A Dynamic Approach to Vulnerability and Risk Analysis of the Transition to eOperations

Finn Olav Sveen, Ying Qian, Stefanie Hillen, Jaziar Radianti, Jose J. Gonzalez,

Research Cell “Security and Quality in Organizations”, Faculty of Engineering and Science,
Agder University College, Serviceboks 509
NO-4898 Grimstad, Norway

Abstract. To reduce costs (by ca. 30%), increase production (by ca. 10%) and extend the life time (by ca. 5 years) of North Sea wells the Norwegian oil & gas industry is developing an infrastructure of "integrated operations" – i.e. eOperations from control centers with reduced personnel on offshore platforms. New technology, new work processes and new knowledge are needed. Increased reliance on information technology introduces risks, with components of threat, vulnerability, and impact depending on how the transition to eOperations is managed. Simulation models show that the risk behavior of the system depends sensitively on how resources for work process development and knowledge acquisition are deployed. Understanding such dynamics facilitates decision-making to minimize security (and safety) risks.

1 Introduction

The aim of eOperations (also known as Integrated Operations) in the Norwegian oil and gas industry to increase production by 10%, reduce costs by 30% and to extend the lifetime of mature fields through better utilization of drilling and production data, and closer collaboration between offshore and land-based personnel. Pilot projects seem to confirm these expectations. E.g. the Brage platform would normally have been closed down around 2005, twelve years after start of production. As Norsk Hydro’s pilot project for introduction of eOperations Brage is still profitable in its operational tail and it is expected to remain profitable until at least 2010. The NPV of the increased value facilitated by eOperations has been estimated as more than 40,000 billions of US dollars.[1]

eOperations is a process that began with a long-term scenario for the Norwegian continental shelf.[2] As to achieve a full integration of operations involving operators, suppliers, contractors, etc., the project evolves through two generations (integration of on- and offshore operations, ca. 2003-2010; integration of companies, ca. 2007-2015).

[1] See http://www.olf.no/english/news/?32101.pdf, quoted 24 May 2006.

[2] Described in Report no. 38 (http://www.dep.no/oed/norsk/publ/stmeld/028001-040009/index-dok000-b-n-a.html) to the Norwegian parliament.

From the point of view of information security, the transition over a long time span (10-12 years) from traditional offshore operations – drilling, production, delivery, etc, mostly locally operated at the offshore platforms – to eOperations, with increasing remote onshore operation, is an “engine” that generates vulnerabilities. In this context, vulnerabilities are weaknesses of the eOperations environment that facilitate unintended or intended incidents. An unintended incident could occur if an onshore operator – believing that the system is in test mode – inadvertently closes valves, thus causing an organizational accident and down-time. A mixture of an intended and unintended incident could be caused by a contractor who – under maintenance operations – connects to the eOperations’ intranet. The contractor might inadvertently introduce malware from his PC to the intranet – i.e. he might act as (super) Trojan Horse for all kinds of malicious agents. An intended incident could be a planned cyber attack, exploiting that an onshore operator is wireless-connected to the eOperations intranet (assuming that the wireless connection is a weak point of the system).

In addition to those risks, the countless software vulnerabilities (a.k.a. system vulnerabilities) in commercial-off-the-shelf (COTS) software are weak points for potentially disastrous attacks [1, p. 9]. In their paper, “Thirty Years Later: Lessons from the Multics Security Evaluation” [2], Karger and Schell argue that the decades-old Multics operating system (which was used in a relatively benign closed environment) is more secure than most operating systems of today: «Given the understanding of system vulnerabilities that existed nearly thirty years ago, today’s “security enhanced” or “trusted” systems would not be considered suitable for processing even in the benign closed environment. Also, considering the extent of network interconnectivity and the amount of commercial off-the-shelf (COTS) and other software without pedigree (e.g., libraries mined from the Web), today’s military and commercial environments would be considered very much “open.” …Thus, systems that are weaker than Multics are considered for use in environments in excess of what even Multics could deliver without restructuring around a security kernel.» eOperations is a (nearly) closed environment, but according to Karger and Schell, its reliance on COTS makes it insecure at the outset, even as detached environment. But then, the eOperations network is not a fully detached environment, since contractors and suppliers are allowed to connect; further weak points are its remote accessibility to authorized personnel via (still quite vulnerable) wireless connections.

Summarizing, the eOperations intranet is exposed to unintended human failures and it is vulnerable to malicious agents (insiders, combinations of insider/outsider, and outsiders with different motives – hackers, criminals, terrorists). Incidents can lead to down-time and they might even jeopardize safety.

Section 2 gives an overview of current literature within the field of risk management, risk analysis and vulnerabilities. Section 3 describes our approach to model risk in the transition to eOperations. Section 4 gives a more detailed description of the model and section 5 discusses the results from simulating the model. Section 6 rounds off the paper with discussion of the current state of the modeling effort and conclusions.

2 Literature review

The vulnerability problem in the network-based infrastructures has drawn the attention of many authors. Vulnerability is closely related to risk. Risk has been defined as something that creates hazard [3, p. 41], a source of danger, a possibility of incurring loss [4, p. 2]. In information security, risk is mostly considered a function of the level of threat, vulnerability and impact, i.e. the value of the asset [5, p. 8-9 and 186]. However, in highly segregated systems with defence in depth, as is the case for networks in eOperations, so far only a small fraction of the security incidents has been due to attacks: most incidents have been unintentional malfunctioning of the system because of software or hardware faults or due to human failure.

Methods for risk assessment and analysis have been developed for all kinds of systems. The references [3, 5] are recent authoritative treatments of risk management in computer systems. The role of risk analysis is to identify and assess important factors that may jeopardize the success of a project or achieving a goal.

Vulnerability is a state of *a missing or ineffectively administered safeguard or control* that allows a threat to occur with a greater impact or frequency, or both [3, p.14]. A vulnerability could be a *flaw or defect* in a technology or its deployment that might lead to exploits of a system [6, p. 54] by malicious agents, i.e. make it susceptible to attack [4, p. 2]. But a vulnerability might also mean a system weakness that, in unfavourable circumstances (e.g. in combination with other adverse factors), might lead to malfunctioning. The term “vulnerability” is also used to denominate the total or aggregate weakness of a system to failure, whether intentional or unintentional.

To recognize the real threat, traditionally a *risk assessment* is conducted, i.e. a computation of risk to determine threats to the project mission. It is also usual to perform a *vulnerability assessment*, a systematic examination of a critical infrastructure, the interconnected systems on which it relies, its information, or product, to determine the adequacy of security measures and identify security deficits [3, p.8]. The findings would lead to a cost benefit analysis and then to an implementation of security measures [3, p.41]. Since an incident often has a cost and can lead to productivity losses, the probability that an event becomes an incident is the main concern of risk and vulnerability analysis.

Threats may come from various agents such as 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 [7]. 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, as is the case in eOperations.

eOperations are closely related to the recent trend of “remote operations” in the process industry. A study examining eleven industries applying remote operations summarizes the incentives for adopting this method of operation [8]: *safety* (protecting personnel against fire, explosion and toxic materials); *cost* (use automated systems to reduce the number of people required to operate the plant) and *efficiency* (through centralising control). The study also identified potential problems of introducing the change to remote operations such as increased workload, difficulty in covering sickness and absence, stress, information overload for operators, additional skills to master a new system interface and less face to face communication. Most assessments in remote operations tend to focus on technical systems, excluding human issues [8]. But, as Reason stated: “the human factor plays the major part in both causing and preventing organizational accidents” [7, p. 61].

3 Dynamic Vulnerability and Risk Analysis

This work is an outcome of ongoing research on information security risks and the associated safety risks in the transition from traditional offshore-based operations to mainly onshore-based eOperations in Norwegian oil & gas companies. Two aligned, collaborating projects AMBASEC and IRMA,[3] sponsored by the Research Council of Norway, study a pilot case of the transition to eOperations provided by the Norwegian Oil Industry Association. The main objective of the projects concerns improvement of security culture and mitigation of risks in the transition to eOperations.

The IRMA project employs a traditional risk assessment, which depicts the frequency and the impact (in terms of cost) of each type of incident in one matrix. The risk matrix is input to an emergent incident management approach based on learning from incidents. Security key performance indicators will be used to monitor performance and guide management decisions. While this approach builds upon events that have been observed for the pilot case itself or in comparable setups, AMBASEC complements IRMA by determining endogenous factors that can cause so far unknown problems. Quoting the recent book on IT Governance by Calder and Watkins [9; p. 11]: «The speed with which methods of attack evolve, and knowledge about them proliferates, is such that it is completely pointless to take effective action only against specific, identified threats.» To include endogenously caused threats, we model the transition to eOperations using *system dynamics*. System dynamics deals with complex adaptive organizations, taking the philosophical position that dynamic behaviour is a consequence of system structure [10-13]. Translated to the topic of this paper, such tenet would suggest that a significant part of the inherent system vulnerability in the transition to eOperations is endogenous. During and after the transition to eOperations the frequency and consequence of incidents will change. For example, new technology is adopted to improve communication onshore and offshore, and, so it is intended, to reduce vulnerability. But, new technology is often immature in itself; people do not yet master it and errors could have security implications. The technological know-how gap actually generates additional vulnerabilities. This is an unintended consequence of the policy. Unintended consequences happen often and are common problems in dynamic systems with feedback [14].

[3] AMBASEC (A Model-Based Approach to Security Culture), grant 164384, is conducted at Agder University College by the Security and Quality in Organizations research cell. IRMA (Incident Response Management), grant 164372, is conducted by SINTEF, the applied research institute at the Norwegian University of Science and Technology (NTNU). Both projects run 2006-2008.

Group model-building workshops were held in Norway in May and September 2005 to capture expert knowledge about the pilot case and to develop a system dynamics model. A facilitation team of SUNY Albany led the sessions; this team has developed protocols for organizing and leading group model-building workshops [15-17]. Each workshop consisted of three stages: 1) developing agenda and scripts within the modeling team (2 days); 2) facilitated meetings with experts in the offshore oil industry (1 ½ - 2 days); 3) debriefing session (1 day). The target of the first workshop was knowledge capture, developing problem focus and consensus building; its outcome was a qualitative system dynamics map and a detailed report. After a follow-up period of analysis that identified some potential dynamic vulnerability patterns [18, 19], the second workshop promoted the emerging system dynamics model to a conceptual model of the pilot case. The model was based on transition from traditional operation to eOperations for work processes, knowledge and technology. Vulnerabilities and their associated risks are seen as an endogenous process tied to adequacy of new knowledge and technology in relation to the new work processes (i.e. eOperations). eOperations in the oil and gas industry is a novel approach with novel challenges and risks. Capturing the mental models of experts, and expressing them as a consensus model that can be simulated, allows predicting how operational risks relate to the main processes in the transition to eOperations. As knowledge grows, the model will be improved in further workshops with experts, in this way ensuring that it will reflect the best current understanding of the problem.

4 A Dynamic Model of Transitioning to eOperations

We base our discussion on the first version of the system dynamics model derived in the group model-building workshops.[4]

4.1 Model Sectors

The model consists of interconnected submodels (sectors): *Work Processes*, *Knowledge*, *Vulnerability* and *Incidents*. The *Incidents* submodel has three subsectors, *Frequency of Incidents*, *Severity of Incidents* and *Learning from Incidents* (Figure 1).

[4] More advanced versions exist (the SUNY Albany team has developed generic models while our team has extended the basic model in further meetings with the experts).

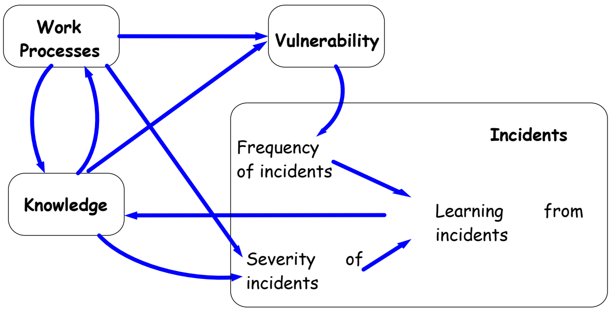


Figure 1 Four submodels and their interactions

Twenty work processes (such as daily production optimization and maintenance, weekly production optimization and maintenance, etc.) are changed in the transition from traditional operations to eOperations. We distinguish between three different stages: traditional, immature new and mature new work processes. A similar structure applies for knowledge (Figure 2).

Knowledge represents the total knowledge bank in the organization, including knowledge about work processes, knowledge about technology, etc. For simplicity we consider "technology" as an aspect of knowledge and aggregate these two aspects to one kind of "knowledge."

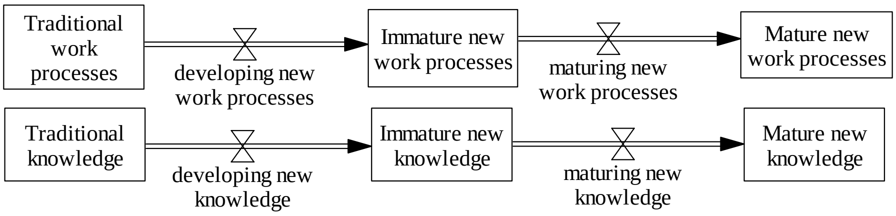

Traditional work processes
developing new work processes
Immature new work processes
maturing new work processes
Mature new work processes
Traditional knowledge
developing new knowledge
Immature new knowledge
maturing new knowledge
Mature new knowledge

Figure 2 The main structure in the work processes submodel and the knowledge submodel

Resources, measured in man hours, are needed to develop and mature both new work processes and new knowledge. The effectiveness of these resources depends on factors such as the organizational change load ("new initiatives burden") and experience of operation transition etc. Besides devoting resources, i.e. man hours, to develop and mature new knowledge, learning from incidents contributes to the maturation of knowledge.

The *Vulnerability* submodel's main function is to generate the '*Vulnerability Index'*, which is an aggregate measure for the system vulnerability. '*Vulnerability Index'* is influenced by immature new work processes, immature new knowledge and adequacy of mature new knowledge (mature new knowledge/mature new work processes). A more detailed explanation of the linkages will be presented in the next section.

There are three subsectors in the *Incidents* submodel. First, the *Vulnerability* sector impacts *Frequency of Incidents* – the higher *Vulnerability Index* is, the more incidents happen. This is a reasonable assumption since our model not only takes into account intentional attacks on the system, but also unintended incidents like operator error. Lack of experience, lack of training and unclear user interfaces and so on may lead to incidents. Second, the sector *Severity of Incidents* is influenced by mature new work processes and knowledge – the more mature new work processes and knowledge, the lower the severity of incidents. The next sector, *Learning from incidents,* is influenced by frequency of incidents, severity of incidents, and immature new knowledge. Learning from incidents can help immature new knowledge to mature, which will in turn reduce the frequency and severity of incidents.

4.2 Causal-loop diagram

The causal loop diagram in Figure 3 shows the most important feedback loops in the model. There are three main parts to the diagram, transition of work processes to the right, transition of knowledge to the left and the three variables in the middle, '*Severity*', '*Vulnerability*' and '*New Initiatives Burden*'. These three variables are shared by the sectors *Work Processes* and *Knowledge*. Transition of work processes and transition of knowledge from traditional to eOperations relate to the two model sectors *Work Processes* and *Knowledge* in Figure 1. '*Severity*' and '*Vulnerability*' relate to the model sectors *Incidents* and *Vulnerability*. '*New Initiatives Burden*' is the transition change load, i.e. unforeseen extra work caused by the transition.

The left hand side of the diagram describes the transition from traditional offshore work processes to eOperations work processes. Development moves work processes from *'Traditional WP'*[5] to *'Immature New WP'*. "Immature work processes" means that new routines exist, but that flaws have not yet been fully removed. As time passes and resources are spent to iron out the last creaks, the processes transition from *'Immature New WP'* to *'Mature New WP'*.

Similarly, the rightmost part of the diagram describes the knowledge transition. Development moves knowledge from *'Traditional Knowledge'* to '*Immature New Knowledge'*. As a deeper understanding is reached through experience and active learning, knowledge transitions to *'Mature New Knowledge'*.

[5] WP is short for work processes.

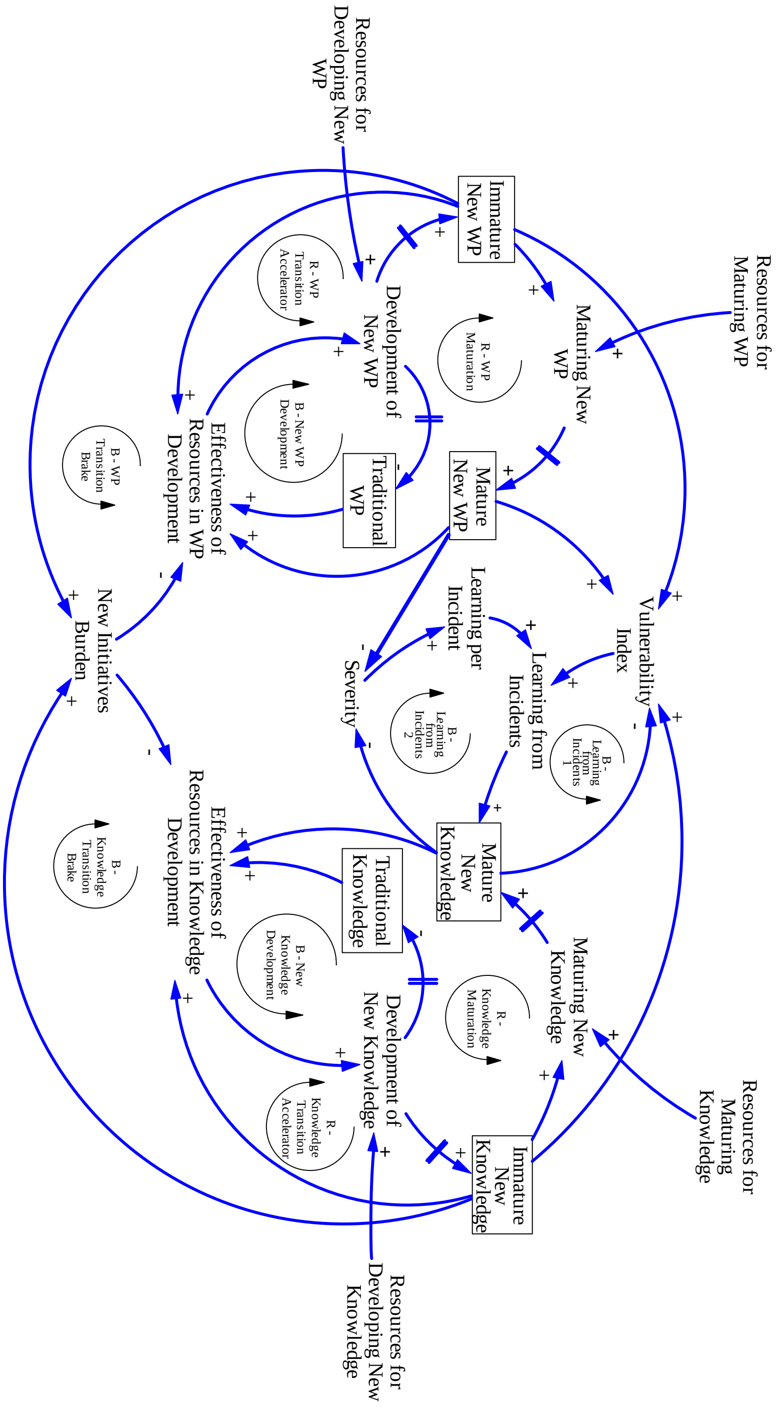

Resources for Developing New WP
Immature New WP
Resources for Maturing WP
Maturing New WP
R - WP Transition Accelerator
Development of New WP
R - WP Maturation
B - New WP Development
Mature New WP
Traditional WP
Effectiveness of Resources in WP Development
B - WP Transition Brake
Vulnerability Index
Learning per Incident
Learning from Incidents
B - Learning from Incidents 1
B - Learning from Incidents 2
Severity
New Initiatives Burden
Mature New Knowledge
Traditional Knowledge
Effectiveness of Resources in Knowledge Development
B - Knowledge Transition Brake
B - New Knowledge Development
Maturing New Knowledge
R - Knowledge Maturation
Development of New Knowledge
R - Knowledge Transition Accelerator
Immature New Knowledge
Resources for Maturing Knowledge
Resources for Developing New Knowledge

Figure 3 The main feedback loops in the model

4.2.1 Link Polarity and Time Delays

The links between the variables in Figure 3 denote causality. A link from A to B means that A causes a change in B. The + and – signs by the arrowheads denote polarity. A causal link from A to B has positive polarity if an increase (decrease) in A yields an increase (decrease) in B. A causal link from A to B has negative polarity if an increase (decrease) in A yields a decrease (increase) in B [11, p. 26].

The // marks are shown on several causal links. These marks denote a time delay. For example, the link from *'Effectiveness of Resources in WP Development'* to *'Development of New WP'* has these marks; showing that it takes time to develop and mature work processes.

4.2.2 B – WP Development

The causal link from *'Traditional WP'* to *'Effectiveness of Resources in WP Development'* has a + by the arrowhead, the polarity is positive. Methods used in traditional work processes can be used to develop new work processes. However, as the amount of traditional work processes declines and more new work processes come into place, fewer of the traditional methods can be utilized in the development of new work processes.

The link from *'Effectiveness of Resources in WP Development'* to *'Development of New WP'* has also positive polarity. The next causal link from *'Development of New WP'* to *'Traditional WP'* is negative. An increase in the development of new work processes leads to a decrease in the amount of traditional work processes in use. If there is a decrease in the development of new work processes, this will cause longer use of traditional work processes.

The three variables *'Traditional WP'*, *'Effectiveness of Resources in WP Development'* and *'Development of New WP'* form the feedback loop, *'B – WP Development'*. If *'Traditional WP'* increases, it will increase *'Effectiveness of Resources in WP Development'*, which increases *'Development of New WP'*. An increase in *'Development of New WP'* leads to a decrease in *'Traditional WP'*. As more work processes are transitioned, the speed of the transition will slow as a decrease in *'Traditional WP'* will lead to less *'Effectiveness of Resources in WP Development',* further causing a decrease in *'Development of New WP'*.

'Traditional WP' will eventually converge towards zero. The feedback loop is a balancing loop, it attempts to control and stabilize[6]. A balancing loop is denoted by a B in the causal loop diagram above.

4.2.3 R – Transition Accelerator

The causal link from *'Development of New WP'* to *'Immature New WP'* is positive with a following positive causal link to *'Effectiveness of Resources in WP Development'*. An increase in *'Development of New WP'* leads to more *'Immature New WP'* which then increases *'Effectiveness of Resources in WP Development'*, causing again an increase in *'Development of New WP'* . The three variables form a reinforcing feedback loop *'R –*

[6] A balancing feedback loop is sometimes called a negative feedback loop. See [3, p. 26-28] for more information.

WP Transition Accelerator'. A reinforcing feedback loop amplifies and destabilizes.[7] Such a loop is denoted by an R in the causal loop diagram above.

4.2.4 R – WP Maturation

An examination of the causal links in the feedback loop *R – WP Maturation'* reveals that the loop has a reinforcing effect. An increase in *'Mature New WP'* will eventually lead to a further increase in *'Mature New WP'*. A decrease in *'Mature New WP'* will eventually lead to a further decrease in *'Mature New WP'*. The impact of the loop on future work processes transitions is much delayed (two causal links are delayed).

4.2.5 B – WP Transition Brake

The balancing feedback loop *'B – WP Transition Brake'* is interesting because it not only affects the work processes transition, but also the knowledge transition. A growth of *'Immature New WP'* increases *'New Initiatives Burden'*. This has a negative effect on *'Effectiveness of Resources in WP Development'*, and in addition a negative effect on *'Effectiveness of Resources in Knowledge Development'*. Thus the effect is not limited to one part of the system, but it spreads over time to other sectors of the system.

4.2.6 Knowledge Transition & its impact on Severity & Vulnerability

The structure for the knowledge transition on the right side of the diagram is almost the same as for the structure for the work processes transition. The difference lies in how knowledge affects *'Severity'* and *'Vulnerability'*; and in how knowledge is affected by them.

'Severity' measures how costly a security incident is. (A more severe incident will cost more money.) Both *'Mature New WP'* and *'Mature New Knowledge'* affect '*Severity'*. In both cases the polarity is negative; an increase in *'Mature New Knowledge'* or *'Mature New WP'* will lead to a decrease in *'Severity'*. In turn, an increase in *'Severity'* causes *'Mature New Knowledge'* to increase. Thus *'Severity'* and '*Mature New Knowledge'* form the balancing feedback loop *'B – Learning From Incidents 2'*. When an incident occurs, precautions will be taken to ensure that it does not happen again.

'Vulnerability Index' is the fraction of security events that become incidents. The structure is similar to the structure for *'Severity,'* with some differences. The most important is that *'Mature New WP'* influences '*Vulnerability'* with positive polarity. If work processes are matured and put into place without the proper knowledge and technology to support them, mistakes will happen that will lead to an increase in vulnerability. In other words, an imbalance in *'Mature New Knowledge'* in relation to *'Mature New WP'* leads to a knowledge gap.

Since both '*Immature New Knowledge*' and '*Immature New WP*' can cause '*Vulnerability Index*' to increase, another potential problem is if work processes and knowledge are slowly or maybe never transitioned to the mature phase, but instead stay immature, leading to a long or permanent high vulnerability situation.

[7] A reinforcing feedback loop is sometimes called a positive feedback loop. See [3, p. 26-28] for more information.

5 Dynamic Vulnerability Analysis

The following section analyses three resource allocation policies that were simulated using Vensim System Dynamics simulation software: 1) A policy where an equal amount of resources have been assigned to developing new knowledge and new work processes (**Equal Resources**). 2) A policy where maturing new work processes gets one third more resources than developing new knowledge (**WP Maturation**). 3) A policy where maturing new knowledge gets one third more resources than developing new work processes (**Knowledge Maturation**).

5.1 Severity

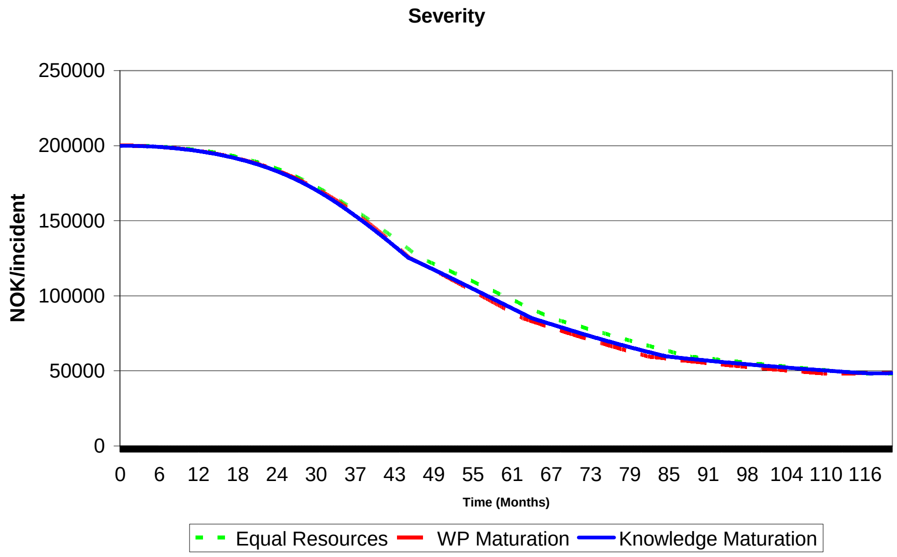


Figure 4 Severity

'Severity' has the same behavior pattern for all three policies. The *Equal Resources* policy has a slightly higher *'Severity'* than the other two policies, while the behavior for the two others is almost the same. To understand why the difference is so slight we must examine the model structure. Both *'Mature New WP'* and *'Mature New Knowledge'* influence *'Severity'*. The polarity is in both cases negative. This means that if *'Mature New Knowledge'* or *'Mature New WP'* increases, *'Severity'* will decrease. This is different from *'Vulnerability Index'* where only *'Mature New Knowledge'* actually decreases *'Vulnerability Index'*. Thus, maturing knowledge is important for reducing *'Vulnerability Index'*. But, from the point of view of *'Severity'* it does not matter whether knowledge or work processes are matured first: Both have a positive effect on reducing *'Severity'* and, thus, on the total cost of incidents.

5.2 Vulnerability Index

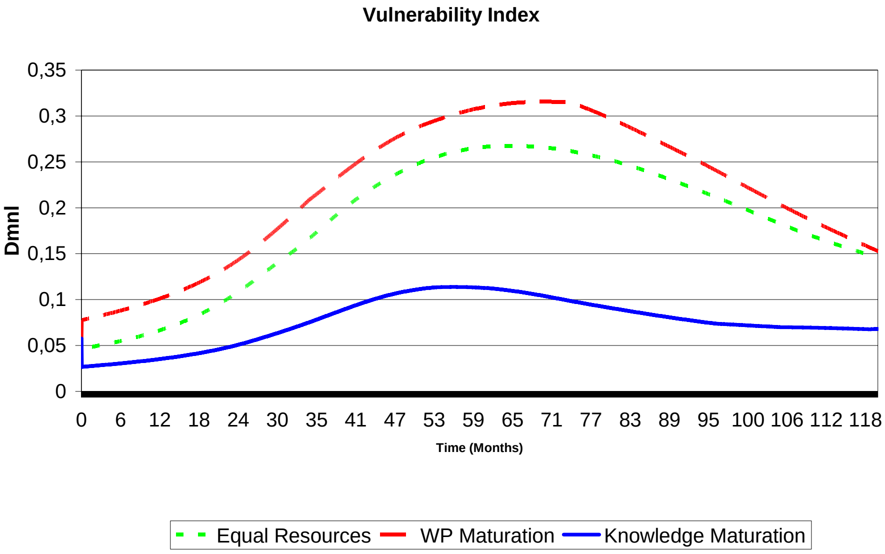


Figure 5 Vulnerability Index

The **Equal Resources** policy yields a marked increase in *'Vulnerability Index'*. The policy **WP Maturation** is even worse, whereas the policy **Knowledge Maturation** behaves much better. There is still an increase in *'Vulnerability Index'*, but the increase is substantially lower than in the other two policies.

5.2.1 Learning from Incidents

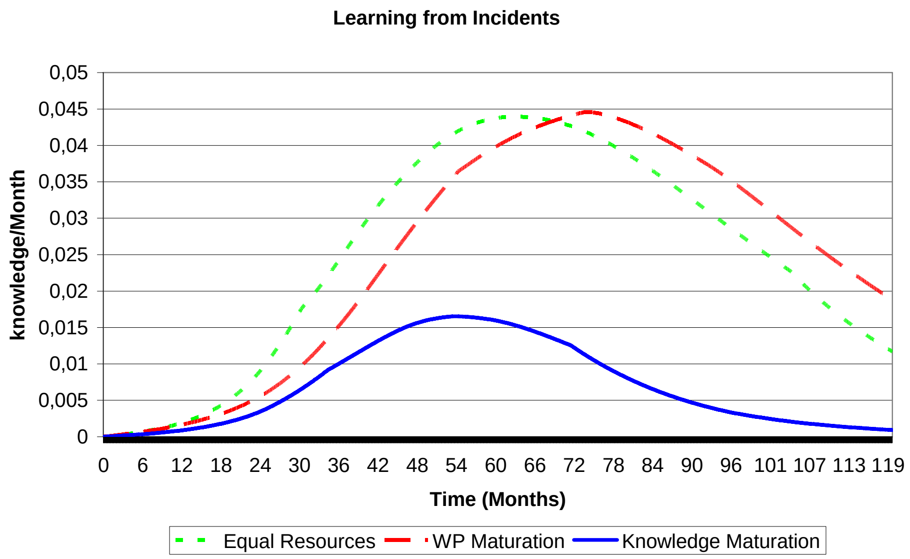


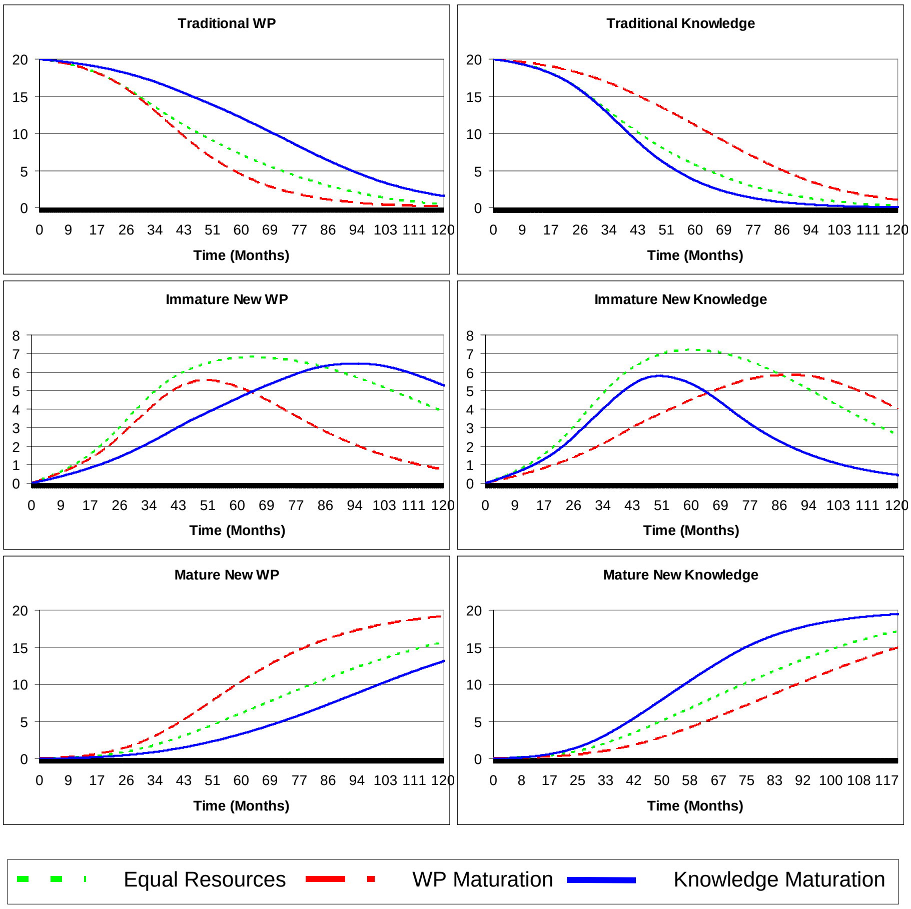
Figure 6 Learning from Incidents

Learning from Incidents is the result of the two loops: *'B – Learning from Incidents 1'* and *'B – Learning from Incidents 2'*. These feedback loops are weakest in the policy **Knowledge Maturation**, where *Learning from Incidents* is correspondingly low. This is the same policy that has the lowest *'Vulnerability Index'*. This suggests that *Learning from incidents* does not play a significant role in reducing vulnerability.

The policy **WP Maturation** has a similar behavior as **Equal Resources**. Both policies have approximately the same maximum values and the same area under the graph. This indicates that the two feedback loops *'B – Learning from Incidents 1 & 2'* have approximately the same strength in both policies. However, they become strong at different points in time. In the **Equal Resources** policy, *'Learning from incidents'* reaches a maximum at around 63 months, while in **WP Maturation, '***Learning from Incidents'* reaches its maximum at approximately 73 months.

5.2.2 Transition Speed

The work processes and knowledge transitions are major parts of the model and they both influence *'Vulnerability Index'*.



Work processes y axis has unit *processes* while Knowledge y axis has unit *knowledge*

Figure 7 WP & Knowledge Transition

5.2.2.1 Work Processes Transition – Equal Resources

At the start of the simulation the feedback loop *'B – New WP Development'* is the main driver behind the development of new work processes. Over time, development of new work processes leads to an accumulation of work processes in *'Immature New WP'*. As it increases, the feedback loop *'R – WP Transition Accelerator'* becomes stronger and the development of new work processes speeds up further. This happens around month 18 where *'Traditional WP'* drops more sharply and there is a corresponding increase in *'Immature New WP'*.

As work processes accumulate in *'Immature New WP'* they start maturing. The feedback loop *'R – WP Maturation'* grows stronger and becomes significant at month 36. At this time *'Immature New WP'* empties faster than it can be refilled. Remember that both *'Immature New WP'* and *'Mature New WP'* increase *'Effectiveness of Resources in WP Development'*, but *'Immature New WP'* also increases *'New Initiatives Burden'*. *'Ma-*

ture New WP' does not have this side effect. Maturing work processes makes the whole work process transition more efficient.

5.2.2.2 Work Processes Transition – WP Maturation

The **WP Maturation** policy behaves similarly as the **Equal Resources** policy. However, more assigned resources strengthen the loop *'R – WP Maturation'*, causing the work processes to transition faster from *'Immature New WP'* to *Mature New WP'*. For the initial 30 months the graph for *'Traditional WP'* is the same for both policies. After 30 months the **WP Maturation** policy empties *'Traditional WP'* faster.

5.2.2.3 Work Processes Transition – Knowledge Maturation

Although the **Knowledge Maturation** policy causes a similar behavior pattern as the other two policies, the transition is much slower. Reduced resources to the development of new work processes cause *'Effectiveness of Resources in WP Development'* to decrease, diminishing the strength of the feedback loop '*B – New WP Development*'.

5.2.2.4 Knowledge Transition – Equal Resources

The transition of knowledge shows a similar behavior as the transition of work processes. '*B – New Knowledge Development*' is the initial driving force for the development of new knowledge. When new knowledge has been developed, '*R – Knowledge Transition Accelerator*' speeds up the transition. '*R – Knowledge Maturation*' then accelerates the transition of the knowledge from '*Immature New Knowledge*' to '*Mature New Knowledge*'.

5.2.2.5 Knowledge Transition – Knowledge Maturation

In the policy **Knowledge Maturation** the knowledge maturation and the whole knowledge transition happen faster, since extra resources are being used to mature the knowledge. This behavior is opposite as for the work processes transition for the scenario **Knowledge Maturation**. The policy yields the lowest area under the graph for *'Immature New Knowledge'*. New knowledge does not stay immature for a long time, but it matures as quickly as possible. The same policy has a much slower maturation of immature work processes. This provides time to spread the knowledge around in the organization before new work processes are introduced and put into practice.

5.2.2.6 Knowledge Transition – WP Maturation

The knowledge transition is slower in the **WP Maturation** policy; this is natural, since resources have been removed from developing new knowledge. This behavior is opposite as for the work processes transition for the same policy. The maturation of work processes is faster than the maturation of knowledge. New work processes are introduced before the people involved have the necessary knowledge to handle them. This leads to an increase in the amount of security incidents.

5.2.2.7 Transition Speed and Vulnerability Index

The policy with the lowest *'Vulnerability Index'*, '**Knowledge Maturation**', is the one yielding the fastest transition from traditional knowledge to mature new knowledge and the slowest transition from traditional work processes to mature new work processes. Similarly, the policy with the highest *'Vulnerability Index'*, '**WP Maturation**' yields the slowest transition from traditional knowledge to mature new knowledge but it causes the fastest transition from traditional work processes to mature new work processes.

5.2.3 Adequacy of Mature New Knowledge

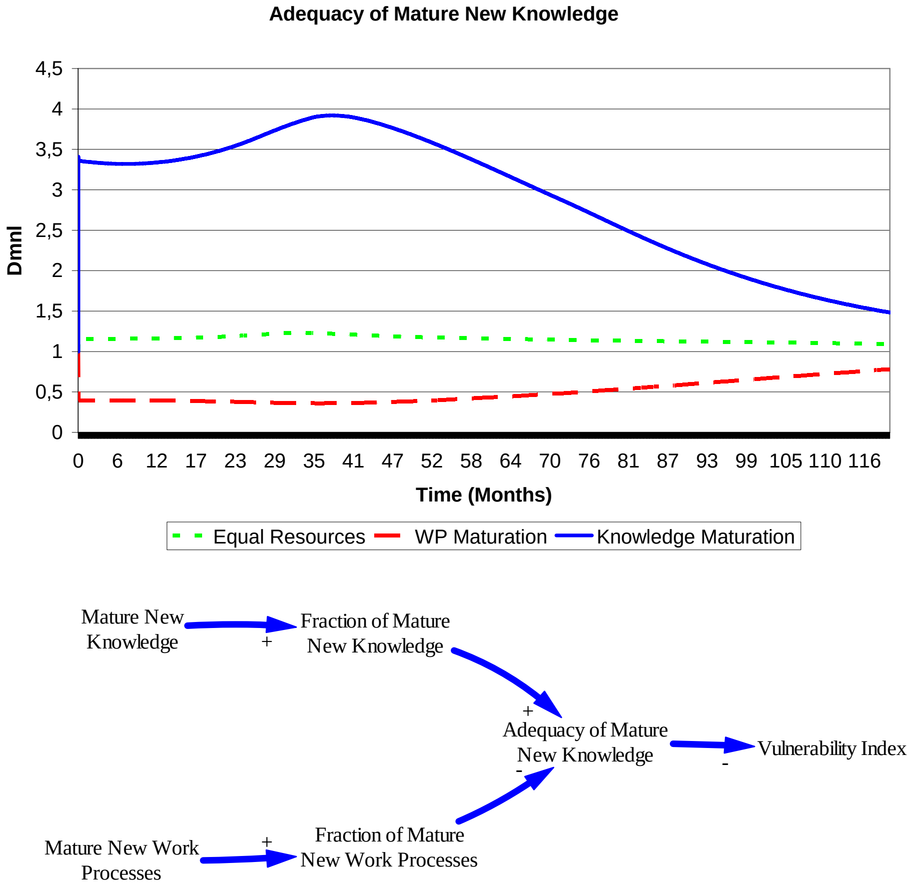


Figure 8 Adequacy of Mature New Knowledge

To understand why a fast knowledge transition combined with a slow work processes transition gives the lowest *'Vulnerability Index'* we must examine the interaction between *'Mature New Knowledge'* and *'Mature New WP'*. *'Adequacy of mature new knowledge'* is the fraction of mature new knowledge divided by the fraction of mature new work processes. *'Adequacy of mature new knowledge'* influences *'Vulnerability Index'*. An increase in adequacy decreases vulnerability.

If new work processes are developed and matured without the proper technology and without spreading the necessary knowledge to the relevant personnel, the level of knowledge in the organization will not be adequate enough to handle the transition and vulnerability will rise. This suggests that resources should be invested into increasing knowledge before new work processes are introduced. The simulation results suggest that such a proactive learning strategy is more effective than a reactive learning strategy in reducing vulnerability.

In the policy **Knowledge Maturation**, *'Adequacy of Mature New Knowledge'* has a hump at around 36 months. This is caused by more knowledge than work processes maturing. At 36 months the growth in knowledge maturation starts to decrease while the growth in work processes maturation starts to increase. The strong loop *'R – Knowledge Maturation'* becomes less powerful as there is less *'Immature New Knowledge'* to mature. *'R – WP Maturation'* is weaker up to 36 months, but as more *'Immature New WP'* becomes available for maturation, the loop becomes stronger. As the amount of *'Mature New WP'* approaches the amount of *'Mature New Knowledge'*, the *'Adequacy of mature new knowledge'* converges towards 1.

In the policies **Equal Resources** and **WP Maturation**, *'Adequacy of Mature New Knowledge'* also has a slight hump. However, it is much less pronounced and in the case of **WP Maturation**, the hump is a minimum rather than a maximum and the adequacy is constantly below unity. *'Adequacy of mature new knowledge'* becomes unity when the level of knowledge matches the level of work processes. When *'Adequacy of mature new knowledge'* is below zero, the knowledge in the organization is not enough to match the requirements of eOperations work processes and the vulnerability rises. The inverted humps are caused by the feedback loop *'R – WP Maturation'* initially being stronger than the feedback loop *'R – Knowledge Maturation'*.

5.3 Reactive vs. Proactive Learning

'Severity' behaves more or less the same in all three policies, leaving little room for improvement through new policies. The simulation results suggest that the greatest potential for reducing the monetary losses caused by incidents is by reducing the *'Vulnerability Index'*.

The policy with the highest *'Vulnerability Index'*, '**WP Maturation**', yields the fastest introduction of new work processes and the slowest introduction of new knowledge. Correspondingly, the policy with the lowest *'Vulnerability Index'*, '**Knowledge Maturation**', yields the slowest introduction of new work processes and the fastest introduction of new knowledge. This supports a policy of "thorough preparation". If one attempts to rush the new work processes into place, the consequences can be the more frequent occurrence of incidents. Although the company will learn from each incident, this learning occurs too late. There has to be a substantial amount of incidents for significant learning to occur, but incidents are expensive and should be avoided.

It can be compared to maintaining your car. If you do not regularly refill the oil, it may run just fine for years, but as time passes it becomes more and more likely that it will break down. If the engine breaks down for lack of oil, you learn that you have to refill the oil once in a while. This is reactive learning. You did learn; however it will still cost time and money to repair the engine. It is a rather expensive learning process. However, if you were a trained mechanic or even had just read the manual, you would have learned that the oil needed to be checked and regularly refilled. The engine repair costs and the time it took repair it would have been avoided. Similarly, security incidents can be avoided by acquiring and spreading the necessary knowledge throughout the organization, preempting incidents that occur because of ignorance or false beliefs. This is proactive learning and the model results suggest that it is much more effective than reactive learning in reducing security incidents. It is unrealistic to assume that all security incidents can be avoided by proactive learning. However, it is realistic to assume that proactive learning can significantly reduce the amount of security incidents. This is especially important in a high risk environment such as offshore oil & gas operations where incidents can be potentially disastrous for human life and the environment.

6 Discussion and Conclusions

Although the model still is a first cut to the problem, there is consensus among the problem-owners that the group model-building process has yielded encouraging results:

- One has gained significant insight gained even though data still is relatively sparse.
- One has achieved consensus on goals and managerial actions.
- One has succeeded in articulating structure and anticipated behaviors.
- The models allow examining effects of changes in staffing and other policies on vulnerability and risk.
- The model provides a mechanism for understanding possible effects of changes and decisions.
- The workshops and ensuing meetings have stimulated validation and discussion about concepts underlying the model.

But maybe the most important outcome is the process of 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.

The model will grow and will be improved as more data is accumulated and is communicated in further workshops involving experts and modelers. There are relatively few instances where information security for an empirical case can be studied in close collaboration between scientists (modelers) and problem-owners. This study seems to indicate that system dynamic models – by working with highly aggregated data – circumvent sensitivity issues that traditionally make collaboration between problem owners and scientists quite difficult.

7 References

1. Lipson, H.F. *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*. 2002 [cited March 27, 2004]]; Available from: http://www.cert.org/archive/pdf/02sr009.pdf.
2. Karger, P. and R. Schell. *Thirty Years Later: Lessons from the Multics Security Evaluation*. In *Eightteenth Annual Computer Security Applications Conference*. 2002. Las Vegas, Nevada.
3. Peltier, T.R., *Information Security Risk Analysis*. 2005, London: Auerbach Publications.
4. Wahlström, B. *Risk Assessment and Safety Engineering; Applications for Computer Systems*. In *The 24th International Conference on Computer Safety, Reliability and Security*. 2005. Fredrikstad, Norway.
5. Jones, A. and D. Ashenden, *Risk Management for Computer Security*. 2005, Oxford, UK: Elsevier Butterworth-Heinemann.
6. Arbaugh W.A., F., W.L and Hugh., J.M, *Windows of Vulnerability: A case Study Analysis.* Computer, 2000. **33**(12): p. 52-59.
7. Reason, J., *Managing the Risks of Organizational Accidents*. 2001, Aldershot, Hants, UK: Ashgate Publishing Ltd. c1997.
8. Henderson, J., Wright, K & Brazier, A., *Human factor aspects of remote operation in process plants*. 2002, Health and Safety Information: Caerphilly.
9. Calder, A. and S. Watkins, *IT Governance: A Manager's Guide to Data Security and BS 7799/ISO*. 2 ed. 2004, London: Kogan Page Ltd.
10. Forrester, J.W., *Industrial Dynamics*. 1961, Cambridge MA: Productivity Press.
11. Richardson, G.P. and A.L.P. III, *Introduction to System Dynamics Modeling*. 1981: Productivity Press, Portland, Oregon.
12. Sterman, J.D., *Business Dynamics: Systems Thinking and Modeling for a Complex World*. 2000, Boston: Irwin/McGraw-Hill.
13. Vennix, J.A.M., *Group model building: facilitating team learning using system dynamics*. 1996, Chichester; New York: J. Wiley.
14. Wolstenholme, E.F., *Towards the definition and use of a core set of archetypal structures in system dynamics.* System Dynamics Review, 2002. **19**(7): p. 7-26.
15. Andersen, D.F. and G.P. Richardson, *Scripts for Group Model Building.* System Dynamics Review, 1997. **13**(2): p. 107-129.
16. Luna-Reyes, L.F. and D.L. Andersen, *Collecting and Analyzing Qualitative Data for System Dynamics: Methods and Models.* System Dynamics Review, 2003. **19**(4): p. 271-296.
17. Richardson, G.P. and D.F. Andersen, *Teamwork in Group Model Building.* System Dynamics Review, 1995. **11**(2): p. 113-137.
18. Gonzalez, J.J., et al., *Helping Prevent Information Security Risks in the Transition to Integrated Operations.* Telektronikk, 2005. **101**(1): p. 29-37.
19. Rich, E. and J.J. Gonzalez. *Maintaining Security and Safety in High-threat E-operations Transitions*. In *Hawaii International Conference on System Sciences.* 2006. Hawaii.