212963/Stmeld_38_2003-2004_Eng.pdf 38, 2004.
- [3] Norwegian Oil Industry Association (Oljeindustriens Landsforening - OLF), "Integrated Operations on the Norwegian Continental Shelf " accessed from <http://www.olf.no/?22894.pdf>, retrieved June 2, 2006.
- [4] S. O. Johnsen, M. B. Line, and A. Askildsen, "Towards more secure virtual organizations by implementing a common scheme for incident response management," presented at The Eighth International Conference on Probabilistic Safety Assessment and Management (PSAM8) May 14-18, 2006, New Orleans, US.
- [5] Norwegian Oil Industry Association (Oljeindustriens Landsforening - OLF), "Potential value of Integrated Operations on the Norwegian Shelf," 2006.
- [6] P. Duchessi and I. Chengular-Smith, "Client/Server Benefits, Problems, Best Practices," *Communications of the ACM*, vol. 41(5), pp. 87-94, 1998.
- [7] J. E. Scott and I. Vessey, "Managing risks in Enterprise System Implementations," *Communications of the ACM*, vol. 45(4), pp. 74-81, 2002.
- [8] E. J. Umble, R. R. Haft, and M. M. Umble, "Enterprise resource planning: Implementation procedures and critical success factors," *European Journal of Operational Research*, vol. 146(2), pp. 241-257, 2003.
- [9] Norwegian Ministry of Petroleum and Industry (Det kongelige Olje- og Energidepartementet), "Faktahefte om olje- og gassvirksomheten," accessed from <http://odin.dep.no/oed/english/doc/reports/026031-120028/dok-bn.html>, retrieved June 13, 2006.
- [10] Norsk Hydro, "Our Remote Control Works 100 Miles Away," accessed from http://www.hydro.com/en/press_room/features/rem_otecontrol.html, retrieved June 14, 2006.
- [11] P. Hocking, "Sikkerhetsutfordringer med Integrerte Operasjoner (Security Risks for Integrated Operations)," BP Oil, Unpublished presentation, 2005.
- [12] J. Henderson, Wright, K & Brazier, A., "Human factor aspects of remote operation in process plants," Health and Safety Information, Caerphilly 2002.
- [13] J. Reason, *Managing the Risks of Organizational Accidents*. Aldershot, Hants, UK: Ashgate Publishing Ltd, 2001.
- [14] C. Johnson, *Failure in Safety-Critical Systems: A Handbook of Incident and Accident Reporting*. Glasgow, Scotland: Glasgow University Press, 2003.
- [15] W. A. Arbaugh, W. L. Fithen, and J. McHugh, "Windows of Vulnerability: A Case Study Analysis," *IEEE Computer*, vol. 33(12), pp. 52-59, 2000.
- [16] G. Richardson and A. Pugh, *Introduction to system dynamics modeling with DYNAMO*. Cambridge, MA: MIT Press, 1981.
- [17] J. W. Forrester, *Industrial dynamics*. Cambridge, MA: MIT Press, 1961.
- [18] J. D. Sterman, *Business dynamics: Systems thinking and modeling for a complex world*. Boston: Irwin McGraw-Hill, 2000.
- [19] J. Rassmussen, "Risk management in a dynamic society: A modelling problem," *Safety Science*, vol. 27(2/3), pp. 183-213, 1997.
- [20] E. Rich, D. F. Andersen, and G. P. Richardson, "OLF-IRMA-AMBASEC Group Modeling Report II," University at Albany, Albany, NY, Technical Report 2006.
- [21] E. Rich, D. F. Andersen, and G. P. Richardson, "OLF-IRMA-AMBASEC Group Modeling Report I," University at Albany, Albany, NY, Technical Report 2006.
- [22] E. H. Schein, "How can organizations learn faster? The challenge of entering the green room," *Sloan Management Review*(Winter), pp. 85-92, 1993.
- [23] J. G. C. Navarro and B. R. Moya, "Business performance management and unlearning process," *Knowledge and Process Management*, vol. 12(3), pp. 161-170, 2005.
- [24] M. J. Tyre and E. von Hippel, "The Situated Nature of Adaptive Learning in Organizations," *Organization Science*, vol. 8(1), pp. 71-83, 1997.