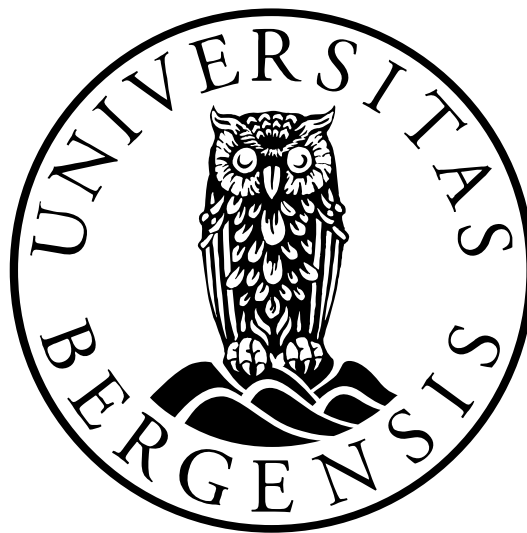


**Mitigating Information security risks during the
Transition to Integrated Operations:
Models & Data**

Ying Qian



Dissertation for the degree philosophiae doctor (PhD)
at the University of Bergen

Dissertation date: Apr 2010

Scientific Environment

This dissertation has been made in an environment consisting of several contributing organizations.

Part of the PhD education has taken place at the University of Bergen, Norway, at the Faculty of Social Science. More specifically, the candidate has been a member of the system Dynamics group at the Department of Geography.



This thesis work is embedded in the AMBASEC (A Model-Based Approach to Security Culture) project. The project team is in University of Agder in Grimstad, faculty of Engineering and Science. More specifically, the candidate has been a member of the research cell “Security and Quality in Organizations” that specialises in applying System Dynamics to research topics indicated by its name.

Norsk Hydro (later merged with Statoil) has been the main research object in this thesis. This organization has been the primary source for gathering empirical information, and its staff has contributed with knowledge, assistance, data and other types of support for the research presented in this thesis.

The IRMA (from Incident Response to Incident Management) project from SINTEF has been a collaboration party. The project team members have contributed with knowledge, assistance, data and other types of support for the research presented in this thesis.

Several other organisations have been involved in this research work through specific engagement for short period of time. These are mentioned in the acknowledgements that follow next.

ACKNOWLEDGEMENTS

Many people have contributed to the work presented in this dissertation. I would like to thank these individuals for their support.

My supervisors, Professor Jose J. Gonzalez, Pål I. Davidsen, and Eliot Rich have guided me throughout the research project. Professor Jose J. Gonzalez initiated this project and established collaboration with other institutions and business partners. Besides, he coached me on daily bases through most of my research. I am very grateful for all his time and effort invested in reviewing the many imperfect drafts of my work and the constructive critique offered. When I had my baby in 2007, he made the suggestion that I work from home. Thus, I can continue work on this research project while take care of my family. Professor Pål I. Davidsen has spent many hours with me discussing issues in this research project. He delivered many invaluable comments that helped to improve the content of the work. He has always been inspiring and encouraging. Eliot Rich came as one of the facilitators for group model-building workshop. Yet after that, he has been offering much supervision for model building, model testing, paper writing, and the others. He was always ready to have a netmeeting with me when I had questions. He was included as my formal supervisor in 2007.

My thanks also go to the group model-building facilitator team from University at Albany, State University of New York: David Andersen, George Richardson, and Eliot Rich. They carefully designed the workshops and successfully executed them, which provided me much information for model building. Moreover, they selflessly passed their experience and knowledge for group model building onto us. It has been a wonderful experience working with them.

This research project has had the benefit of many hours of discussions with the management term of our client, Norsk Hydro. Trond Lilleng, the leader of the Integrated Operations project, participated in the first group model-building workshop and the following ones. He had been positive to our research method and provided us further resources, including access to private data and relevant persons. Trond Ellefsen, the chief information security officer in Norsk Hydro, has provided us useful insights about the system structure. Bjørn Holst, the platform chief, provided us specific data about the Brage platform.

I had the pleasure to work with the IRMA team in this research project, including Odd Helge Longva, Stig O. Johnsen, Maria B. Line, Martin G. Jaatun and Inger Anne Taondel. They provided me with their insightful information about Integrated Operations and information security risks. Even after the formal collaboration ended, they were still willing to participate in my model validation interview in helping me validate my model. Their professional opinions added confidence to my model and their suggestions led to new policy analysis.

This doctoral research was financed by the Research Council of Norway. Most of the work was carried out at the Faculty of Engineering and Science, department of Information and Communication Technology at University of Agder. I am grateful to the staff at the faculty such as Gunnar Oftedahl, the director of the Faculty, who provided support for this research project, Anita Fosse who has helped me with all the administrative work, Maren Assev, our secretary, who was kind, caring, and helpful to my work and life, Gerd Lillian Andersen, our librarian, who helped with finding many literature sources.

It has been a fortune to be in the “Security and Quality in Organizations” research cell, where I met a collection of intelligent and hard-working researchers from all over the world: Stefanie Hillen, Felicjan Rydzak, Jaziar Radianti, Agata Sawicka, Johannes Wiik, and Finn Olav Sveen. We had many discussions that led to improvement of my work.

Many friends have helped me in this research. Special thanks to Yulin Fang, (former fellow student in system dynamics in University of Bergen, now assistant professor in City University in Hong Kong), for helping me to shape my ideas, suggesting relevant literature, and reviewing and improving my draft chapters. Most importantly, he has always showed great confidence in the work, which was a strong mental support to me in those difficult times. My long-time friend Xiaoqin Zhai, freely lent her home to me as my working place. This quiet and comfortable place saw me struggling with my thesis. Fang Chen (Ph.D. student in University of Agder), hosted me every time I visited Norway. Moreover, he has been reviewing my thesis as someone not familiar with system dynamics and provided many suggestions for improvement. To finalize my thesis, my husband Xin Fan, my friends Tuya Sun and Li Xu have helped to review and comment on my thesis. Their time and efforts have improved the quality of this thesis. To those friends who volunteered to participate in testing my model validation interview booklet: Xin Fan, Xiaoqin Zhai, Yueping Chen, Yulin Fang, Jing Yuan, Jie Chen, Yan Chen, Jaziar Radianti, and Finn Olav Sveen, I would like to say that your time and effort had helped me a lot.

Last, not least, my thanks go to all my family members. They have always been supportive, encouraging and patient. My parents and my parents-in-law helped me take care of my child while I needed to work. This work is dedicated to my husband Xin Fan, and our child Hai'ou Fan. Hai'ou grew up together with this thesis. She has been a source of happiness and given me many pleasant surprises during the difficult times. I love you all.

The cumulative contribution of all these people and many others over time has made this dissertation possible. My sincere thanks to all of you.

Abstract

This research studies the change of information security risks during the transition to Integrated Operations (an operation extensively utilize advanced information communication technology to connect offshore facilities and onshore control centers and even vendors.) in Norsk Hydro, a Norwegian oil and gas company. The specific case for this study is a pilot platform in transition to Integrated Operations, Brage: twenty traditional work processes are to be replaced by new work processes. The operators on the Brage platform have to build up relevant new knowledge to work effectively with new work processes. The new work processes, new knowledge and their interrelationship all affect information security risks. The management of Norsk Hydro is concerned with the problem of the increasing information security risks, which might cause incidents with severe consequences. We look for policies that support a successful (smooth and fast) operation transition.

System dynamics is adopted in this research to model the causal structure (mechanism) of the operation transition. We chose system dynamics because operation transition is a process rich in feedback, delays, nonlinearity and tradeoffs. All these features are captured by system dynamics models. Moreover, system dynamics models can be used to simulate various scenarios. The analyses of these scenarios can lead to insights on policy rules. We specifically investigate policies concerning transition speed, resource allocation during the transition to Integrated Operations and investment rules in incident response capability.

Since historical time series data about incidents and information security risks are scarce, we use following model-based interventions to elicit structural information from our client and experts:

May 2005	First group model-building workshop	Problem articulation
Sep 2005	Second group model-building workshop	Model conceptualization
Dec 2005	Model-based interview	Model formulation
Year 2006	Series of model-based meetings	Model refinement
Nov 2008	Model-based interview	Model validation

The Brage model was developed and validated through these model-based interventions. The analyses of various simulation results lead to the following policy insights:

1. Transition speed. The operation transition should be designed with a speed that allows the operators not only to get familiar with new work processes, but also to build up the detailed knowledge supporting these work processes. The relevance of such knowledge, which is mostly tacit, is sometimes underrated. If the operators only know what to do, but not how to do it effectively, the benefit of the new technology (embedded in the new work processes) will not be fully realized, and the platform will be more vulnerable to information security threats.
2. Resource allocation. Resources (operators' time) are needed to learn new work processes and to acquire related knowledge. Generally, the operators will first put their time into achieving the production target. Investment on learning activities will not be prioritized if these activities hinder reaching the production target, even if the operators know this short-term performance drop is the cost for obtaining long-term higher performance. Nevertheless strategic decision should never be influenced by operative goals and high level managements should be responsible to make decisions on whether focusing on long-term profits and accept short-term performance drop as a trade-off.
3. Investment in incident response capability. The management in Norsk Hydro is aware of the increasing information security risks changing from unconnected platforms to integrated ones. However, investment in incident response capability to handle increasing incidents is not made proactively. Only if the frequency of incidents has increased or severe incidents has occurred or the incident cost have been proved high, will the management decide to invest more on incident response capability. The Brage model simulations illustrate that these reactive decision rules will trap the management into ignoring the early signs of increasing information security risks, and cause underinvestment, which results in inadequate incident response capability, and subsequently leads to severe consequence. Proactive decision rules work effectively in reducing severity of incidents.

This work helps our client in two ways. First, the model-based communication helps the management in Norsk Hydro clarify the problem it is facing and understand the underlying mechanism causing the problem. There is an increased insight into the relevance of new knowledge acquisition. Second, the Brage model offers the management a tool to investigate the long-term operation results under different policies, thus, helping improve the management decision process.

This work contributes to the information security literature in three ways. First, previous research in information security is mostly on risk assessment methodology and information security management checklist. The dynamics of information security risks during the operation transition period has not been well studied before. In this fast changing society, this aspect of changing information security risks is of importance. Second, we introduce a dynamic view with the long-term perspective of information security. Although incidents happen in random manner, the underlying mechanism that leads to such incidents often exists for a period. Understanding such mechanism is the key to prevent incidents. Last, but not least, we demonstrate how formal modeling and simulation can facilitate the building of theories on information security management. Information security management involves not only “hard” aspects, such as work processes and technology, but also “soft” aspects, such as people’s awareness, people’s perception, and the cultural environment, - and all of which change over time. These soft aspects are sometimes the major factors affecting information security.

This work also contributes to the system dynamics literature by adding examples of how model-based interventions are used to identify problems, conceptualize and validate models. The activities of group model-building workshops and model validation interviews are carefully documented and reflected. It is an important step towards the accumulation of knowledge in model-based intervention.

Table of Contents

Scientific environment	i
ACKNOWLEDGEMENTS	ii
Abstract	v
Table of Contents	viii
List of Figures	xii
List of Tables	xii
1 Introduction	1
1.1 Research motivation	1
1.2 Case information	5
1.2.1 Integrated Operations in the Oil and Gas Industry	5
1.2.2 The Brage platform	12
1.3 Research Questions	13
1.4 Thesis structure	16
1.4.1 Background information	17
1.4.2 Methodology	17
1.4.3 Research activities and results	18
1.4.4 Conclusion	18
1.5 Closing Remarks for Chapter 1	19
2 Literature Review	20
2.1 Definitions of the Key Concepts	20
2.1.1 Information Security and Computer Security	21
2.1.2 Risk	22
2.1.3 Incident	23
2.1.4 Threat	24
2.1.5 Vulnerability	25
2.1.6 Computer Security Incident Response Team (CSIRT)	25
2.2 Research on Information Security	26
2.2.1 Managing Information Security: Technological Aspect	27
2.2.2 Managing Information Security: Human Aspect	29
2.2.3 Managing Information Security: Organizational Aspect	32
2.2.4 Information Security during Operation Transition	40
2.3 Closing Remarks for Chapter 2	40
3 Methodology	42
3.1 The characteristics of the case under study	42
3.1.1 Structural characteristics: Dynamic	43
3.1.2 Structural characteristics: Delays	44
3.1.3 Structural characteristics: Feedback	47
3.1.4 Structural characteristics: Nonlinearity	48
3.1.5 Behavioral characteristic: Counterintuitive	50
3.1.6 Behavior characteristic: Trade-offs	51

3.1.7 Other characteristics: Long-term perspective	52
3.1.8 Other characteristics: Multidisciplinary.....	52
3.1.9 Other characteristics: Lack of historical data.....	53
3.2 Research Design	57
3.3 Closing remarks for chapter 3.....	59
4 Group model-building workshops: models and data.....	61
4.1 Introduction to system dynamics group model-building workshops	61
4.2 First AMBASEC group model-building workshop.....	64
4.2.1 Purpose	65
4.2.2 Participants	65
4.2.3 Exercises and data obtained.....	66
4.2.4 Model development after workshop	89
4.3 Second AMBASEC group model-building workshop	91
4.3.1 Purpose	91
4.3.2 Participants	92
4.3.3 Exercises and data obtained.....	92
4.3.4 Model development after workshop	99
4.4 Following model-based interventions for model development.....	100
4.5 Closing remarks for chapter 4.....	101
5 Model of Brage's Transition to Integrated Operations	103
5.1 Model Overview	103
5.1.1 Model sectors.....	103
5.1.2 Concepts of work processes and knowledge.....	106
5.2 Major causal loop diagrams	111
5.2.1 Casual loop diagrams for operation transition.....	112
5.2.2 Causal loop diagram for incident response capability	114
5.2.3 Incident cost affect operation transition speed.....	116
5.3 Formal model description	117
5.3.1 Sector 1—Work processes	117
5.3.2 Sector 2—Knowledge.....	122
5.3.3 Sector 3—Vulnerability	125
5.3.4 Sector 4—Incident cost.....	129
5.3.5 Sector 5—Learning from incidents.....	132
5.3.6 Sector 6—Incident response capability.....	133
5.3.7 Sector 7—Production and profit	136
5.4 Model behavior	138
5.5 Closing remarks for chapter 5.....	147
6 Model Validation tests.....	148
6.1 Introduction to model validation.....	148
6.2 Direct structure tests	151
6.3 Structure-oriented behavior tests	156
6.4 Behavior tests.....	160
6.5 Closing remarks for chapter 6.....	161
7 Model Validation Interviews.....	162

7.1 Purpose of the Interviews.....	162
7.2 Interview design.....	163
7.2.1 The rational for using a structured interview	163
7.2.2 The interview booklet	164
7.2.3 Booklet testing	165
7.3 Interview Administration	166
7.3.1 Recruitment of subjects.....	166
7.3.2 The process of the interview	167
7.3.3 Data capture	168
7.4 Result of the model review interview	168
7.4.1 Interview results—scenario review.....	168
7.4.2 Interview results—closing questions	178
7.5 Closing remarks for chapter 7.....	180
8 Policies	181
8.1 Single Policy	181
8.1.1 Transition speed	182
8.1.2 Resource allocation during operation transition.....	190
8.1.3 Management policy on investment in incident response capability.....	195
8.2 Mixed Policy	210
8.3 Model extension.....	216
8.3.1 Extended causal loop diagram	216
8.3.2 Policies under the model extension.....	217
8.4 Closing remarks for chapter 8.....	220
9 Conclusion	222
9.1 Recapitulation of the research and its findings	222
9.1.1 Model development.....	222
9.1.2 Model insights.....	224
9.2 Research contribution	230
9.2.1 Contributions to the client.....	230
9.2.2 Contributions to information security management.....	231
9.2.3 Contributions to the field of system dynamics.....	232
9.3 Critique on the model-building process	234
9.4 Future research direction.....	236
9.4.1 Disaggregate the model.....	236
9.4.2 Extend the model	238
9.4.3 Link to the risk matrix developed by IRMA	239
9.5 Closing remarks for chapter 9.....	242
Reference	243
Appendix.....	249
Appendix I Model Equations	249
Appendix II List of look up functions.....	266
Appendix III Extreme Tests	275
Appendix IV Sensitivity tests.....	291
Appendix V Model validation interview booklet.....	318

Introduction.....	318
Section 1 Background information	319
Scenario 1 Base.....	323
Scenario 2 Focus on production.....	329
Scenario 3 Focus on knowledge	334
Scenario 4 Quicker to build IR capability.....	339
Scenario 5 Higher initial IR capability	344
Scenario 6 Delay transition.....	349
Closing questions.....	355

List of Figures

Figure 1-1 Number of security incidents reported to the CERT/CC from 1991 to 2003.	1
Figure 1-2 Root causes of information systems failures.	2
Figure 1-3 The AMBASEC Project Setting.....	5
Figure 1-4 Two generations of Integrated Work Processes	7
Figure 1-5 Traditional operation	9
Figure 1-6 Integrated Operations generation 1-Integration of on- and offshore operations.....	10
Figure 1-7 Integrated Operations generation 2-Integration of companies.....	10
Figure 1-8 Organization structure change	11
Figure 1-9 Efficient Operations in the Brage field.....	13
Figure 2-1 Basic behavior modes of compliance	31
Figure 2-2 Typical framework of risk assessment	34
Figure 3-1 New work processes transition.....	43
Figure 3-2 New knowledge transition.....	44
Figure 3-3 Delay	45
Figure 3-4 Examples of material delay and information delay	46
Figure 3-5 Subsystems interact through nonlinearity.....	50
Figure 3-6 Mental, written, and numerical database	56
Figure 3-7 Research plan	58
Figure 4-1 Stakeholder mapping	68
Figure 4-2 Variables behavior on a time graph.....	69
Figure 4-3 Variables related to the process of transition to Integrated Operations	70
Figure 4-4 Variables related to knowledge and vulnerability	71
Figure 4-5 Variables related to incidents	72
Figure 4-6 Policy lever mapping.....	74
Figure 4-7 Dynamic story 1—Virus Exposure in a Virtual Organization.....	76
Figure 4-8 Dynamic story 2—Suppliers as Trojan Horses	77
Figure 4-9 Illustration of operation transition.....	78
Figure 4-10 Reflection on the first dynamic story	79
Figure 4-11 Reflection on the second dynamic story.....	79
Figure 4-12 Stock-and-flow diagram.....	81
Figure 4-13 Concept model stage (a)	81
Figure 4-14 Concept model stage (b).....	82
Figure 4-15 Concept models stage (c).....	83
Figure 4-16 Backbones on the wall for model structure elicitation	84
Figure 4-17 Model structure elicitation finished.....	85
Figure 4-18 Two reinforcing loops emerged from the structure elicitation	86
Figure 4-19 The third reinforcing loop emerged from the structure elicitation	87
Figure 4-20 Dynamic hypothesis about incident response knowledge	87
Figure 4-21 Dynamic hypothesis about resistance to change	88
Figure 4-22 Problem articulation	88
Figure 4-23 Concept model.....	95

Figure 4-24 General model structure derived from the second workshop	98
Figure 4-25 The prototype model developed after the second workshop	99
Figure 4-26 Model formulation process.....	101
Figure 5-1 The Brage model overview	103
Figure 5-2 General model structure	104
Figure 5-3 Aging chains for operation transition.....	107
Figure 5-4 Timeline of the evolvement of operation transition	109
Figure 5-5 Causal loop diagram for the transition to Integrated Operations.....	112
Figure 5-6 Causal loops for incident response capability	114
Figure 5-7 Causal loops from incident cost to operation transition speed	116
Figure 5-8 Work processes transition	118
Figure 5-9 Knowledge transition	123
Figure 5-10 Vulnerability Index	126
Figure 5-11 Effect of immature new WP on the vulnerability index.....	128
Figure 5-12 Effect of immature new knowledge on the vulnerability index	128
Figure 5-13 Effect of mature knowledge adequacy on the vulnerability index	128
Figure 5-14 Incident cost	129
Figure 5-15 Effect of new work processes on events.....	130
Figure 5-16 Learning from incidents	132
Figure 5-17 Incident response capability	134
Figure 5-18 The effect of adequacy of incident response capability on incident detected	135
Figure 5-19 Production and profit.....	136
Figure 5-20 Work processes transition	139
Figure 5-21 Knowledge transition	140
Figure 5-22 The operators resources to mature new work processes and knowledge	141
Figure 5-23 The Vulnerability Index	142
Figure 5-24 Knowledge gap.....	142
Figure 5-25 Frequency of incidents, Severity of incidents, and Expected incident cost.....	143
Figure 5-26 Adequacy of incident response capability	144
Figure 5-27 Incident response capability, incident detected, and frequency of incidents.....	145
Figure 5-28 Profit, revenue, and product cost and expenditure	146
Figure 6-1 System dynamics model validation.....	150
Figure 8-1 Experts opinion on the new work processes implementation.....	182
Figure 8-2 Simulation results for different transition speed policies	184
Figure 8-3 Simulation results of different resources allocation policies.....	192
Figure 8-4 Mature new work processes and knowledge and frequency of incidents resulting from a reactive vs. a proactive investment policy	197
Figure 8-5 Severity of incidents and Incident response capability resulting from a reactive vs. a proactive investment policy.....	198
Figure 8-6 Incident detected resulting from a reactive vs. a proactive investment policy.	199
Figure 8-7 Structure adjustment for severity based policy	201
Figure 8-8 Mature new work processes and knowledge and frequency of incidents resulting from policies on severity of incidents	203

Figure 8-9 Severity of incidents and incident response capability resulting from policies on severity of incidents	204
Figure 8-10 Structure adjustment for cost based policy.....	207
Figure 8-11 Mature new work processes and knowledge and frequency of incidents resulting from policies on incident cost	208
Figure 8-12 Incident cost, Severity of incidents and incident response capability resulting from policies on incident cost	209
Figure 8-13 Simulation results for mixed policy.....	213
Figure 8-14 Causal loop diagram of feedback from a major incident.....	216
Figure 8-15 Simulation results for extended model	218
Figure 9-1 Transition speed	225
Figure 9-2 Net Benefit from group model-building workshop	227
Figure 9-3 Disaggregate work processes and knowledge	237
Figure 9-4 Expectation has an impact on the effectiveness of using new technology	239
Figure 9-5 Link risk matrix in the Brage model.....	240
Figure 9-6 Sample future risk matrix	241

List of Tables

Table 1-1 Benefits from integrated operations.....	8
Table 1-2 Modeling process.....	18
Table 2-1 Likelihood definitions.....	35
Table 2-2 Magnitude of Impact Definitions.....	36
Table 2-3 Risk-level matrix	36
Table 3-1 Modeling process.....	54
Table 4-1 Five different roles in group model building	63
Table 4-2 Group model-building exercises	64
Table 4-3 Key variables and their behaviors over time	69
Table 4-4 Five archetypes identified.....	89
Table 4-5 Risk matrix from IRMA	94
Table 4-6 Ideas of work processes development timeframe	97
Table 4-7 Overview of the two group model-building workshops	102
Table 5-1 Work processes and knowledge.....	107
Table 5-2 The effects on the vulnerability index	127
Table 6-1 Comparison of causal and correlational models	148
Table 6-2 Direct structure tests	151
Table 6-3 Model constants	152
Table 6-4 Initial value of stocks.....	154
Table 6-5 Model boundary.....	156
Table 6-6 Structure-oriented behavior test.....	157
Table 6-7 List of Extreme tests performed	157
Table 6-8 List of sensitivity tests performed.....	159
Table 7-1 The objectives of using interviews during model development	163
Table 7-2 Volunteers who participated in the interview booklet testing.....	165
Table 7-3 Base Run.....	169
Table 7-4 Focus on production	171
Table 7-5 Focus on knowledge	173
Table 7-6 Quicker to build IR.....	174
Table 7-7 Higher initial risk awareness	176
Table 7-8 Delay transition.....	177
Table 7-9 Closing questions.....	179
Table 8-1 Transition speed policies	182
Table 8-2 Resource allocation policies	190
Table 8-3 Response capability investment policies:	196
Table 8-4 Policy combination set-up	212
Table 8-5 Policy settings for extended Brage model	217

1 Introduction

This chapter consists of four sections. It starts with a discussion of our research motivation: information security risks are becoming more important with the wide use of computer and Internet. Research for this problem from organizational view is in need. In the second section, we introduce the problem domain: in the context of the transition to Integrated Operation (also called “operation transition” in the following) in a Norwegian oil and gas Company, Norsk Hydro (the short form “Hydro” is used in the following). In the third section, we present our research questions with a brief explanation about them, while in the fourth section we provide an overview of the thesis structure.

1.1 Research motivation

Today, computer and the Internet have penetrated most organizations and normal households, changing the way we live, work, and play. At the same time, we are facing increasing threats from information security risks. Figure 1-1 shows the fast growth of number of security incidents reported to the Computer Emergency Response Team Coordination Center (CERT/CC). A security incident, also referred as incident or information security incident in this document, is defined as an occurrence that actually or potentially jeopardizes an information system or the information in the system (NIST 2006). Detailed information on the definition of security incidents is provided in Section 2.2.3.

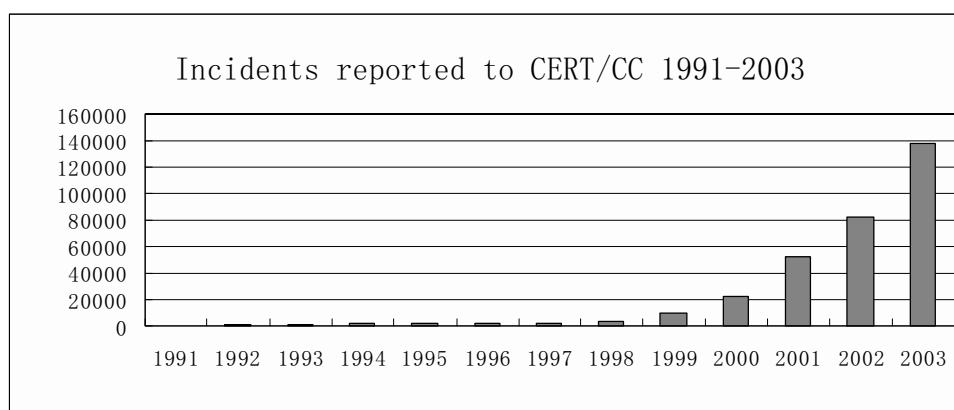


Figure 1-1 Number of security incidents reported to the CERT/CC from 1991 to 2003.

(Source: <http://www.cert.org/stats/historical.html>) NB: From 2004, the CERT/CC stopped publishing incident statistics. With the increase in automation, counting single incidents

became misleading. One and the same attack could trigger a large number of incidents.)

Research on information security surfaced with the development of computers in the 1960s. Given the fact that computers were products of advanced technology, information security naturally boiled down to technology measures. The security solutions for the first 20 years were almost exclusively technology-focused (Schou and Shoemaker 2007). As computers are now accessible to most of the public, technological measures alone can no longer ensure minimal damages and misuse. In Deloitte's 6th annual Global Security Survey¹ (Protecting What Matters: The 6th Annual Global Security Survey 2008), it has been identified that the root causes of information systems failures can be attributed to human error, technology, operations, and third parties, among others (See Figure 1-2). The top cause of information systems failures for the years 2007 and 2008 was identified as human error. It has risen from 79% in year 2007 to 86% in 2008. This could be attributed to “the increasing adoption of new technologies and social network spaces”, explained the survey report.

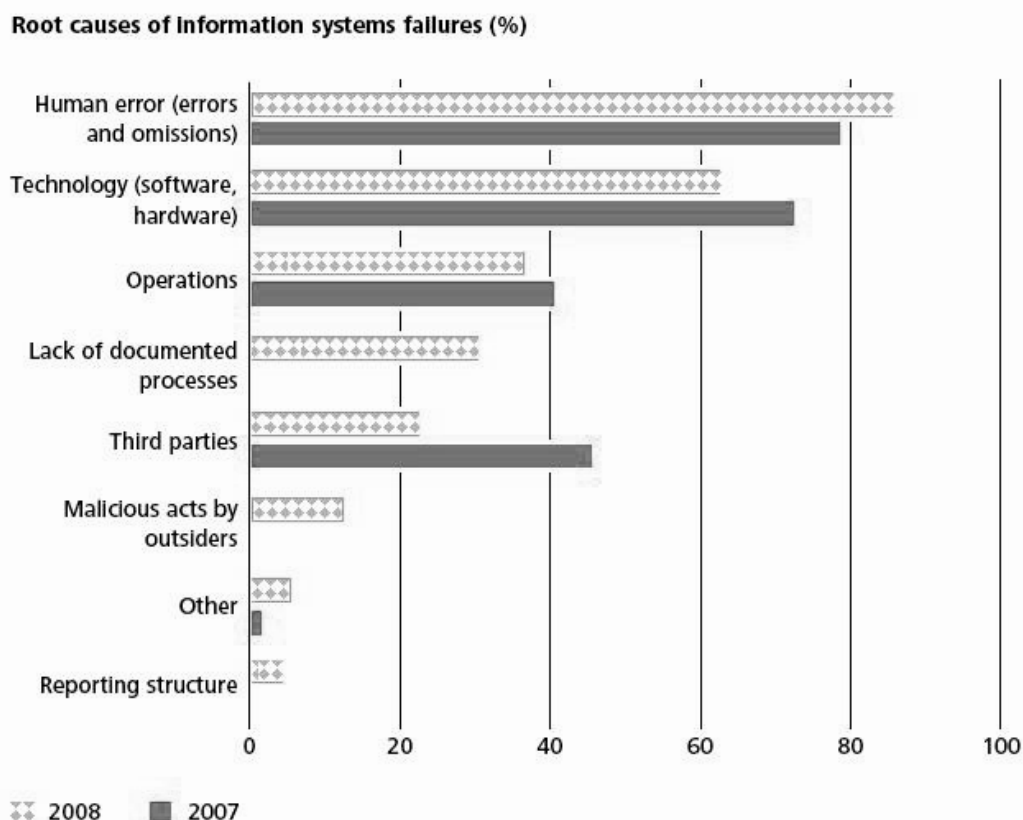


Figure 1-2 Root causes of information systems failures.

(Source: The report from Deloitte's 6th annual Global Security Survey p.30)

¹ The report is accessible at http://www.deloitte.com/dtt/cda/doc/content/dtt_fsi_GlobalSecuritySurvey_0901.pdf.

In the recent two decades, more researchers have realized the importance of human factors and organizational factors in information security. For example, Gifford pointed out that even the most sophisticated security system is worthless if disks are left lying about and passwords are not secured (Gifford 1998). Werlinger et al. identified many organizational factors that weaken security:

“Tight schedules may result in human errors that could make the organization more vulnerable. Tight schedules may also result in security controls not being implemented in the systems unless the implementation of security controls is integrated with the development process.” (Werlinger, Hawkey, and Beznosov 2009)

Organizational factors become important as the number of organizations that use advanced Information Communication Technology (ICT) is increasing. Even in the high-hazardous industry such as oil and gas production, where the consequences of incidents could be major, there are plans to utilize advanced ICT on the oil platforms. Technology helps organizations to become more efficient, however, the cost to organizations is that the technology is often more complex, takes specialized support and resources, and creates a rich environment for breeding vulnerabilities and risks, especially during the technology adoption process, when employees have to change their traditional working routines and learn to work with new technology.

The technology adoption process, changing from using traditional technology to advanced ICT, is of great challenge to organizations. Repenning and Sterman studied cases of implementing innovations for a decade, and concluded: “the inability of most organizations to reap the full benefit of these innovations has little to do with the specific improvement tool they select. Instead, the problem has its roots in how the introduction of a new improvement program interacts with the physical economic, social, and psychological structures in which implementation takes place (Repenning and Sterman 2001).” Many researchers have studied the process of operation transition and the factors that make this process successful, such as (Winch 1997; Fichman 2001; Brown and Duguid 2001; Brown and Duguid 1991). The focus of these studies is to answer the question of why some firms are successful in new technology adoption while others are not and how to make the new technology adoption successful. However, the information security risks induced in the changing process is not considered in this bunch of literature. In the literature of information security, the research focus is mostly on technological solutions, such as firewall,

intrusion detection and prevention systems. Emerging research on human factors and organizational factors has studied user interfaces, counterproductive computer usage, security checklist, risk assessment, etc. (See chapter 2 Literature review). The studies of information security seldom consider how information security risks change during the process of operation transition. The question of how information security risks change during operation transition is the cross-section of the above two research areas, while ignored by both of them. Therefore, we would like to investigate information security risks during the operation transition. We have a case of a Norwegian oil and gas company, Hydro, transitioning from tradition operation to Integrated Operations (detailed information about the case will be presented in Section 1.2). Our research is not only motivated by the fact that this specific problem has not been addressed before, but also by the practical needs of our client. A severe information security incident on an oil and gas platform could lead to major consequences (injuries, deaths or environmental damage). Such a catastrophe might result in postponement of the transition to Integrated Operations, and even threaten the continuous operation of the company. Therefore, information security is a crucial factor for the success or failure of operation transitions. Efforts to investigate the change in information security risks during the operation transition and look for policies that foster a successful operation transition are needed.

This research is embedded in the research project AMBASEC (A Model Based Approach to Security Culture), which was required to collaborate with a related project IRMA (from Incident Response to Incident Management) by the project sponsor, the Research Council of Norway (RCN). The Norwegian Oil Industry Association (OLF) contributed to IRMA funding. In return, OLF called for IRMA to investigate the information security issues in the current Oil and Gas Industry, which was planning to start transition to Integrated Operations. Therefore, AMBASEC also worked with this case. Hydro², as one member of OLF, volunteered to be the client for both projects, supplying us the case of transition to Integrated Operations on the Brage platform (a pilot platform in operation transition). The project setting is illustrated by Figure 1-3. Information about the transition to Integrated Operations and the Brage platform is introduced in section 1.2.

² When the research project started, Hydro Oil and Gas was a company division under the Hydro group. At the end of year 2006, Hydro Oil and Gas merged with Statoil, the biggest oil and gas company in Norway and formed a new company StatoilHydro, which finally was renamed to just Statoil.

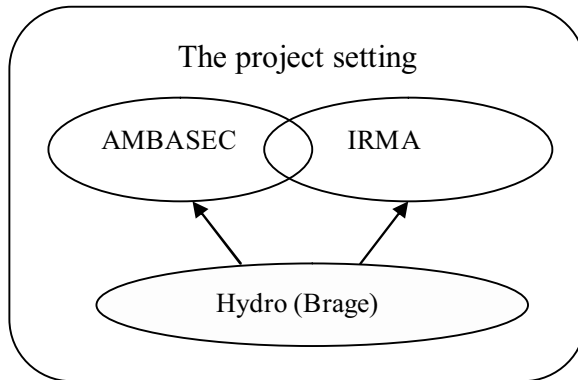


Figure 1-3 The AMBASEC Project Setting

1.2 Case information

The oil and gas industry is Norway's most important industry and the country's largest source of revenue. Oil and gas have made an important contribution to economic growth and to financing the Norwegian welfare state (Facts: The Norwegian Petroleum Sector 2007). Integrated Operations in Norwegian oil and gas companies utilize advanced ICT technology to connect offshore facilities to onshore control centers and even vendors. The motivation for changing from traditional operation into Integrated Operations is to improve productivity and reduce operation costs. The operation transition will take years to complete and it has a huge impact on the oil and gas industry in Norway.

1.2.1 Integrated Operations in the Oil and Gas Industry

1.2.1.1 The Oil and Gas Industry in Norway

In the report of Norwegian Petroleum Sector published in year 2005 (Facts: The Norwegian Petroleum Sector 2005), it was estimated that one-fourth of the oil and gas resources on the Norwegian Continental Shelf (NCS) have been produced. Under the right circumstances, oil production on NCS could continue for at least 50 years and gas production for at least 100 years. In this same report, the Minister of Petroleum and Energy pointed out that significant portions of the NCS were now in a mature phase, with declining output and increasing operating costs, as well as lower expectations for the sizes of future discoveries. The falling output of the oilfield leads to increased unit costs. When the unit cost exceeds the revenue, the oilfield will be

abandoned because it cannot create value any more. Yet, considerable oil reserves remain in the oilfield. In 2004, the average recovery rate for oil from the NCS was 46 percent. For the mid and long-term well-being of the petroleum industry, it was of extreme importance to improve average recovery rate and reduce operating cost so that the lifetimes of the fields could be extended. The Norwegian Petroleum Directorate set the average recovery target for oil at 50 percent in 2004 and was still seeking possibilities to raise this figure (Facts: The Norwegian Petroleum Sector 2005).

1.2.1.2 The transition to Integrated Operations

In order to improve oil recovery and efficient operations, the oil companies on NCS have been working on several solutions. The most promising one has been Integrated Operations or eOperation.

Integrated Operations adopts new ICT technology, mainly remote control of hardware, collaborative video conferencing and real-time decision support, to link onshore, offshore, and other parties (vendors, external experts, etc) together through high-capacity networks. The advanced ICT technology enables almost real-time data sharing to all parties. Pilot projects on offshore and onshore collaboration of drilling functions have shown improved well placement and drilling efficiency. Furthermore, projects utilizing suppliers' condition monitoring centers have also resulted in fewer breakdowns and increased regularity and production.

Based on the results of pilot projects and an overall evaluation of Integrated Operations, it is planned that Integrated Operations will be implemented in two stages: Generation 1 (G1—Integration of on- and offshore operations), and then Generation 2 (G2—Integration of companies, such as vendors). G1 (ca. 2003-2010) will integrate processes and people onshore and offshore using ICT solutions and facilities that improve onshore ability to support offshore operationally. G2 (ca. 2007-2015) will help the operators utilize vendors' core competencies and services more efficiently (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005).

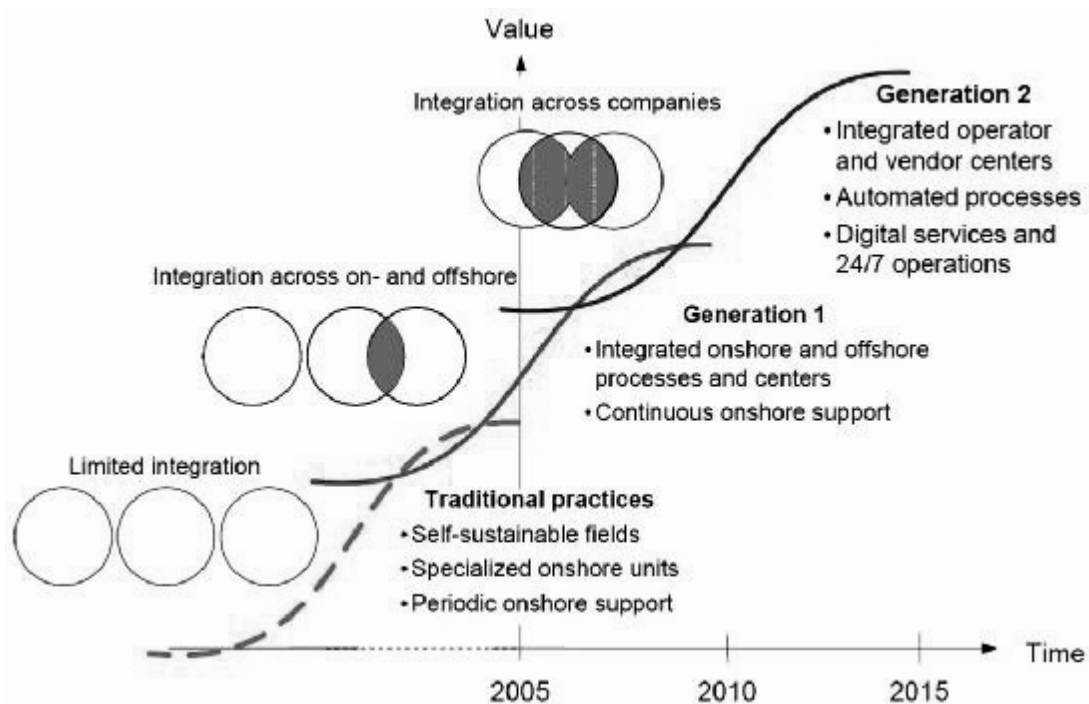


Figure 1-4 Two generations of Integrated Work Processes
(Source: presentation slide on OLF conference on June 2, 2005)

There has been a vision on changing from today's manned platforms towards future's unmanned platforms. The technology for remote control is already present. But how to utilize the technology on platforms in a safe and secure way still needs further research. Integrated Operations, a closer coupling and integration between the onshore and the offshore installations, is a step towards the vision: the organization onshore is developing from being a support-function into becoming a control-function.

1.2.1.3 The benefit of Integrated Operations

The core benefits of Integrated Operations are the availability of almost real-time data to experts and the increased accessibility to experts using video conference on broadband connection. Thus, critical decisions, such as (oil and gas) well placement, well completion and production optimization, can be made with the continuous support of experts onshore, of vendor representatives, and of specialists in other organizations. Better decisions will increase production and lead to high revenue. At the same time, with the help of the advanced ICT technology, it is possible to move some offshore functions to onshore control center and use the existing human resources more efficiently. For example, instead of having an expert in geology at every platform, the expert may be stationed on land and be available for consultation

for several offshore platforms. The reallocation of human resources from offshore to onshore has a big impact on cost saving. Every person located offshore is costly. They require accommodation, transportation (by helicopter), administrative support, managing, and insurance. Moreover, people offshore are paid high for working in a high hazardous environment. Reducing the basic manning on the platform not only reduces costs but also reduces the number of people at risk when incidents or accidents happen. As such, it can be said that the total impact of Integrated Operations on production, recovery rates, costs and safety is profound. Table 1-1 briefly summarizes the major benefits of Integrated Operations.

Table 1-1 Benefits from integrated operations

1.	Increased production
	Better well placements
	Intelligent well completions
	Improved production optimization
2.	Reduced cost
	Increased resource flexibility
	Faster decision making
	Down-sized manning of the platform
	Improved availability and up-time of critical equipment
	Reduced maintenance cost
3.	Reduced risk
	Better decision with less risk
	Earlier detection of degradation
	Reduced personnel expose to risk
	Quick access to experts when incidents happen

It is estimated that when Integrated Operations is fully implemented, the production could increase by 10% and the cost of operating could be reduced by 30% (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005). OLF estimated that the program might generate an incremental net present value of 250 billion NOK (\$41 billion USD).

1.2.1.4 From traditional operation to Integrated Operations

To realize the benefit of new technology, profound changes are necessary to many work processes including (oil and gas) well planning, well completion, production optimization, and maintenance management.

In traditional operation, each offshore platform acts as an independent “factory”. Most operation decisions are made offshore, in isolation, or with limited support from experts onshore. On-platform personnel manage daily operations and have sole responsibility for the safe operation of their machinery. Communication with onshore personnel is periodic. Production plans are relatively rigid and primarily changed at fixed intervals. In the face of malfunctioning equipment, experts will be transported by helicopter to the platform if needed. The IT systems are specialized, and it is difficult and time-consuming to gather the data necessary to optimize processes.

In essence, each platform is an island; all the resources need to be on-platform, at significant cost and some risk to personal safety. The offshore field is essentially a closed system.

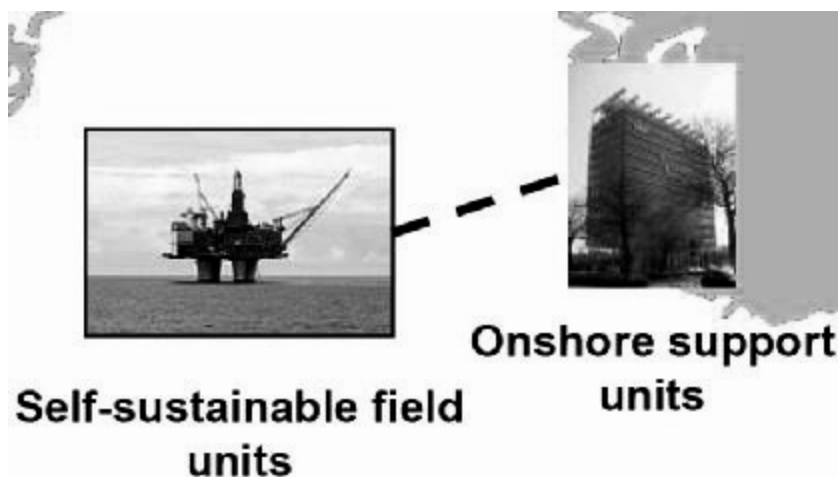


Figure 1-5 Traditional operation

The transition to Integrated Operations will take 2 generations. In generation 1, onshore centres will closely collaborate with offshore personnel through ICT technology solutions that share real-time data and provide real-time collaboration facilities. When coming up with operation decisions, professionals onshore can carry out “what-if” analyses and discuss consequences of various decisions with personnel offshore via high-fidelity audio and video systems to find out what can be done to optimize operations further. Both personnel onshore

and offshore can monitor operations in real-time, compare actual data with simulations, and identify operational as well as safety-related problems (see Figure 1-6 below).

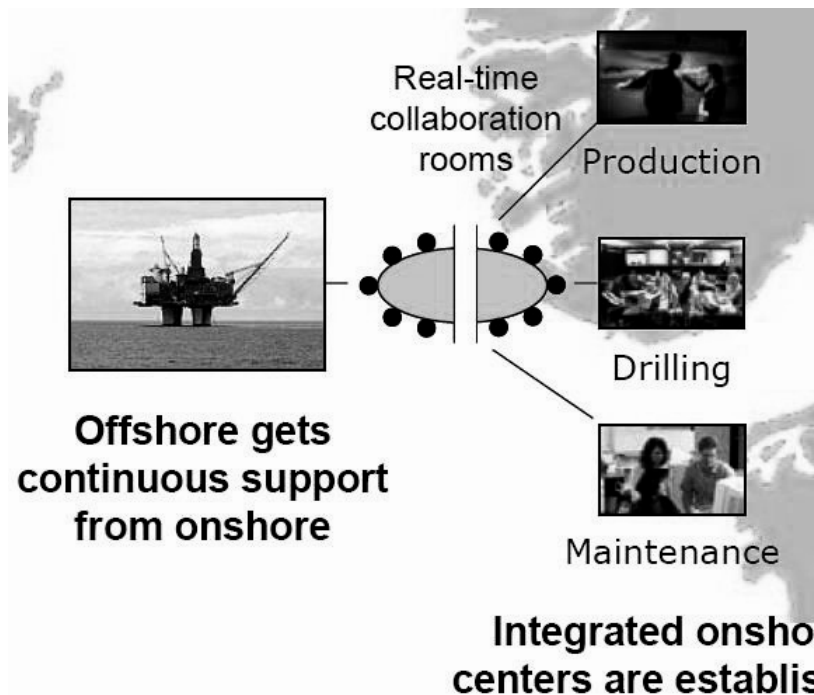


Figure 1-6 Integrated Operations generation 1-Integration of on- and offshore operations

In generation 2, technology implemented will facilitate a closer integration of the work processes of the operators and vendors. An oil and gas field will be operated by personnel located in operation centres belonging to both the operators and vendors. A large portion of the services required to operate a field will be delivered “over the net”. The vendors will take over some of the daily work and decision-making processes that were earlier carried out by the operators, e.g., monitoring, analyzing and optimizing tasks, and will deliver services to the operators in real time, digitally “over the net” (see Figure 1-7 below).

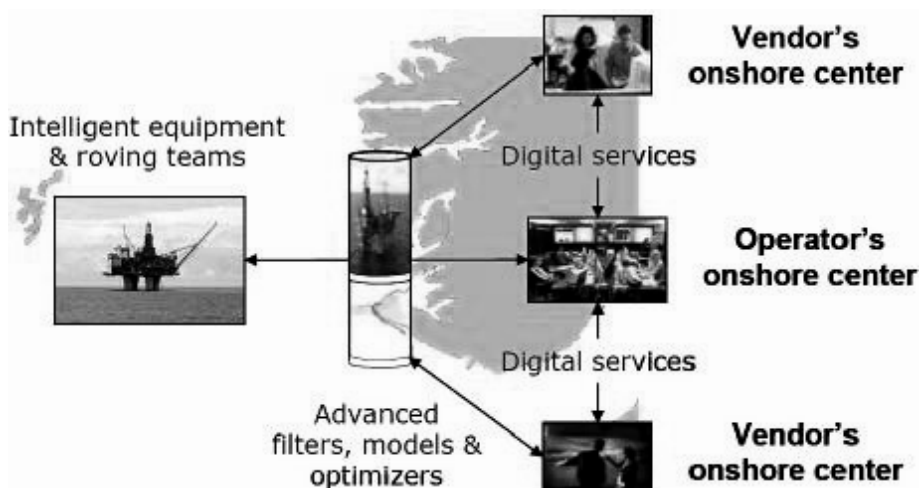


Figure 1-7 Integrated Operations generation 2-Integration of companies

The organizational structure needs to be changed as well. In traditional operation, onshore and offshore personnel belong to several different units with different goals. Production plans are made and problems are solved in a fragmented manner. In Integrated Operations, personnel from different units and in different disciplines all come together in the operation centre to collaborate in decision-making and problem solving.

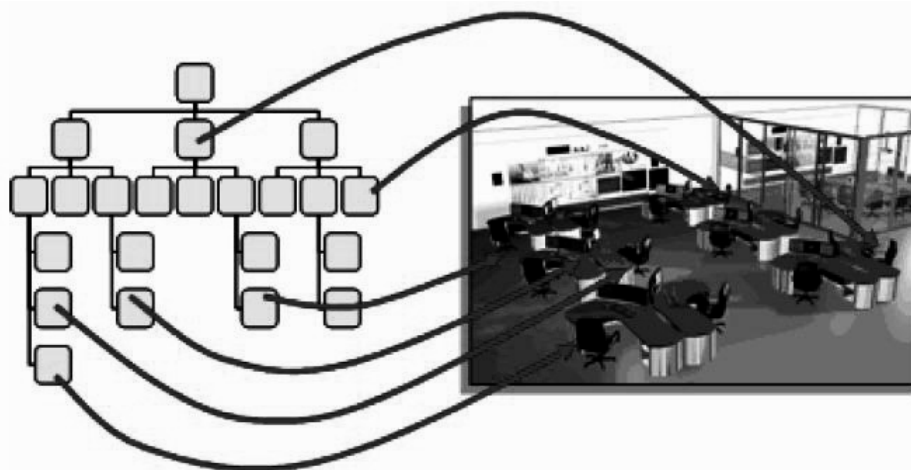


Figure 1-8 Organization structure change

1.2.1.5 The challenges of the operation transition

Oil and Gas Companies constitute a predominantly hazardous industry. A one-day outage may cost millions of dollars, while catastrophic failure can result in the loss of lives and huge damage to the environment. There are concerns for the HSSE (Health, Security, Safety and Environment) during the transition from the traditional setup to Integrated Operations.

From the technological aspect, the prevalence of standard PC hardware and commercial off-the-shelf (COTS) software, and the availability of remote control, create a new opening for malware to control the operation systems. The increased interconnections between process control networks and office networks create more points where the combined network may fail or be exploited by outsiders (Askildsen 2004).

From the human aspect, change is a difficult and painful process. When advanced technology is in place and new work processes are implemented, operators need to

take time and effort to familiarize themselves with the new system. Technology unfamiliarity is one possible reason behind human errors (Wantanakorn, Mawdesley, and Askew 1999). The new operation presupposes an effective communication and collaboration via video conference, which is completely different from the traditional operation. It would be a challenge for people to learn to communicate effectively in the new way. For those who are moved from offshore to onshore, new competency will be needed for the new tasks.

From the organizational aspect, new work assignments and new work locations could disrupt the company's social structures and their associated "know-who" networks. Rebuilding one takes time. Above all, the company is moving into an uncertain area where no former experience exists. What to do, how to do, when to do are questions that must be considered with care (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005).

1.2.2 The Brage platform

The Brage platform serves as a pilot project in the transition to Integrated Operations. Brage started production in 1993, and reached its peak production in 1998 with 120,000 barrels of oil per day. In year 2003, the production dropped to 40,000 barrels of oil per day. Brage is a so-called mature platform and it has reached its tail-stage. Revenue from 40,000 barrels per day barely covers the production cost. A further drop of production will lead to the close down of the platform because it will no longer be profitable. The platform was originally planned to shut down in year 2006 without measures to boost production efficiency.

However, upon utilization of the advanced ICT, the basic manning on the platform has been reduced from 41 to 25 persons. Reduced manning has a huge impact on cost reduction. Three shifts work on Brage. Each shift work two weeks on a platform and have four weeks time off. One basic manning on the platform means three employees all of whom are highly paid because they work in a hazardous environment. Given that Brage has achieved 25% cost reduction, amounting to 100 million NOK a year, the lifetime of the Brage platform has been successfully prolonged. It is still operating now. The platform chief suggested that it might continue operation until year 2015.

Good collaboration between the operational organization offshore and on land is an essential factor in cutting costs. It is planned that the basic manning of the platform is to be reduced to 20 people. The extended life time of the Brage platform implies additional revenues of several billions of dollars. Figure 1-9 provides a general illustration.

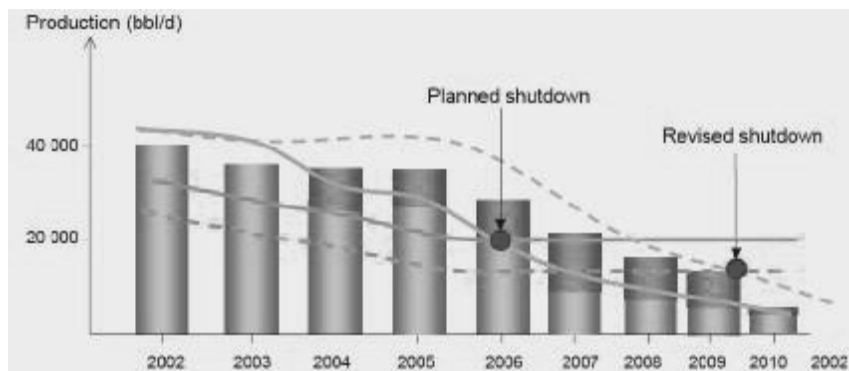


Figure 1-9 Efficient Operations in the Brage field

Source: PPT from Oil & Energy Business Area Seminar 2-3 June 2004

NB: Only for illustration. Not for precise data. The extension of the lifetime of Brage is expected to be until 2015.

In 2004, the management team examined operations on Brage, after which they identified that 20 traditional work processes to be modified or give room for new work processes, i.e., Integrated Operations. This transition started in year 2005 and would continue over several years. In the first year, 5 key new work processes, mainly related to production optimization would be introduced and then 2 new work processes every year thereafter.

1.3 Research Questions

The information infrastructure (including hardware and related device, software, and network connection) becomes vital to the operations of the Norwegian Oil and Gas Industry. If a major failure of information infrastructure occurs, it could lead to devastating consequences. Studies have shown that, although one can readily buy machinery that embodies new technology, the knowledge needed to use the modern production technology is acquired much more slowly and with considerably more difficulty (Attewell 1992; Brown and Duguid 1991). Without the adequate level of knowledge to operate new work processes, the system will be more vulnerable. There will be more human errors. Rasmussen's studies show that without adequate

knowledge, human error rate is high; and when knowledge is built up, the human error rate will be reduced (Rasmussen 1982, 1987). The extensive utilization of new technology will introduce new threats, new vulnerabilities, which might cause information security incidents.

According to an interview with the NPD (Norwegian Petroleum Directorate), human mistakes, knowledge, and attitudes are considered as the most critical factors during operation transition (Askildsen 2004).

In this research, we will look into the following aspect and seek answers to the specific questions listed below:

1) Transition speed

Transition speed is defined as how many new work processes is implemented in certain time period, for example, a year. A fast transition to Integrated Operations is desirable because the management would like to reap the benefit of the advanced technology immediately. However, fast transition might cause problems. It is possible for the management team on Brage to develop and implement new work processes at a short interval, but it is difficult for the operators on Brage to learn the new work processes and acquire the related knowledge with little time. Johnsen et al. noted that the ICT teams did not always understand the demands of production and support teams. There is a knowledge void that requires concerted communication and cooperation, something that may not be part of the existing operational culture. Moreover, control room staff was not familiar with the risks associated with information technology, and that their skills in identifying potential computer-generated hazards (e.g., software bugs, viruses, intrusions) are limited (Johnsen, Line, and Askildsen 2006). Building new knowledge for new ways of operation takes time and effort. Moving into new ways of operation without necessary knowledge is risky. The key question here is: what is a proper transition speed that can on the one hand, avoid severe incidents and on the other hand, realize the benefit of advanced technology soon?

Research question 1: What is an appropriate speed for the transition to Integrated Operations considering the trade off between financial gains and information security risks?

2) Resource allocation

There are limited resources on the platform. A fixed number of the operators work on a platform. Normally, they work 12 hours a day and work continuously for 14 days until another team takes the shift. During operation transition, the operators have to not only complete routine production work but also need to learn new work processes and acquire related knowledge. Resource allocation here means how to allocate the operators' time for routine production, for learning new work processes and for learning new knowledge.

The learning of new work processes and knowledge has two forms: 1) special training program which takes the operators off routine production job; and 2) on-job training. The former, as it takes the operators off-job, clearly claims the operators' time and causes production disruption, which lead to reduced output. On-job training is sometimes perceived as costless. In fact, it also needs the operators' time but in small slices that are not so obvious, which also reduces output.

Repenning studied why most firms failed to achieve the desired improvement when implementing new tools, techniques, and technologies. He found that under throughput pressure, the operators tend to ignore efforts needed to improve long-term productivity (that is learning), but focus on achieving short-term throughput target (Repenning and Sterman 2001). Similarly, the operators' on the Brage platform also have the pressure to achieve their product target. In this research, we will investigate how resource allocation during the operation transition affects the long-term productivity and information security risks.

Research question 2: How does resource allocation during operation transition affect the effective use of new technology and the information security risks?

3) Investment in incident response capability

One of the ways to mitigate information security risks is to invest in incident response capability so that the information security incidents are timely detected and properly handled. As a result, the severity of incidents can be controlled. However, most organizations view security control as an overhead costs and adopt a reactive security management approach, i.e., they address security concerns only when security

incidents happen. Indeed, “actions taken to secure an organization’s assets and processes are typically viewed as disaster-preventing rather than payoff-producing, which makes it difficult to determine how best to justify investing in security, and to what level” (Allen 2005). For those responsible for security, it is often difficult to persuade senior executives and board members of the need to implement information security in a systemic way. Caralli and Wilson point out that the reason why security is viewed as overhead is the lack of financial justification. They argue that “organizations do not routinely require return on investment calculations on security investments, nor do they attempt to measure or gather metrics on the performance of security investments” (Caralli and Wilson 2004).

Based on the group model-build workshops, and model validation interviews, we identified that the current decision rules for investment in incident response capability on the Brage platform are as follows:

1. make investment in incident response capability when increasing number of incidents happen.
2. make investment in incident response capability when the severity of incidents exceeds a pre-set warning line.
3. make investment in incident response capability when incident cost goes beyond certain pre-set amount.

In this research, we will investigate how different decision rules affect the information security risks, especially during the operation transition period.

Research question 3: How do management decision rules on investment in incident response capability affect information security risks?

These are the three research questions that we investigate in this research. It is because of them that we choose to use system dynamics (see chapter 3). And the model is built focusing on these questions (see chapter 5). They are investigated in chapter 8, using the model we developed. Below we will present the thesis structure.

1.4 Thesis structure

This thesis contains nine chapters, which could be categorized into four parts. The first part provides background information for this research. The second part discusses

the methodology used in this research. The third part presents the main research activities and results. The last part discusses the research activities and findings. Below, we offer more detail information about each part of the thesis.

1.4.1 Background information

The first part of the thesis presents an overview of the research problem and the rationale for this research. Two chapters are included in this part: chapter 1 Introduction and chapter 2 Literature Review. Chapter 1 discusses the research motivation first. Then it provides background information for the case: the transition to Integrated Operations on the Brage platform. Based on the above two, the specific research questions are raised. Finally, the structure of this thesis is described. Chapter 2 covers the relevant literature on information security, technology aspects, human aspects and organizational aspects. This review of literature provides a base for this research. We argue that current methods could not address the research questions because they have not included the dynamic feature that this case requires. System dynamics is a method specifically designed to address problems with dynamics features. Thus, we will propose the use of system dynamics to address the problems in our case (See section 3.1).

1.4.2 Methodology

The methodology part contains only chapter 3, which discusses the rationale for choosing system dynamics as a method for this research. The chapter explains the characteristics of the case—dynamic, long-term, with delays, feedback, nonlinearity and lack of data, which can be addressed by system dynamics. System dynamics is designed to deal with dynamic complexity, which includes feedback, delays, nonlinearity. It is an interdisciplinary approach which allows us to address issues that belong to different fields. Moreover, system dynamics models are built on the assumption that the underlying causal structure of a system is what governs its behavior. The model-building process starts with qualitatively identifying causal structures. The model itself and the simulation experiments it allows us to undertake, enable us to identify the information that is most relevant, i.e. to allow us to distinguish between a valid and an invalid causal structure. In such a way, model based information collection can be made very efficient. Even with imprecise data, given the right model structure, the model is able to simulate and generate insight.

The characteristics of the case under investigation are very well captured by system dynamics and, therefore, we choose to use system dynamics to address the research questions. Chapter 3 also presents how system dynamics is used in this study to tackle the research problem.

1.4.3 Research activities and results

This research unfolds in several steps in compliance with the system dynamics modeling process. Most experts in system dynamics agree that the modeling process includes the following stages: model conceptualization, model formulation, model testing and model implementation (Randers 1980; Luna-Reyes and Andersen 2003). We fit our research activities according these stages.

Table 1-2 Modeling process

Model Conceptualization	Chapter 4 Group model building workshops
Model Formulation	Chapter 5 Formal model presentation
Model Testing	Chapter 6 Model validation tests Chapter 7 Model validation interviews
Model Implementation	Chapter 8 Scenarios and Policies

Chapter 4 presents how we articulate the problem, form dynamic hypothesis and obtain qualitative and quantitative data for model development in the two group model-building workshops. Chapter 5 explains the model structure using causal loop diagram and describes the formal model sector by sector. Chapter 6 presents how we validate our model. Chapter 7 presents the experts' opinions of the model as a means of behavior validation. Chapter 8 discusses various scenarios and policy recommendations based on the insights from the model.

1.4.4 Conclusion

Chapter 9 revisits the model building process and the model insights for policy recommendations. Moreover, the research methodology will be discussed reflectively: what could be improved for this study? Finally, there is a section for future research directions.

1.5 Closing Remarks for Chapter 1

Information security research has been mostly technology focused. As computer and Internet has reached normal households and most of the organizations, investigating information security problems from human and organizational aspects is of increasing importance. We foster studies of information security from human aspect and organizational aspect. The case for this Ph.D. study is information security risks during the transition from traditional to Integrated Operations in Hydro, a Norwegian oil and gas company. The operation transition will continue for several years, adopting advanced ICT technology to connect off-shore platforms with on-shore facilities and vendors. The management of Hydro has concerns for information security risks during the operation transition, when new work processes and knowledge are introduced. Literature has pointed out that human error rate is high without adequate knowledge. The knowledge building is affected by transition speed and resources available for learning. Therefore, two research questions concern transition speed and resources allocation respectively. Investment in incident response capability is one way to reduce information security risk. But literature also pointed out the difficulties to make proactive investment in incident response capability. As a result, the third research question concerns how the decision rules on investment in incident response capability will affect information security risks during the operation transition.

2 Literature Review

The purpose of this chapter is to provide a review of the relevant literature. The review presents the state of the current information security research and practice, which will provide the basis for the selection of the methodology for our research.

This literature review starts with the definitions of the key concepts of this research such as information security, risk, vulnerability, incident, and others. The precise definitions are the basis for further discussion.

Afterward we review the research and practice in the information security area. First, a brief overview of the technological development of information security is presented. The reason for a technology-focused view is then discussed, as well as the limitations of the technological approach in the current information security. Second, research on human factors in information security is examined. Third, the theory and practice of organizational factors in information security is discussed.

2.1 Definitions of the Key Concepts

Definitions are the basis for discussion. Looking into the literature, we found that the same information security terms sometimes have different meanings, while some different terms have the same meaning. This makes it difficult to make comparisons, conduct confrontations, or draw conclusions. Here, we present the definitions of the key concepts used in this work, allowing us to express our thoughts in a common language.

The definitions of the key concepts mostly come from the “Glossary of Key Information Security Terms” (NIST 2006), a summary document from the National Institute of Standards and Technology (NIST). NIST is one of the main government agencies involved in security program development. Taken from the NIST Federal Information Processing Standards (FIPS) and the Special Publication (SP) 800 series, this glossary summarizes the most frequently used security terms. We will refer to it as “the NIST Glossary” here after.

2.1.1 Information Security and Computer Security

In the NIST Glossary (NIST 2006), information security is defined as follows:

The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide the following:

- 1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity
- 2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information
- 3) availability, which means ensuring timely and reliable access to and use of information

In the international quality assurance standard for information systems ISO 17799³, information security is defined as the protection of confidentiality, integrity, and availability of information. The above two definitions are similar. The main difference is that the ISO 17799 definition only emphasizes information, while the NIST definition emphasizes both information and information systems. To protect information, information systems must be protected. That could be the reason that ISO 17799 has not made specific emphasis on information systems. However, we think it is still necessary to stress the protection for the both information and information systems. Some attackers and events have direct consequence to information systems but not to information. For example, an operator from the vendor unintentionally introduces a virus to the system while updating the system. This virus does not jeopardize information integrity, confidentiality, and availability. Instead, it weakens the information system, which may cause further problems of production.

The ISO 17799 standard specifies that information exists not only in electronic form but also in other forms, such as printed in paper. However, as most of the information storage and exchange take the electronic form today, most of the current research in information security focuses on electronic information on computer, which is sometimes referred to as computer security. This study investigates the behavior of

³ The ISO 17799 has been replaced by the ISO 27000 series since 19 Dec 2008, in particular, ISO/IEC 27002: Code of Practice for Information Security Management.

information security during the transition to Integrated Operations using advanced ICT. Therefore, we will also focus on protection of information in electronic form.

2.1.2 Risk

According to the NIST Glossary (NIST 2006), risk is defined as follows:

The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals, resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. This definition is in line with that given by ISO 17799, which can be expressed by following mathematical equation:

$$\text{Risk} = \text{Likelihood of incident occurring (Probability)} * \text{Potential impact (potential damage)} \quad (1)$$

ISO 17799 further points out that the probability that a damaging incident happen concerns threat as well as vulnerability, which can be expressed by following mathematical equation:

$$\text{Likelihood of the incident occurring} = \text{Threat} * \text{Probability of the threat penetrating the vulnerability} \quad (2)$$

Combining equation (1) an equation (2), risk can be formulated as:

$$\text{Risk} = \text{Threat} * \text{Probability of the threat penetrating the vulnerability} * \text{Potential impact (potential damage)} \quad (3)$$

With more threats, the risk will be higher. With higher vulnerability, the probability of the threat getting through will increase and the risk will become higher. When the potential impact is bigger, the risk is higher.

The NIST glossary (NIST 2006) gives some examples of how IT-related risks may arise:

“IT-related risks arise from legal liability or mission/business loss due to, but not limited to, the following:

- Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information
- Non-malicious errors and omissions
- IT disruptions due to natural or man-made disasters

- Failure to exercise due care and diligence in the implementation and operation of the IT”

Non-malicious or accidental actions are under the scope of information security risks. In safety research, two categories, error and violation, are used to distinguish unintentional and intentional breaches of safe measures (Reason, Parker, and Lawton 1998).

- Error: unintentional deviations from a planned course of action or in the case of mistakes, incorrect plans arising from various kinds of informational underspecifications.
- Violation: intentional deviations from safe operating procedures, standards, or rules.

Within the violation category, further distinction can be made, depending on whether the intention is malicious or not. A violation with malicious intention (to cause damage to the system) is referred to as sabotage in information security. A violation without malicious intention, such as corner-cutting, does not have a clear label. We will use the term non-malicious violation.

Therefore, we can summarize that information security risks arise from sabotage, non-malicious violation, and human errors. Sabotage can come from the outside or inside, sometimes referred to as an outsider attack and insider attack, respectively. The realization of sabotage risks lies in both how vulnerable the system is and how skillful the attacker is. A well-defended system can prevent sabotage attempts from getting through. However, even the best-defended system has holes and can be penetrated. For errors and violations, the realization of such kinds of risks mostly depends on the vulnerability of the system. A well-designed and well-regulated security system can prevent or mitigate most of these risks, while a poor vulnerable system can facilitate such risks to materialize and develop into severe incidents.

2.1.3 Incident

Incident is defined as “an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent

threat of violation of security policies, security procedures, or acceptable use policies” (NIST 2006).

Note that an incident may not incur actual cost if it only potentially jeopardizes information or information systems. An example is when a hacker penetrates the system just for fun, goes into the system, and then leaves without doing any damage. Actually, a great number of incidents are relatively costless, but they have a consequence of the employees becoming frustrated and perceiving their job situation as being disturbed, thus resulting in reduced working efficiency (Jaatun et al. 2007). More harmful incidents may put out technical equipment and interrupt business continuity. Severe incidents may even cause a chain of consequences resulting in large economical losses, environmental damage, and injuries or loss of life.

2.1.4 Threat

In the NIST glossary, threat is defined as “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability” (NIST 2006).

A threat can be categorized as an outside threat or an inside threat depending on the source of the threat. If a threat comes from an unauthorized entity from outside the domain perimeter, then it is an outside threat. If a threat comes from an entity with authorized access to the domain perimeter, then it is considered an inside threat. However, in the cases of outsourcing, virtual organization, and Integrated Operations, in which companies are connected using advanced ICT, the domain perimeter is vague. Threats from suppliers or virtual teams are not purely from insider or outsider. Furthermore, in some other cases, outsiders work together with insiders to penetrate the system.

2.1.5 Vulnerability

According to the NIST glossary, vulnerability is defined as “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source” (NIST 2006).

In some other information security literature, vulnerability is often regarded as weakness in the software, and the way to manage vulnerability is through patching (Chuvakin 2006). In the NIST glossary, we can see that vulnerability is not about the software only, as it includes weakness in procedures, controls, or implementation, which means the whole system. The weaknesses in human beings, organization, software, hardware, and network are all vulnerabilities. We will use this broader definition of vulnerability in this document.

2.1.6 Computer Security Incident Response Team (CSIRT)

In the NIST glossary, Computer Security Incident Response Team is defined as “a capability set up for the purpose of assisting in responding to computer security-related incidents; also called a Computer Incident Response Team (CIRT) or a CIRC (Computer Incident Response Center)” (NIST 2006). There are different types of CSIRTs, for example, International Coordination Center, National Team, Network Service Provider Team, IT Vendor, and Corporate Team (West-Brown et al. 2003). In this case, we consider the corporate team.

According to the Handbook for CSIRTs (West-Brown et al. 2003), the mission of a corporate CSIRT would be “Improve the security of the corporation’s information infrastructure and minimize threat of damage resulting from attacks and intrusions.” (p. 62). And the service objective for such a CSIRT is to:

“Provide a center of excellence for incident handling support to system and network administrators and system users in the corporation.

Provide on-site technical support for incidents impacting company systems to isolate and recover from intruder threats and attacks.” (p. 62)

When incidents happen, it is the response team's responsibility to handle them. If handled with efficiency, the impact of the incidents can be reduced. Otherwise, the impact will become bigger.

A corporate CSIRT can be a formal team or an ad hoc team (gathered when needed). In our case, the Brage platform uses the later form. Therefore, we will use the term "incident response capability" in the following discussions.

IRMA proposed the following tasks for incident response capability on Brage (Line et al. 2007):

- Prepare: Planning for and preparation of incident response
- Detect and recover: Detect incidents and restore to normal operation
- Learn: Learning from incidents and how they are handled.

Preparation phase includes activities such as risk assessment, documentation of the detailed configurations, awareness creation and monitoring.

Detection and recovery phase includes activities such as altering (by others reporting of deviation or by use of technical security measures), assessment of the altering, immediate response and recover.

Learning phase includes activities such as identifying root cause of the incidents, recommending security improvements, and evaluating the incident handling process.

2.2 Research on Information Security

With the expansion of the computer and Internet users, information security has gained increasing attention. For many people, technology is the most effective way to secure a system. A large portion of the research effort is devoted to advance security technology, such as the implementation of firewalls and intrusion detection systems. Lately, it has been acknowledged that a major part of security and safety problems is due to human factors (Sawicka 2004). It is no longer technology that constrains the reliability of the systems. Research on information security focusing on human and organizational factors has emerged. Below, we will review the research on information security from the technological aspect, as well as the human and organizational aspect.

2.2.1 Managing Information Security: Technological Aspect

The concept of information security surfaced in the 1960s. The concerns ranged from forced entry into computer and storage rooms to destruction by natural or man-made disasters such as earthquakes, hurricanes, and fire. Recent attention has focused on protecting information systems and data from accidental or intentional unauthorized access, disclosure, modification, or destruction. The consequences of these events can range from degraded or disrupted operation to corporate failure (Loch, Carr, and Warkentin 1992).

2.2.1.1 Information Security Technology Advancement

Research on information security with a technological aspect has a long history. Research interests have evolved over time with the development of computers and the Internet.

In the 1960s and 1970s, when computers were mainframes, information security was mostly concerned with internal operating system security. Substantial research efforts were devoted to secure operating systems design and security mechanisms against subversions, resulting to the emergence of security-oriented subsystems such as IBM's Resource Access Control Facility and Computer Associates' ACF-2 and Top Secret (Arce 2003).

During the 1980s, the use of personal computers spread in companies and households. In using the floppy disk to transfer information between computers, a new security threat became imminent: the virus. Research focus was then on the desktop computer and its susceptibility to computer viruses. Newly discovered viruses and virus infection incidents were extensively documented and analyzed.

In the 1990s, with the fast development of networks, the security concern was focused on network security. The interconnectivity of multiple networks via Internet Protocol Standards made the networks of academic, business, government, and even military organizations open to attackers. The firewall emerged to separate the internal network from the outside. Extensive study on the security of networking protocols and

infrastructure components led to better solutions in Internet protocols, user authentication systems, and others.

At the end of the 1990s, with the full adoption of the World Wide Web and the Internet to conduct daily business, the organizations' perimeter got blurred. It became less obvious to differentiate internal users from external attackers. Solutions such as firewalls, cryptographically strong authentication systems, network and host-based intrusion detection systems, VPN devices, and cryptography additions to networking protocols were not enough. Research attention turned to server security, operating system controls, patch management, and additional defenses.

Today, workstation security attracts much research interests. Solutions such as personal firewalls, host-based intrusion detection and prevention systems, workstation access control software, file integrity checkers, and patch management systems help to secure workstations. However, we must realize that humans operate and control workstations, and no technological solution alone can secure us if human and organizational behaviors are not included in a comprehensive security strategy.

2.2.1.2 Limitations of the Technological Approach

What security technology does in information security is to “seal” the organization perimeter and prevent outsiders (malicious outside attackers) from getting into the system and wreaking damage. In retrospect, there are many reasons for this technology-focused view.

In the early years of computers and Internet development (before the 1980s), computers existed only in those “superior” organizations, such as academic and government organizations, and were available only to experts who had the expertise and were by and large virtuous. There was not much to worry about human errors or violations or insider attacks. The major task of information security was to keep malicious agents outside the system.

In the 1980s and early 1990s, with the widespread of personal computers and the fast growth of the Internet, people who use computers and the Internet generally had little knowledge about computers and the Internet, even less knowledge about information

security. Human errors and violations have caused increasing number of computer incidents. However, the impacts of such incidents were small compared with those caused by malicious attackers. Human errors and violations normally generated minor incidents, while the malicious attacks, if successful, caused extreme impacts. Therefore, the information security focus was still on preventing attacks, which is heavily dependent on technology improvement.

Nowadays, daily business operations are fully dependent on the Internet connection. It is the case even for highly hazardous industries such as nuclear plants, chemical refineries, and oil and gas productions. This changes the whole information security paradigm because human errors and violations can lead to severe incident, huge financial losses, and even injuries and loss of lives.

As Arce pointed out (2003),

“Information security—both as a practical discipline and as an academic field—has steadily increased in complexity since the 1950s. A wider range of problems must now be considered to devise effective security architectures for today’s organizations. Security solutions should account for our IT infrastructure’s technological challenges and the particular aspects of human and organizational behavior.”

2.2.2 Managing Information Security: Human Aspect

The research on human error has long been in the realm of psychology research. Human error research in the industrial setting started in the late 1950s and early 1960s when formal methods for identifying and classifying human errors in missile development systems were developed. The nuclear power accident in Three Mile Island in 1979 raised the importance of human error, leading to better understanding of its causes, manifestation, and consequences in the 1980s. The 1990s had seen a maturing of some of the Human Reliability Assessment techniques and a broadening of the models of human error to account for organizational influences on error.

Although it is widely accepted that human factors contribute to a large portion of information security incidents, theory and know-how in this specific area are limited. How to deal with human factors in information security and why people are such obstacles are still not well understood (Sawicka 2004).

In the current literature on human factors in information security, we can find three main research lines: one concerning user interfaces of security-related systems, one concerning counterproductive computer usage, and the other concerning human behavior related to security risks.

The usability researchers believe that bad security is mainly caused by the poor design of security applications. They are difficult to learn and use. Improving the usability of security products can achieve better security. This kind of research is under a much broader computer-human interaction (CHI) field. Although software applications improved in effectiveness with better computer-human interaction design, how much it would work for security products is still in doubt. The fundamental problem lies in the difference of functionality in normal application and security application. A normal application has functionality if things that are supposed to happen do happen. But a security application has functionality if things that are not supposed to happen do not happen. Security developers are interested in the latter, while end users tend to be more interested in the former (Gutmann 2008). This is why Schneier emphasized that “people cannot be trusted to implement computer security policies” (Schneier 2000).

At the extreme end of counterproductive computer use is “insider attack.” Insider attacks are often found in security incidents, and they often cause high consequences. Anderson argued, “We find that almost all attacks on banking system involved blunders, insider involvement, or both. High tech attacks are rare...” (Anderson 1994). A total of 671 respondents participated in the 2007 e-Crime Watch Survey conducted by the U.S. Secret Service (USSS), Carnegie Mellon University, Software Engineering Institute’s CERT Program, and Microsoft Corporation. In cases where respondents could identify the perpetrator of an electronic crime, 31 percent were committed by insiders.

Software Engineering Institute’s CERT Program has devoted some of its research capacity to study insider attacks. A study on 150 actual insider attack cases from 1996 to 2002 looked for common threads in insider attacks by asking the following:

- Who did it?
- What was stolen/modified?
- How did they steal/modify it?

■ Known Issues (Why did people do it?)

Many reasons that cause insider attacks are identified, such as problems with supervisors, physical threat from outsiders, and the others. (Cappelli and Moore 2008). The insights from this study are helpful, but it is still hard to prevent inside attack. The recommended practices mainly concern improving security policies and security awareness in organizations. The following are some examples:

- Enforce separation of duties and least privilege
- Institute periodic security awareness training for all employees

Human behavior related to security risks mainly focus on human compliance with information security policies and security awareness. Sawicka devoted her Ph.D. work to studying the dynamics of human compliance in IT-based environments (Gonzalez and Sawicka 2002; Sawicka 2004; Gonzalez and Sawicka 2003). Based on two established psychological theories, cumulative prospect theory of choice under risk and behavioral regulation approach to instrumental conditioning, she assumed that people compliance would drop until security incidents happen.

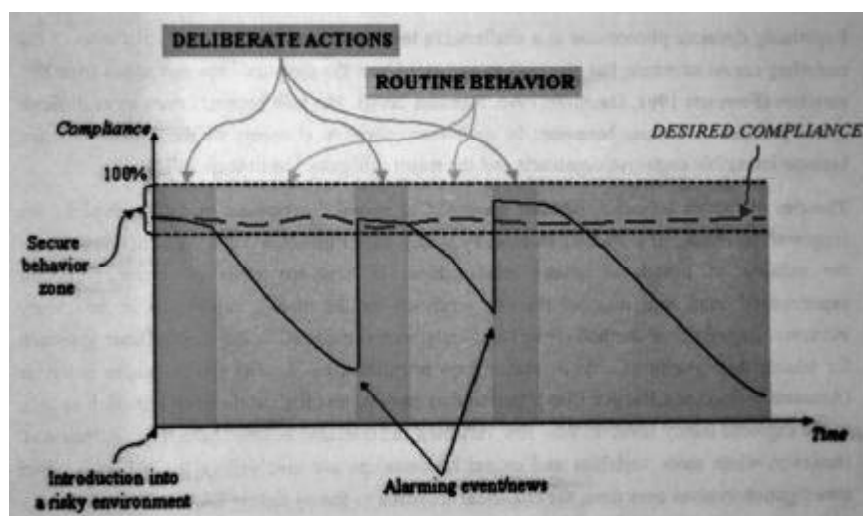


Figure 2-1 Basic behavior modes of compliance

Source: (Sawicka 2004 p. xv)

A system dynamics model of individual compliance was developed. The model behavior-compliance pattern was tested with two series of laboratory experiments in the context of a simple data registration task. The actual data registration patterns provided some evidence in support of the proposed model. However, some observed behaviors could not be explained by the model's structure. Understanding the basic

mechanism of individual compliance will lead to a major improvement in security and safety.

Humans do err. However, most human errors have underlying social and organizational reasons. As Clarke and Jr. Short stated, “The intellectual problem is that as a theory of sociotechnical breakdown, human error presumes more than it explains, obscuring the complexities of interaction between humans, machines, and organization” (Clarke and Jr. Short 1993). They further pointed out that we can learn more about how risks are produced by theorizing organizational factors such as production pressures, managerial expectations, and regulatory effectiveness.

2.2.3 Managing Information Security: Organizational Aspect

Today, many organizations have become so dependent on computers and computer-based ICT that disruptions may cause outcomes ranging from inconvenience to catastrophe. Protecting a corporation's information system and data has gained increasing management attention (Loch, Carr, and Warkentin 1992). The information security methods mostly used are checklists and standards, risk management (RM), and others (Siponen 2005).

2.2.3.1 Information Security Checklist and Standards

The information security checklist and standards aim to capture the best practice and put it in a list. Research from CERT pointed out the following:

“There are no widely accepted (de facto or de jure) standards of best practice (with the possible exception of ISO 17799 [ISO 00b]), metrics for characterizing security performance against some measure of adequacy, or industry-accepted benchmarks. However, there is an ever-growing number of guidelines and checklists that identify practices that are considered acceptable by most professionals, thus passing the test of reasonable practice.” (Allen 2005)

The International Standards Organization ISO/IEC 17799 is often cited as one of the most authoritative sources for defining and deploying an enterprise-wide approach to information security. According to ISO 17799,

“Critical success factors: Experience has shown that the following factors are often critical to the successful implementation of IS within an organization:

- Security policy, objectives, and activities that reflect business objectives
- An approach to implementing security that is consistent with the organizational culture
- Visible support and commitment from management
- A good understanding of the security requirements, risk assessment, and risk management
- Effective marketing of security all managers and employees
- Distribution of guidance on IS policy and standards to all employees and contractors
- Providing appropriate training and education
- A comprehensive and balanced system of measurement which is used to evaluate performance in IS management and feedback suggestions for improvement.”

Among the critical successful factors listed above, risk assessment is a critical task because measurement can help us to understand the problem with precision. As Tom DeMarco stated, “You cannot control what you cannot measure.”

2.2.3.2 Risk Assessment

Risk is assessed by identifying the threats and vulnerabilities, and then determining the likelihood and impact for each risk. As straightforward as it sounds, risk assessment is a complex process. Most of the risk assessment processes fall in the following framework, which is shown in Figure 2-2 (Stephenson 2004): first, identify the purpose of risk assessment and the work scope; second, evaluate risks based on threat and vulnerability identified and information of the likelihood of the occurrence and impact of the risk; third, identify possible measures to reduce the risk and evaluate them; finally, document the whole risk assessment processes for the review

of a high management team and in support of the management decision on investment in security.

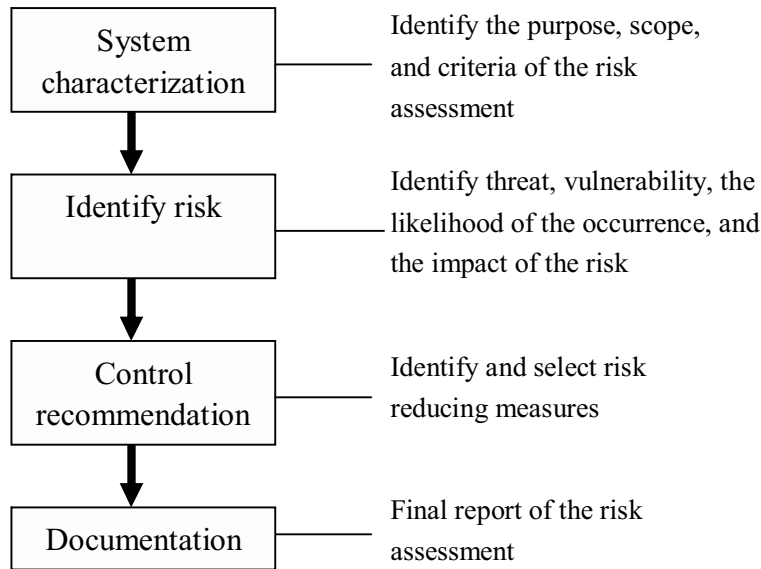


Figure 2-2 Typical framework of risk assessment

Many different methodologies and tools exist for risk assessment. Some of them are qualitative, while some are quantitative. The choice of a qualitative measurement vs. a quantitative measurement is dependent on the organizations' characteristics. Both of the approaches have their own advantages and disadvantages.

Qualitative risk assessment

Here, we use the methodology developed by the NIST called the "National Institute of Standards & Technology Methodology" as an example to illustrate how qualitative risk assessment is conducted. This methodology requires nine steps for risk assessment, as listed below (Stoneburner, Goguen, and Feringa 2002).

- Step 1 System Characterization
- Step 2 Threat Identification
- Step 3 Vulnerability Identification
- Step 4 Control Analysis
- Step 5 Likelihood Determination
- Step 6 Impact Analysis
- Step 7 Risk Determination
- Step 8 Control Recommendations
- Step 9 Results Documentation

We can see that these nine steps fit well with the framework. Step 1, Step 8, and Step 9 correspond to box 1, box 3, and box 4 in the framework respectively. Steps 2 to 7 all work for risk identification, which correspond to box 2 in the framework. We will look into the details of these steps.

Step 2 is to identify threat. Threat is identified from the source of threat, motivation, and threat action. For example, the source of a threat is an insider; the motivation is monetary gain; and the threat action is fraud and theft. For each threat source, the vulnerability in the system is identified (step 3). To derive an overall likelihood rating that indicates the probability a potential vulnerability may be exercised, the implementation of current or planned controls must be considered. This is why step 4 is needed.

Having investigated threat, vulnerability, and the controls in the system, the likelihood that a potential vulnerability could be exercised by a given threat-source can be categorized as high, medium, or low. (Step 5)

Table 2-1 Likelihood definitions

Likelihood Level	Likelihood definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede the successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

(Source: “Risk Management Guide for Information Technology Systems” from NIST)

Step 6 is to determine the adverse impact resulting from an incident. The adverse impact of a security incident can be described in terms of loss or degradation of integrity, availability, and/or confidentiality.

Table 2-2 Magnitude of Impact Definitions

Magnitude of impact	Impact definition
High	Exercise of the vulnerability (1) may result in the high cost loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

(Source: "Risk Management Guide for Information Technology Systems" from NIST)

Based on the likelihood of threat and the magnitude of impact, a risk-level matrix can be developed to measure risk.

Table 2-3 Risk-level matrix

	Magnitude of impact		
Likelihood of threat	Low	Medium	High
High	<i>Low</i>	<i>Medium</i>	<i>High</i>
Medium	<i>Low</i>	<i>Medium</i>	<i>Medium</i>
Low	<i>Low</i>	<i>Low</i>	<i>Low</i>

For high risk, there is a strong need for corrective measures. The existing system may continue to operate, but a corrective action plan must be put in place as soon as possible. For medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time. For low risk, the management team could determine whether corrective actions are still required or decide to accept the risk.

The main advantage of qualitative risk assessment is that it prioritizes the risks and identifies areas for immediate improvement. The disadvantage is that it does not provide specific quantitative information on the magnitude of the impacts, therefore making cost-benefit analysis difficult. For business organizations, decisions on investment are mostly based on cost-benefit analysis and return on investment (ROI)

calculation. Quantitative measurement is needed to enable defensible management decisions (Ryan and Ryan 2008).

Quantitative risk assessment

Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. The assumption is that the impact of an incident could be measured in terms of monetary costs, and so could risk. Some impacts such as lost revenue, cost of repairing the system, or expenses required to correct problems are originally recorded as monetary cost. Other impacts such as loss of public confidence, loss of credibility, or damage to an organization's reputation are not directly measured in cost. However, they can be translated into monetary cost with estimation of revenue loss and cost required to make up for the adverse effect.

The process of quantitative risk assessment is similar to that of qualitative risk assessment. The only differences exist in determining the "likelihood of occurrence" and the "impact magnitude": instead of qualitatively leveling them in qualitative risk assessment, in quantitative risk assessment, the "likelihood of occurrence" and the "impact magnitude" have to be determined with a numerical figure. The risk is then quantified as: $\text{Risk} = \text{likelihood of occurrence} * \text{potential impact}$

The "likelihood of occurrence" should be measured for a certain period, in most cases one year. It is sometimes referred to as the "Annualized Rate of Occurrence." "Potential impact" is the expected value of a single loss. As a product of the likelihood of occurrence and potential impact, risk is measured as the "Annualized Loss Expectancy." If one investment in information security can reduce the annualized loss expectancy more than its cost, then this investment is financially justified. On the contrary, if one investment costs more than the reduction of annualized loss expectancy, then this investment is financially unjustifiable.

The benefit of quantitative risk assessment is that it provides financial bases for decision making. The disadvantage is the difficulty in evaluating the probability of occurrence and impact magnitude.

We cannot know with certainty the probability of occurrence because it concerns events that have not turned into incidents (most of such events go unnoticed).

Although we can still estimate the probability of occurrence, for sure, there is an estimation gap. If there are historical data, we will have more confidence on the estimation. Unfortunately, historical data are rare in the information security area.

The way to measure impact magnitude is mostly asset based, that is, based on the value of the asset, the potential impact of incidents can be determined. This requires the identification and evaluation of the information system asset. The information system asset could be an application, system, or information, which is hard to evaluate. Even if it is possible to evaluate the information asset, the estimation of the impact of an incident is quite uncertain. In this highly coupled system, an incident in one part of the system may cause damage in other parts of the system and even in other systems. It is hard to predict how many information assets will be damaged. Again, historical data could be helpful but they are, in most cases, not available.

The current method of quantitative information security risks analysis is not reliable. The evaluation of the frequency of incidents and consequence of incidents are both difficult, if not impossible. Statistical data on threats, numbers of attacks, and the consequences of attacks that are necessary reference for the evaluation are usually not available. It is difficult to find historical data to support quantitative information security risks analysis.

Workshop-based risk assessment

Faced with the data problem, some researchers have developed methods to involve internal experts in risk assessment. The experience and knowledge of internal experts are assumed to be more reliable sources for risk assessment.

The Software Engineering Institute (SEI) of Carnegie Mellon University developed the Operationally Critical, Threat, Asset, and Vulnerability Evaluation (OCTAVE) process. OCTAVE is workshop-based rather than tool-based, which means that rather than including extensive security expertise in a tool, the participants in the risk assessment are the ones who understand the risk of the organization.

There are three phases in the workshop. Phase 1 gathers knowledge of the senior management, operational area management, and staff to create threat profiles. Phase 2 gathers knowledge from the operational area managers to identify key components

and evaluate selected components. Phase 3 gathers knowledge from the staff to conduct risk analysis and develop protection strategy.

Going through these three phases is a demanding process with a series of workshops involving a high, middle management team and operational staff. OCTAVE Allegro offers a streamlined process that is specifically aimed at information assets and their resiliency (Caralli et al. 2007).

Thomas Peltier has created a more cost-effective method for risk assessment: the Facilitated Risk Analysis and Assessment Process (FRAAP) (Peltier 2005). This methodology emphasizes that the external expert is only the facilitator, and it is the user community who owns the risk analysis and assessment. Acting in the owner capacity, the management and staff get the opportunity to see the risks in the business process in the facilitated workshop.

The FRAAP's main session (facilitated workshop) is only four hours with 15 to 30 client representatives. The final report will be ready in several working days after the main session. The final report is a comprehensive risk assessment document wherein the threats, risk levels, and controls are documented. It also includes an action plan created by the owner of the problem.

The FRAAP requires fewer resources from the client, which is a big advantage. Another advantage is that it creates ownership of security policy, which may help in the implementation of the result. Attention is needed to avoid bias, which could arise from choosing the participants for the workshop and during the main facilitated workshop.

Nevertheless, such a workshop-based methodology is still an improvement. It involves people within the organization who have experience and situational knowledge (risk picture specific to this organization). As Stephenson said,

“The desired future state of risk management, given the practicalities of cyber space as it exists today, is that we can be proactive in managing risk, managing the elements of risk and managing incidents. A first step towards that objective is to view the enterprise and its security measures holistically. We must stop thinking in terms of risk analysis, vulnerability assessment,

incident response, etc., as separate, mutually exclusive, functions. They are not. Everything that impacts the enterprise impacts its security. Therefore, we must deal with everything in the enterprise” (Stephenson 2004).

2.2.4 Information Security during Operation Transition

Stephenson’s observation “everything that impacts the enterprise impacts its security” is probably true given the dependence we have on computers and networks to perform daily routine tasks. In the case of this study, the organization’s operation is transitioned from traditional, platform-centric, to Integrated Operations. The organization will face many challenges during the operation transition. It is a complex, long-term, and dynamic process with feedback, delays, and trade-offs (see section 3.1), among others. The risk picture will change along the way, which makes the above-mentioned risk assessment methods even less relevant. The workshop-based risk assessment needs experience and situational knowledge, which are not available for this study. We are looking into a future situation which differs largely from the current one. Even the internal staff and management do not have experience and adequate knowledge about the future. We need a methodology that, instead of looking at the existing behavior (experience and situational knowledge), can capture the fundamental structure of the system. Thus, we can use this structure to investigate the behavior of information security risks during the operation transition. We propose to apply system dynamics to this research. System dynamics build simulation models are based on the causal relationships, that is, the fundamental structure of the system under study. Such structure rules system behavior. If the system structure is correctly portrayed by the model, the simulated model behavior shows the future behavior of the system with confidence. In such a way, we can study the future behavior of a system. Therefore, system dynamics is a plausible candidate for this study. In the next chapter, we will explain in detail the reasons why system dynamics is chosen as the research methodology.

2.3 Closing Remarks for Chapter 2

As we have reviewed, the methods for mitigating information security risks have evolved in the past five decades. More and more researchers have realized that technology alone is not enough to address the problem. Human and organizational factors play a big role in improving information security. The awareness of the

importance of the economics of information security has emerged recently (Wang, Chaudhury, and Rao 2008; August and Tunca 2008; Schneier 2008; Andersen and Moore 2006; Anderson 2001). This is a young principle that established since year 2000. “People have realized that security failure is caused at least as often by bad incentives as by bad design” (Andersen and Moore 2006). Therefore, the tools and concepts of game theory and microeconomic theory are becoming a research interest.

At the same time, more and more organizations have recognized the need to improve information security. Information security is becoming a factor that helps achieve an organization’s mission. Various methods exist for assessing information security risks. For different organizational situations, missions, and purposes, a different methodology should be used. In our case, upon the start of a long-term transition to a new operation, where no historical data is applicable for assessing risk, we find it important to systematically understand the transition process and how it will affect information security. System dynamics is a suitable method to investigate long-term changing processes. Therefore, we propose to use system dynamics as a research method. Reasons for choosing system dynamics is explained in detail in next chapter.

3 Methodology

In Chapter 1, we described our case: the development of information security risks during a transition from traditional to Integrated Operations, and raised our research questions:

- What is an appropriate speed for the transition to Integrated Operations considering the trade off between financial gains and information security risks?
- How does resource allocation during operation transition affect the effective use of new technology and the information security risks?
- How do management decision rules on investment in incident response capability affect the security risks?

In Chapter 2, we reviewed the existing literature on information security research. The current research methods are not suitable for answering the research questions because they do not consider the problem in a dynamic and integrated perspective. To investigate the problem at hand, system dynamics, a method especially designed to tackle problems in dynamic complex systems, is proposed.

The selection of a methodology is dependent on the nature of the problem being investigated. Therefore, in the first part of this chapter, we analyze the characteristics of our case and explain how system dynamics could be used to address these features. In such a way, we justify the selection of system dynamics as a research method. In the second part of this chapter, we explain how this research is designed i.e. how system dynamics is applied in the research.

3.1 The characteristics of the case under study

We study information security risks during the transition to Integrated Operations. Repenning studied the literature that speaks to the question of what processes determine the effective use of technological innovations. He concluded that all the literature regard the implementation of new technology as a dynamic process involving the complex interaction of multiple factors (Repenning 1999). Below we will analyze the characteristics of the operation transition in detail and explain how system dynamics can be used to tackle problems with such characteristics.

3.1.1 Structural characteristics: Dynamic

The term *dynamic* is defined by the Merriam Webster Online Dictionary as “marked by usually continuous and productive activity or change.” In other words, when a system changes over time, it is a dynamic system.

In our case, the transition to Integrated Operations is a mechanism that causes changes: twenty traditional work processes are to be replaced by new work processes. New work processes and knowledge have to be introduced and integrated across both onshore and offshore, and across the operators and vendors. Moreover, operation information must be shared, in almost real time, with all related parties. The operators offshore are not used to information sharing, as traditionally offshore platform has been a closed production environment. Profound and continuous changes must take place to realize the benefit of Integrated Operations (Integrated Work Processes: Future work processes on the Norwegian Continental Shelf 2005). Thus, operation transition is a dynamic process.

During the operation transition, new work processes are gradually introduced to the operators and over time the operators get familiar with what to do in the new way of operation. When the operators are familiar with new work processes and can work with them unassisted, we say that these new work processes are mature. The mature new work processes accumulate over time. Similarly, new knowledge is gradually introduced and acquired by the operators over time. There is an accumulation of mature new knowledge.

These changes and accumulations are best presented by the system dynamics concepts of stocks and flows. Stocks are the accumulations. They represent the system’s state. Flows represent changes, which accumulate in stocks (see Figure 3-1).

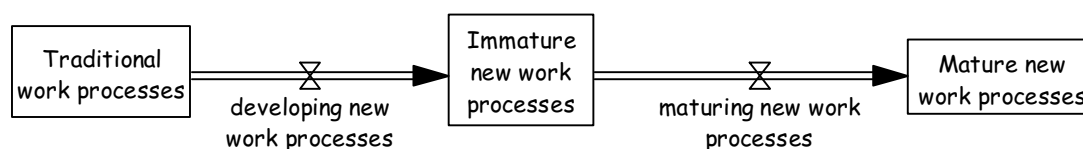


Figure 3-1 New work processes transition

As new work processes are developed and implemented, traditional work processes change into new work processes. At this stage, they are immature. It takes time and

effort for the new work processes to mature. The maturing of new work processes is a learning process whereby the operators get familiar with what to do in Integrated Operations.

A similar structure applies for new knowledge.

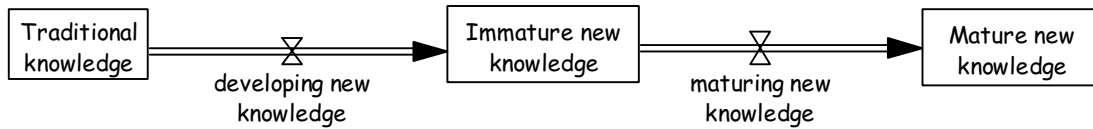


Figure 3-2 New knowledge transition

When new work processes are implemented, new knowledge corresponding to the new work processes is also introduced. Knowledge refers to the details of how to work with the new work processes. At the beginning, the operators cannot grasp all the details well. For example, they know what to do but do not understand why to do in such a way. Such stage is named immature knowledge. The maturation of new knowledge takes time and effort too. It is a learning process whereby the operators grasp how to work efficiently, why to do in this way and how to handle different situations in Integrated Operations.

The system dynamics stock and flow structure is fundamental to capture dynamics. It represents how state of system changes over time. If there is no stock, there is no state of the system. If there is no flow, there will be no change of the stock and thus, no dynamics. The stock and flow structure is able to illustrate how different development and maturation rates (developing new work processes, maturing new work processes, developing new knowledge, maturing new knowledge) affect the state of the system (traditional work processes and knowledge, immature new work processes and knowledge, mature new work processes and knowledge) on the Brage platform. The new work processes and knowledge and their maturity are identified as the key factors influencing information security risks during operation transition. Therefore, using system dynamics help us investigate the change of information security risks during the operation transition.

3.1.2 Structural characteristics: Delays

Delays exist in most of the systems. It takes time to measure and report information. Likewise, it takes time to make decisions and for decisions to affect the state of a

system (Sterman 2000 p. 411). In our case of operation transition, for example, it takes time to learn the newly implemented work processes and acquire the related knowledge. Mature new work processes and mature new knowledge lag behind the introduction of new work processes and knowledge.

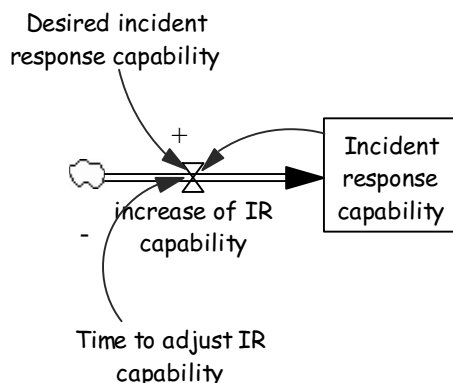
In system dynamics, delay is defined as a process whose output lags behind its input.



Figure 3-3 Delay

There are two types of delay: material delay and information delay. A material delay captures the physical flow of material through a delay process. An information delay represents the gradual adjustment of perceptions or beliefs (Sterman 2000 p. 412-433). In our case, an example of material delay is the building of incident response capability. When the management has decided to recruit people to improve incident response capability, it takes time to announce the opening, interview candidates, and find the right person. It also takes time to train the new employee for the specific work. Several months time is needed from the decision is made to achieve the capacity (see Figure 3-4 left). An example of information delay is the change of risk perception. In a traditional operation, the platform is a closed system and information security risks are relatively low. When moving into Integrated Operations, with the adoption of advanced ICT technology and network connection, information security risks are much higher. However, the perception about information security risks will not change immediately. When the staff on the platform observe incidents happening, they will gradually realize the higher information security risks they are now facing (see Figure 3-4 right).

Delay in building incident response capability



Delay in change of perception

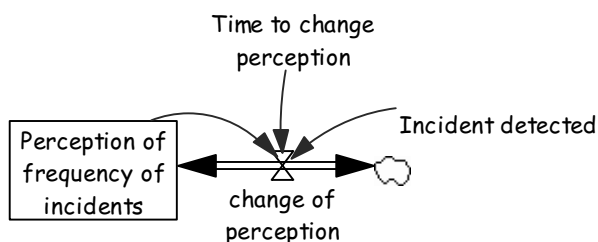


Figure 3-4 Examples of material delay and information delay
(NB: IR represents incident response)

The left part of Figure 3-4 is a material delay. The “*Desired incident response capability*” is a management decision on how much incident response capability is needed on the platform. It takes time (“*Time to adjust IR capability*”) to adjust the actual “*Incident response capability*” to the desired level. As mentioned above, the recruitment process usually takes several months. The lay-off process also takes several months, deciding whom to lay-off, negotiating with the employee on lay-off terms, providing time for hand over and etc. The right part of Figure 3-4 shows an information delay. The “*Perception of frequency of incidents*” is formed based on the “incident detected”. (Undetected incidents are latent, which will not affect perception). The perception is gradually adjusted (over the “*time to change perception*”). The first time that unusually many incidents are detected, the staff may consider such occurrence as occasional. But when this happens again and again the staff will perceive the increasing frequency of incidents.

As the decision to invest in incident response capability is based on perception of risks (“*Perception of frequency of incidents*”), the information delay could cause underinvestment or overinvestment. Moreover, the material delay of building incident response capability additionally slows down the adjustment of incident response capability. When incident response capability is inadequate, the delays in adjustment will leave the Brage platform insufficiently protected for months, which increase the possibility of severe incidents occurring.

Delays are important elements of a dynamic system. Delays create distance between cause and effect in time and sometimes introduce instability and oscillation to the system (Sterman 2000 p. 410). In our case, delays in learning new work processes and acquiring new knowledge make the system vulnerable; and delays in perceiving information security risks and building incident response capability can make incident response capability inadequate, leading to severe incidents. Delays cannot be neglected when we consider information security risks during the operation transition.

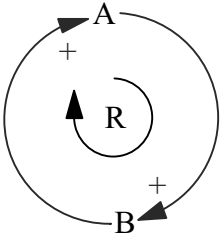
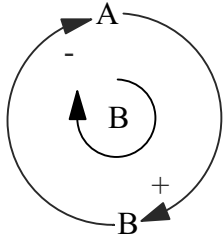
3.1.3 Structural characteristics: Feedback

Feedback is the process whereby an initial cause ripples through a chain of causation to ultimately re-affect itself (Roberts et al. 1981). This chain of causation is sometimes referred to as a closed loop, or a feedback loop.

During the operation transition, the changing factors are interrelated by a relatively large variety of relationships, many of which form feedback relationships. For example, the more new work processes the operators learn, the more experience they have working with new work processes; and the faster they could learn the new work processes. This feedback loop works virtuously toward a successful operation transition. However, there is another feedback loop that counteracts with this one: a diminishing return on investment in learning. The more new work processes the operators have learnt, the less new work processes are left for learning, leaving less potential for further learning to take place. Thus, the learning of new work processes will be reduced. Besides these two examples, there are other feedback loops. Identifying these feedback loops is a key to understanding the mechanism of the operation transition.

The fundamental perspective of system dynamics is that the behavior of complex systems over time is caused by the interrelationships among system components and feedback loops within the system (Sterman 2000 p. 12). There are two types of loops, namely reinforcing loop and balancing loop. Details are summarized in the table below:

Table 3-2 Reinforcing loop and balancing loop

Feedback loops	Reinforcing loop	Balancing loop
Graph representation		
Definition	Trace the effect of a small change in one of the variables as it propagates around the loop. If the feedback effect reinforces the original change, one has a reinforcing loop (Sterman 2000 p. 144).	Trace the effect of a small change in one of the variables as it propagates around the loop. If the feedback effect opposes the original change, one has a balancing loop. (Sterman 2000 p. 144)
Behavior	Exponential growth Exponential decay	Goal seeking Oscillation (with delay)

These two types of feedback loops can be well understood for themselves. However, a system may have many feedback loops, and their overall impact is often difficult to predict with the unaided mind. The system dynamics model captures all the feedback loops related to the problem under investigation, which helps to understand how the system's behavior arises from the interaction of these networks of feedback loops (Sterman 2000).

3.1.4 Structural characteristics: Nonlinearity

In social organizational systems, nonlinearity is often observed. There are two types of nonlinearity: the nonlinear effect of one variable on another variable and the nonlinear interaction between variables.

Effects are often disproportional to causes under which they happen. For example, when a new work process is implemented, learning takes place. The rate of learning is not linear. It is greatest at first when "ignorance" is greatest; it decreases as ignorance decreases. When most parts of the new work process have been learned, and there is little left to learn, the learning rate approaches zero. This type of nonlinearities has

been recognized for centuries; however, they are not widely used in models because precise quantitative data for nonlinear functions do not always exist. Such non-linear functions are mostly simplified as linear function by, for example, regression method. Such simplification might work for research with short-term perspective. However, to investigate the long-term development of a problem, such simplification might cause problems.

In system dynamics models empirical nonlinear relations are mostly captured using table functions, where the relationship is specified as a table of values for the independent and dependent variables.

Table for effect of X on Y = $(X_1, Y_1), (X_2, Y_2), \dots, (X_n, Y_n)$

There are ways to make the estimation of nonlinear relationship realistic and robust. For example, identify reference points, check the extreme condition, specify the domain for the independent variable, and discover the plausible shapes for the function (Sterman 2000 p. 554-559).

The appropriate shapes and values for nonlinear functions draw on all available information, both qualitative and quantitative. The information can be gleaned from various sources, including statistical studies, fieldwork, interviews, considerations of extreme conditions, and physical laws. The nonlinear relationship could also be tested through sensitivity tests.

The other form of nonlinearity encompasses the non-linear interaction between variables. For example, multiplication: $C = A * B$ (see Figure 3-5). C is the multiplication between two variables, A and B, where one of them, A, typically originates from a part of a system (A-D-E) while B originates from a different system (B-F-G). The implication is that the value of one variable, B, determines the impact that the other, A, has (on C). Thus the value of C is an interaction of the subsystems that gives to the values of A and B, respectively, - they synthesize in the production of a value for C. In short, subsystems interact through and only through nonlinearity.

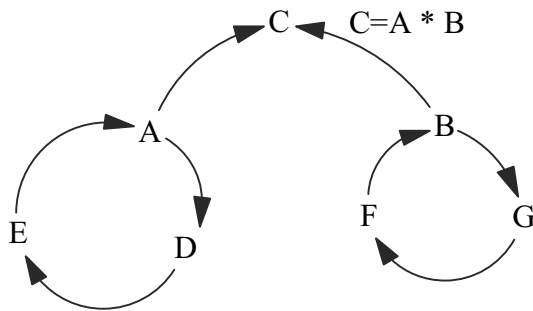


Figure 3-5 Subsystems interact through nonlinearity

For example, the incident cost is calculated as the product of frequency of incidents and severity of incidents. Frequency of incidents is mainly affected by the operation transition, which determines how vulnerable the system is; while the severity of incidents is mainly affected by the incident response capability, which determines how incidents are handled. Thus, the behavior of incident cost is the result of an interaction of the subsystems that generate the values of frequency of incidents and severity of incidents. Because the frequency of incidents and severity of incidents change through different mechanisms, the cost of incidents shows non-linear behavior.

A system dynamics model usually contains many feedback loops. Variables belonging to different feedback loops can interact with each other. In this way, system dynamics models are able to capture the non-linear interactions between variables.

3.1.5 Behavioral characteristic: Counterintuitive

Two structural reasons cause counterintuitive behavior. One is the existence of non-linear relationships. Our intuitive thinking is related to linear relationship, where effects are proportional to causes. For example, typically, people think that if the operators use more time for production, the throughput will increase proportionally. This is true in the cases where productivity is constant, such as production on assembly line. The longer the operators work, the more products they produce. However, during operation transition, the productivity is changing. Throughput is not linearly related to the time for production. $\text{Throughput} = \text{time for production} * \text{productivity}$. Productivity is determined by the subsystems of operation transition. More time for production means less time available to learn new work processes and knowledge. Without enough knowledge to operate the new work processes, operators

cannot fully realize the benefit of the new technology. The long-term productivity will be lower. Therefore, more time for production might cause less output in the long run.

The other structural reason that causes counterintuitive behavior is delay. Because of the time delay, the real cause could be distant in time to the effect. Our intuitive thinking is that efforts follow causes closely in time. For example, we often believe that if investment is made to increase incident response capability, the incident response capability will increase very soon and the severity of incidents will decrease as more incident response capability is in place. However, the building of incident response capability takes time. As our analysis in section 3.2.2 shows, with information delays in changing the perception of risks and material delays in actually building up incident response capability, the adjustment of incident response capability is far slower than immediate. During this delay time, management might feel that their investment in incident response capability is not enough as the incidents are still not timely handled, and thus, make more investment. This leads to overinvestment in incident response capability. On the contrary, management might feel their investment in incident response capability is not worthwhile because the expected outcome has not been achieved. They might stop the investment. A right policy might be suspended because the (intuitively) expected result has not been achieved.

Without the understanding of the counterintuitive characteristics of a complex system, policies based on naïve intuition (current experience, limited insight) often fail or actually worsen the situation. This property of complex systems is known as policy resistance. “All too often, well-intentioned efforts to solve pressing problems create unanticipated side effects” (Sterman 2001 p. 3). System dynamics models capture the non-proportional responses and responses that change over time as a consequence of the state of the system itself. Using system dynamics models, we are able to reproduce the counterintuitive behavior and investigate the reasons for them. This helps us to form long-term sustainable policies.

3.1.6 Behavior characteristic: Trade-offs

The reason for the need of making trade-offs is mainly because the limited availability of resources. In a highly competitive world, enterprises seek tight cost control. Adding resources to one function, for example, production, probably means cutting

resources in other functions, for example, training. The improvement of performance in one function is at the expense of the performance drop (or less performance increase) in other functions. An optimal resource allocation is a common pursuit of most management.

The consequence of resource allocation decision might differ for short-term and long-term because of delays in the system. The operators spending more time for production will generate more output immediately. However, due to less time available to develop knowledge, in the long run, productivity will not be as high as in the scenario of having more time for learning. On the contrary, allocating more resources to training could lead to immediate throughput drop. But in the long run, productivity will be higher and so will the production throughput.

3.1.7 Other characteristics: Long-term perspective

Different time horizons dramatically influence the perception of the problem (Sterman 2000 p. 91). In this research, we are not assessing information security risks over a short period of time, for example, the next quarter or next year, in which case, traditional risk assessment method might be more suitable. Instead, we are concerned with the changes in information security risks over the entire transition period, that is, a 10-year time period. We are addressing policies that have long-term effects, such as how to allocate resources, or how to choose a proper transition speed. Because we are working with a long time perspective, we will need to include in our analysis relationships that span over long periods of time, i.e. carry effects through the system relatively slowly and that impact the system through feedbacks in the long run. In a short-term perspective, these relationships could be ignored. This long-term perspective contributes significantly to define the system we work with, its boundaries and appropriate method to be used. System dynamics, capturing the mechanisms (feedback, delay, nonlinearity) of how the states of the systems change over time, is thus a proper method for this study.

3.1.8 Other characteristics: Multidisciplinary

Consider the managers who are concerned with planning and decision making in matters of information security during the operation transition. To design policies and strategies, they must use disciplines as varied as computer networks, wireless

technology, information technology, cryptography, software, hardware, organization science, psychology, and law (Gonzalez et al. 2005). Competence in technology or any single discipline is insufficient for forming a high-leverage policy. The information security problem involves the interaction of technology, organization, and human behavior during the dynamic complex transition process. An integrated (comprehensive) understanding of the problem should constitute the basis for decision making. System dynamics has been used to investigate problems in various areas: business strategy, urbane planning, environmental studies, and etc. A system dynamics model is built on the causal structure of a problem. All the factors that are important to the problem will be included in the model. The model combines the knowledge of different disciplines. Therefore, system dynamics models can be used to address multidisciplinary problems.

3.1.9 Other characteristics: Lack of historical data

Reliable, empirical data is required in order to investigate a problem. Such data advance our understanding of the problem and serve as reference for our research effort. However, in the information security area, we seldom find relevant data:

“Unfortunately, relevant data on cyber-threats does not always exist, nor is existent data available, nor is available data without error or bias” (Rich et al. 2005).

Three reasons explain data shortage, reflecting a shortage of information for information security incidents (Andersen et al. 2004).

- First, successful information attacks depend, to some degree, on deception and surprise. Thus, attackers must conceal as much information as possible on their attacks in order to preserve the utility of their methods (Lipson 2002).
- Second, defenders of information assets are often overburdened. They are not motivated to do large-scale data collection activities. Data are generally collected only if they are useful for a specific defensive task, for forensic purposes, or for documenting relevant damage for legal proceedings.
- Third, data on attacks may be withheld owing to concerns over publicity, reputation, or worries about copycat activities.

Beyond the fact that scarce data exist for information security, in this case we are concerned with the operation transition, where time series data on the past cannot be

reference for future. What is more readily available is information on structure or information on what assumptions can reasonably be made about the underlying structure of the system at hand. This allows us to obtain a fundamental (structurally founded) understanding of the problem we face and will constitute the predominant information basis for this thesis.

System dynamics utilizes qualitative data to a great extent during the modeling process. It is the structure information that system dynamics models are based on. Below we will explain how qualitative information is used in different stages of model building based on the research from (Luna-Reyes and Andersen 2003).

The modeling processes can be grouped into four stages: model conceptualization, model formulation, model testing, and implementation.

Table 3-1 Modeling process

Stages	Qualitative data used
Model Conceptualization	Qualitative information are used to understand the system and the problem Reference mode could be qualitative
Model Formulation	Soft variable, non-linear relationship are formed based on qualitative information Some parameters are estimated based on qualitative information
Model Testing	Direct structure validation is qualitative. The evaluation of the model is qualitative
Implementation	Policy formulation is sometimes qualitative

During the model conceptualization stage, the modeler focuses on understanding a part of the real world where the problem is embedded. This is a highly qualitative process. Interviews, oral histories, and focus group discussions are potential techniques to be used. Sometimes, behaviors over time (reference modes) come in a quantitative form. However, it is more likely that reference modes are in qualitative forms. For example, the management might know that one variable will increase over the next several years but they cannot be sure about how much exactly the amount will be.

The model formulation stage is concerned with the mathematical representations of the model, which requires more numerical data. In cases where exact numerical data

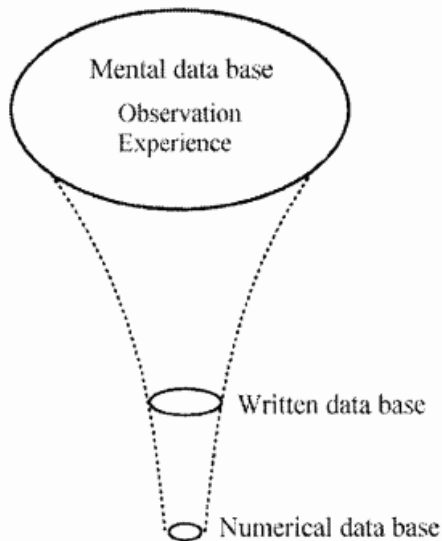
do not exist, such as in soft variables⁴ and in some nonlinear relationships, the measurement scale or table functions are built based on qualitative data. Some scientific researchers omit soft variables and simplify nonlinearities into linear functions because they feel unsettled with qualitative data. Yet, Sterman pointed out, “Omitting structures or variables known to be important because numerical data are unavailable is actually less scientific and less accurate than using your best judgment to estimate their values” (Sterman 2002 p. 523).

Model testing can be categorized into direct structure tests, structure-oriented behavior tests, and behavior pattern tests (Barlas 1996). Behavior pattern tests require numerical data and use formal/statistics tools. Such tests are more appealing to the general audience. However, experts in system dynamics have pointed out that behavior pattern tests cannot separate spurious behavior accuracy (i.e., “right behavior for the wrong reasons”) from true behavior validity. Therefore, the most important tests are direct structure tests that assess if the model structure is consistent with the real world. Such tests are highly qualitative in nature. “In most instances, the structure verification test is first conducted on the basis of the model builder’s personal knowledge and is then extended to include criticisms by others with direct experience from the real system” (Forrester and Senge 1980 p. 416).

Finally, the last step in the modeling process is implementation, which deals with policy design and evaluation. This is a qualitative process that requires discussion more than changing parameter values. Policy design includes the creation of entirely new strategies, structures, and decision rules.

Overall, system dynamics models largely depend on qualitative data, especially during model conceptualization. Information from people’s mind (mental database) is the largest source for model conceptualization in most cases. Early on, experts in system dynamics have noticed the importance to use the qualitative information in people’s mind and in written documents: not only because numerical data are scarce and cannot cover the related areas, but also because numerical data are more about system behavior while qualitative data are more about system structure and policies.

⁴ Compared to hard variables that can be measured with little error, soft variables are those that involve greater measurement errors or great measurement difficulties. For example, intelligence, happiness, satisfaction, and morale are all soft variables.



“As suggested by the figure, the amount of available information declines, probably by many orders of magnitude, in going from mental to written information and again by another similar large factor in going from written to numerical information. Furthermore, the character of information content changes as one moves from mental to written to numerical information. In moving down the diagram, there is a progressively smaller proportion of information about structure and policies.” (Forrester 1992 p. 72)

Figure 3-6 Mental, written, and numerical database

Source: (Forrester 1992)

During the model formulation, quantitative data play a more important role. However, even with limited numerical data, there are ways to make estimation based on qualitative data. Such estimation could be based on qualitative information from written database or mental database. Sensitive tests could be used to test the reliability of these estimated data. With the correct causal structure of the system, a system dynamics model can be simulated based on estimated data and through behavior and feedback analysis, one gets insights about the reasons behind the behaviors. Such insights can help to form high-leverage policies. That is the reason why system dynamics method still can be useful even if quantitative data are in scarce.

Moreover, experts in system dynamics have developed ways to use model-based intervention to elicit data (both qualitative and quantitative) from clients. One example is group model-building. It focuses on building system dynamics models with teams to obtain information, enhance team learning and to foster consensus (Vennix 1996; Vennix 1999; Vennix, Andersen, and Richardson 1997; Richardson, Andersen, and Luna-Reyes 2005; Richardson and Andersen 1995; Andersen and Richardson 1997; Andersen, Richardson, and Vennix 1997). Since we face severe data shortage in the information security area, we apply model-based interventions for model building and model validation. Below, we introduce the design of this research.

3.2 Research Design

In this research, a system dynamics model is used to represent hypotheses regarding the structural origin of the information security problem the client faces. The client is involved in the model-building process as an expert on the problem and it is primarily the client's understanding of the problem that the model is intended to portray. For that purpose, the model is used as a vehicle to elicit the client's expert knowledge (expertise), - so called model-based knowledge elicitation. The model not only constitutes a knowledge repository. When subject to simulation it may be used to feed the behavioral consequences of the structural assumptions, represented in the model, back to the client. This process calls for a response from the client in the form of a behavior recognition. A failure to recognize the simulation results is part of a model validation process whereby the model must be modified until the client acknowledges the model and its behavior as a representation of its problem understanding and, thus, takes ownership of the model.

The process of this research will run iteratively. A series increasingly detailed model will be developed in stages. Each stage, model-based intervention will be conducted. With the elicited knowledge from the intervention, we will further develop the model. We will use the client as a resource of model improvement. The further stages we reach, the less changes of model behavior there will be—despite the fact that we will add new variables, new sectors and better data to the model. In such an iterative way, we prove the validity/robustness of the model. Below, we present the detail research plan.

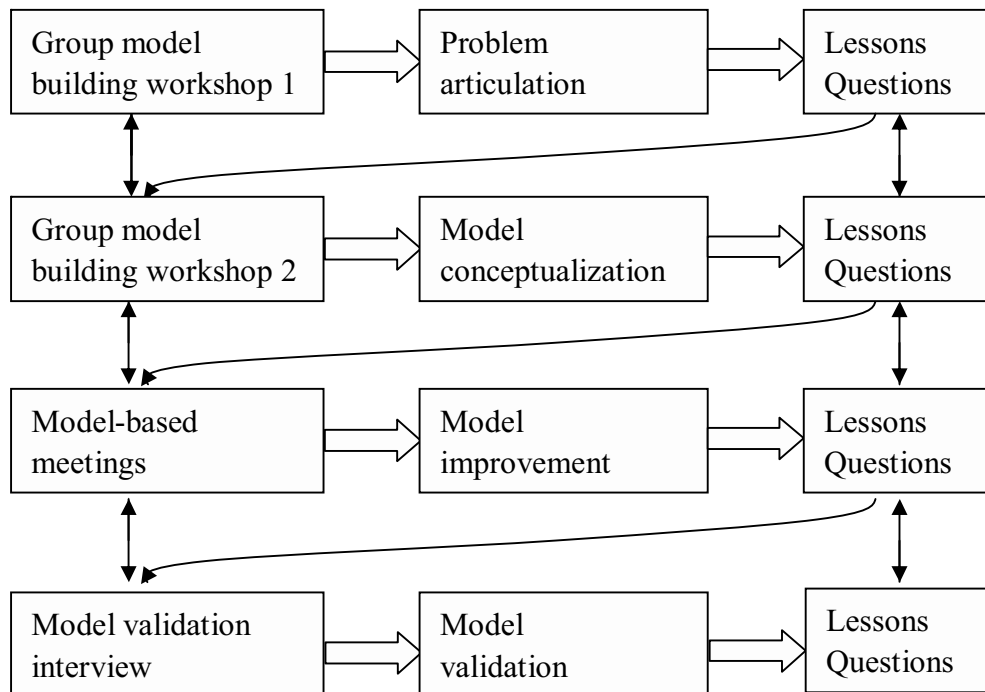


Figure 3-7 Research plan

The first system dynamics group model-building workshop articulates the dynamic problem that is to be addressed. “For a model to be useful, it must address a specific problem and must simplify rather than attempt to mirror an entire system in detail” (Sterman 2000 p. 89). In this process, the modeler seeks answers for questions such as, “What is the real problem, not just the symptom of difficulty?” or “What is the purpose of the model?” This is the most important step in the model-building process.

The second system dynamics group model-building workshop identifies the dynamic hypotheses. Dynamic hypotheses are working theories of how the problem arises. This means that the dynamic problem is explained with an endogenous view, that is, a feedback structure. Based on the dynamic hypotheses, a conceptual model is formed.

A series of model-based meetings are arranged to improve the model. In these meetings, we first present the structure of the model developed and its simulation results. This serves as a base for discussion. The client raises questions/comments about model structure and behavior. Some of them can be addressed immediately and our explanation helps the client to better understand the model structure and behavior. Some questions/comments point to additional structure for model development in the next stage. After the meeting, the model is updated according to client’s questions and

comments. When the model reaches to the next stage, another model-based meeting will be held. The client's recognition of the model structure and behavior is one of the model validation procedures.

When the model is completed (reaching its boundary and no further development required), we perform standard model validation procedures. The direct structure tests and structure-oriented behavior tests are performed by the modeler. Due to the lack of historical time series data, standard behavior tests are not applicable in the case. We use interviews with experts as an alternative for model behavior tests. During the interviews, the model behaviors of different scenarios are shown to the experts. Recognition of the model behaviors adds confidence to the model, while failure to recognize simulation result must lead to model modification.

Given all the model-based interventions and model development, policies to mitigate information security during the transition to Integrated Operations are proposed. We use model simulation to compare the long-term effect of different policies. By analyzing these simulation results, we conclude the policies to reduce information security risks during the operation transition.

3.3 Closing remarks for chapter 3

Davis, Eisenhardt, et al. pointed out, "Simulation is particularly useful when the theoretical focus is longitudinal, nonlinear, or processual, or when empirical data are challenging to obtain" (Davis, Eisenhardt, and Bingham 2007). The case under this study fits such profile. Information security risks issue arising during operation transition is a problem characterized by accumulation processes (causing the dynamics of the problem), associated delays causing the development to unfold at various rates, and a variety of nonlinearly interacting feedback loops. The result is a development over time that typically defies intuition and that includes trade-offs. This problem is multidisciplinary, - technical as well as social (organizationally) and calls for an integrated approach. Also it extends over a long time period and is therefore comprehensive (encompasses a multitude of long-term feedback processes). Finally, the problem domain is characterized by a scarcity of empirical time series and must be investigated from a fundamental perspective, based on a structural understanding of the system.

Because of the characteristics of the problem, we choose to use system dynamics as a research method. System dynamics is a method designed to cope with a dynamic system, which could capture the structural characteristics of feedback, delay, nonlinearity, and thus able to reproduce the behavior characteristics of counterintuitiveness and trade-offs. System dynamics is an interdisciplinary approach that offers a holistic view of the problem and with a long-term perspective. Moreover, it is able to deal with the data scarcity problem through model-based intervention with client.

We use system dynamics model-based intervention for the research to: 1) gather information from the client for model building; and 2) convey model insights to the client. The iterative process of model development and model-based intervention helps elicit more and better data. Such process also enhances learning, fosters consensus, and creates commitment (Qian and Gonzalez 2006).

4 Group model-building workshops: models and data

The design of this research is an iterative process of mode-based intervention and model development. At the beginning of this research project, two sequencing group model-building workshops were conducted to articulate problem and conceptualize model. We record the activities and outcomes of these two workshops in detail in this chapter.

The reasons for recording these two workshops in detail are two-fold. First, problem identification and model conceptualization are two key steps during the model building process. As the purpose of the model is to address the client's problem, a clear problem definition is the base for model building. The model should only include the aspects that relevant to the problem. Model conceptualization forms basic dynamic hypotheses of the problem, which will be the base for model structure. The client is the one who knows the problem best. It is primarily the client's understanding of the problem that the model is intended to portray. Second, as we have discussed in chapter 3, few data on information security incidents are available and relevant to this research. As a result, we use group model-building workshops to elicit information (both qualitative and quantitative information) from our client. Thus, it is important to document the two group model-building workshops, illustrating what data we obtained, how the problem was identified and how the model was conceptualized.

4.1 Introduction to system dynamics group model-building workshops

Almost since the inception of system dynamics, researchers in this area have involved the client in the model-building process. In his first book on system dynamics, Forrester pointed out the need to access the mental database of managers to be able to construct system dynamics models of strategic problems in business (Forrester 1961). Vennix summarized three reasons for client participation (Vennix 1996): first, to

capture the required knowledge in the mental models of the client group; second, to increase the chances of implementation of model results; and finally, to enhance the client's learning process.

The concept of system dynamics group model-building emerged in 1980s, in two different places at almost the same time. In the Netherlands, Vennix and Gubbels started experimenting with the process of model construction that involved client group. In a series of projects, several ways of working with client group emerged. Meanwhile, in the United States, Richardson in University at Albany, State University of New York (SUNY) worked with the Decision Techtronics Group to produce the first case of what we now call group model-building (Andersen et al. 2007).

Since then, system dynamics group model-building has made considerable progress. It has diffused from its origins in public sector to become a consulting practice used in private, public, and not-for-profit organizations (Richardson, Andersen, and Luna-Reyes 2005). Building models directly with client groups has become increasingly common in the field of system dynamics.

The system dynamics group model-building practice has involved a cycle of theoretical reflection, practice with client, and continuing updating of the method. These efforts led to a more detailed description of the different roles in working with teams (Richardson and Andersen 1995) and the notion of scripts for group model-building, i.e., refined pieces of small group processes, which chained together, direct the stream of group activity in group model-building sessions (Andersen and Richardson 1997; Andersen et al. 1997). The five different roles in group model-building facilitation are summarized in Table 4-1. For detailed information, see Richardson and Andersen (1995).

Table 4-1 Five different roles in group model building

Roles	Function	Activities	Characteristics
Facilitator	Group facilitator and knowledge elicitor	Pays constant attention to group process, the roles of individuals in the group, and the business of drawing out knowledge and insights from the group	Most visible, constantly working with the group
Modeler/reflector	Model developer	Thinks and sketches, and reflects information back to the group, restructures formulations, exposes unstated assumptions	Mostly work on one's own, except when reflecting information back to the group
Process coach	Process watcher	Observes the dynamics of individuals and subgroups within the group	Work invisible, serves the facilitator
Recorder	Note taker	Writes down and sketches the important parts of the group proceedings	Works on his/her own
Gatekeeper	Group model building workshop initiator	Helps frame the problem, identifies the appropriate participants, works with the modeling support team to structure the sessions, and participates as a member of the group	A person within, or related to, the client group who carries internal responsibility for the project

The facilitator and the modeler should be seasoned system dynamists. The recorder should have enough knowledge about system dynamics so that he/she knows what to record. The process coach does not necessary know system dynamics. Some of these five roles may be combined, or distributed among the consultants and the clients in a group model building project. But experience show that all five roles or functions must be present for effective group support.

The different group activities in group model-building could be categorized into four types of exercises. These exercises are summarized in Table 4-2. For more detailed

information about these activities, see Andersen and Richardson (1997).

Table 4-2 Group model-building exercises

Exercises	Activities	Purpose
Divergent tasks	Individuals or small subgroups generating lists of ideas or concepts	To obtain as many ideas as possible from participants, such as reference modes, policies, etc.
Convergent tasks	Members work together as a plenary group or as the need arises; they work in big subgroups first and then report to the plenary afterwards	To form a consensual view reflected in the model structure design, problem description
Ranking and evaluation	Each member is given a fixed number of votes to cast in favor of ideas, concepts, and tasks	To identify the important ideas
Presentation	The modeler/reflector presents and the clients sit and listen	To reflect on the achieved work and recap the dynamic insights

Depending on the purpose of the group model-building workshop, various activities are undertaken. The schedule of the group model-building workshop is typically planned out in 15 minute blocks, with the task and group technology specified in overview and detail.

Assigning the five different roles to skilled persons and planning the schedule carefully provides a more effective group process. However, executing a group model-building workshop is like a football coach executing a game plan: after compulsively detailed advance planning, there is always room for improvisation. The facilitation skills are of great importance. Therefore, experienced experts from SUNY Albany were invited as the facilitation team for the two group model-building workshops we conducted in our project. Below, we will report on them.

4.2 First AMBASEC group model-building workshop

The first AMBASEC group model-building workshop was held on May 25 and 26, 2005, in the University of Agder, Grimstad. Hydro had concerns and worries about

information security risks during the operation transition. But the problem had not been clearly stated. Thus, we decided that the first AMBASEC group model-building workshop should be devoted to gathering information and articulating the problem. The AMBASEC team, together with the Albany team, designed the agenda for the workshop, which included divergent and convergent exercises, ranking and evaluation exercises, as well as presentation exercises, all of which were carefully sequenced to make best use of the allotted two days so as to achieve the purpose of the workshop.

4.2.1 Purpose

The purpose of the first AMBASEC group model-building workshop was to articulate the client's problem. The main expected outcomes of the first group model-building workshop were to answer questions such as "What is the problem?", "What is the structure of the system causing the problem?" and to elicit both qualitative and quantitative information for further model development.

4.2.2 Participants

Fourteen persons from different parties, with different roles, participated in this workshop.

Client group:

Hydro: *Trond Lilleng (leader of the Integrated Operations project)*

IRMA: *Odd-Helge Longva, Stig O. Johnsen, and Maria B. Dahl (researchers in information security)*

AMBASEC: *Jose J. Gonzalez, Agata Sawicka, and Johannes Wiik (researchers in information security)*

Facilitation group:

AMBASEC: *Ying Qian (modeler), Stefanie Hillen, and Magne Myrtveit (process coach), Maren Assev (secretary)*

Albany: *David Andersen (facilitator), George Richardson (modeler), and Eliot Rich (recorder)*

Trond Lilleng from Hydro, three experts from the IRMA team and three experts from the AMBASEC project jointly served as client group in the workshop. The Albany

team and four experts from the AMBASEC project jointly served as facilitation group.

Only one person from Hydro (the leader of the Integrated Operations project) attended the first group model-building workshop. The plan was to have four to five people from Hydro. However, at a very short notice, Hydro informed us that not all of them could attend, owing to extremely high work pressure. The IRMA team has been working with Hydro for more than half a year on incident response management. They have accumulated information about the operation transition and information security issues in Hydro. The three experts from AMBASEC had extensive research in information security. Before the workshop, the purpose of this workshop had been clarified to the experts from IRMA and AMBASEC.

To prevent confusing the terms “client”, which refers to Hydro, with “client group”, which refers to the group of experts both from Hydro and from research institutes participating in the model-building workshop, we use the term “group members” or simply “members” to refer to the “client group.”

4.2.3 Exercises and data obtained

In this part, we introduce the exercises we did in the first group model-building workshop and the data we obtained from the exercises. We also provide an analysis on the process of exercises and/or on the data we obtained.

- Exercise 1: Presentation—General introduction about the projects

At the beginning of the workshop, representatives from AMBASEC, IRMA, and Hydro spent several minutes each to briefly introduce their project. The presenters were encouraged to classify their project goals, research methods and design, and other related information.

Analysis: This introduction exercise was scheduled at the beginning of the workshop to establish a common understanding of the interests and roles of the different parties in the workshop.

From the presentation, we obtained an overall view of the transition to Integrated Operations: how the traditional operation was on the offshore platform, how the Integrated Operations will be, the benefit of utilizing new technology and the concerns for operation transition.

- Exercise 2: Hopes and fears

“Hopes” and “fears” are expectations that participants have about the workshop. This is a divergent exercise: the group members were given pieces of paper to write simple phrases to express their hopes and fears (one on each piece of paper). The members were invited to write as many “hopes” and “fears” as they could think of. Then the pieces of papers were collected using the Nominal Group Technique—moving from one person to another and collecting one idea at a time. The collection continued for as many rounds as needed until all ideas are collected. The pieces of paper gathered were clustered on the wall, with similar ideas near one another.

Analysis: This exercise helps in three aspects. First, it is a group-forming exercise, allowing the group members to work and interact as a group. Second, it is important to know the “hopes” and “fears” of the members at the start point. Some hopes and fears concerned the rationale of the research project itself, providing clues on the possible future direction of the research. For example, there was a “hope” to “get a few really dynamically interesting cases” and a “fear” to “come up with artificial cases”. This showed concerns over the case, whether it was real and whether it was dynamically interesting. Some “hopes” and “fears” concerned the workshop process itself. For example, one “fear” was “too little time to be successful” (related to the workshop). For these, the facilitator would pay attention to. Third, “hopes” and “fears” could serve as checkpoints. At the end of the day or at the end of the workshop, the facilitator could return to this list to measure the progress of the workshop against the original goals.

- Exercise 3: Stakeholder mapping

Using a divergent exercise again, more than 40 stakeholders were identified. The pieces of paper were clustered on the wall according to the stakeholder’s influence and interest on the problem. The X axis and Y axis represents how much interest and

influence these stakeholders have on the problem, respectively. The high-influence/high-interest stakeholders, located at the upper right-hand corner of the X-Y frame, are the stakeholders we need to keep in close contact with during this project.

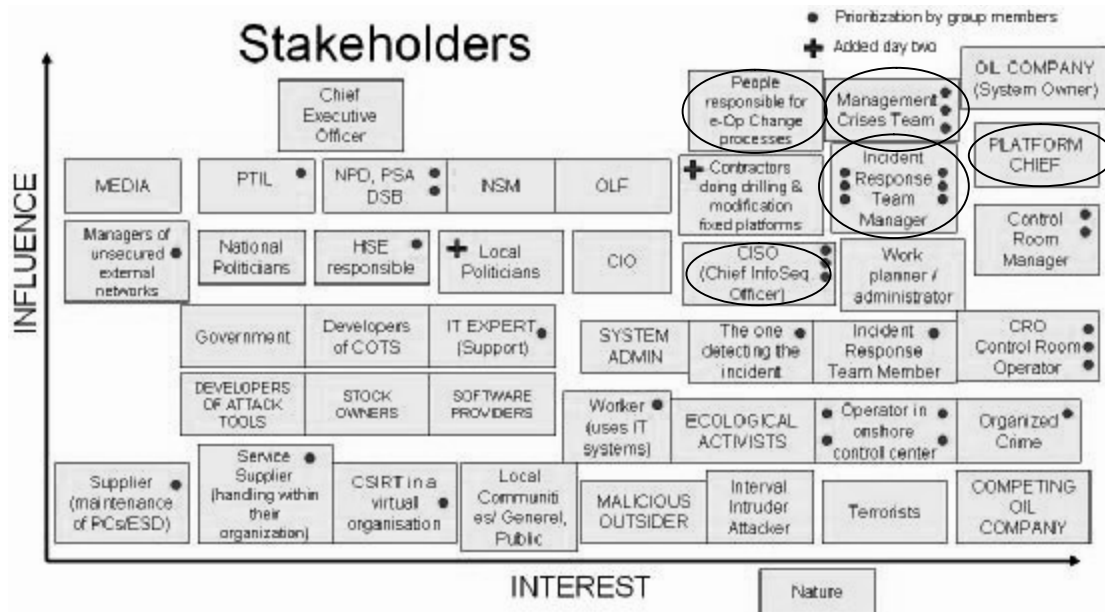


Figure 4-1 Stakeholder mapping

Source: OLF-IRMA-AMBASEC Group Model-Building Technical Report I May 2005 (Rich, Andersen, and Richardson 2005)

Then, a ranking exercise was conducted. The members were given five dots each, and were asked to place them on those whom they would like to invite for the next workshop. The stakeholders that got most dots were: the incident response team (6), control room manager and the operator (5), the operator in the onshore support center (4), chief information security officer (3), and management crisis team (3).

Analysis: The stakeholders who received most of the dots were located in the upper-right corner. It supported our assumption that they were the persons we needed to keep in contact with during our project. In the second workshop, the platform chief, the chief information security officer, and the person responsible for the transition to Integrated Operations, all attended. There was no crisis management team or incident response team on the Brage platform. Such function only exists onshore. The researchers in the IRMA team were investigating the issues of incident response management for the Brage platform. Therefore, they could be regarded as representatives for the incident response team on Brage. Stakeholders identified as having a high-influence and high-interest on the problem attended the second

workshop, which signified that we had the most relevant people for the second workshop.

■ Exercise 4: Behavior over time

Using another divergent exercise, nearly 40 variables and their behavior over time were identified.



Figure 4-2 Variables behavior on a time graph

Source: OLF-IRMA-AMBASEC Group Model-Building Technical Report I May 2005 (Rich, Andersen, and Richardson p.9)

Figure 4-2 is a general overview of the results on the wall. The variables identified are listed in Table 4-3. We do not discuss all the variables here, but only analyze those that are important for future model building.

Table 4-3 Key variables and their behaviors over time

Power of attack tools	Intrusions
Required attacker know-how	Number of known vulnerabilities in the software
Migration to virtual organizations	Migration to integrated operations
New technology and work processes	Integration of ICT systems
Migration to integrated operations	Net benefit
Number of incidents / per network	Focus on information security in organizations

Unsecured hosts	Incidents vs. openness and learning
Number of incidents	Average severity of incidents
Work load of CSIRTS	Complexity of IT systems
CSIRT workload and its ability to respond effectively	Danger of Internet break-down
Number of PCs connected to the Internet	Number of e-mails sent
Involved stakeholders in e-operations	Government regulations on security
CRO's compliance with security rules	Knowledge gap
Interest/influence of the general public and media economic actors	Organization's average knowledge about the ICT system
Density of vulnerability situational awareness	Dependency of IT systems
CRO's perceived risk	Unintended human errors
Number of known vulnerabilities in software	Density of vulnerability
Learning and forgetting	Safety and security culture
Handoff awareness	Threats

Analysis: Several variables describe the process of transition to Integrated Operations.

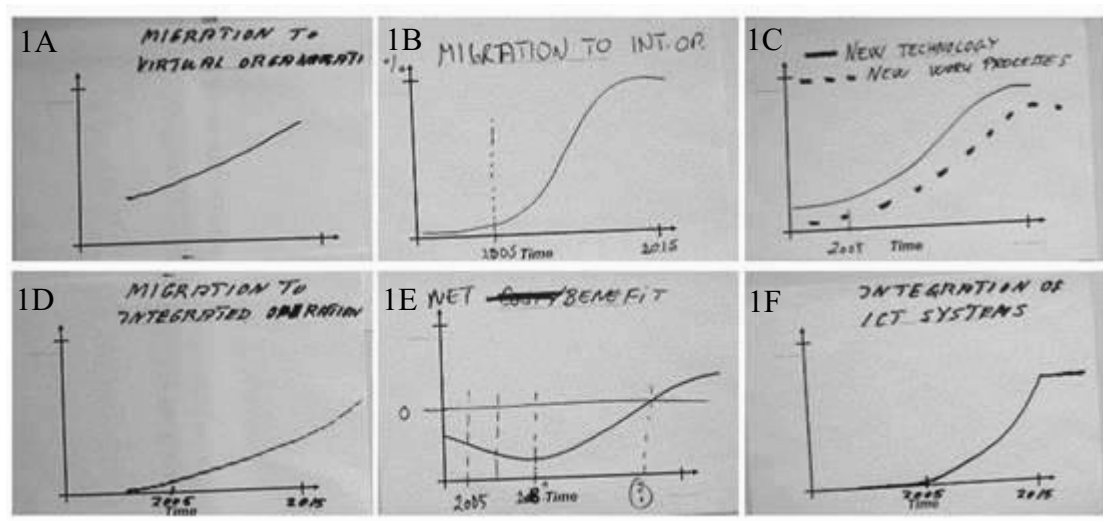


Figure 4-3 Variables related to the process of transition to Integrated Operations

The unit of the curves of 1A, 1B, 1C, 1D, and 1F is either the percentage of operation transition completed (as articulated in 1B) or the actual amount of new work processes implemented. Regarding the shape of the curve, 1A is almost linear, similar in shape with that presented on 1D. The difference of 1A and 1D lies in that 1D starts from 0 at time earlier than 2005 and in years after 2015 1D showed a slightly increasing growth rate. It seems that 1A only presents part of 1D's behavior, between

2005 and 2015. 1F shows a curve with increasing growth rate, starting in 2005. When the operation transition ends in 2015, the curve becomes a horizontal line. 1B is an S-shaped curve from 2005 to 2015. 1C shows an S-shaped curve similar to that of 1B. At the same time, 1C also shows the idea that technology advancement was faster than work process change. All these graphs show that the group members had consensus on the time period of operation transition, that is, from 2005 to 2015. They generally agree that the transition would start slowly, and then would speed up. Three of them (1B, 1C, 1F) mentioned that the transition speed will be reduced towards the end. 1E showed that in the first several years, the net benefit of Integrated Operations is negative, while, in later years, the net benefit of Integrated Operations becomes positive.

The following are variables on knowledge and vulnerability.

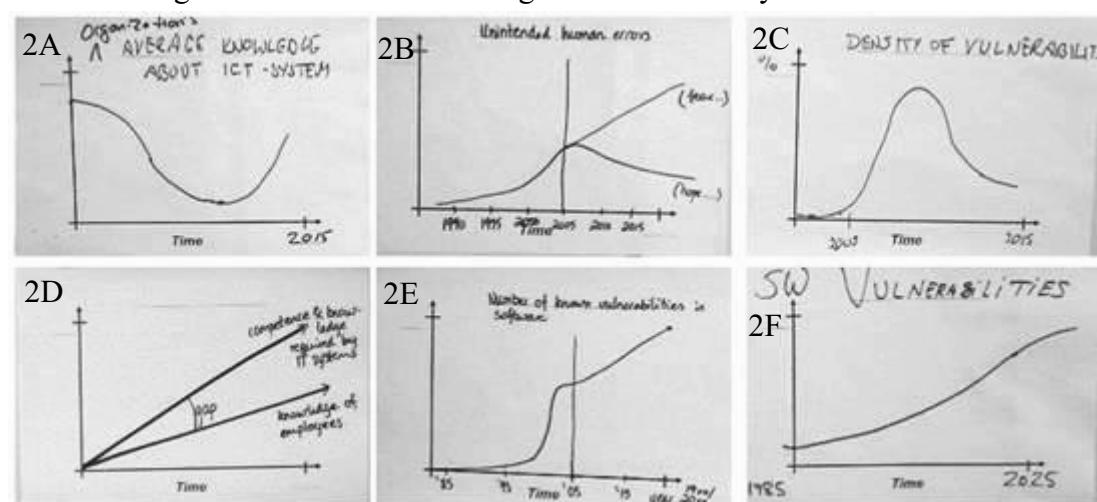


Figure 4-4 Variables related to knowledge and vulnerability

2A says that the organization's average knowledge about ICT system will first drop and then increase. This is because that the operation transition brings in new ICT system that the operators do not know about. The knowledge about the new ICT system will be acquired over time. 2B says that unintended human error increases in the past; after 2005, there is hope that it could decrease, and at the same time, there is fear that it could continue to increase. 2C shows that the density of vulnerability started to increase after 2005, only to decrease sometime later. The pattern is related to that of 1A. When the average knowledge of ICT is low, the density of vulnerability will be high; and when the average knowledge increases, the density of vulnerability will be low. 2D expresses the idea of a knowledge gap. The competence (knowledge)

required increases faster than the competence (knowledge) the operators acquire. As a result, although the operators are gaining more competence, the knowledge gap actually grows larger. Graphs 2E and 2F illustrate the vulnerabilities in software, both showing an increasing pattern.

The following are variables related to incidents.

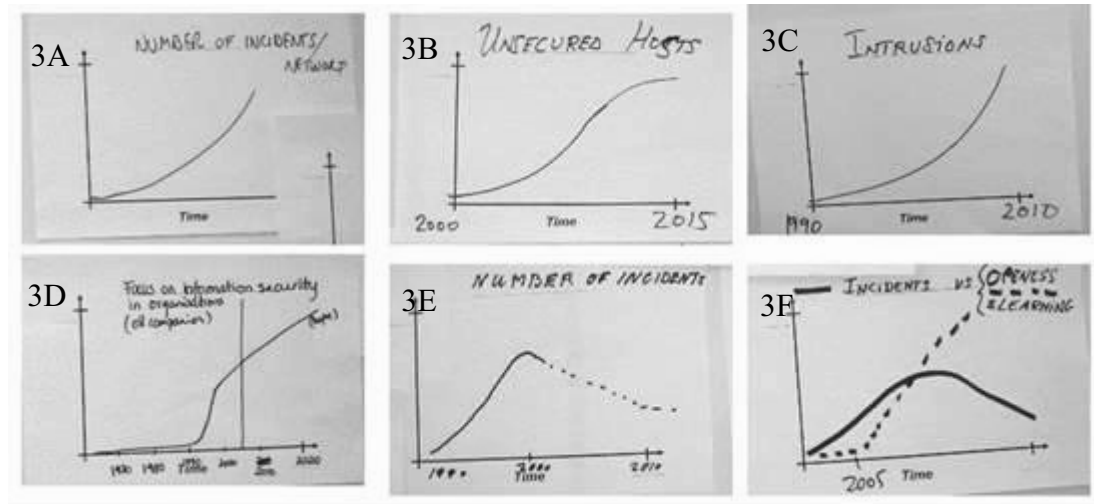


Figure 4-5 Variables related to incidents

3A and 3C show that the number of incidents and intrusions will grow with increasing speed. 3B shows that the unsecured hosts will grow in an S-shape. 3D shows an increased focus on information security in organizations, especially oil companies. 3E and 3F both express the view that the number of incidents would increase and then decrease. 3F also shows the reason for the decrease, which is openness and learning. If people could openly discuss incidents and learn from them, the number of incidents would decrease. We found that what 3A suggests is different from what 3E and 3F suggests. One possible reason could be that the definition of “incident” for 3A is not the same as that for 3E and 3F. 3A defines it as similar to threats or intrusions, which might become incidents and might not. Threats will always increase as more people are using computers and Internet and the tools for attacks advances, while with proper protection, incidents might be reduced, as shown in 3E and 3F.

This exercise provided information important to our understanding of the transition to Integrated Operations, as well as the change in average knowledge, vulnerability, and incidents during the operation transition. Some graphs served as the reference modes for the model development. Some graphs were found to be of little relevance. For

example, learning and forgetting develops over a time scale of several weeks. This research focused on the process of operation transition that would take place in a 10-year period, and these short-term dynamics should, therefore, not be included. Government regulations, and human compliance were not the focus of this research.

During the exercise, group members sometimes came up with the same variable but with different behaviors over time. It could be that the same-named variables refer to different concepts. It could also be that different ideas about the time trajectory (behavior) of this variable existed. There were discussions about the behavior and definition of such variables. Identifying the disagreements, presenting different views from different members, and reaching a consensus through discussions altogether comprise a learning process. Even if consensus was not reached during the workshop, the discussion still pointed out where disagreements exist and where further research effort would be needed.

- Exercise 5: Policy mapping

Using another divergent exercise, the group members identified more than 30 policies, which were clustered on the wall.

Then a ranking exercise was conducted. The highest-ranking policies identified were monitor/measure risk change (auditing) (4), create formal CSIRTS (4), improve incident reporting (4), annual awareness champions measures on security culture (3), and higher level of security (3).

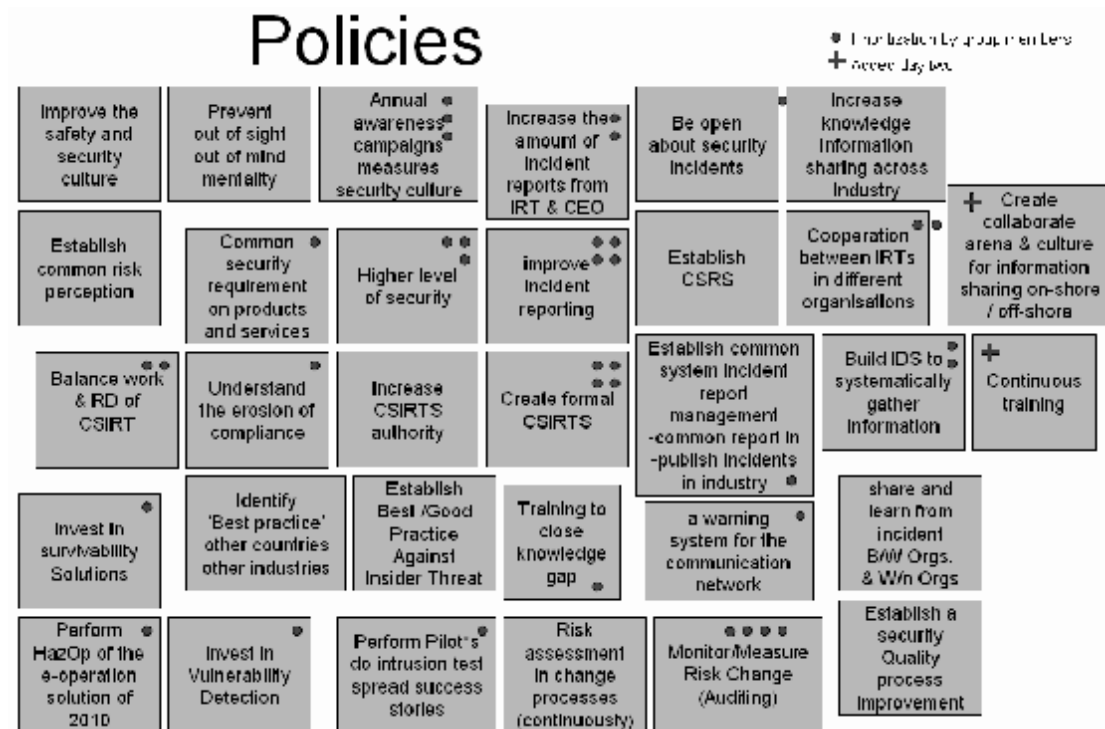


Figure 4-6 Policy lever mapping

Source: OLF-IRMA-AMBASEC Group Model-Building Technical Report I May 2005 (Rich, Andersen, and Richardson 2005 p.17)

Analysis: The group members came up with more than 30 policy statements. Some policies were technology solutions, such as “Invest in survivability solutions,” “Build IDS (Intrusion Detection System) to systematically gather information,” “Perform HazOp of the e-operation (Integrated Operations) solution of 2010,” and “a warning system for the communication network.” However, most policies were related to human and organizational issues. Two policies were related to training: “Training to close knowledge gap” and “Continuous training.” This implied that knowledge building during the operation transition might not be sufficient for the operators to work effectively. Three policies were related to the incident response team: “Create formal CSIRTS,” “Establish CSRS,” and “Increase CSIRTS authority”, which pointed out the need to establish a formal incident response team on the platform. It indicated the worry that the current incident response capability might not be sufficient to handle increasing incidents. Some of the above policies are tested using our model, which is documented in Chapter 8.

Not all proposed policies are the focus of this research. Two policies for risk assessment “Risk assessment in change processes (continuously)” and “Monitor/Measure Risk Change (Auditing)” were the research focus of the IRMA

team. Several policies were directed at incidents reporting: “Improve incident reporting,” “Increase the amount of incident reports from IRT & CEO,” “Be open about security incidents,” and “Establish a common system for incident report management.” This implied that incident reporting was not satisfactory. We confirmed this weakness during later communication with Hydro and IRMA. However, incident reporting is not the focus of this study. Another member of our research cell, Finn Olav Sveen, devoted his PhD work on incident reporting.

- Exercise 6: Dynamic stories

After several divergent exercises, a convergent exercise was conducted. The members were divided in two groups. Each group was asked to pick several pieces of paper from previous divergent exercises “stakeholders”, “behavior over time”, and “policies” to form a picture on how the operation transition develops. The story should have two versions—one “base run” without policy intervention and the “policy run” with policy intervention.

After intensive discussions, each group developed one dynamic story (two versions). The outline of the dynamic stories was written on a large piece of paper and was stuck on the wall, together with the associated stakeholders, behavior over time, and policies. A representative of each group presented the story to the plenary group.

The two stories developed were “Virus exposure in a virtual organization” and “Suppliers as Trojan Horses.” Both of these dynamic stories will be presented below.

Dynamics Story 1—Virus Exposure in a Virtual Organization

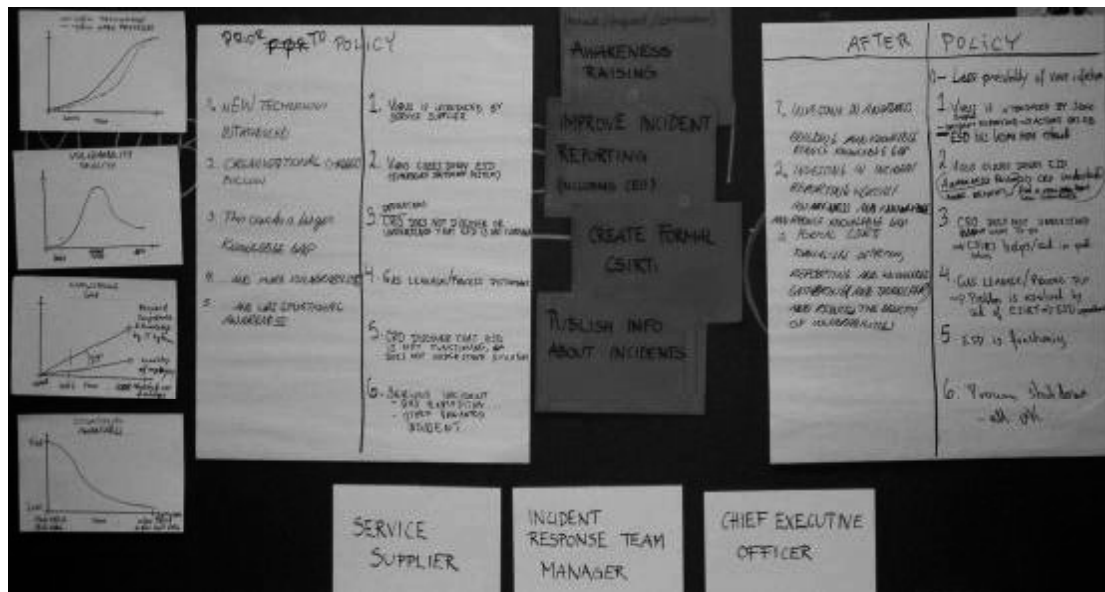


Figure 4-7 Dynamic story 1—Virus Exposure in a Virtual Organization

Base Run:

A new technology is introduced, followed by organizational changes. The change creates a knowledge gap, leading to increased vulnerabilities and low situational awareness, which might lead to severe incidents.

Policy Run:

A new technology is introduced, with organizational changes following suit. The change creates a knowledge gap, leading to increased vulnerabilities and low situational awareness. Investing in awareness raising and continuous training reduces the knowledge gap and increases situational awareness, which in turn reduces the probability of the occurrence of incidents. Nevertheless, when incidents do happen, the knowledge, as well as the formal CSIRT, helps resolve incidents quickly.

Dynamic Story 2—Suppliers as Trojan Horses

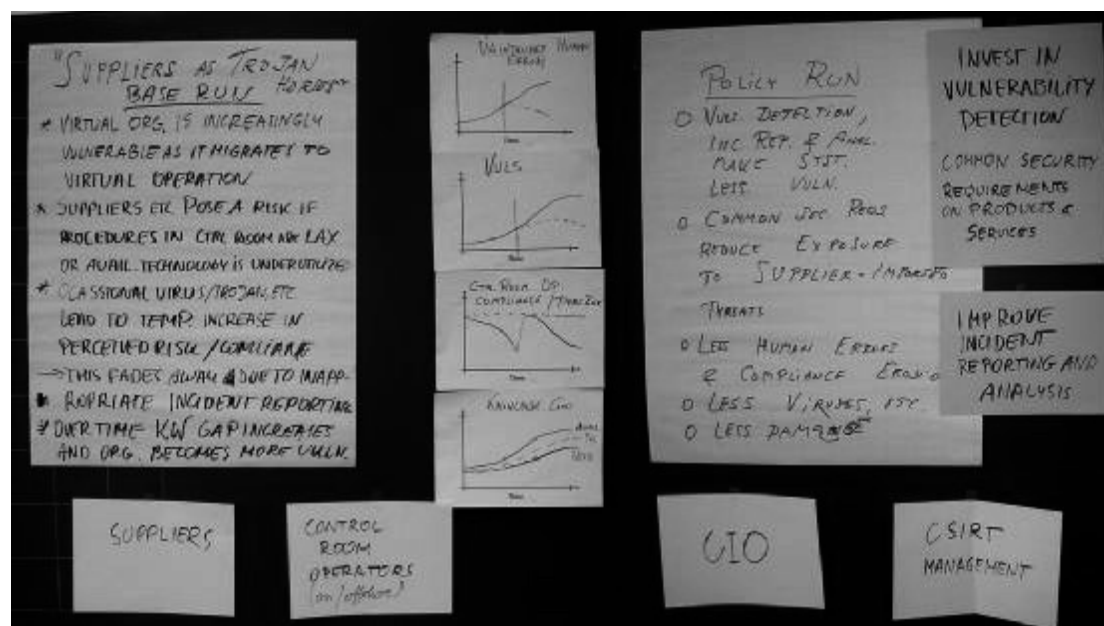


Figure 4-8 Dynamic story 2—Suppliers as Trojan Horses

Base Run:

An organization becomes increasingly vulnerable as it migrates to virtual operation. Suppliers and other stakeholders pose a risk if procedures in the control room are lax or if available technology is underutilized. The occasional virus, Trojan horses, and spyware lead to a temporary increase in perceived risk and compliance. Moreover, this perception is soon forgotten due to unmindful and inappropriate incident reporting. Over time, the knowledge gap increases, and the organization becomes more vulnerable.

Policy Run:

Vulnerability detection, increased reporting and analysis would make the system less vulnerable. Common security requirements reduce exposure to suppliers in the form of imported threats. Less human error and compliance erosion lead to fewer viruses and minimal damage.

Analysis: Both stories were derived from real incidents that had happened on the Brage platform. The key message conveyed in the two stories was the same, that is, the organization becomes increasingly vulnerable because the operation transition brings new technology and generates knowledge gap. As a result, a common understanding of the problem emerged.

- Exercise 7: Modeler's reflection

The modelers delivered a presentation to the plenary group to reflect on the information gathered from the group members. The presentation was supported by a series of diagrams in overhead transparencies. The diagrams were developed in different layers, using different transparencies and different colors. The transparencies were placed sequentially one over the other on an overhead projector, to illustrate the accompanying explanation.

The first presentation reflected on the information about Integrated Operations: the inner blue circle represents the traditional operation, where offshore controls the operation and has the data to itself; the outside red circle says that as the oil production depletes and unit cost increases, there are pressure to move to Integrated Operations and investment is made; this leads to the green lines and variables where data are shared to onshore control room and operation control become remote.

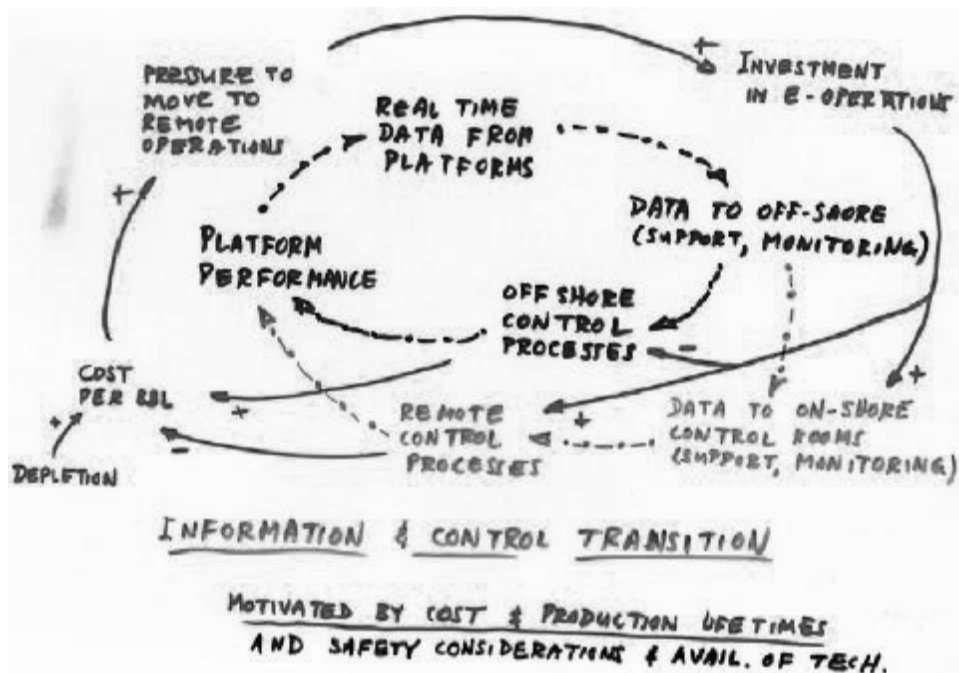


Figure 4-9 Illustration of operation transition

Then there was a reflection on the two dynamic stories.

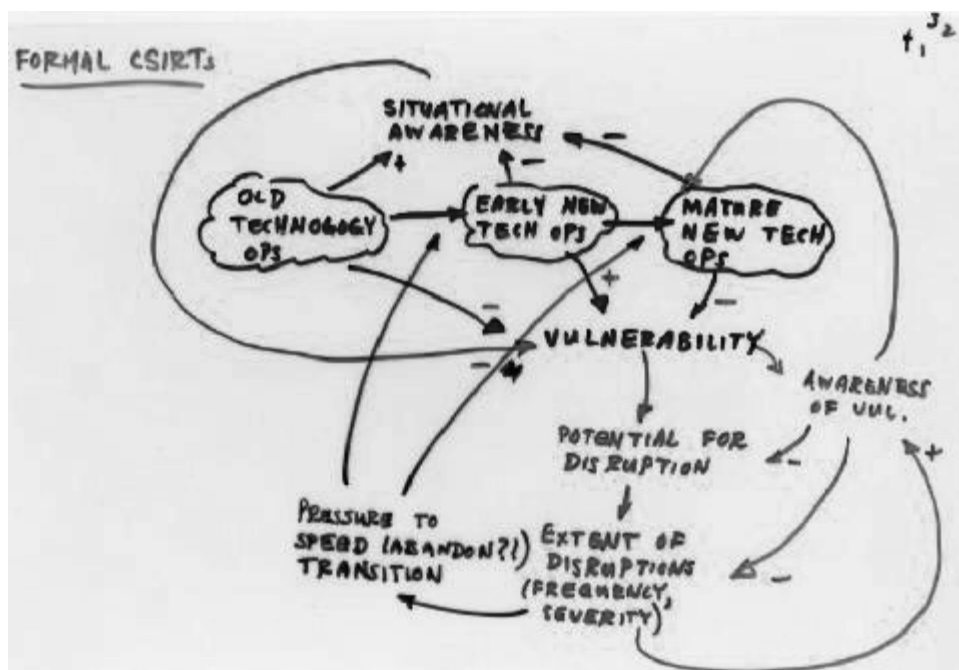


Figure 4-10 Reflection on the first dynamic story

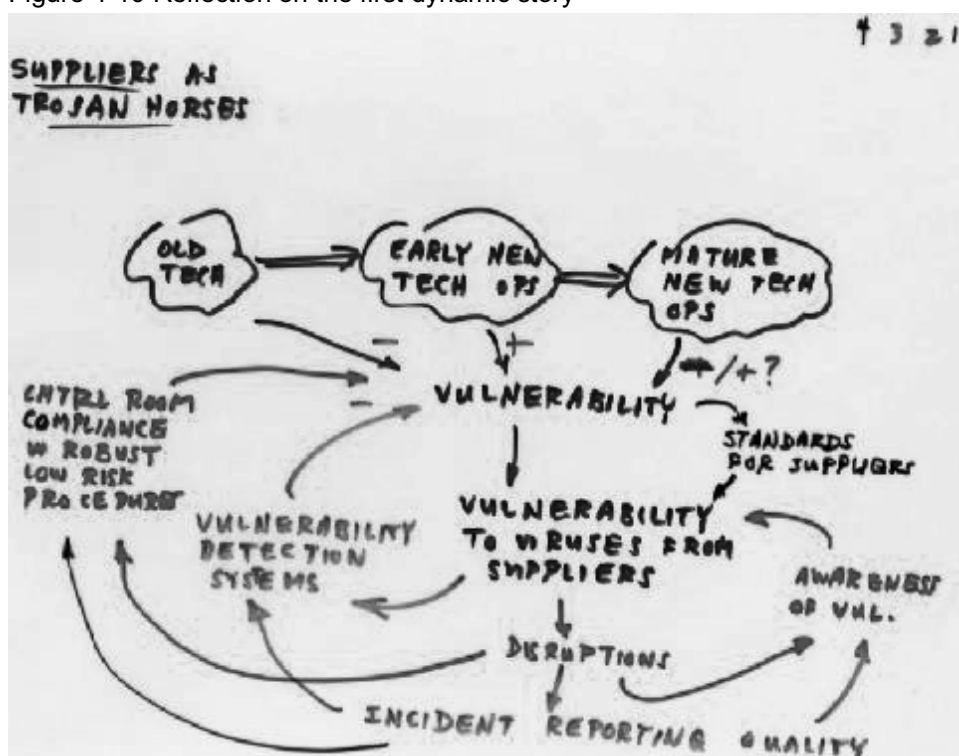


Figure 4-11 Reflection on the second dynamic story

Analysis: The reflection on the dynamic stories shows that both of them were focused on a structure of operations transition, changing from operations using old technology to operations using new technology. In this process, the vulnerability increased when the technology is new to the operators. When the new technology matured, the vulnerability would be reduced. However, whether the vulnerability could be reduced

to less than the original level (when using old technology) is uncertain. (Therefore, there is a question mark above “vulnerability” beside -/+ on Figure 4-11).

The modeler’s reflection clarified emerging ideas. During the presentation, the modeler frequently checked with the group members whether the diagrams represented their ideas. Confirmation from the group members enhanced consensus. Moreover, the modeler expressed the ideas using a language that is similar to that used by system dynamics. This made it easier for the group members to move on to the subsequent exercise on system dynamics concept model.

The first day of our group model-building workshops ended after the modeler’s reflection. Thanks to the scheduled activities, all the participants felt they had increased their knowledge about the operation transition and issues related to it.

- Exercise 8: Review the work from the previous day

As the first exercise in the second day, the recorder led the group members to review the work from the previous day. This exercise not only helped the group members remember what had taken place the previous day, but also checked consensus, detecting possible discrepancies and resolving them.

- Exercise 9: Concept model presentation

Concept models are preliminary models that are visually very simple and contain easy-to-understand algebra. They serve to lead the group members in the direction of building system dynamics models for the problem at hand (Andersen, Richardson 1995).

The modeler drew the concept model on the wall. While drawing, he explained the concept model using common language, just like telling a story of what was going on: we have capacity to work in traditional operations on the platform; now we are going to change them into capacity to work in integrated operations. The speed of the transition to Integrated Operations is affected by the potential traditional capacity that is available for the transition. The capacity in traditional operations and capacity in Integrated Operations associate with different risk level. Therefore, overall risk level for the platform changes as the operation transition continues.

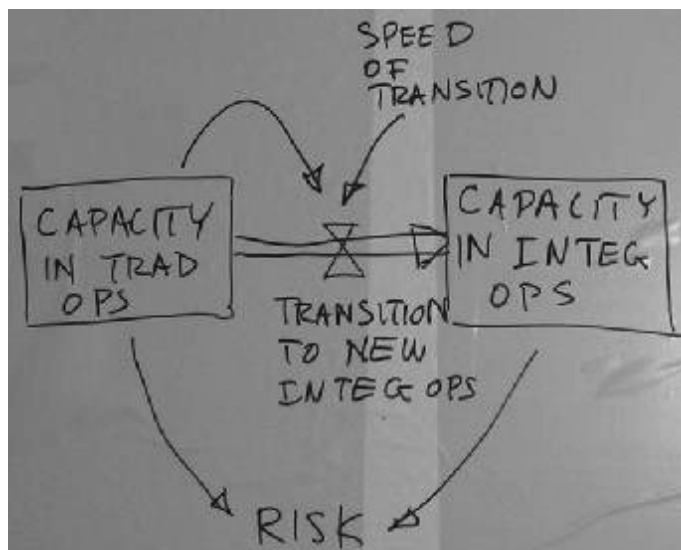


Figure 4-12 Stock-and-flow diagram

Then the modeler built the concept model in a system dynamics application, Vensim and simulated the model. The resulting behavior was explained by referring to the model structure.

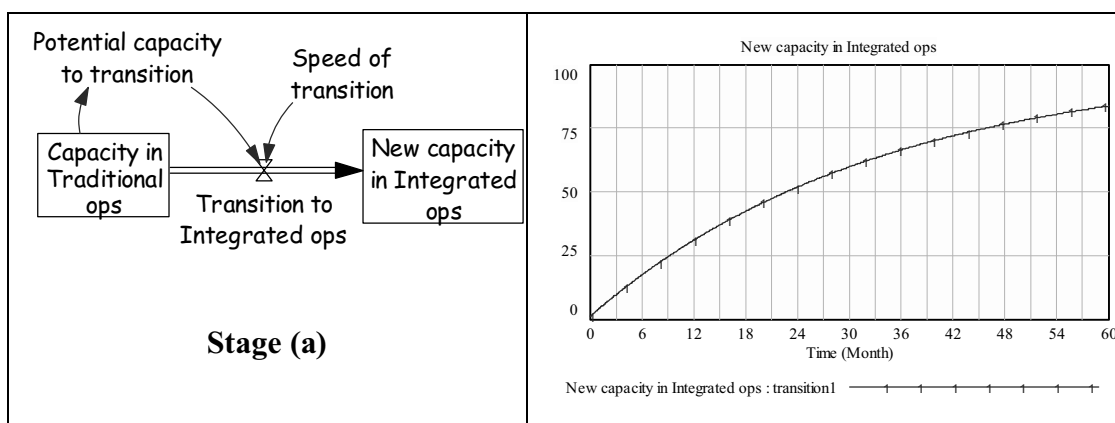


Figure 4-13 Concept model stage (a)

Three additional links were added to create concept model stage (b) (see Figure 4-14): the accumulation of new capacity in Integrated Operations brings experience with them. Such experience will speed up the operation transition. The behavior of the “New capacity in integrated Ops” changed into an S-shaped growth in stage (b).

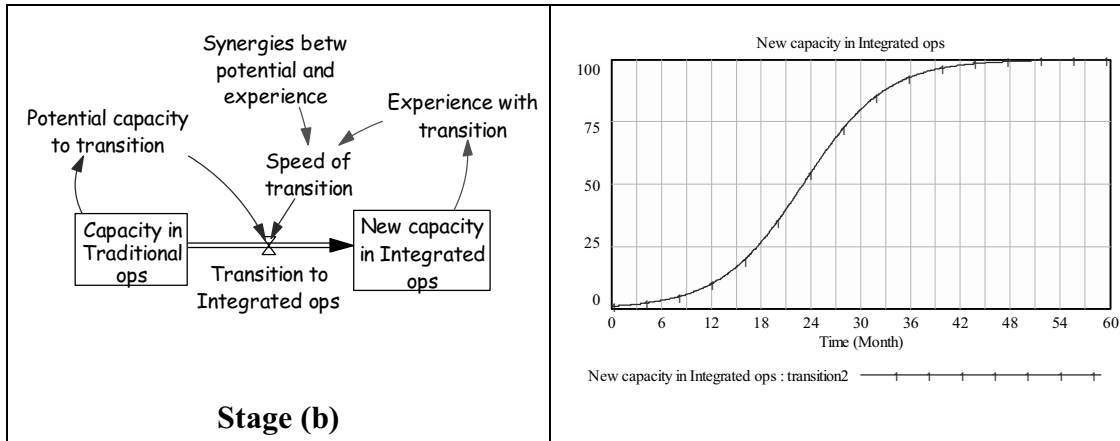
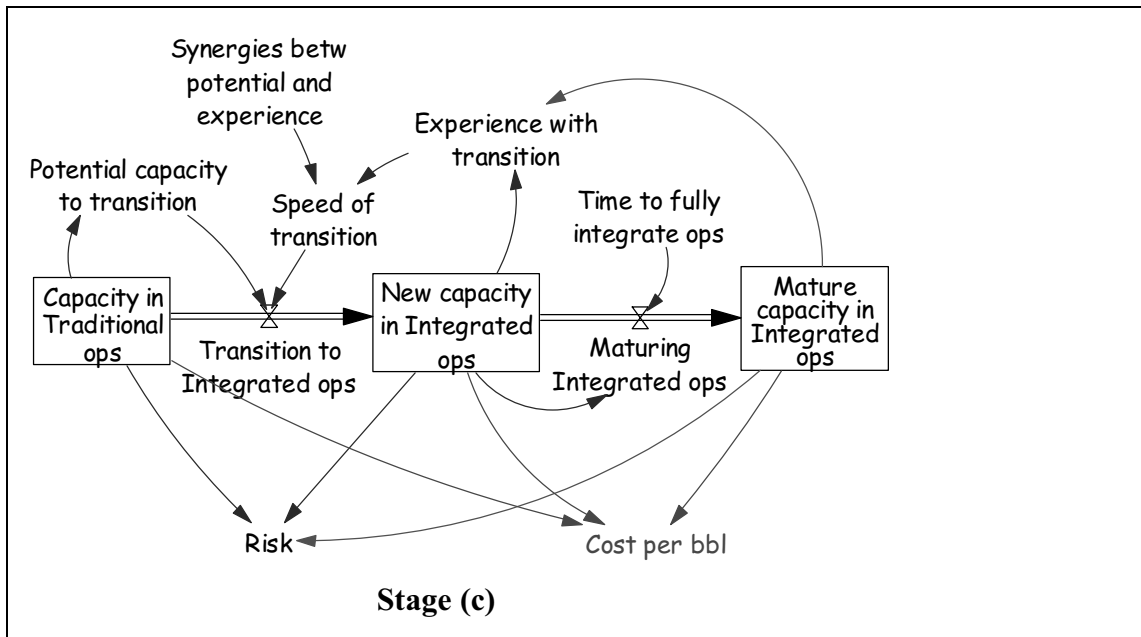


Figure 4-14 Concept model stage (b)

Again, small pieces of structure were added to form concept model stage (c): the capacity in Integrated Operations is separated in two stages: new capacity and mature capacity. Once again, the model behavior of “New capacity in integrated Ops” changed. Using this model, we also simulated how “risk” and “cost per bbl” changed during the operation transition (see Figure 4-15).



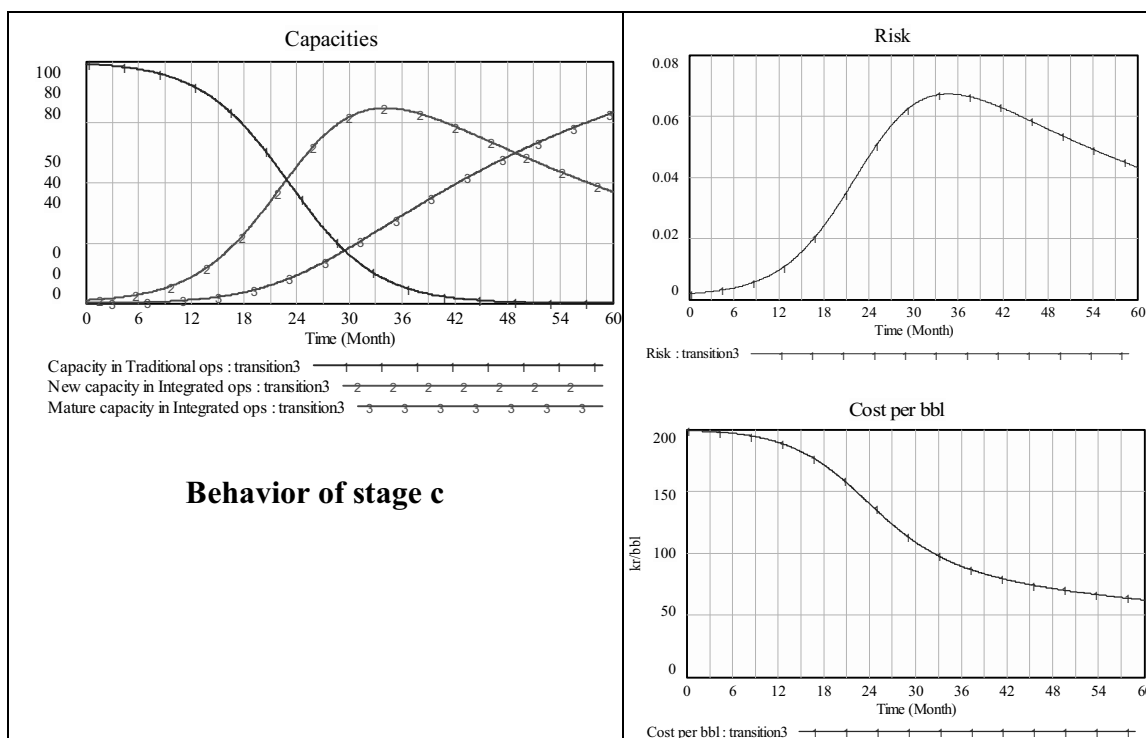


Figure 4-15 Concept models stage (c)

Analysis: The concept model introduced the language used in system dynamics to the group members. Some group members might not have anticipated that the outcome of the workshop would be a simulation model. Simulation models are sometimes perceived as complicated, black-box, difficult-to-understand products. In comparison, the system dynamics concept models have an easy-to-understand, simple structure and variables that are familiar to the group members. The behaviors of model variables are generated by the model structure and can be explained by it. The group members can build such a model with their knowledge of the problem structure using hand drawings as illustrated by the modeler.

The simulation behavior was analyzed in such a way as to clearly communicate that system behavior was determined by system structure: adding pieces of new structure would change model behavior. Presenting the model in three stages demonstrated the iterative nature of the model-building process. Normally, modelers start from a key concept. As more information about the problem is identified, the model will be extended. This process continues until the model boundary is reached.

Finally, the concept model was a primary model, and sometimes, deliberately a grossly simplified (i.e. wrong) model, developed to stimulate group discussion on

how the model could be extended and corrected. It was used to start the conversation about the problem in dynamic terms.

■ Exercise 10: Elicitation of model structure

After presenting the concept model, the group members had basic ideas about system dynamics models and also they had in their minds what to add to the model. Thus, the exercise to elicit model structure with the group members started.

Based on the concept model and information from previous exercises, the facilitation team selected some key stocks and wrote them on the wall as a starting point.

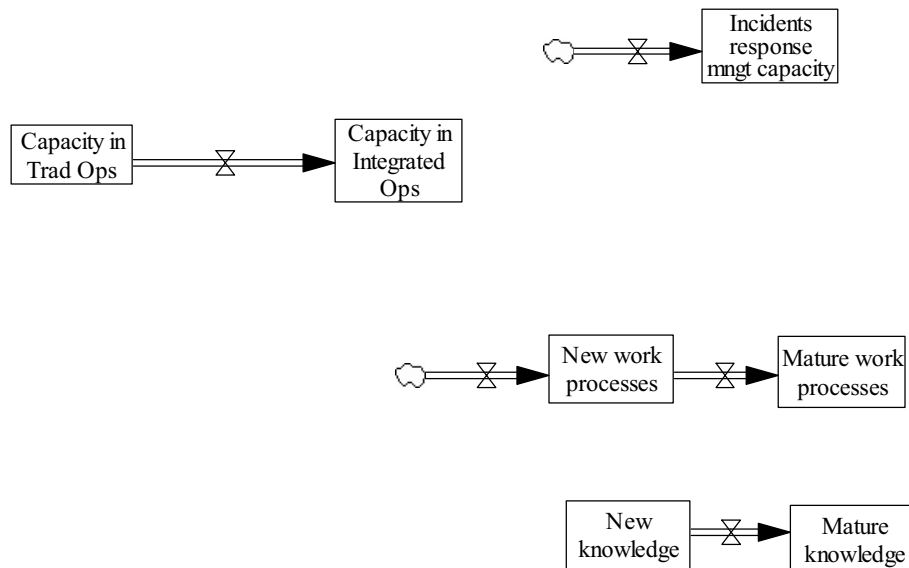


Figure 4-16 Backbones on the wall for model structure elicitation

Then the facilitator asked the group members to identify the variables that “help” open or close the faucet of these stocks. The group members began to suggest causal relations linked to these initial stocks and their corresponding rates. The facilitator recorded the added variables and linkages, and constantly reminded the group members to think of additional causal relationships. When some variables and causal relations were added, the facilitator would summarize by telling the story embedded in the model so far, asking the group to add further causal explanations. The story telling was predominantly used when a feedback loop was identified. For example, the group members suggested that the new technology could create a “collaborative arena” where people work together in virtual space. The effective use of a “collaborative arena” could help people learn new work processes and acquire new

knowledge, therefore increasing the speed by which they mature. The mature new work processes and knowledge would enhance a more effective use of the “collaborative arena.” The facilitator told the story to the group members and double-checked with them whether the loop correctly represented the reality.

After working with the group members for three hours, several feedbacks, many variables and causal relationships were identified. We present the final picture resulting from this exercise in Figure 4-17.

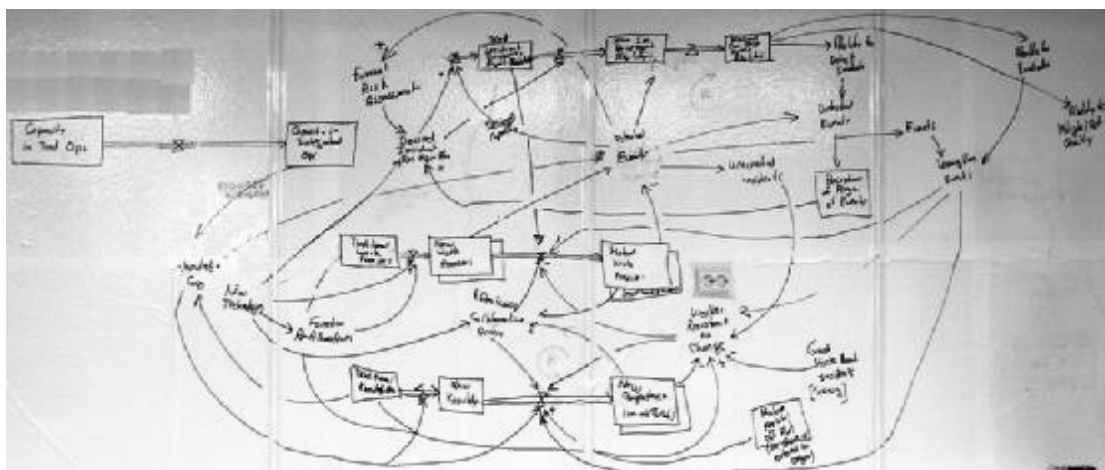


Figure 4-17 Model structure elicitation finished

Analysis: It was not easy for the group members to think in terms of feedback loops. Although many variables and links were added to the wall graph, only several loops emerged with the help of the facilitator. These loops concerned the operation transition and incident response. For those variables that didn’t form feedback loops, it was still important to record them and their linkages. The group members suggested that they are related to information security risks during the operation transition and further research might close the feedback loops for them. This way, we could gather as many ideas from the group members as possible.

Pen and eraser were utilized during the process of eliciting model structure. The group members felt free to make additions and corrections to the model. Therefore, the group members felt involved in the model-building process. Simulation models are often perceived as requiring advanced or sophisticated competencies and they are seen as difficult to comprehend. Consequently, many people are unwilling to use them. However, in this exercise, the group members took an active part in building models using a language and the tools they were familiar with. This created an ownership in

the model: the model was built by the group members themselves. They fully understood the structure of the model; thus, it would be easier for them to analyze model behavior and suggest policy recommendations for the model.

This exercise also helped build consensus. Before one variable was added, the group members would debate on the meaning of the variable and the nature of its causal linkages. The facilitator would add the variable when consensus was reached. If not, such variables would be recorded on a list indicating that further research was needed on the variable. Therefore, what was recorded on the wall was agreed by the group members. We copied the graph on the wall into the Vensim software and asked the group members to check the correctness of the copy. Together, the group members checked each variable and each linkage to ensure we got everything right in the computer.

- Exercise 11: Modeler's reflection

The modelers again offered a reflection section on the second day of the workshop. A series of transparencies were prepared beforehand. First of all, the three loops identified in the structure elicitation exercise were revisited as shown in Figure 4-18 and Figure 4-19.

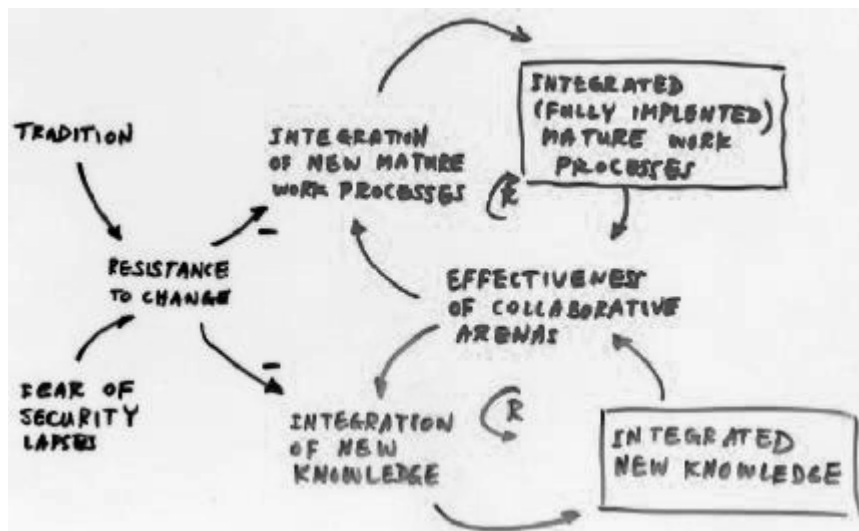


Figure 4-18 Two reinforcing loops emerged from the structure elicitation

The first two reinforcing loops concerned the effective use of the collaborative arena: the more the operators work with collaborative arena, the faster the maturation of new work processes; the more mature the new work processes, the more people work with

collaborative arena; the same mechanism works for maturation of new knowledge.

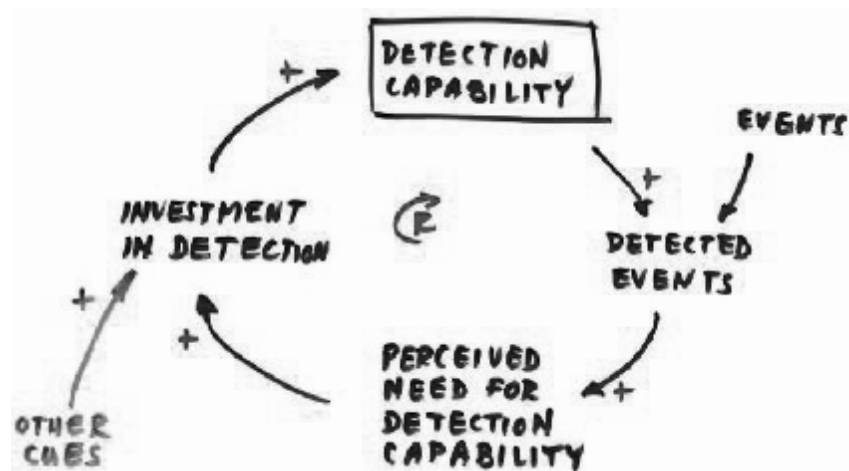


Figure 4-19 The third reinforcing loop emerged from the structure elicitation

The third reinforcing loop concerned the investment in incident detection capability: the more investment made, the more detection capability available, and the more events detected, which resulting higher perceived need for detection capability and more investment again.

Another two dynamic hypotheses based on the outcome of group discussions were presented in Figure 4-20 and Figure 4-21.

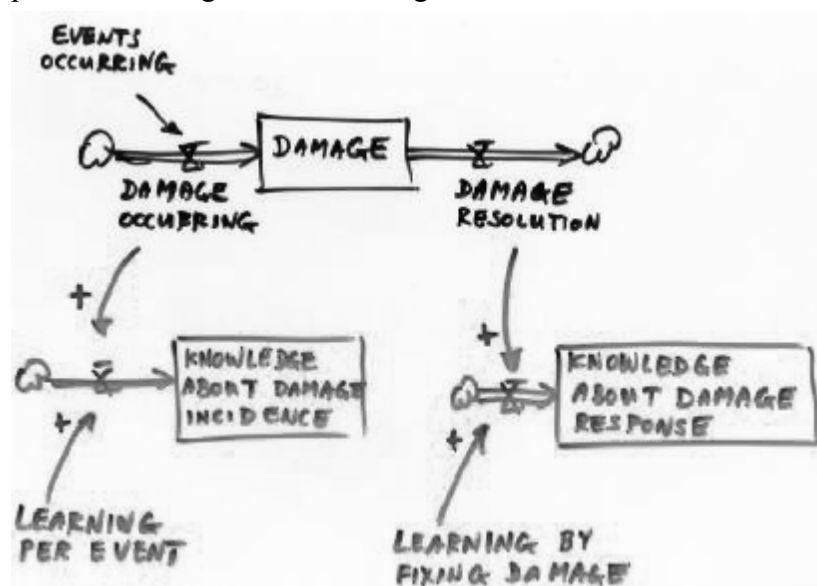


Figure 4-20 Dynamic hypothesis about incident response knowledge

This one concerned learning from damage that was caused by incidents. When damage occurs, learning about incident also occurs. This learning increases the knowledge about damage incidents. When damage resolves, learning about fixing damage also occurs. This learning increases the knowledge about damage response.

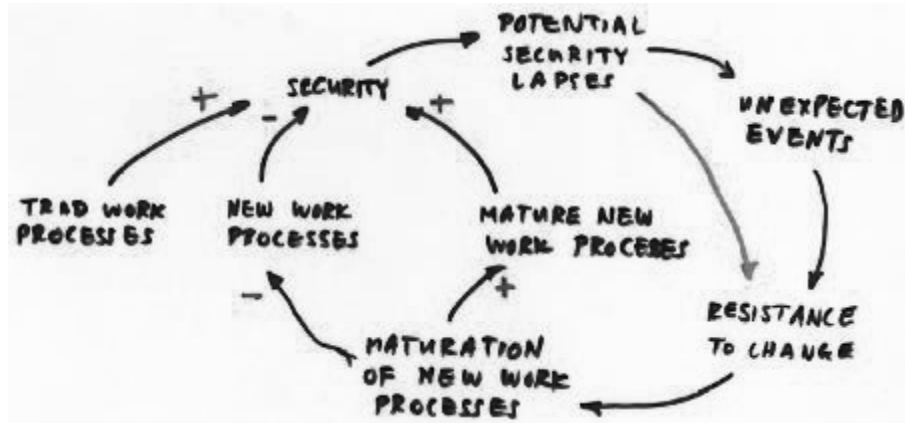


Figure 4-21 Dynamic hypothesis about resistance to change

The second hypothesis concerns the information security: newly implemented work processes reduce information security, leading to more unexpected events, which cause resistance to change and reduce the speed of maturation of new work processes. This results in fewer mature new work processes and more new (immature) work processes. Thus, the information security is lower than it otherwise would have been.

Finally, the problem was articulated: the operation transition will introduce new work processes and knowledge to the platform. Time and resources are required for new work processes and knowledge to mature. A knowledge gap will be generated as new knowledge takes longer time to mature. New (immature) work processes, new (immature) knowledge and the knowledge gap all make the platform vulnerable, thus, generate high information security risks (see Figure 4-22)

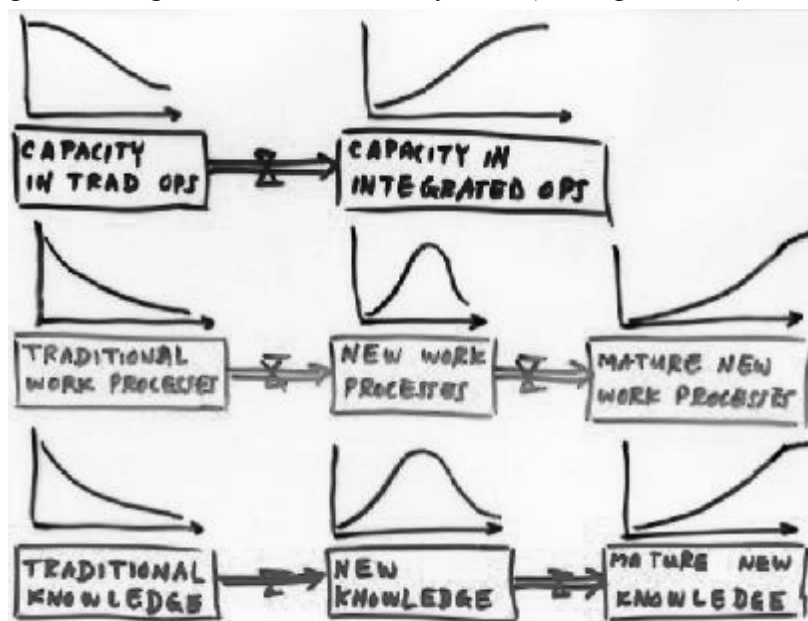


Figure 4-22 Problem articulation

The foremost question is the speed of the operation transition and the speed of maturation (related to resources availability). All the group members agreed on this problem definition.

4.2.4 Model development after workshop

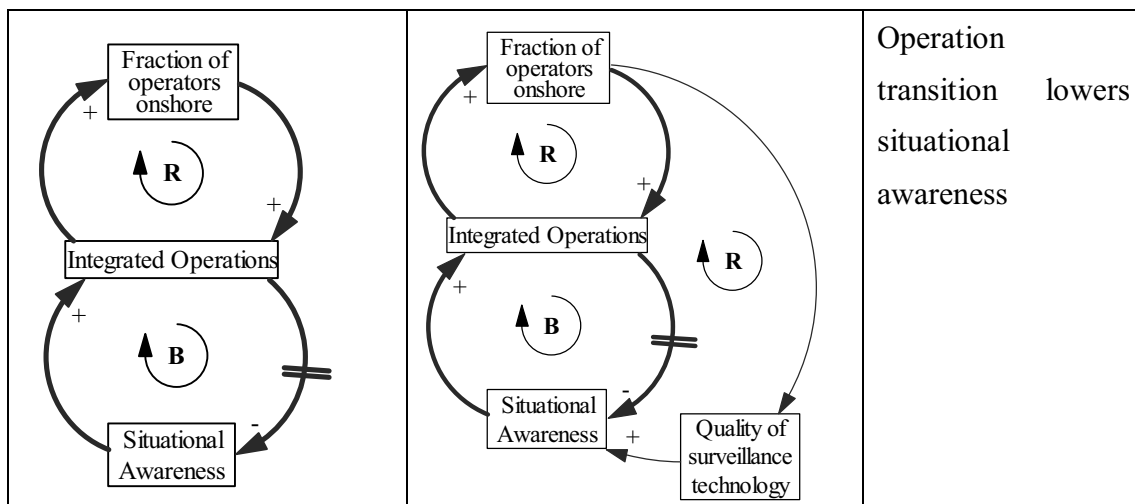
Following Wolstenholme’s approach, we developed five archetypes after the first group model-building workshop. Archetypes are short-hand version of more complex models. Archetypes are almost never detailed enough to facilitate a formal simulation, but they are for communicating knowledge about the dynamics of a system. They can be easily understood by people who have little or no training in system dynamics (Wolstenholme 2003; Wolstenholme 2004). Wolstenholme suggests that problems arise from the unintended consequence of human actions. Therefore, his problem archetypes contain feedback loops with intended consequence and unintended consequence. The solution archetype adds a further feedback loop that inhibits the unintended outcome.

In the following section we present the problem archetypes that describe information security problems associated with the transition to Integrated Operations; these problems in turn feed back on the performance of Integrated Operations as unintended consequence. We also sketch potential solution archetypes.

Table 4-4 Five archetypes identified

Problem archetype	Solution archetype	Description
		<p>Transition to Integrated Operations generates higher vulnerability</p>

		<p>Trust perception leads to overinvestment or underinvestment in incident response capability</p>
		<p>Excessive work load causes erosion of compliance</p>
		<p>Redundancy of Information leads to communication vulnerabilities</p>



Here, we will not go into a detailed analysis of these archetypes. For more information, please refer to the paper (Qian, Gonzalez, and Sveen 2005).

4.3 Second AMBASEC group model-building workshop

The second group model-building workshop was held on September 7-8, 2005 in Hydro, Bergen. Again, experts of group model-building workshops from the University at Albany were invited to facilitate the workshop. Based on the results of the first workshop, the AMBASEC team, together with Albany team, decided that the purpose of the second group model-building workshop should be to elicit more system structures and identify reference modes for further model development. Again, the agenda for the two-day workshop was designed with different exercises carefully sequenced to achieve the target in the best possible manner.

4.3.1 Purpose

The purpose of the second group model-building workshop was to elicit more system structures and identify reference modes for further model development. Likewise, we aimed at gathering qualitative and quantitative data for the model formulation. The expected outcome was an improved model with more representative structures that could serve as a starting point for model formulation. We also expect to identify areas for further model building.

4.3.2 Participants

Twenty persons from different parties, with different roles, participated in the second workshop.

Client group:

Hydro: *Trond Lilleng (leader of the Integrated Operations project), Trond Ellefsen (CISO), Anders Bjørsvik, and Lars Grøteide (ICT department), Bjørn Holst (the Brage platform Chief)*

IRMA: *Odd-Helge Longva, Stig O. Johnsen, and Maria B. Dahl (researchers in information security)*

AMBASEC: *Jose J. Gonzalez, Agata Sawicka, and Johannes Wiik (researchers in information security)*

NTNU: *Tor Onshus (researcher in cybernetics)*

Facilitation group:

AMBASEC: *Ying Qian (modeler), Stefanie Hillen, and Magne Myrtveit (process coach), Jaziar Radianti, and Felicjan Rydzak (process observer)*

Albany: *David Andersen (facilitator), George Richardson (modeler), and Eliot Rich (recorder)*

Five key personnel from Hydro, including the Brage platform chief, the chief information security officer (CISO) and the leader of the Integrated Operators, participated in the second workshop, indicating greater client engagement. Interestingly, the participants were mostly those with high interest/high influence listed on the stakeholder map (see Figure 4-1), such as the platform chief and the chief information security officer. We like to believe that the stakeholder map attracted the attention of the most significant actors and that they perceived the group model-building workshop as relevant to their professional interests and work.

4.3.3 Exercises and data obtained

- Exercise 1: Presentation

Representatives from Hydro presented detailed information about the transition to

Integrated Operations. The presentation included the vision of the Integrated Operations, the executive plan, and the current stage. It also included information about the setting of collaboration room onshore and offshore, which offered an understanding of how people work in Integrated Operations.

One of the most important new work processes, daily production optimization, was introduced to all the participants in detail: it included collaborative meetings that were organized in the morning, noon, and afternoon. During these meetings, staff from onshore and offshore, from different departments, sat together in a videoconference to review related data and decide on what to do next and how to implement that decision. Besides these fixed meetings, a videoconference could be called whenever required. Experts could be consulted for a discussion of a particular situation or a particular problem. This could cause a larger portion of the oil-in-reserve to be retrieved, - implying higher revenue.

Members of the Hydro team also presented Brage's Information System architecture. They explained how information (data) flows from the platform to the control center and vice versa.

Members of the IRMA team presented the risk matrix that they had previously developed for the Brage case. The two dimensions of the matrix are the frequency and consequences of incidents, respectively. The figure below shows various incidents, represented by different points in the matrix.

Table 4-5 Risk matrix from IRMA

Frequency	F5	F4	F3	F2	F1
Consequences	From 100 year and up	Between 10 to 100 year	Between 1 to 10 years	Several times a year	More than once a month
K5 Very Critical Cost 20 to 200 mil NOK				U2-SCADA goes down	
K4 Critical Cost. 2 -20 mil NOK		U8- Missing situational awareness from Central Control Room Operator	U1- Component failure Jamming SCADA		
K3 Dangerous Cost 100.000 to 2 mill			U5- Changes in system without verification (not patched) U6- Changes done outside hierarchy	U-3 Virus / Worm from external sources	
K2 Serious Cost 10 - 100.000,-				U7- Failed to optimise production real time	U4- Downtime central hardware components
K1 Less serious Up to 10.000,-			U9- Equipment used in communication failing.		

Source: OLF-IRMA-AMBASEC Group Model-Building Technical Report II (Rich, Andersen, and Richardson 2005)

Analysis: The presentations provided us with important insights into the transition to Integrated Operations: the details of how people are expected to work in Integrated Operations, the settings of their new working environment and the information flows.

IRMA's presentation provided information about different types of incidents that were occurring and their frequency and consequence. The final system dynamics model includes variables as the frequency of incidents and severity of incidents. The IRMA's risk matrix offered quantitative information for model building.

- Exercise 2: Review of the previous workshop

The facilitator led the group members to review the result of the first workshop. First the model structure elicited in the first workshop was presented to the group (Figure 4-17). Some of the important feedback loops and causal relationships were explained.

■ Experiment with the concept model

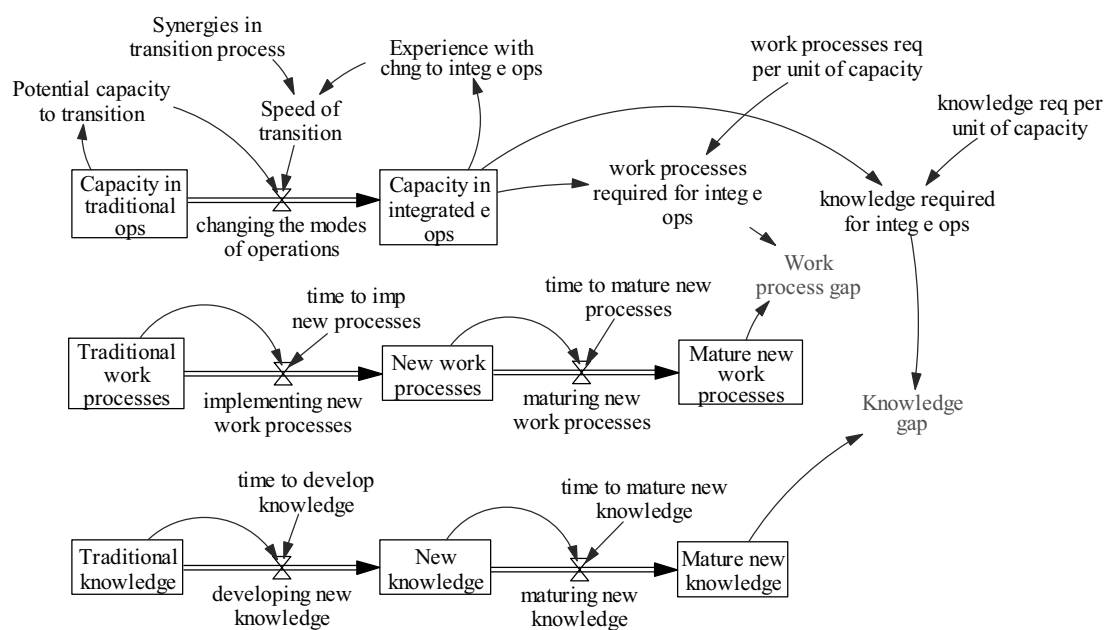


Figure 4-23 Concept model

A ready-built open-loop model (Figure 4-23) that represented the origin of work process and knowledge gaps served as the concept model for this workshop. Instead of presenting the concept model step by step, this time the group members were invited to experiment with the concept model.

The group members were divided into three subgroups. Each subgroup was asked to invent a policy with the intention to improve the operation transition. The policies are implemented in the model by changing the value of one or more of the parameters. Each subgroup should tell a story of what these parameters mean, identify their dynamic impact, and predict what would happen.

All subgroups engaged in lively discussions. After they submitted their policy, told the story and stated their prediction, the modeler simulated the concept model in Vensim using the parameter values suggested by each of the subgroups. The predicted results were similar to the simulation results for two groups but not for the other one.

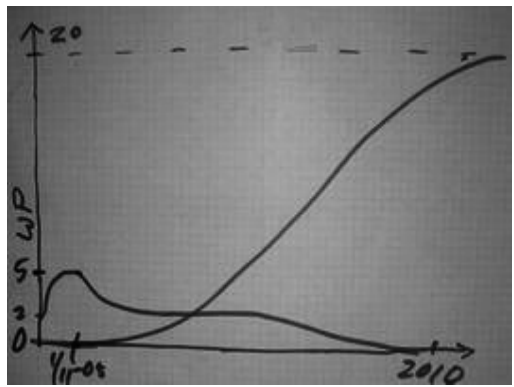
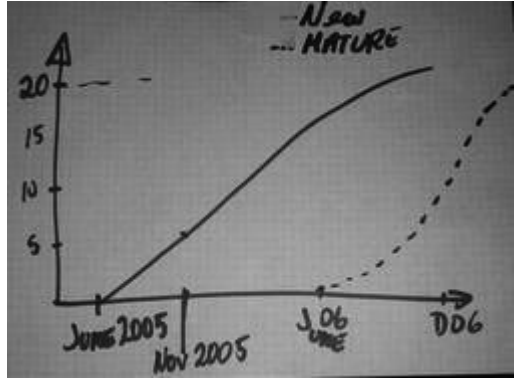
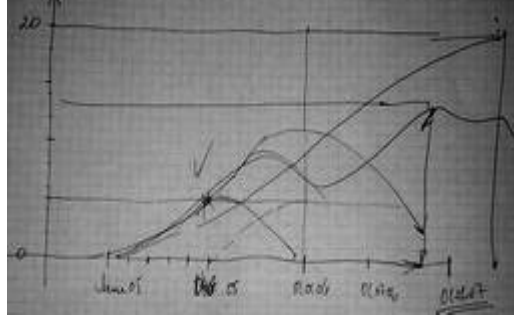
Analysis: After several presentations, this exercise made the group members more actively involved in the workshop. During the exercise, the group members were asked to predict the result for their policies. This stimulated the understanding of the model structure and helped the participants to relate the observed (or desired) behavior to the underlying model structure.

The group members were also challenged to tell a story about what a parameter change means in reality. For example, a policy targeting to reduce the time needed to mature new work processes and knowledge would mean to have more training programs. In this way, the group members related the model to reality. Sometimes, people conceive models to be very theoretical and find it difficult to apply insights gained from model to reality. That is one reason some people are reluctant to use modeling methods. This exercise demonstrates that system dynamics models are closely linked to the real world.

- New work processes implementation timeframe

The three subgroups were asked to participate in the exercise for developing ideas about the rate at which work processes would be implemented and matured. We obtained three different ideas from the three different subgroups, presented in the following Table 4-6.

Table 4-6 Ideas of work processes development timeframe

 <p>Presented by Bjørn Holst, the Brage platform chief.</p>	<p>The lower curve represents the rate of new work processes implementation. The curve ends high shows the accumulation of new work processes on the platform.</p> <p>In this scenario, five new work processes are to be implemented in short-term, followed by two new work processes per year, ending with a total of 20 new work processes implemented at around 2010.</p> <p>This figure focuses on the implementation schedule. It doesn't have information on the maturation of new work processes.</p>
 <p>Presented by Lars Grøteide, from ICT department</p>	<p>The solid line represents the new work processes implemented. The dashed line represents the new work processes matured.</p> <p>In this scenario, the introduction of 20 new work processes will take place at a constant rate over one and half years. Maturation of new processes follows with a time lag of around one year.</p>
 <p>Presented by Trond Lilleng, the head of operation transition project</p>	<p>The curve that ends up at level of 20 represents the new work processes implemented. The other curve with fluctuation shows mature work processes.</p> <p>In this scenario, 5 new work processes are to be implemented in 2005. In the best case, 20 processes are to be implemented in late 2007.</p> <p>As processes are reviewed and matured, some of the processes may be withdrawn and re-introduced, delaying the maturation of new work processes.</p>

Analysis: the Brage platform chief forecasted that it would take more than five years to implement all the new work processes: five new work processes in the short-term and then two to three new work processes per year afterwards. The other two groups estimated a shorter time for the implementation of new work processes. Lars Grøteide, from ICT department, estimated that 20 new work processes could be implemented in

one and a half years. In his mind, the implementation of new work processes is more related to get the technology ready in place, which could happen fast. Trond Lilleng, the leader of the operation transition project planned that twenty new work processes should be implemented in 3 to 4 years time. This could be a sign that the management hoped for a fast transition to Integrated Operations, but they might have underestimated the amount of time and effort actually required to implement new work processes and did not consider the possibility (implicitly stated by the platform chief) that this implementation could not be completed successfully too hastily.

We chose to use the timeframe provided by the Brage platform chief as our reference mode for modeling. The platform chief best knows the platform and the local implementation schedule. During policy analysis, we also tried scenarios with fast implementation of the new work processes as suggested by Trond Lilleng.

- Model structure elicited

Together with the group members, we spent much time identifying and drawing feedback loops. This resulted in a more complete model structure. To summarize, we simplified some of the linkages and shaped them into round circles to form a general model structure. In that way, it is easy to view the whole picture of the feedback processes that govern the operation transition at Brage.

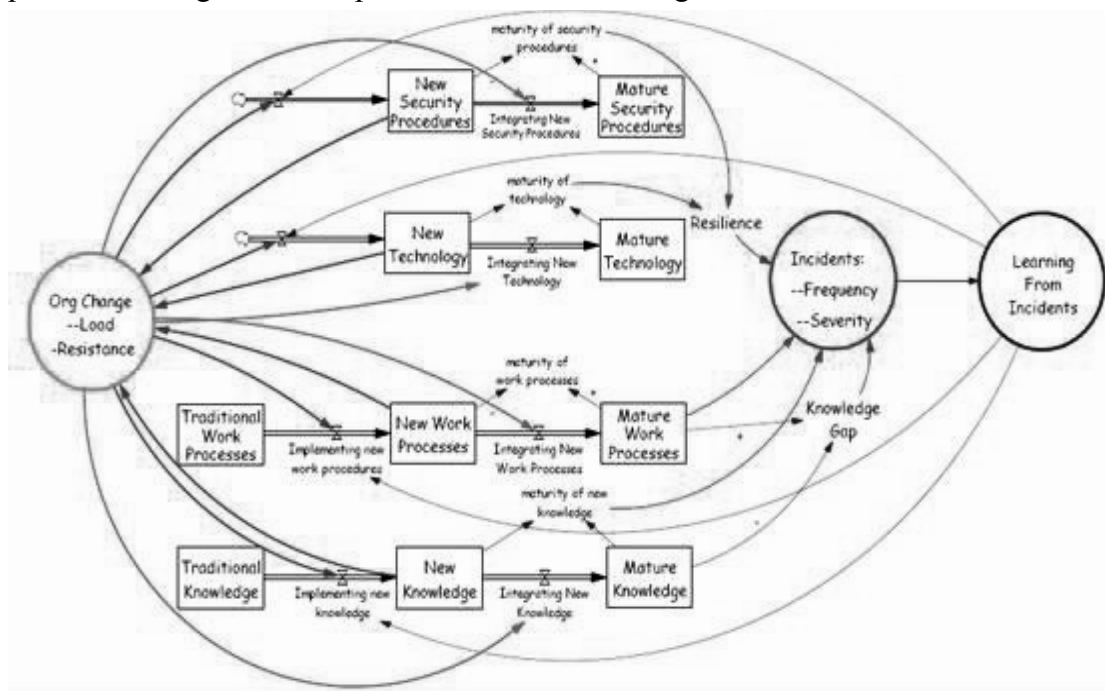


Figure 4-24 General model structure derived from the second workshop

The stocks and flows characterize the operation transition. The three circles, representing organizational change, incidents, and learning from incidents, all illustrate the key issues that the model should capture. The future modeling work will address the issues implied in these circles.

We formed a more complete dynamic hypothesis as follows: *The introduction of new technologies facilitates new work processes that require new knowledge. It takes time for new work processes to mature and even longer time for knowledge to mature. Thus, knowledge gap is generated, leading to higher vulnerability. Immature new work processes and immature new knowledge also contribute to higher vulnerability. Maturing new work processes and knowledge reduce vulnerabilities. Attention to incident response will reduce damage from incidents.*

4.3.4 Model development after workshop

After the second group model-building workshops, a prototype model was developed. It includes four sectors: work processes, knowledge, vulnerability, and incidents. The “work processes” sector captures the transition from traditional to Integrated Operations work processes; the “knowledge” sector captures the transition of knowledge for traditional operation to knowledge for Integrated Operations. These two sectors corresponded to the work processes chain and knowledge chain in the general model structure; the “incident” sector in the general model structure was also included in the prototype model with key variables as the “*frequency of incidents*” and the “*severity of incidents*” affected by the operation transition. “Learning from incidents” is also included in the “incidents” sector.

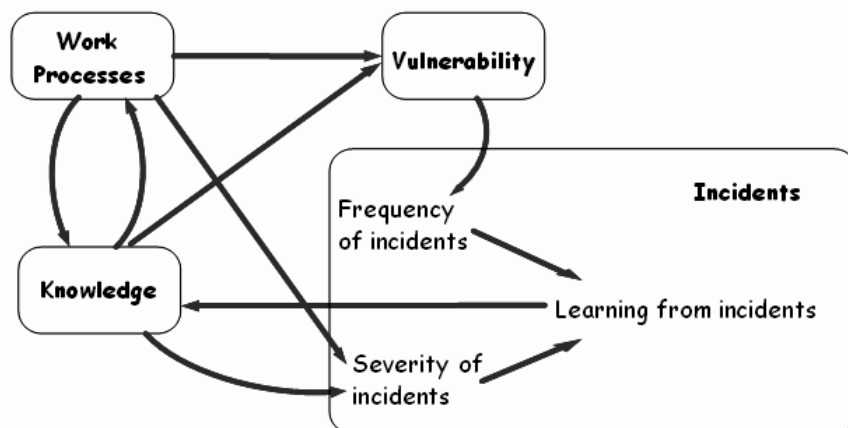


Figure 4-25 The prototype model developed after the second workshop

4.4 Following model-based interventions for model development

After the second workshop, we, the AMBASEC project team, arranged a series of model-based meetings for model improvement.

In the first teleconference with Hydro and IRMA, the prototype model was presented. We first clarified the model structure, the relationship of the sectors, and the input and output of each sector. We then showed the simulation results based on the data we plotted into the model. The client gave their consent to the model structure and showed interest in the model behavior. It was then arranged that the Brage platform chief would provide the specific data based on the Brage platform so that the model could better represent the Brage case.

The interview with the platform chief, Bjørn Holst, was conducted through a structured process. The interview protocol we developed was sent to Bjørn Holst before the interview. The questions were not only about specific data on Brage but also about the definitions of the key variables. The interview helped us quantify many of the model variables. At the same time, this interview enhanced the understanding of the abstracted variables for both parties.

Another teleconference with Hydro was arranged, wherein we presented the model using the Brage data, the analysis of the model structure and behavior, and several different scenarios. In the latter part of discussion, we agreed on the steps to be undertaken to develop the model further. This interactive process of model-based communication, model development, and model-based communication continued until the model was fully developed. When Hydro was not available to participate in the consultations, meetings with the IRMA team were arranged instead.

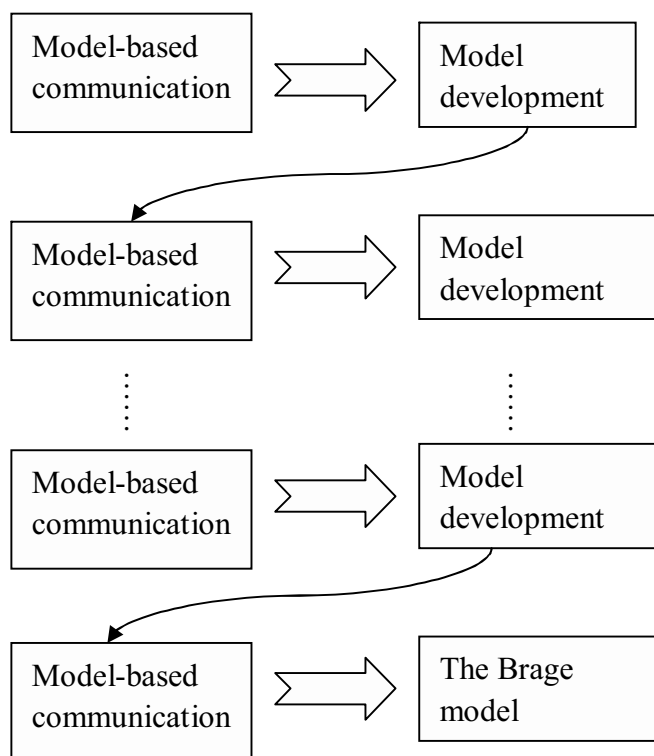


Figure 4-26 Model formulation process

After these model-based communication processes, the model was extended to seven sectors. The sectors added were ‘incident response capability’, ‘learning from incidents’, and ‘production and profit’. We will introduce the model in details in chapter 5.

4.5 Closing remarks for chapter 4

The two group model-building workshops helped shape our ideas. The problem definition was gradually revealed through various exercises in the first group model-building workshop. The transition to Integrated Operations brings new work processes, new knowledge and knowledge gap to the platform. They cause the platform to be more vulnerable, resulting in more incidents and severe incidents. This is Hydro’s main concern. On the second workshop, we scouted for more details, such as the specific work process and IT architectures. Through the discussions, more data were collected.

More importantly, through the workshop, our client started to trust us. At the beginning of the first workshop, the leader of Integrated Operations project said he was not sure whether Brage was a proper case for the research. After the workshop,

he expressed his interest in our approach. He told us that what he did not like was the “black-box” modeling which showed simulation results without properly demonstrating and explaining the logic behind the model. However, he realized that system dynamics was different. He liked the discussion and felt ownership of the model. He was quite convinced that the approach could address Brage’s problem and promised to assign more people to participate in the second workshop. In the second workshop, several high influence/high interest stakeholders participated. We had intensive discussions about the operation transition, technology, incidents, and other concerns. Needless to say, the information they provided were of great importance.

Our research project made significant progress during the two group model-building workshops. Below we present the summary of these two workshops.

Table 4-7 Overview of the two group model-building workshops

	First group model-building workshop	Second group model-building workshop
Purpose	Problem identification	Model conceptualization
Data	<ul style="list-style-type: none"> - Stakeholder map - Policy lever map - Key indicators and their behavior over time - Dynamic stories (with stakeholders, policies, and key indicators) 	<ul style="list-style-type: none"> - Overview of the transition to Integrated Operations - Information about one concrete work process flow - Risk Matrix - New work process implementation timeframe
Insights	<ul style="list-style-type: none"> -Basic problem: transition to Integrated Operations generates security risks -Inadequate knowledge in relation to work processes causes system vulnerability 	<ul style="list-style-type: none"> - New technologies enable new work processes but also introduce new vulnerabilities - Maturing technologies, work processes, and knowledge reduce vulnerabilities - Incident response and knowledge management speed maturation
Model developed	<ul style="list-style-type: none"> - Some feedback loops - Archetypes 	<ul style="list-style-type: none"> - General model structure - Prototype model (four sectors)
Client attitude	<ul style="list-style-type: none"> - From skeptical to supportive - Positive remarks about the approach 	<ul style="list-style-type: none"> - Positive remarks about the approach - Committed to act as model reference group

Results on the two group model-building workshops are reported in (Qian and Gonzalez 2006; Gonzalez et al. 2005; Qian, Gonzalez, and Sveen 2005).

5 Model of Brage's Transition to Integrated Operations

In this chapter, we present the model addressing the change of information security risks during Brage's operation transition. This model will be referred to as the Brage model. This chapter starts with a model overview showing the model sectors and their interrelationships. Next, the meanings of the key model concepts are explained. Then the major causal loops are presented, both with causal loop diagrams and with a verbal explanation. These loops are the driving forces underlying the model behavior. Thereafter, the formal model is described sector by sector, accompanied by explanation of the main structures, equations, and variables. Finally, we present the model behavior to facilitate the understanding of the model structure.

5.1 Model Overview

5.1.1 Model sectors

The Brage model contains seven sectors: Work Processes, Knowledge, Vulnerability, Incident cost, Incident Response Capability, Learning from Incidents, and Production and Profit. Their linkages are shown in Figure 5-1 as follows:

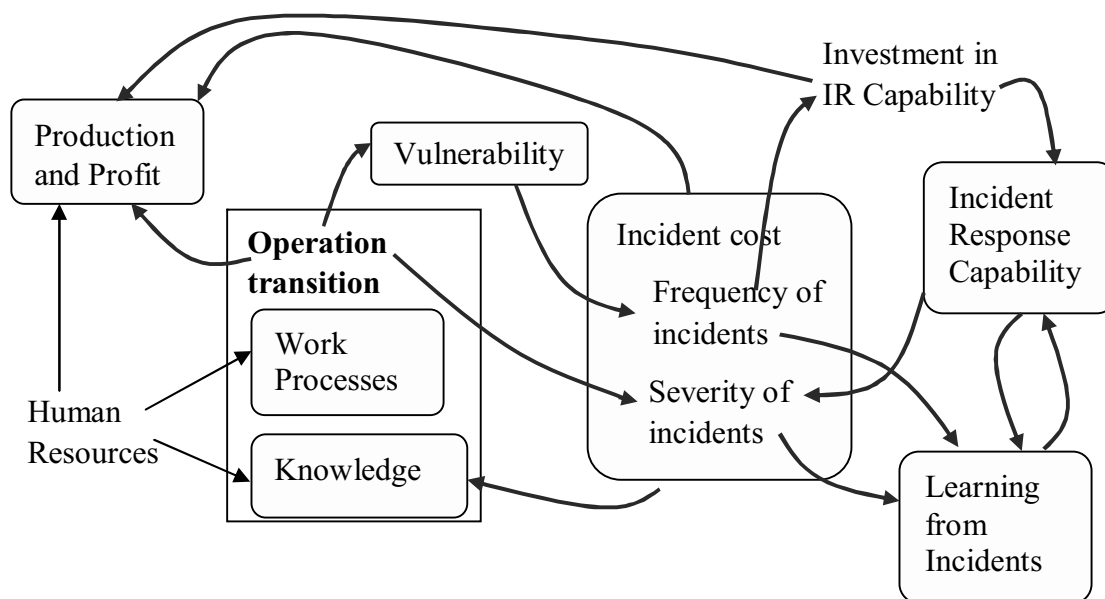


Figure 5-1 The Brage model overview

The Brage model is largely based on the general model structure derived from the second workshop. Here, we will first explain how the Brage model is related to the general model structure.

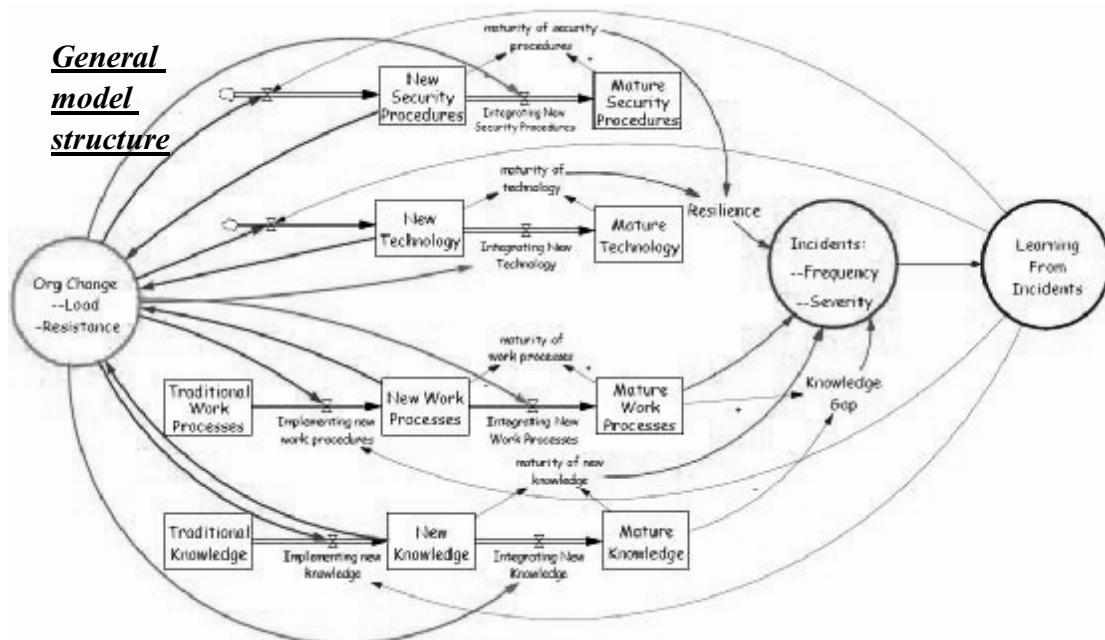


Figure 5-2 General model structure

The two sectors in the Brage model in Figure 5-1, “Work Processes” and “Knowledge” are grouped under “Operation transition” because both are encompassed by that concept. Both capture the development and maturation of new work processes and knowledge, respectively. They correspond to the two stock and flow chains of work processes and knowledge transition in the general model structure in Figure 5-2 (lowest two stock flow chains). There were discussions about the transition of technology during the group model-building workshop, resulting in the stock and flow chain of technology transition in Figure 5-2 (second stock flow chain from the top). However, in the Brage model, there is no technology sector. New technology is associated with new work processes. The implementation of new work processes is a prerequisite for using new technology. Therefore, the technology transition is embedded in the transition of new work processes and knowledge. There is no separate technology sector in the Brage model. It was suggested in the workshop that the maturation of the security procedures would increase the resilience of the Brage platform, resulting in the stock and flow chain of security procedures in the upper part of Figure 5-2. The security procedures and technology affect the

“Resilience”. Resilience is defined as an ability to recover from or adjust easily to misfortune or change⁵. Further discussion with our client showed that the ability to recover from incidents is mostly related to the incident response capability. Therefore, in the Brage model, the security procedures are replaced by the “Incident response capability” sector (see upper right part in Figure 5-1).

The circle “organization change” on the left side of Figure 5-2 is mainly represented by the concept “new initiatives burden” in the Brage model inside the work processes and knowledge sector. New work processes require a new organizational structure. The organizational change disrupts the social structure and “know-who” network. Not knowing who to contact, or not knowing the contact person well, causes difficulties in communication, and leads to extra work load for the operators. The difficulties for communication are named as “new initiatives burden”, which reduces the effectiveness of learning the new work processes and acquiring new knowledge. Concerning the “resistance to change” in the circle of “organization change” in Figure 5-2, we had several discussions with our client on this topic. Hydro representatives suggested that the operators’ resistance to the operation transition was mainly due to the fear of losing their job and reducing their salaries when reallocated from offshore to onshore. Such resistance does not have a dynamic feature. One solution is to have clear communication with the operators about the operation transition plan and its impact on them. Another solution is to have dialogs with the union about position reallocation and change of income level. Therefore, the “resistance to change” is not included in the Brage model.

The sector “incidents” on the right side of Figure 5-2 includes the frequency of incidents and severity of incidents. Both variables are endogenously included in the “incident cost” sector in the Brage model (see Figure 5-1). The frequency of incidents is related to the threats to the Brage platform and the vulnerability of the platform. Both threats and vulnerability are affected by the operation transition. Severity of incidents is mostly influenced by the incidents response capability, and also by the operation transition.

As mentioned above, the sector “incident response capability” in the Brage model (upper right in Figure 5-1) is a replacement of “security procedures” in the general

⁵ see <http://www.merriam-webster.com/dictionary/resilience>

model structure (Figure 5-2). In the first group model-building workshop, there was discussion about how an investment decision in incident response capability was made and a feedback loop was identified. The modeling of the incident response capability is mainly based on this feedback loop (see Figure 4-19).

At the right-hand side of the general model structure (Figure 5-2) is a sector for “learning from incidents”, which affects the maturation of new work processes and knowledge. In the Brage model (lower right in Figure 5-1), we have included a sector for “learning from incidents”, but it only affects the incident response capability, not the maturation of new work processes and knowledge. Learning from incidents is limited as information of incidents is normally not shared among the operators unless they are severe incidents. However, severe incidents do not occur frequently.

In addition, the Brage model has a simplified financial sector (upper left of Figure 5-1) including revenue, cost of production, cost of incidents, and cost for incident response capability. Revenue is related to production, which is dependent on the resources available for production, and the productivity of the resources. Productivity is related to operation transition. New technology is supposed to improve productivity, but this can only be achieved with sufficient knowledge. Similarly, cost of production is related to operation transition. Meanwhile, cost of incidents and cost of incident response capability are the output from the “incidents” and the “incident response capability” sectors, respectively.

5.1.2 Concepts of work processes and knowledge

The transition to Integrated Operations is represented by the chains of work processes and knowledge; - from “traditional” work processes and knowledge, through “immature new” work processes and knowledge, into “mature new” work processes and knowledge.

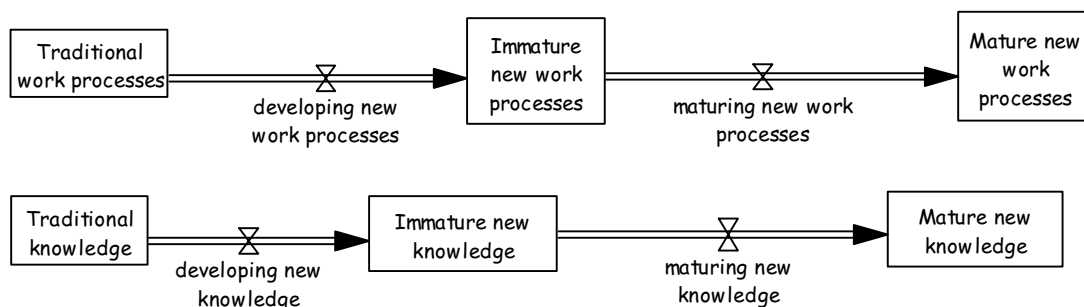


Figure 5-3 Aging chains for operation transition

For the purpose of this study, *work processes* are those completed in accordance with formal descriptions developed to guide the processing to a successful completion. These formal descriptions are “abstracted from actual practice. They inevitably and intentionally omit the details” (Brown and Duguid 1991). *Knowledge* is comprised of insights and experience, embodied in individuals or embedded in organizational processes or practice⁶. It includes all the details that help complete the task *effectively*.

Basically, work processes are related to “*what to do*,” while knowledge is related to “*how to do*.” In another paper by Brown and Duguid (2001), they summarized Ryle's famous contrast between know that (what) and know how. “Acquiring know that (what) does not lead to being able to use it. Know how, moreover, is not acquired like know that, which may circulate as precepts and rules. It is, Ryle insists, quite different. ‘We learn how,’ he argues significantly, ‘by practice’”. This statement echoes our concept of new work processes (know what) and new knowledge (know how). As Ryle pointed out, without knowledge, work processes alone cannot achieve the desired improvements. To adopt new technology, operators not only need to learn what to do (new work processes), but also how to do (new knowledge). Only when operators have fully learnt what to do and how to do can they work effectively with the new technology and achieve the desired improvements.

Table 5-1 Work processes and knowledge

	Work processes	Knowledge
About	What to do	How to do
Feature	Abstracted	Detailed
How to acquire	Circulate as precepts and rules	Learn by practice

Having summarized the definition of work processes and knowledge from the literature, we can now have a look at what the model variables mean in reality.

Developing new work processes: This process encompasses reviewing traditional work processes, identifying necessary changes, and documenting new work processes so that this documentation is ready to be disseminated as an operator’s guide to new work processes. The persons from the management team on Brage are responsible for

⁶ See http://en.wikipedia.org/wiki/Knowledge_management

developing new work processes. This variable concerns the rate at which new work processes are being developed.

Maturing new work processes: This process encompasses obtaining familiarity with what to do, and memorizing them. The operators on Brage are responsible for maturing new work processes. This variable concerns the rate at which the operators on the platform familiarize themselves with the new work processes.

Immature new work processes: When new work processes are implemented, the operators are not used to them. Sometimes, the operators unintentionally switch back to old work habits. They need instructions, typically in the form of their supervisors' guidance, colleagues' reminders, or a manual for operations. Work processes in such a stage are named "immature new work processes." The productivity at this stage is lower than desired. Immature new work processes accumulate as new work processes are implemented and deplete when they mature.

Immature new work processes =

$$\int (\text{developing new work processes} - \text{maturing new work processes}) dt$$

Mature new work processes: When the operators have familiarized themselves with the new work processes and can work with them unassisted, we label these new work processes "mature new work processes." The productivity at that stage is higher than when the new work processes are immature. However, whether the desired productivity is achieved, depends on the level of maturity of new knowledge.

$$\text{Mature new work processes} = \int (\text{maturing new work processes}) dt$$

Developing new knowledge: This process encompasses developing information material and training programs for new work processes. The persons from the management team of Brage are responsible for developing new knowledge. This variable concerns the rate at which new knowledge is developed and made accessible

Maturing new knowledge: This process encompasses learning how to work with the new processes, why to work in such way and how to react when deviation happens. The operators on Brage are responsible for maturing new knowledge. This variable

represents the rate at which the operators on the platform learn the details of *how* to work with the new work processes.

Immature new knowledge: When new knowledge is introduced together with new work processes, the operators do not know well *how* to work. They might work suboptimally, for example, contact the wrong persons for information, or not interpret appropriately the data available. Therefore, their productivity would be lower than what is desired. Knowledge at such a stage is named “immature new knowledge.” Immature new knowledge accumulates as new knowledge is developed and depletes as it matures.

Immature new knowledge =

$$\int (\text{developing new knowledge} - \text{maturing new knowledge}) dt$$

Mature new knowledge: When the new operation details have become routine, and there is no explicit effort to think about them, we label such knowledge as “mature new knowledge.” At this point in time, the desired productivity is achieved. Mature new knowledge accumulates as new knowledge matures.

$$\text{Mature new knowledge} = \int (\text{maturing new knowledge}) dt$$

Figure 5-4 contains a horizontal timeline illustrating the change in work processes and knowledge over time.

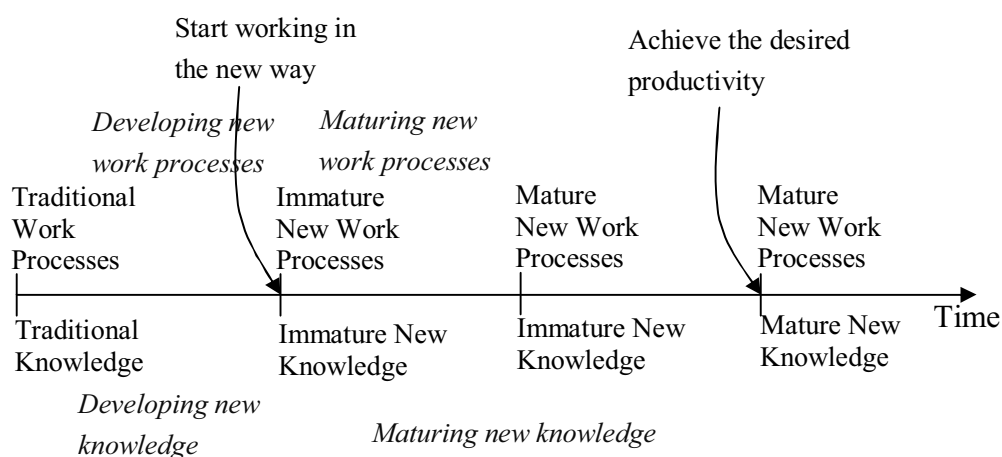


Figure 5-4 Timeline of the evolution of operation transition

When the new work processes and knowledge are being developed and introduced, the operators start to work in the new way. At that point in time, both the new work

processes and knowledge are immature. As the operators work with new work processes, they gradually learn *what to do* and *how to do*. It takes longer time to learn how to do than what to do. Therefore, new knowledge matures more slowly than new work processes. When both of them have matured, the desired productivity of the Integrated Operations is reached.

Knowledge gap:

In the model, we assume that one new work process corresponds to one set of new knowledge, and that acquiring that knowledge (getting to know how to work and why to work in this way) is a prerequisite for working effectively in accordance with the new work process. When new work processes are being introduced, corresponding (i.e. relevant) mature new knowledge is desired. Yet knowledge maturation takes time. The gap between the desired mature new knowledge and the actual mature new knowledge is named the “knowledge gap”. See the below equations:

$$\textit{Knowledge gap} = \textit{Desired mature new knowledge} - \textit{Mature new knowledge}$$

$$\textit{Desired mature new knowledge} = \textit{New work processes} * \textit{Mature knowledge per work process}$$

$$\textit{New work processes} = \textit{Immature new work processes} + \textit{mature new work processes}$$

Time to mature new work processes:

From the interview with the platform chief, we learned that, on the average, it takes around four months to mature one immature new work process. Common sense dictates that people might need several weeks to memorize what to do if new work processes are implemented. However, an oil platform has its own special working schedule. People on the Brage platform work continuously for two weeks at a time and then take four weeks of time off. Three groups of people work in shifts. After four weeks of time off, the operators typically forget some of the new work processes they have learned previously. When they come back to work on the platform, they have to be guided once more on the procedures of the new operation. The platform chief suggested that, after three rotations, people could memorize the entire new work processes quite well, and there is no need to remind them of what to do. One rotation takes six weeks; hence, three rotations will take eighteen weeks, which is equal to four months.

Time to mature new knowledge:

The literature points out that it takes much longer time to learn knowledge than to learn work processes. Attewell (1992) argues that, although one can readily buy the machinery that embodies an innovation, the knowledge needed to use modern production innovations, is acquired much more slowly and with considerably more difficulty. He also cites Arrow's study result that manufacturers using new process technologies are "learning by doing"—their productivity improves for several years after adopting a new technology, as they gradually learn to use the technology to its best effect. However, quantitative information regarding how much time it takes to mature knowledge is not available. In the model, we assume that, given enough resources (the operators' time), it takes the operators six rotations, that is, eight months to learn all the details necessary to achieve the desired productivity for Integrated Operations. In this study, this (estimated) parameter has been the subject of a sensitivity test (See Appendix IV Sensitivity tests, S10).

5.2 Major causal loop diagrams

In system dynamics we work under the assumption that the behavior of a system is governed by the internal mechanism that constitute causal relationships that form non-linear feedback structures and use causal loop diagrams to represent such structures. In this paragraph, we will outline some of the causal loops that form the major feedbacks in the system we study.

5.2.1 Casual loop diagrams for operation transition

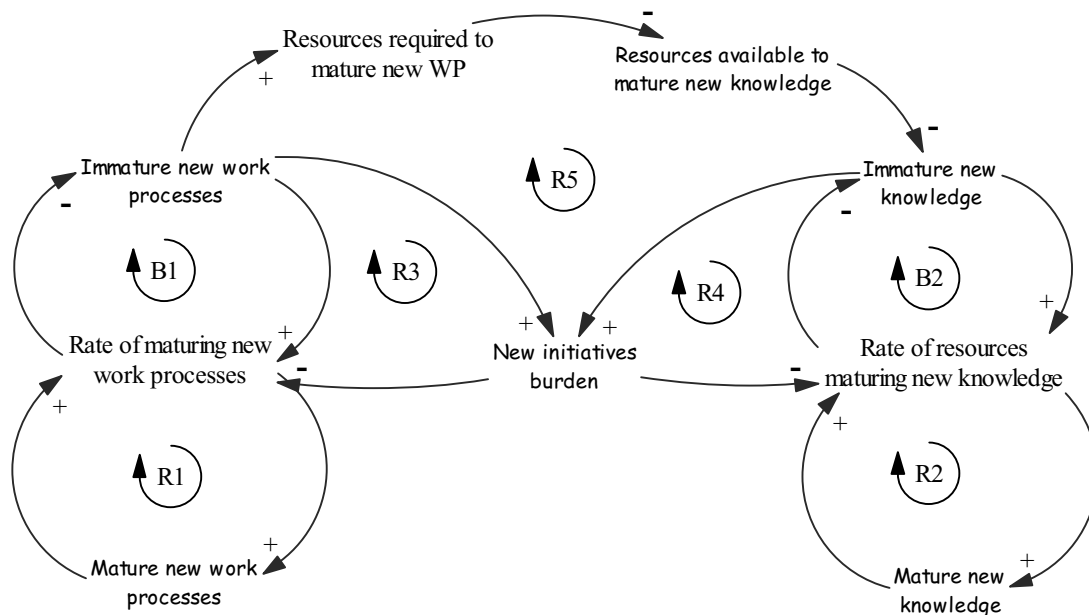


Figure 5-5 Causal loop diagram for the transition to Integrated Operations

In Figure 5-5 we portray a causal loop diagram of the processes of work processes and knowledge maturation resulting from the introduction of immature new work processes (upper left).

B1 and B2: New work processes and knowledge facilitate the maturing process

B1 and B2 constitute the maturation processes that drains (converts) immature work processes and knowledge (to produce mature ones).

The introduction of more new work processes and associated knowledge mean that there is a higher potential for the incorporation of new work processes and for learning about those processes. The maturation processes drains this potential (immature new work processes and knowledge) by incorporation and learning, i.e. to produce more mature work processes and knowledge. As more immature new work processes and knowledge mature, fewer immature new work processes and less immature new knowledge will be left to mature next time around, - causing a lower rate of maturation of new work processes and knowledge to take place. So these balancing loops tend to match the demand for maturation and slow down the process as this demand (potential) erodes.

R1 and R2: Experience assists the maturing process

R1 and R2 constitute the maturation processes that produce mature work processes and knowledge, based on the accumulation of experience (incorporated work processes and mature knowledge).

When more new work processes and knowledge are matured, the operators have accumulated experience in working with the new work processes and the new technology embedded in them. Such experience facilitates the process of maturing additional new work processes and knowledge and accumulation of additional experience. So these reinforcing loops tend to speed up the process of maturation as experience builds.

R3 and R4: New initiatives burden slows down the maturation of new work processes and knowledge

R3 and R4 constitute the maturation processes that produce mature work processes and knowledge, affected by the organization change (associated with the immature new work processes and knowledge).

New work processes require new organization structure. People generally prefer to work with those they know well. Unfamiliar contact persons often cause difficulty in communication, which leads to extra work. This concept is represented by the “new initiatives burden” which reduces the speed of learning new work processes and acquiring new knowledge. As the operators learn to work in the new way, immature new work processes and knowledge are gradually matured and then new initiatives burden is reduced, leading to even faster maturation of the remaining new work processes and knowledge.

R5: Resources constrain the maturing of new knowledge

R5 constitutes the resource allocation that constrains the maturation of new work processes and knowledge.

When immature new work processes increase, the resources required to mature them also increase, resulting in fewer resources available to mature new knowledge. This leads to a slower maturation of new knowledge and more immature new knowledge will be accumulated than it otherwise would be, which will result in a higher new initiatives burden and will in turn reduce the rate of maturing new work processes, causing more immature new work processes than it otherwise would be. Therefore, fast introduction of new work processes causes slow maturation not only because of the new initiatives burden but also because of the resource constraint.

5.2.2 Causal loop diagram for incident response capability

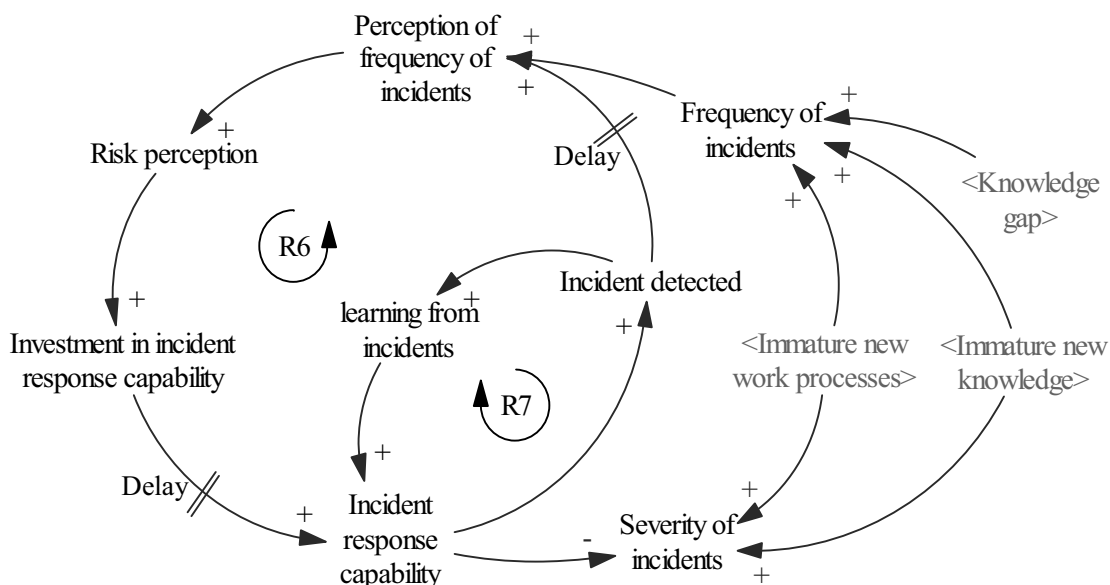


Figure 5-6 Causal loops for incident response capability

In Figure 5-6 we portray a causal loop diagram of building incident response capability (lower middle) which results from the investment decision (middle left) and learning from incidents (middle in the circle). The grey variables with brackets are those generated in the sectors of operation transition. The “frequency of incidents” and “severity of incidents”, which characterize incidents, are affected by variables from operation transition and incident response capability.

R6: Incident response capability raises risk perception

R6 constitutes the investment processes that build up incident response capability, based on the perception of information security risks.

High incident response capability improves the detection of incidents. As more incidents are detected, risk perception increases, leading to more investment in incident response capability, which will result in higher incident response capability. The effect of this reinforcing feedback loop could be overinvestment in incident response capability. However, the more serious problem would be if the reinforcing loop operates in the opposite sense—the risk perception trap: inadequate incident response capability leads to low detection of incidents, which causes low risk perception and underinvestment in incident response capability. Inadequate incident response capability might lead to improper handling of incidents, which causes severe incidents.

R7: Learning from incidents increases incident response capability

R7 constitutes the learning from incidents that build up incident response capability, based on the experience of incident handling.

Considering the incident response team, the more they learn from an incident, the higher the incident response capability will be. Therefore, the incident response team can detect more incidents, handle more incidents and acquire more knowledge about incidents. This loop will generate higher incident response capability. However, during our interview and meetings with related experts, we found that there is no deliberate learning process: incidents are not properly reported and the information about incidents is seldom shared. Incident response team learns little from incidents. Thus, this reinforcing loop is currently weak.

5.2.3 Incident cost affect operation transition speed

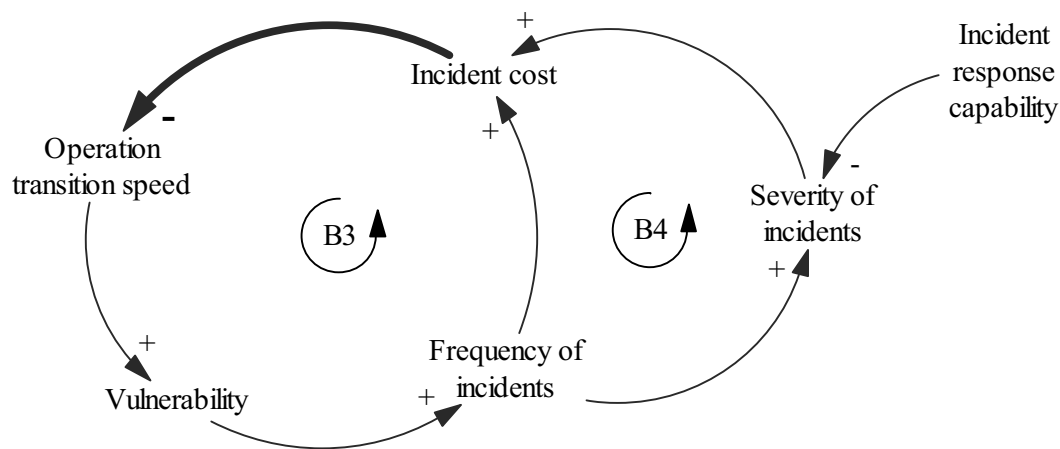


Figure 5-7 Causal loops from incident cost to operation transition speed

In Figure 5-7, we portray a causal loop diagram of changing the operation transition speed (upper left), that is, the speed of introducing new work processes. The operation transition speed is affected by the incident cost (upper middle).

B3 and B4 High incident cost reduces operation transition speed

B3 and B4 constitute the change of operation transition speed (speed of introducing new work processes), based on the incident cost.

When incident cost is high, the management considers the Integrated Operations risky and decides to reduce the transition speed, which means slow down the introduction of new work processes and knowledge. As the immature new work processes and knowledge mature over time, there will be fewer immature new work processes and knowledge in place. This will reduce vulnerability and thus lower frequency of incidents. Under certain incident response capability, fewer incidents mean that more response capability is available to handle each incident, leading to better incident handling and reduced severity of incidents. With fewer incidents and reduced severity of incidents, the incident cost will be lowered.

5.3 Formal model description

In this section we present detailed information about the model structure sector by sector. Given the level of complexity, it is not possible to explain every variable and equation. We will discuss pieces of structures as well as key equations and variables. For detailed information on equations and variables, please refer to Appendix I: List of Equations (p. 249). Additional information on how lookup functions are formulated is available in Appendix II: List of lookup functions (p. 266).

5.3.1 Sector 1—Work processes

This sector represents the work processes transition. The stock and flow chain in Figure 5-8) captures the transition of work processes from traditional ones (*“traditional work processes”*) to newly implemented ones (*“immature new work processes”*) and finally, to mature ones (*“mature new work processes”*).

Some short forms are used in the model:

- IO represents Integrated Operations;
- WP represents Work Processes;
- IR represents Incident Response

Work Processes Transition

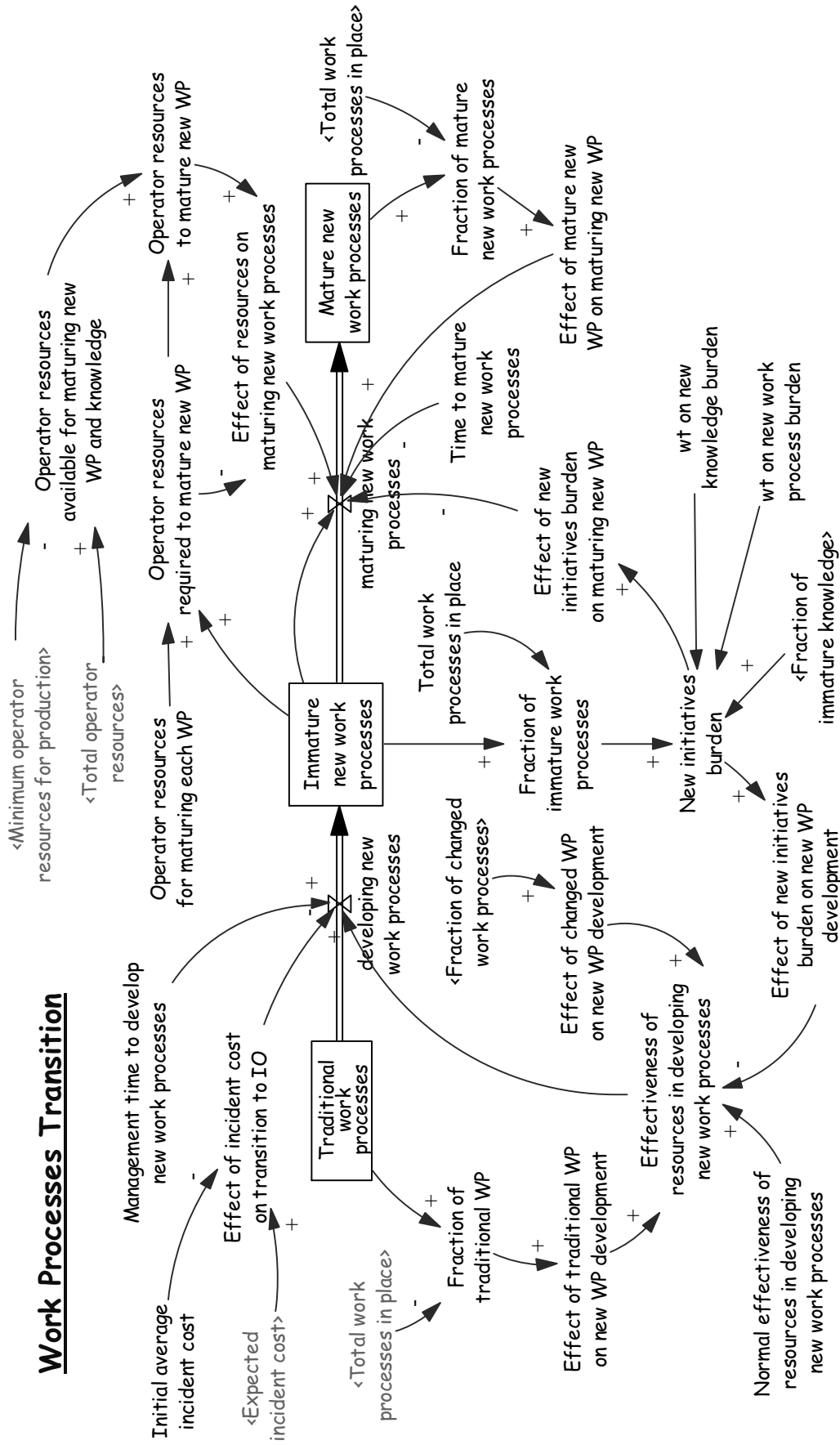


Figure 5-8 Work processes transition

The left part of Figure 5-8 focuses on the flow “*developing new work processes.*”

$$\begin{aligned} \text{Developing new work processes} = & \text{Management time to develop new work} \\ & \text{processes} * \text{Effectiveness of resources in developing new work processes} * \\ & \text{Effect of incident cost on transition to IO} \end{aligned}$$

The “*Management time to develop new work processes*” (located above the flow) is a decision variable based on the operation transition schedule. A tight schedule will require more management time to develop new work processes. As suggested by the platform chief, heads of several key departments are involved in new work processes development. These persons are in management and supervision roles. The time they allocate to develop new work processes will not affect the production output.

The “*Effectiveness of resources in developing new work processes*” (located below the flow), is affected by the “*Effect of traditional WP on new WP development*”, the “*Effect of new initiatives burden on new WP development*” and the “*Effect of changed WP on new WP development*” (changed work processes include both “*immature new work processes*” and “*mature new work processes*”). More traditional work processes mean more potential for new work processes development, which increases the “*Effectiveness of resources in developing new work processes*”. New initiatives burden represents the communication difficulties related to organizational change that lead to extra work load. Extra work load requires resources. Thus, fewer resources can be allocated to develop new work processes. As a result, the rate of developing new work processes is slowed down. In the Brage model, we do not go into the details of modeling the resources that are shared for the extra work load from new initiatives burden, but simplify the model in the way that new initiatives burden reduces the “*Effectiveness of resources in developing new work processes*”. More changed work processes mean more experiences in developing new work processes, which increase the “*Effectiveness of resources in developing new work processes*”.

The “*Effect of incident cost on transition to IO*” is another decision variable. This variable links the incident cost to operation transition speed, which forms the feedback presented in section 5.2.3 (p. 116). When the incident cost reaches a certain level, the management might feel it is too dangerous to continue the operation transition. The management might decide to suspend the operation transition. The

idea of delaying operation transition has been brought up several times during our communication with the client. Yet, the client does not have a clear idea about the quantitative measure: it is not clear under what circumstance the client will decide to suspend the operation transition, or how long the delay will be. There is no preset rule. On the one hand, this effect that adjusts the rate of developing new work processes and knowledge, has a major impact on the model behavior. On the other hand, there is no information available that we can utilize to quantify this variable. Under such circumstances, we choose to first simulate the model without consideration of the “*effect of incidence cost on transition to IO*” (this parameter is set to 1) to study the transition speed, resource allocation and investment in incident response capability. Then, in a separate section (section 8.3), we will investigate several scenarios specifically testing how management’s response to incident cost affects the operation transition and information security risks (“*Effect of incident cost on transition to IO*” will be assigned different values).

The right part of Figure 5-8 focuses on the flow of “*maturing new work processes.*”

$$\begin{aligned} \text{Maturing new work processes} = & \text{Immature new work processes} / \text{Time to} \\ & \text{mature new work processes} * \text{Effect of resources on maturing new work} \\ & \text{processes} * \text{Effect of the new initiatives burden on maturing new WP} * \text{Effect} \\ & \text{of mature new WP on maturing new WP} \end{aligned}$$

The “maturing new work processes” is a process of learning, which converts immature new work processes into mature ones. The learning curve is in diminishing return shape: rate of learning is greatest at first when “ignorance” is greatest; rate of learning decreases as ignorance decreases. The function “*Immature new work processes / time to mature new work processes*” represents this curve. When more immature new work processes exist, the rate of learning is high. When learning occurs, immature new work processes are converted into mature ones, leaving fewer immature new work processes, and the rate of learning is reduced. At the same time, learning is also affected by the “*Effect of resources on maturing new work processes*”, “*Effect of the new initiatives burden on maturing new WP*”, and “*Effect of mature new WP on maturing new WP*”. If the resources to mature new work processes is not sufficient, meaning the operators do not have enough time to learn new work processes, the rate of maturation process will be reduced. The “*new initiatives burden*” requires resources. As a result, “*new initiatives burden*” will slow down the

maturation process. On the other hand, when mature new work processes accumulate, meaning people have experience working with the new work processes and the new technology embedded in them, the maturation process will speed up.

The upper right part of Figure 5-8 captures the resources allocation. Here, resources refer to the operators' time. It is measured as a percentage of the total operators' working time. "*Total operator resources*" is, by definition, 100% of operators' working time. The operators work 12 hour/day on the platform. The absolute amount of "*Total operator resources*" equal to 12 hour/day or 360 hour/month. The "*Minimum operator resources for production*" is a policy variable—the management could decide what percentage of the operators' time to reserve for production based on its production target. As suggested by the platform chief, 10%-15% of the operators' time is allocated to learn new work processes and acquire new knowledge. In the base scenario, the "*Minimum operator resources for production*" is set to 90%, which means 324 hour/month in absolute amount. The "*Operator resources available for maturing new WP and knowledge*" is, then, 10% of operators' working time, 36hour/month, about 1.2 hour/day.

$$\text{Operator resources available for maturing new WP and knowledge} = \text{Total operator resources} - \text{Minimum operator resources for production}$$

The platform chief estimated that 4% of the operators' time is needed to mature one new work process. Therefore, the "*operator resources for maturing each WP*" is 4% of operators working time/process (equal to 0.48 hour/day/process). The overall operators' resources required to mature new work processes is the product of "*operator resources for maturing each WP*" and "*immature new work processes*". When one new work process is implemented, 4% of operators working time are needed to learn this new work process. As time goes by, the operators have learnt part of the new work process, and then less time is needed to mature the remaining immature part. When the new work process is completely matured, there is no need of time for learning.

$$\text{Operator resources required to mature new WP} = \text{Operator resources for maturing each WP} * \text{Immature new work processes}$$

If many "*immature new work processes*" are in place, then the "*Operator resources required to mature new WP*" will be high. However, there is a constraint on resources

that is the resources available, - “*Operator resources available for maturing new WP and knowledge.*” It is not possible to have more resources than what is available. On the other hand, it is not necessary to have more resources than what is required. Therefore, the actual operator resources to mature new work processes are the minimum of the two variables, “*Operator resources required to mature new WP*” and “*Operator resources available for maturing new WP and knowledge.*”

Operator resources to mature new WP = min (Operator resources required to mature new WP, Operator resources available for maturing new WP and knowledge)

When the “*Operator resources required to mature new WP*” is higher than the “*Operator resources available for maturing new WP and knowledge,*” meaning not enough resources are available to mature all the “*immature new work processes,*” then the rate of maturation is reduced, which result in longer time to mature all the immature new work processes.

5.3.2 Sector 2—Knowledge

The sector of knowledge transition has a similar structure as the sector of work processes transition. The stock and flow chain captures the transition of knowledge from the traditional one (“*Traditional knowledge*”) to the newly acquired one (“*Immature new knowledge*”), and on to the mature one (“*Mature new knowledge*”).

The left part of Figure 5-9 focuses on the flow of “*developing new knowledge.*”

*Developing new knowledge = Management time to develop new knowledge * Effectiveness of resources in developing new knowledge * Effect of incident cost on transition to IO*

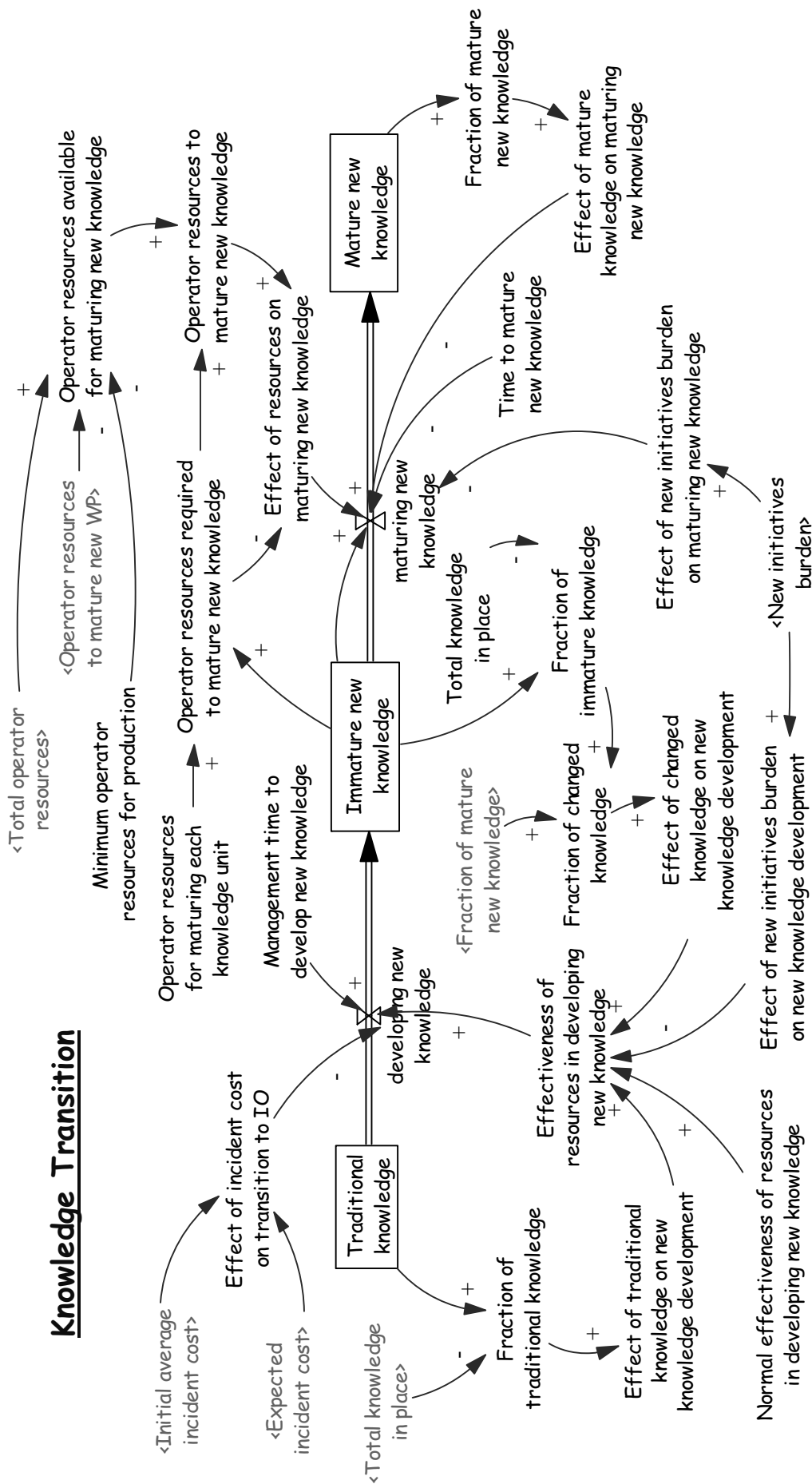


Figure 5-9 Knowledge transition

The right part of Figure 5-9 focuses on the flow of “*maturing new knowledge.*”

$$\text{Maturing new knowledge} = \text{Immature new knowledge} / \text{Time to mature new knowledge} * \text{Effect of resources on maturing new knowledge} * \text{Effect of new initiatives burden on maturing new knowledge} * \text{Effect of mature knowledge on maturing new knowledge}$$

These two pieces of structure are analogous as those for the work processes transition. Hence, we will not go into the details.

The upper right hand side of Figure 5-9 captures the resources allocation. The allocation of the operators’ time is in the following order: first a certain percentage of their time is reserved for production; the remaining time is then prioritized to mature new work processes; after that, the available time is to mature new knowledge. This is because knowledge is mostly tacit, - its development is not so observable. Therefore, the operators tend to ignore knowledge development when resources are not available to mature both new work processes and knowledge.

$$\text{Operator resources available for maturing new knowledge} = \text{Total operator resources} - \text{Minimum operator resources for production} - \text{Operator resources to mature new WP}$$

The remaining structure is analogous to that of the work processes transition. The operators’ resources for maturing each knowledge unit is estimated to be 4% of the total operators’ resources, which is the same as that needed to mature each new work process. The overall resources required to mature new knowledge are the product of “*Operator resources for maturing each knowledge unit*” and “*Immature new knowledge*”.

$$\text{Operator resources required to mature new knowledge} = \text{Operator resources for maturing each knowledge unit} * \text{Immature new knowledge}$$

However, it is not possible to have more resources than what is available.

$$\text{Operator resources to mature new knowledge} = \min(\text{Operator resources available for maturing new knowledge}, \text{Operator resources required to mature new knowledge})$$

When the “*Operator resources required to mature new knowledge*” is more than “*Operator resources available for maturing new knowledge,*” meaning not enough resources are available to mature new knowledge, the rate of knowledge maturation is reduced and thus, the maturation of new knowledge will be prolonged.

The assumption of resources allocation used in this model (first to production, then to mature new work processes, and finally to mature new knowledge) was presented to client and related experts. All of them agreed to this assumption.

5.3.3 Sector 3—Vulnerability

This sector of the model represents the overall vulnerability level of the Brage platform during the operation transition. We use the term “*Vulnerability Index*” to express how vulnerable the platform is. This term reflects the fraction of events (those have the potential to become incidents) that actually turn into incidents. For example, receiving an email with a virus in attachment is an event. If the receiver has the knowledge that an attachment can contain a virus, and does not open the email, then, this event will not turn into an incident. On the other hand, if the receiver doesn't have that knowledge and opens the attachment and the computer is affected by the virus, then, this event becomes an incident.

The vulnerability index will increase if operators do not know what to do, - the fraction of immature new work processes affects vulnerability index. The vulnerability index will increase if operators do not know how to do, - the fraction of immature new knowledge affects vulnerability index. The vulnerability index will increase if operators do not understand why to work in this way. “Knowledge gap” is an indicator for the amount of new work processes that operators do not know why to work in this way. Therefore, the knowledge gap affects vulnerability index.

The vulnerability index could be reduced by getting to know what to do (mature new work processes), how to do (mature new knowledge) and why to work in this way (mature new knowledge).

Vulnerability Index

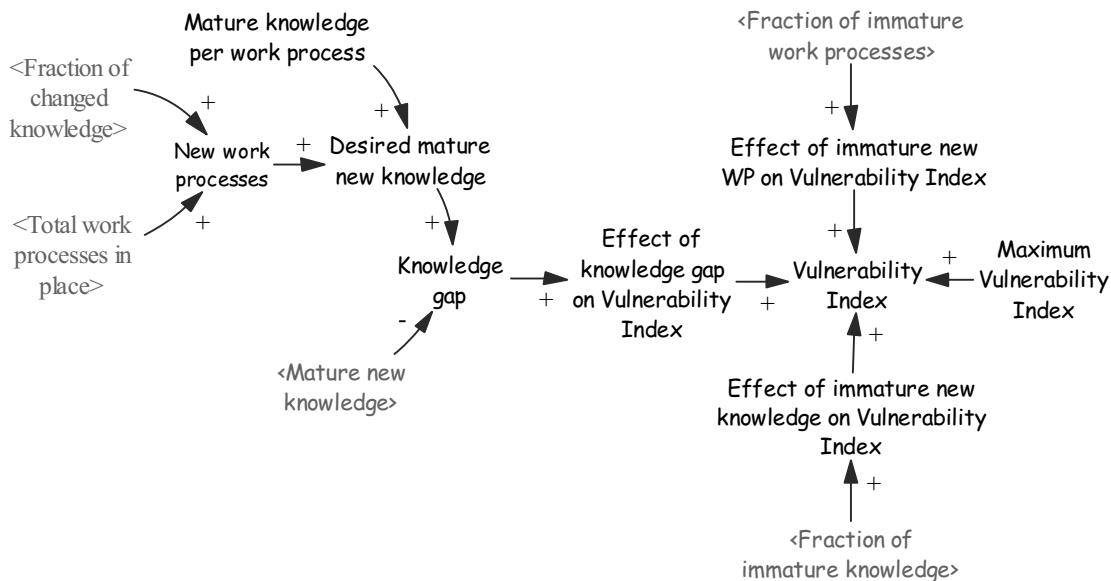


Figure 5-10 Vulnerability Index

$$\text{Vulnerability Index} = \text{Maximum Vulnerability Index} * \text{Effect of immature new WP on Vulnerability Index} * \text{Effect of immature new knowledge on Vulnerability Index} * \text{Effect of knowledge gap on Vulnerability Index}$$

“Maximum Vulnerability Index” is a reference point based on the theoretical worst case, in which every event turns into an incident. Therefore, it is 100%. However, in reality, this theoretical worst case will never be reached no matter how bad the situation is, “luck” prevents some events from turning into “incidents”. We use multiple factors to set the range (upper and lower limits) of vulnerability index. These factors are, as shown in the above equation, “Effect of immature new WP on Vulnerability Index,” “Effect of immature new knowledge on Vulnerability Index,” and “Effect of knowledge gap on Vulnerability Index”.

There are no numerical data for these three factors. We have to make our own assumptions for them. We use table functions to quantify these effects. The way we formulate these table functions involves two steps: first, identify the range of the output variable, and second, determine the shape of the curve.

Table 5-2 summarizes the formulation of these three effects, followed by the detailed verbal explanation. Figure 5-11, Figure 5-12, and Figure 5-13 show the graphic image of these three effects respectively.

Table 5-2 The effects on the vulnerability index

	Lower level	Upper level	Shape
<i>Effect of immature new WP on Vulnerability Index</i>	40% of the maximum when all the work processes are mature	90% of the maximum when all the work processes are immature	Goal seeking. See Figure 5-11
<i>Effect of immature new knowledge on Vulnerability Index</i>	40% of the maximum when all the knowledge is mature	80% of the maximum when all the knowledge is immature	Goal seeking. See Figure 5-12
<i>Effect of knowledge gap on Vulnerability Index</i>	40% of the maximum when the knowledge gap is 0	80% of the maximum when the knowledge gap is 20	Linear See Figure 5-13

The low level: In the best situation, when the operators are familiar with all the work processes and knowledge and there is no knowledge gap, the vulnerability index will be low. We assume that it is lower than 10%. Each of the three effects would equally contribute on the vulnerability index. Therefore, we set the low level of each of the three effects on vulnerability index as 0.4, resulting vulnerability index at 6.4%.

The high level: In the worst situation, we assume that around half of the events will become incidents. During our interview, all experts thought that the immature work process has the biggest impact on the vulnerability index, while the immature knowledge and the knowledge gap impact on the vulnerability index similarly. Therefore, we set the “*effect of immature new work processes on vulnerability index*” at 90% of maximum level, while “*effect of immature new knowledge on vulnerability index*” and “*effect of knowledge gap on vulnerability index*” at the 80% of maximum level. These maxima lead to a 57.6% of events turning into incidents.

The shape of the curves, the “*effect of immature new work processes on vulnerability index*” and the “*effect of immature new knowledge on vulnerability index*” are similar. They are both in diminishing return shape. Introducing new work processes and associated new knowledge increases vulnerability index. The rate of the increase is decreasing because all the new work processes and knowledge are based on advanced ICT that connect offshore platform to the onshore control center and other facilities. The basics of what to do and how to do in Integrated Operations have similarities. Additional new work process and knowledge has a decreasing impact on the

vulnerability index. Therefore, the curves have a marginal decreasing shape. The shape of the curve, the “*effect of knowledge gap on vulnerability index*”, is linear. Each new work process has its specific reasons why the new work process is arranged in this way and how to react to deviations. Since we do not differentiate work processes, one knowledge gap will have the same effect as another knowledge gap. Therefore, the “*effect of knowledge gap on vulnerability index*” is linear.

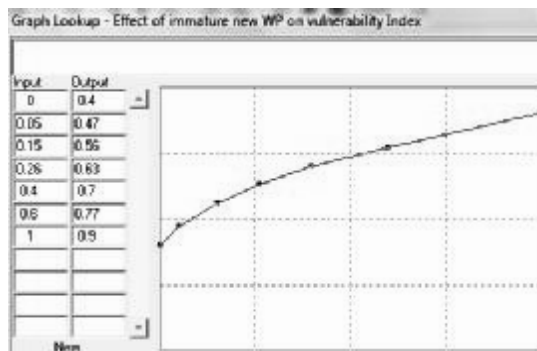


Figure 5-11 Effect of immature new WP on the vulnerability index

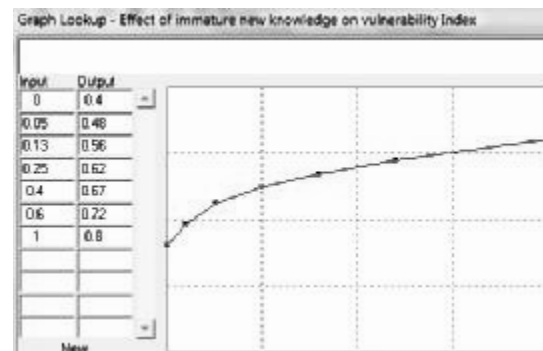


Figure 5-12 Effect of immature new knowledge on the vulnerability index

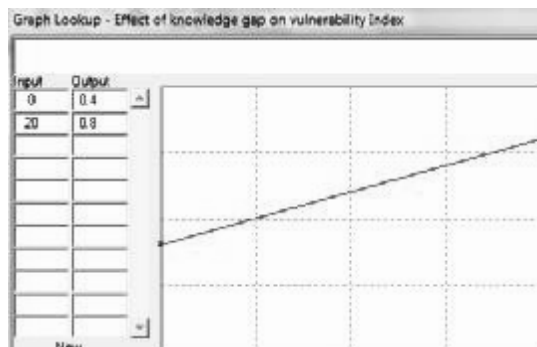


Figure 5-13 Effect of mature knowledge adequacy on the vulnerability index

To sum up, the vulnerability index ranges from lowest at 6.4% ($0.4 \cdot 0.4 \cdot 0.4$), when there are no immature new work processes, no immature new knowledge, and no knowledge gap, to highest at 57.6% ($0.9 \cdot 0.8 \cdot 0.8$) when all the new work processes and all new knowledge are immature and the knowledge gap is the greatest. The highest point of vulnerability is 9 times as high as the lowest point. Sensitivity tests on these estimated table functions are performed, details see Appendix IV Sensitivity tests p. 291).

5.3.4 Sector 4—Incident cost

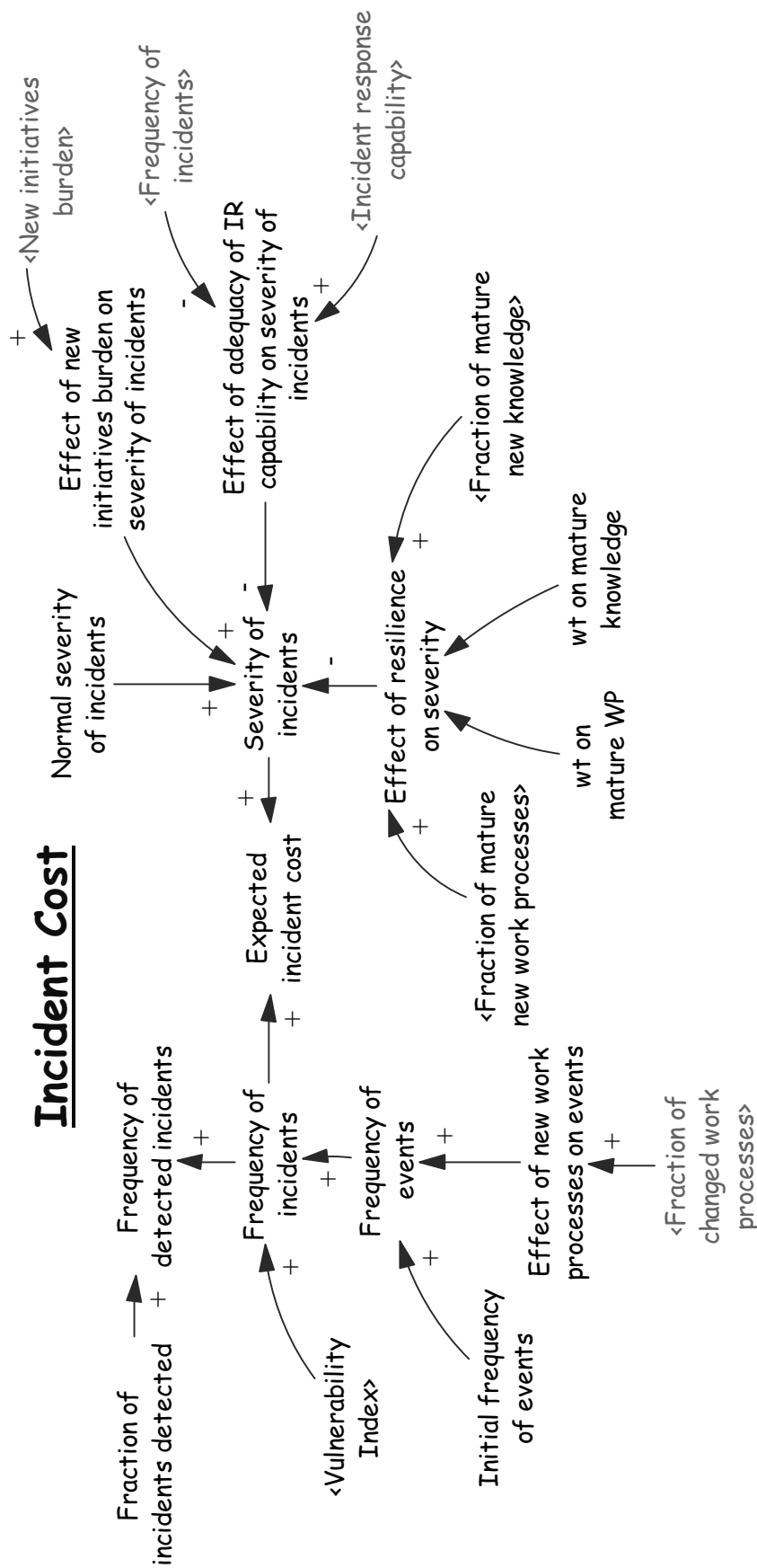


Figure 5-14 Incident cost

This sector of the model focuses on incident. The key variables are the “*Frequency of incidents*”, “*Severity of incidents*” and “*Expected incident cost*”. “*Frequency of incidents*” represents how frequently incidents happen. This variable is measured as incident/month. “*Severity of incidents*” represents how severe incidents are. This variable is measured as NOK/incident, the total cost incurred because of the incidents. “*Expected incident cost*” represents the average incident cost per month. This variable is the product of “*Frequency of incidents*” and “*Severity of incidents*”, measured as NOK/month.

$$\text{Expected incident cost} = \text{Frequency of incidents} * \text{severity of incidents}$$

“*Frequency of incidents*” is the product of the “*Vulnerability Index*” and the “*Frequency of events.*” The “*frequency of events*” represents the threats to the computer system. Only those threats that successfully exploit the vulnerabilities become incidents.

$$\text{Frequency of incidents} = \text{Frequency of events} * \text{Vulnerability Index}$$

“*Frequency of events*” is affected by the operation transition.

$$\text{Frequency of events} = \text{Initial frequency of events} * \text{Effect of new work processes on events}$$

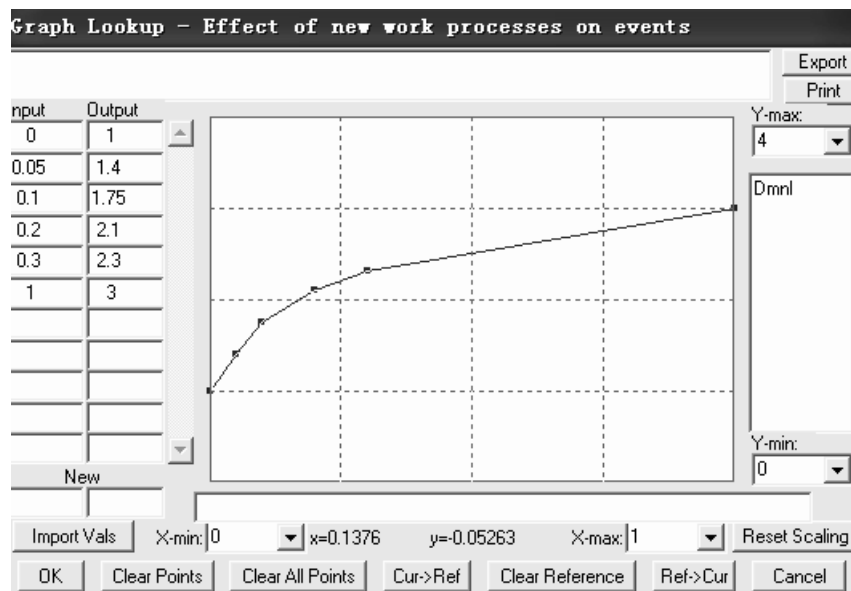


Figure 5-15 Effect of new work processes on events

The formulation of “*effect of new work processes on events*” is based on the rationale that when there is no operation transition there is no change of the “frequency of

events”, - meaning “*effect of new work processes on events*” should be 1. When the operation transition starts, there is a sharp increase of “frequency of event” since the platform starts to connect to the office LAN and from there to the Internet. Many threats on the Internet and office LAN that originally could not affect offshore platforms now can. After a period of fast increase, “*frequency of events*” enters a period of slow and steady increase. This increase is due to that more parties are gradually involved in Integrated Operations, bringing with them new threats. At the end, the threats are three times as high as that in traditional operation. Common sense might point to even higher threats. However, as suggested by our client, several layers of technical security defenses have been put in place so that not so many threats actually reach the operation system on platform.

“*Severity of incidents*” represents the average cost of an incident. This cost includes the cost of loss of production and the cost to restore everything back to its normal state. “*Severity of incidents*” is affected by the resilience of the system, the new initiatives burden, and the incident response capability.

$$\text{Severity of incidents} = \text{Normal severity of incidents} * \text{Effect of resilience on severity} * \text{Effect of new initiatives burden on severity of incidents} * \text{Effect of adequacy of IR capability on severity of incidents}$$

The more resilient an organization is, the quicker it would recover from the incidents, lowering the cost of loss of production, thus, reducing the severity of incidents. The new work processes are supposed to increase the platform’s resilience because the new technology enables quick access to experts. In traditional operations, experts have to be transported to the platform using helicopters, which takes time and is costly. In the Integrated Operations, experts can access the visual information and data information of offshore platform via net connection. Therefore, experts can investigate the offshore problem in their local place. The access to experts is much faster and less expensive in Integrated Operations than in traditional operation. As a result, the cost of handling incidents will be reduced. However, when new work processes and knowledge are immature, the new initiatives burden (not knowing who to contact) will add difficulty to incident handling. Meanwhile, the adequacy of the incident response capability is also a key factor affecting the severity of incidents. If incident response capability is inadequate, some incidents are not detected and handled in time. This gives them the opportunity to develop into more severe

incidents.

As discussed in the Literature Review, Section 2.2.2 (p. 22), risk is defined as the probability that a damaging incident happens (when a threat occurs because of vulnerability) multiplied by the potential damage: “Risk = Threat * Probability of the threat penetrating the vulnerability * Potential impact”. Therefore, the “expected incident cost” represents the overall information security risks.

5.3.5 Sector 5—Learning from incidents

This sector models learning from incidents.

Learning from Incidents

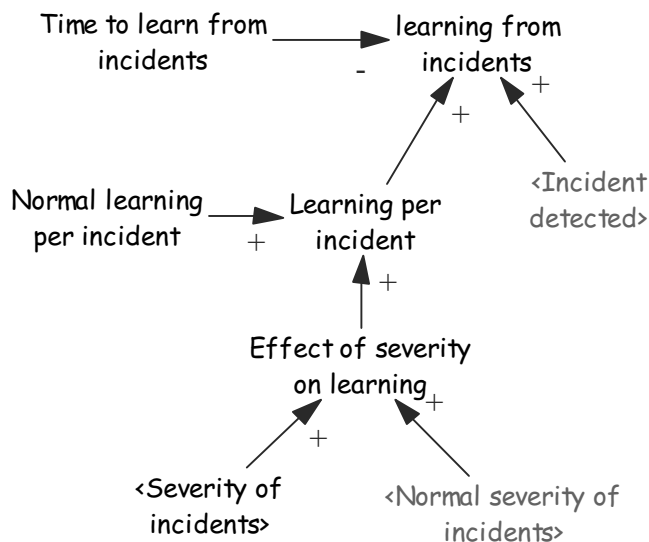


Figure 5-16 Learning from incidents

How much the incident response team can learn from incidents depends on the number of incidents detected (- it is not possible to learn from undetected incidents.) and how much is learned from each incident “*learning per incident*”. Learning takes time. After the incidents, people need to reflect on what has happened, find out the causes, develop documentation, and share information. We assume that the learning takes place in the course of a three-month period (“*time to learn from incidents*”) after the incidents happened. Therefore, we use a smoothing function⁷ to represent

⁷ Smooth functions are to present information delay. Instead of having an immediate impact at full height, smooth functions gradually reach the full height of the impact.

the process “*learning from incidents.*”

$$\text{Learning from incidents} = \text{SMOOTH}(\text{Learning per incident} * \text{Incident detected}, \text{Time to learn from incidents})$$

“*Learning per incident*” is affected by how severe the incident is. Experience shows that one learns more from severe incidents and tends to ignore minor incidents. Our client believes this is true also in the client organization.

$$\text{Learning per incident} = \text{Normal learning per incident} * \text{Effect of severity on learning}$$

5.3.6 Sector 6—Incident response capability

This sector of the model represents the incident response capability. This capability is defined as the number of incidents (with normal severity, which is 500,000 NOK/incident) that could be handled in a month (unit: incident/month). A less severe incident needs less response capability while a more severe incident requires more response capability. The incident response capability has two aspects: one is how many resources (people*time/month) are devoted to the work, and the other is how productive these resources are (incident/(people*time)). A decision to increase incident response capability could be to add more resources to this work or to improve the productivity of the existing resources. In either way, financial investment is needed. According to IRMA, the work scope of the incident response capability is mainly to detect incidents, handle incidents and learn from incidents.

The incident response capability becomes obsolete over time. New attack tools, new vulnerabilities, and new viruses, emerge quickly in the area of information security. In the model, we assume that incident response capability obsoletes after one year.

Incident Response Capability

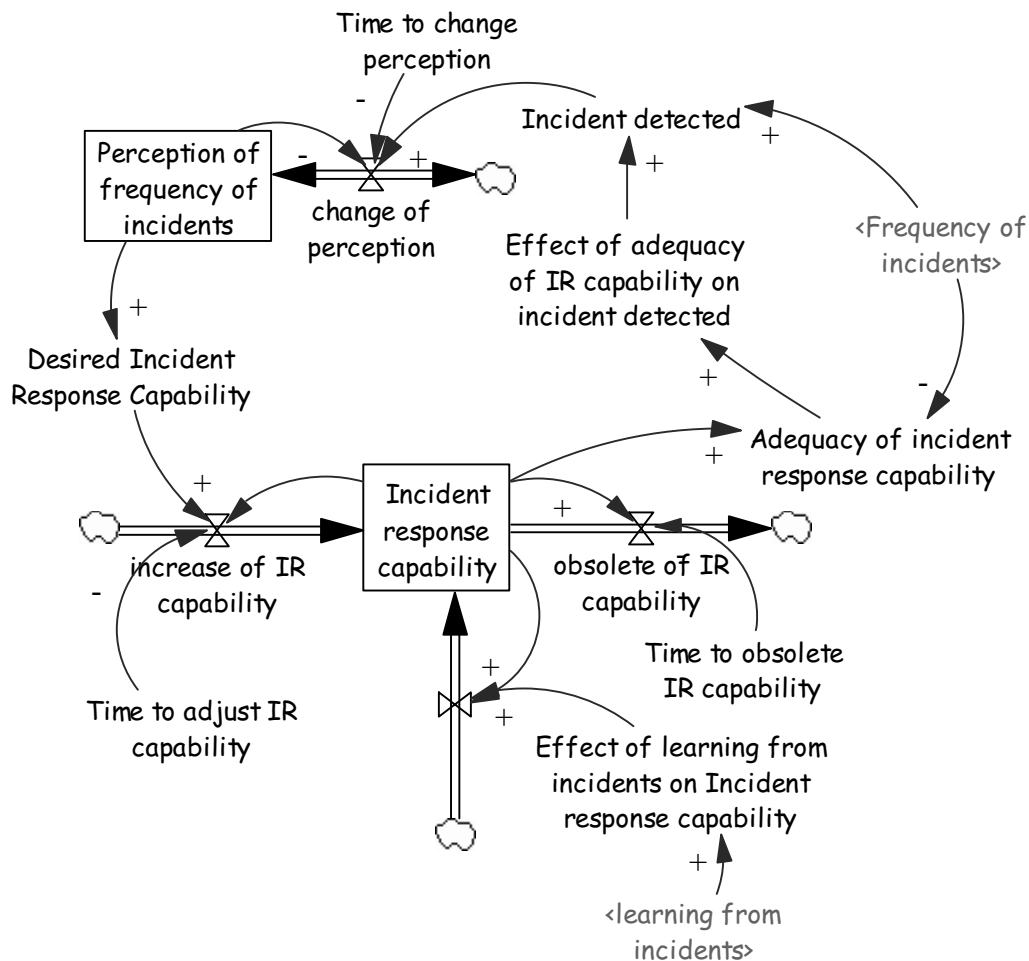


Figure 5-17 Incident response capability

The lower part of Figure 5-17 focuses on the change of incident response capability. Learning from incidents improves incident response capability. However, as suggested by the IRMA team, as the incident response team is ad hoc, there is no deliberate learning process in place. Thus the positive effect to improve incident response capability from “*learning from incidents*” is weak. The increase in incident response capability is mainly from the management’s investment. The management decides the desired level of incident response capability and makes investments to reach that level. The desired incident response capability is based on the perception of the frequency of incidents.

The upper part of Figure 5-17 focuses on formulation of the perception of frequency of incidents. This perception is based on incident detected. Management only knows about those incidents that have been detected. Those undetected ones go unnoticed. It

is common that some incidents are not detected. The fraction of incidents that could be detected is dependent on the adequacy of incident response capability.

$$\text{Incident detected} = \text{Frequency of incidents} * \text{Effect of adequacy of IR capability on incident detected}$$

$$\text{Adequacy of incident response capability} = \frac{\text{Incident response capability}}{\text{Frequency of incidents}}$$

If the adequacy of incident response capability is high, a higher fraction of incidents will be detected. If the adequacy of incident response capability is low, a lower fraction of incidents will be detected. Figure 5-18 shows the formulation of the “*effect of adequacy of incident response capability on incident detected*”.

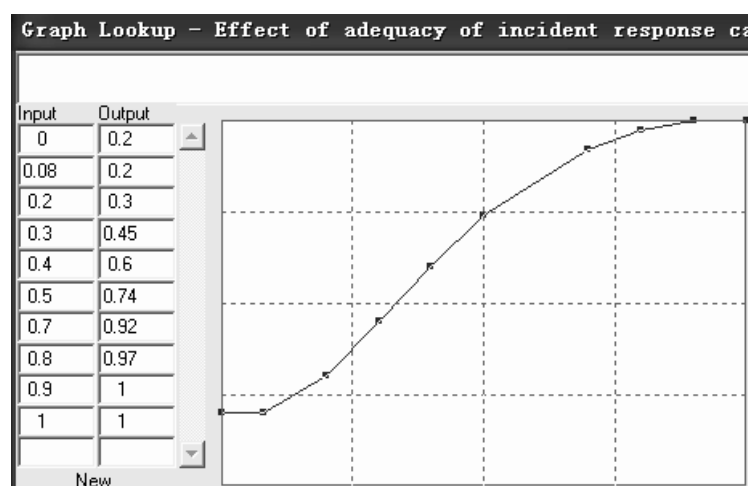


Figure 5-18 The effect of adequacy of incident response capability on incident detected

The “*effect of adequacy of incident response capability on incident detected*” is given by an S-shaped curve, starting from (0, 0.2), which means even there is no incident response capability, 20% of the incidents will be detected. When the adequacy of incident response capability reaches 90%, then all the incidents could be detected (0.9, 1). At the low end, when the adequacy of incident response capability is so low, adding additional incident response capability will not lead to major improvement in incident detection. Therefore, the output increases slowly. At the high end, when most of incidents could be detected, adding additional incident response capability, leads to diminishing return on the output. Therefore, the curve has an S-shape.

5.3.7 Sector 7—Production and profit

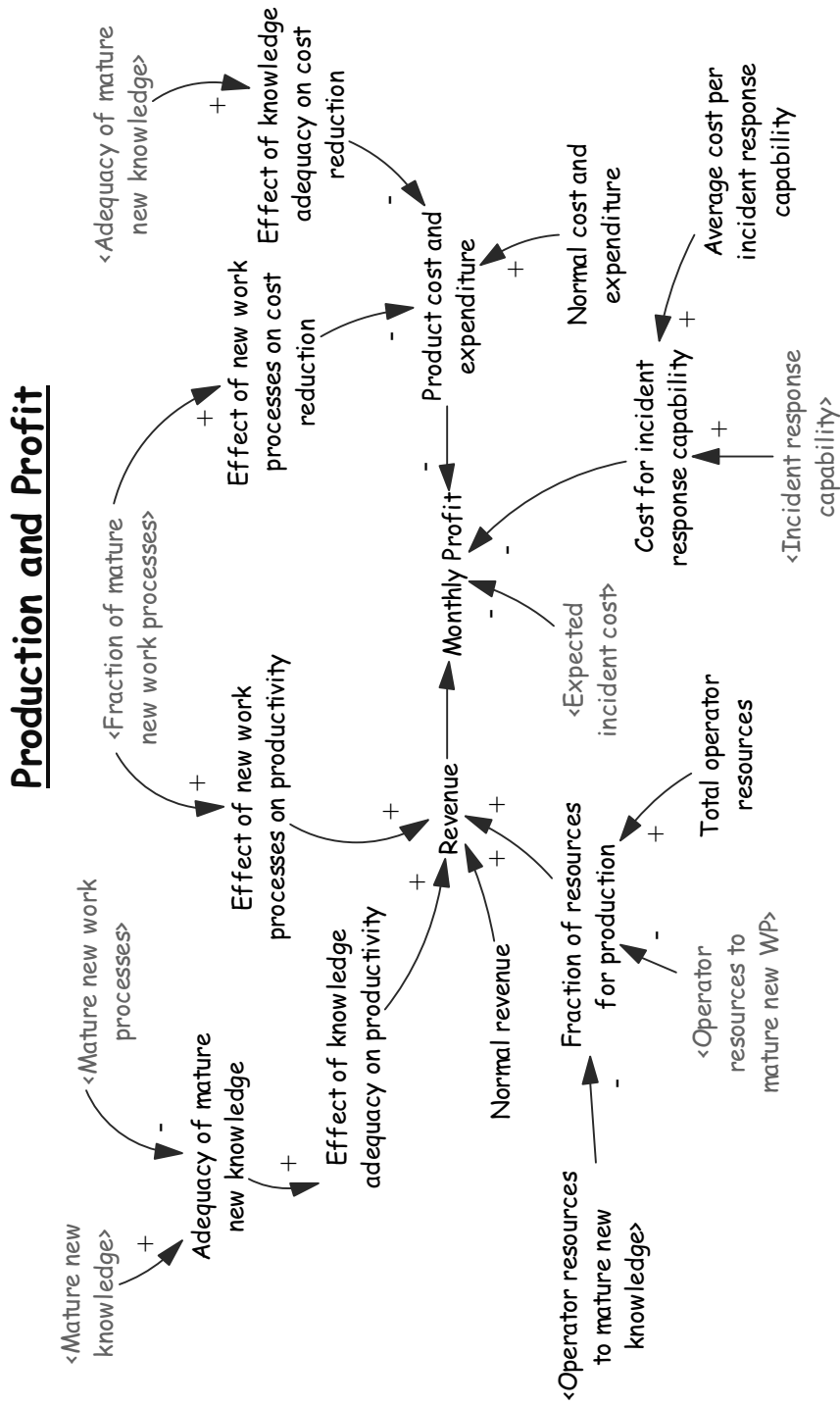


Figure 5-19 Production and profit

This sector of the model represents the production and profit resulting from the Brage operations. As introduced in Chapter 1, the Integrated Operations is expected to generate an 10% increase in revenue and a 30% reduction in production cost. These benefits will gradually be realized as the transition to Integrated Operations continues.

The “*Monthly profit*” is in line with its definition as a financial term. It is formulated as “*revenue*” minus “*product cost and expenditures*”, “*incident cost*” and “*cost for incident response capability*”.

$$\text{Monthly Profit} = \text{Revenue} - \text{Product cost and expenditure} - \text{Expected incident cost} - \text{Cost for incident response capability}$$

“*Expected incident cost*” and “*cost for incident response capability*” are outputs from the “*incident cost*” sector and the “*incident response capability*” sector, respectively. “*Revenue*” and “*Product cost and expenditure*” are affected by the operation transition:

$$\text{Revenue} = \text{Normal revenue} * \text{Fraction of resources for production} * (1 + \text{Effect of new work processes on productivity} * \text{Effect of knowledge adequacy on productivity})$$

“*Normal revenue*” is a constant. There is no consideration of oil price change. This is because, first, oil price is an external factor; and moreover, we would actually like to exempt the effect of oil price on revenue and profit. This way, we can observe the change of production and profit that is caused solely by the mechanism of operation transition. Revenue is only related to production, which is affected by the resources for production and the productivity change during the operation transition. When new work processes are implemented, there is a potential to raise the productivity. However, this potential cannot be fully realized without maturing the related new knowledge. Here, we do not take into account the production change due to the change of oil reserve for the same reason as why we do not consider the oil price change.

Similar to “*revenue*”, “*product cost and expenditure*” is also affected by the new work processes and knowledge implemented and by the maturity of them. The change in salary and other raw material prices are not considered. We only focus on the effect of operation transition on product cost and expenditure.

$$\text{Product cost and expenditure} = \text{Normal product cost and expenditure} * (1 - \text{Effect of new work processes on cost reduction} * \text{Effect of knowledge adequacy on cost reduction})$$

The outputs of this sector, revenue, product cost and expenditure and monthly profit, are most important indicators for business organizations. High profit is always desirable. Moreover, the purpose of the transition to Integrated Operations is to generate high profit. By using the model for simulation purposes, we may investigate how profit changes during the operation transition.

5.4 Model behavior

We now present the model behavior. This scenario is called the base run scenario. All other scenarios, either for model testing or for policy testing, are compared with this base run scenario. In some studies, model behavior analysis is also regarded as one way of model validation (Andersen et al. 1983). In this study, we present it to foster the understanding of the model structure. We will present our model validation in the next chapter.

In the base run scenario, the operation transition speed is according to the real plan on the Brage platform: 5 new work processes are implemented in the first year and 2 new work processes each year after that. There are more management resources to develop new work processes and knowledge in the first year and fewer in the following years. In the base run, the minimum of the operators' resources reserved for production are 90% of the total the operators' resources. Figure 5-20 shows the transition of work processes.

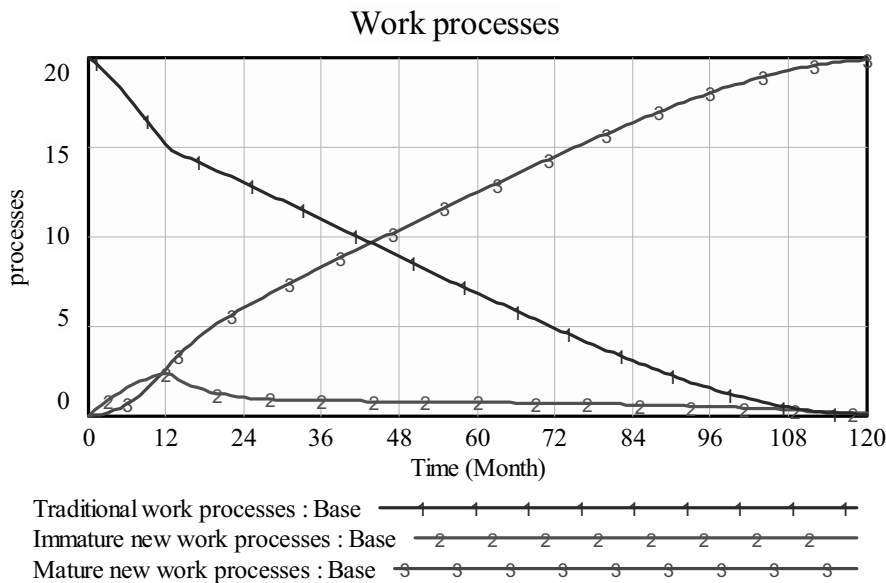


Figure 5-20 Work processes transition

In Figure 5-20, the “*traditional work processes*” (blue line with number 1) decrease according the operation transition plan. The “*immature new work processes*” (red line with number 2) increase in the first year and then decreases. This is because in the first year, there are not enough resources for maturing all 5 of them at the rate they are introduced. Around 2.5 new work processes are matured and leaving around 2.5 new work processes immature. From the second year on, when the transition speed lowers to 2 new work processes a year, the “*immature new work processes*” decrease. The “*mature new work processes*” (green line with number 3) increase slowly at the beginning because no previous experience exists for Integrated Operations. After year one, it increase steadily, reaching more than 19 mature new work processes by the end of year 9, and slowly reaching 20 during the last year of the transition.

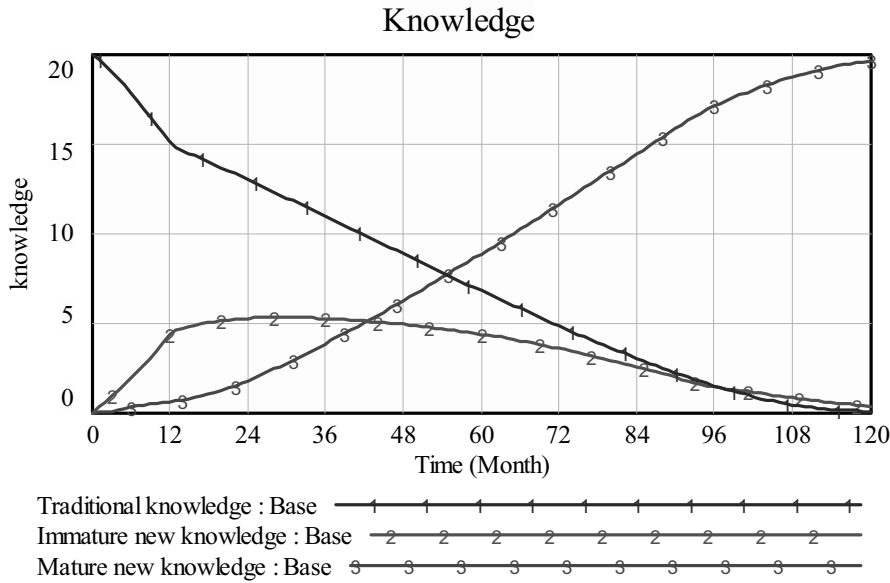


Figure 5-21 Knowledge transition

In Figure 5-21, the “*traditional knowledge*” (blue line with number 1) decreases according the operation transition plan. The “*Immature new knowledge*” (red line with number 2) increases to almost 5 during the first year and remains at that level until month 48 after which it decreases gradually until month 96 (reaching around 2). During the last two years, it decreases slowly, approaching 0. The “*Mature new knowledge*” (green line with number 3) increases slowly during the first two years (reaching around 2 at the end of year 2) and then increases progressively until month 96 (reaching around 17). In the last two years, it approaches 20 with a decreasing speed. The behavior is a typical S-shape behavior.

The behavior of “*Immature new work processes*” and “*Immature new knowledge*” were quite different. There are several reasons for that. First of all, knowledge maturation was slower than work processes maturation. It took 4 months for new work processes to mature, while 8 months for new knowledge to mature. Therefore, the “*immature new knowledge*” accumulated to a higher level.

The second reason was the shortage of resources to mature knowledge, especially during the first year, when 5 new work processes were introduced. In Figure 5-22, the lower part in blue color represents the resources to mature new work processes and the upper part in red color represents the resources to mature new knowledge. We can see that when more and more new work processes and knowledge are introduced, there are not enough resources to mature both of them. Since the operators prioritize

the maturation of new work processes, the time available to mature new knowledge is reduced, reaching the lowest at the end of year 1 when there are so many immature new work processes that little time is left for maturing new knowledge. After year 1, when the implementation speed reduces to 2 new work processes per year, the immature new work processes are reduced and more resources could be allocated to mature new knowledge.

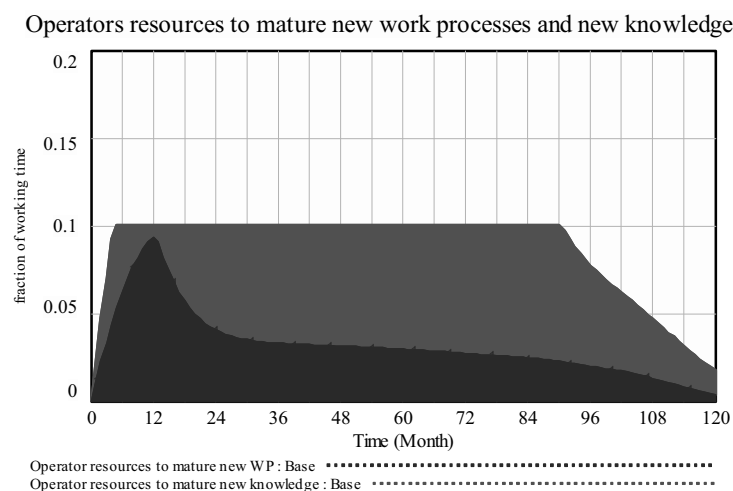


Figure 5-22 The operators resources to mature new work processes and knowledge

The third reason for the slow development of mature new knowledge during the first two years is the reinforcing loop R4 (see section 5.2.1). With more immature new knowledge, the initiatives burden is high, thus reducing the speed to mature new knowledge. The other loop R2 (see section 5.2.1) is weak at that point because not much knowledge has matured yet. Therefore, not much experience to facilitate knowledge maturation. After the first two years, the mature knowledge has gradually accumulated, which facilitates the maturation of new knowledge, - the speed of new knowledge maturation is increased. After month 96, the maturation of new knowledge slows down again. This is because the effect of the balancing loop B2 is significant at that point: when only little knowledge remains immature, the further maturation of new knowledge is of great challenge and the rate of maturing new knowledge is reduced.

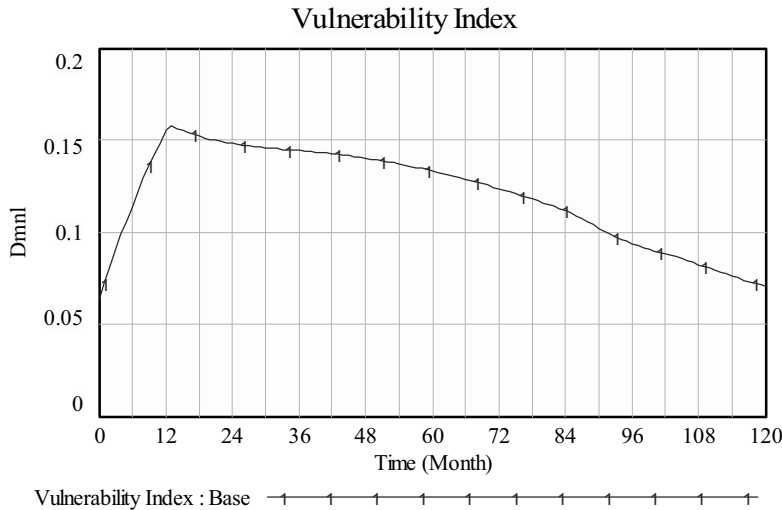


Figure 5-23 The Vulnerability Index

The vulnerability index sharply increases during the first year because “immature new work processes,” “immature new knowledge,” and “knowledge gap” make the platform vulnerable. During the second year, “immature new work processes” drops to about half its value (see Figure 5-20). This leads to the decrease in the vulnerability index. However, the decrease is not much because “immature new knowledge” (see Figure 5-21) and “knowledge gap” (see Figure 5-24) still are increasing. The vulnerability index drops slowly during year 3 and 4, as “immature new work processes,” “immature new knowledge,” and “knowledge gap” decrease slightly. From year 5 on, as more knowledge mature, the “immature new knowledge,” and “knowledge gap” both decrease faster. Thus, the vulnerability index decreases correspondingly.

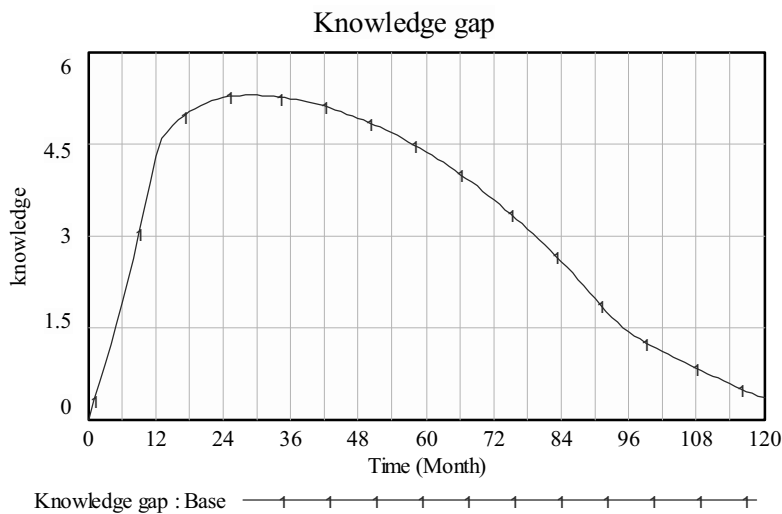


Figure 5-24 Knowledge gap

The “*expected incident cost*” is the product of the “*frequency of incidents*” and the “*severity of incidents*”. Since both “*frequency of incidents*” and “*severity of incidents*” increase sharply in the first year, so does the “*expected incident cost*”. It peaks around the end of the first year and drops quickly to a relatively low level after month 48. This is because of the decrease in the “*severity of incidents*”. After that, the “*expected incident cost*” slightly decreases, - mainly due to the reduction in the “*frequency of incidents*”.

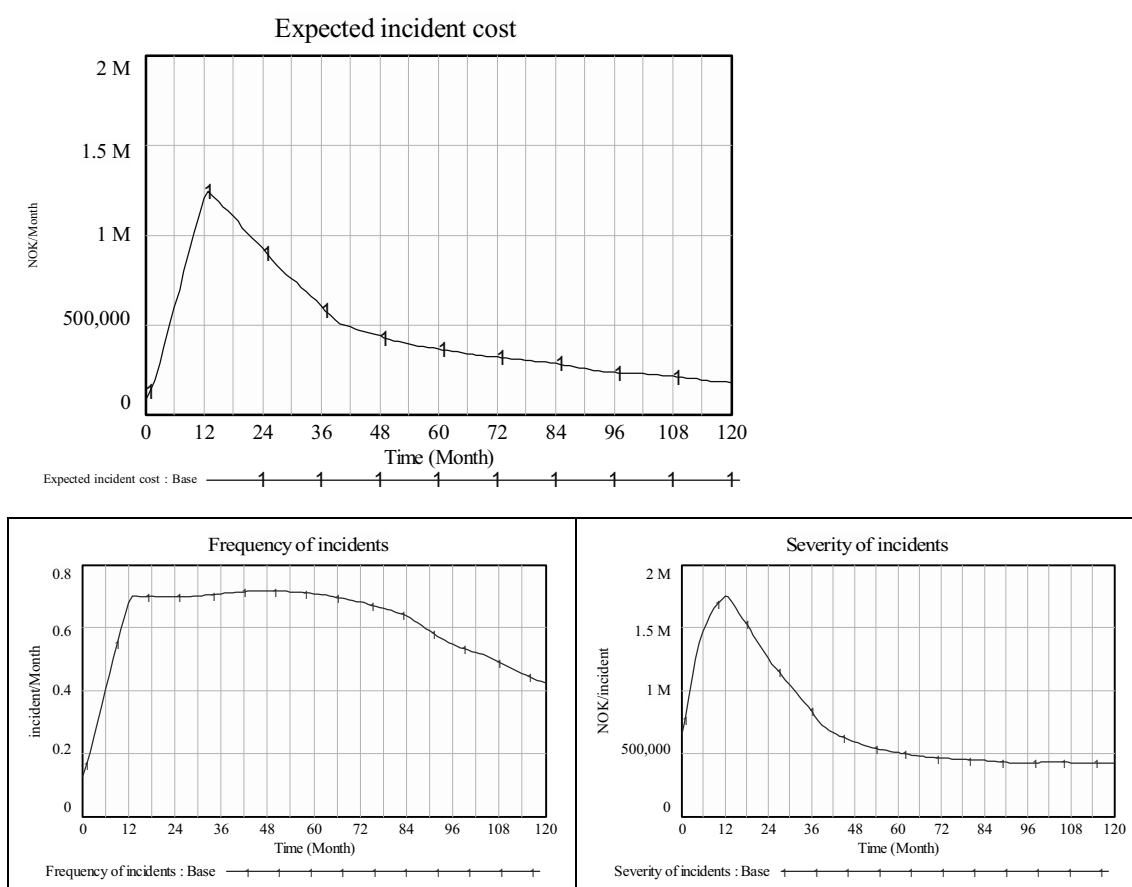


Figure 5-25 Frequency of incidents, Severity of incidents, and Expected incident cost

The “*frequency of incidents*” increases sharply in the first year. This is mainly due to the rapid increase of the “*Vulnerability Index*” during the first year (see Figure 5-23). Despite the fact that the “*Vulnerability Index*” decreases from the second year on, the “*frequency of incidents*” remains high until end of year 5. This is because of the increasing threats as the platform moves into the Integrated Operations. Until when, after year 5, the vulnerability index decreases increasingly, and the “*frequency of incidents*” starts to decrease.

The “*severity of incidents*” increases sharply during the first year because the “*adequacy of incident response capability*” (see Figure 5-26) decreases significantly. In traditional operation, the “*incident response capability*” is very low because there are few information security incidents. With a rapid increase in incidents during year 1, there is not enough incidents response capability to handle the work load. Therefore, the “*severity of incidents*” rises quickly. It takes time to realize the inadequacy of incident response capability and to build up incident response capability. As the “*incident response capability*” builds up from year 2, the “*adequacy of incident response capability*” increases, and the “*severity of incidents*” starts to decrease. The “*adequacy of incident response capability*” stabilizes after year 5, and so does the “*severity of incidents*”.

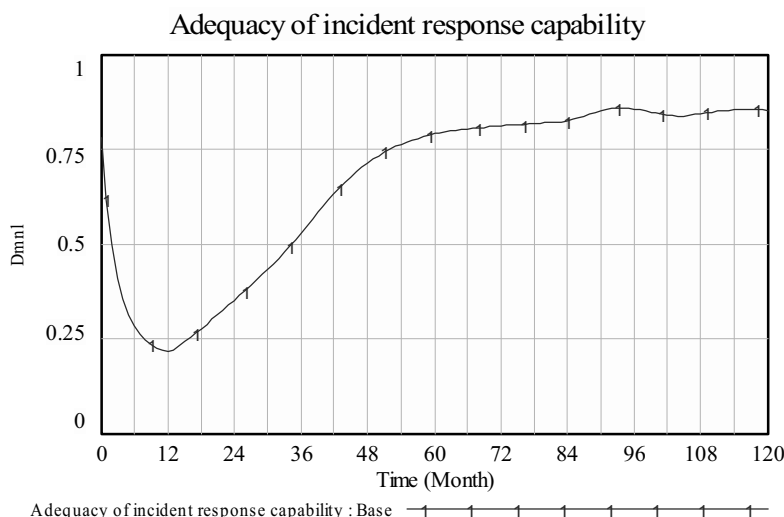


Figure 5-26 Adequacy of incident response capability

The sharp decrease in the “*adequacy of incident response capability*” is caused mainly by the sharp increase in “*frequency of incidents*” during the first year (green line with number 3 in Figure 5-27), while the “*incident response capability*” (blue line with number 1 in Figure 5-27) remains low during the first year. The slow increase of “*incident response capability*” during the first two years is caused by the reinforcing loop R7 (see section 5.2.2). When the “*incident response capability*” is low, the fraction of incidents that could be detected is low, which means few incidents are being detected (red line with number 2 in Figure 5-27). Thus, the management’s perception of the frequency of incidents is low and the investment in “*incident response capability*” is insufficient. Therefore, despite the rapid increase in incidents, the “*incident response capability*” increases slowly. As “*incident response*”

capability” gradually builds up, more incidents are detected, leading to a decision for more investments in “incident response capability.” The reinforcing loop then causes the “incident response capability” to increase at an increasing rate. After month 60, as the decrease of “frequency of incidents” leads to fewer “incident detected”, fewer investments in “Incident response capability” are being made, and a decrease in the “incident response capability” results.

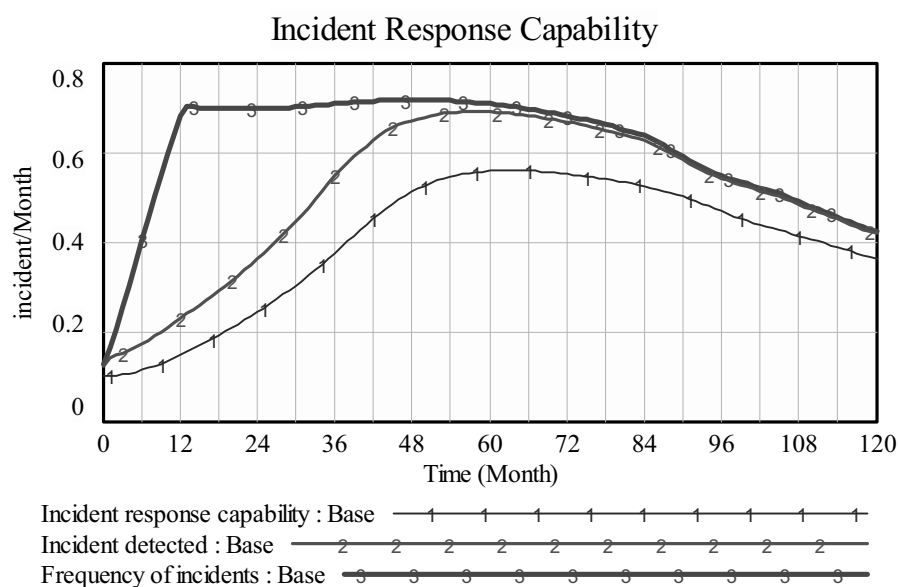


Figure 5-27 Incident response capability, incident detected, and frequency of incidents

The “monthly profit” (the upper one in Figure 5-28) decreases during the first year mainly due to the drop in revenue (blue line with number 1 in the lower one in Figure 5-28). The revenue drop is because resources are allocated to learning activities that mature new work processes and knowledge. As the benefit of Integrated Operations is gradually realized, “revenue” increases, and “product cost and expenditure” (red line with number 1 in the lower one in Figure 5-28) decreases. Therefore, the “monthly profit” increases. It exceeds the original level after two years.

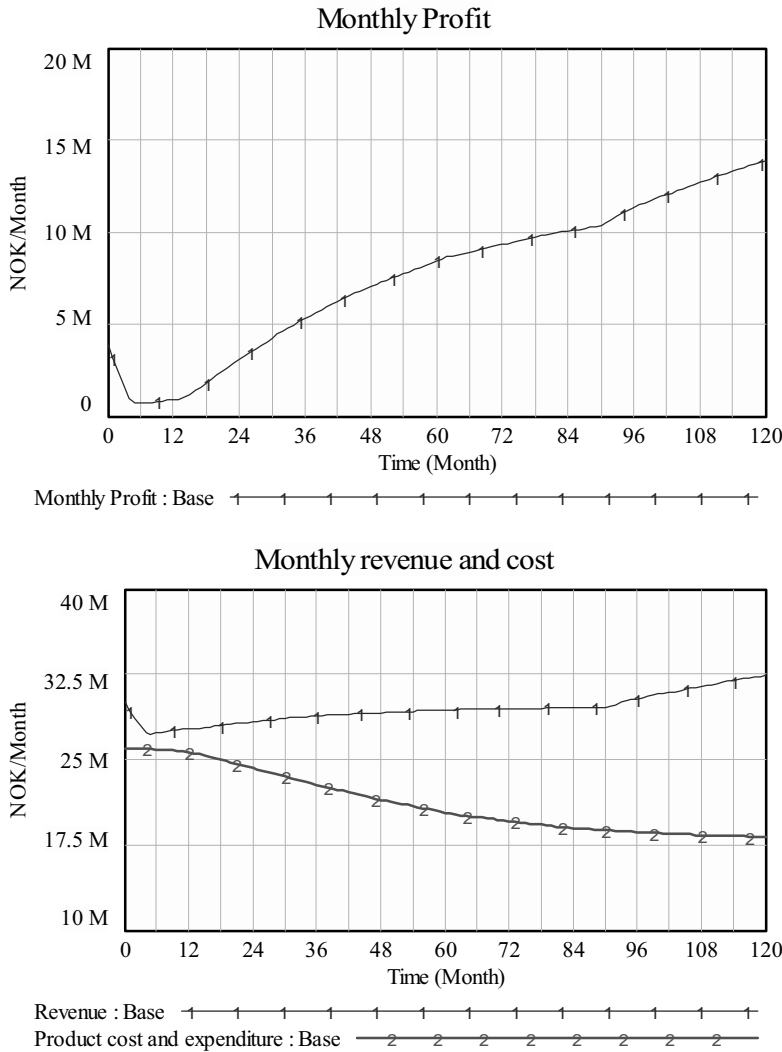


Figure 5-28 Profit, revenue, and product cost and expenditure

After month 92 or seven and a half years, the “*monthly profit*” increases more rapidly. This is because with fewer immature new work processes and less immature knowledge on the platform, resources are released from the maturation activities to focus on production (see Figure 5-22). Therefore, production has picked up, leading to higher revenue.

We have thus far explained the behavior of the base run scenario. We see that the most dangerous period is the first two years of the operation transition. Many unfavorable indicators peak during this period, such as the vulnerability index and the severity of incidents. This is because 1) Integrated Operations, which extensively utilizes advanced ICT technology, is something totally new to the platform and introduces new threats and vulnerability to the platform; 2) the tight operation transition schedule for the first year generates many immature new work processes

and knowledge; and 3) the severity of incidents increases sharply because the incident response capability is very low in the traditional operation and cannot handle the increasing incidents adequately. The monthly profit decreases at the beginning mainly because the operators' time is allocated to mature new work processes and knowledge. This kind of decrease in profit at the beginning of the operation transition is often observed for a new technology adoption process. However, in the long-term, the operation transition generates a huge financial benefit.

5.5 Closing remarks for chapter 5

This chapter introduces the Brage model. First, the causal loop diagrams are presented. The loops identified are the basic driving forces underlying the model behavior. Then the formal Brage model is explained sector by sector, with key model variables and equations. The model structure is based mostly on the information we obtained from the group model-building workshops. The values of some of the parameter are obtained from interview with our client. Others are estimated based on qualitative information. In the following chapter, these estimated variables will undergo sensitivity tests. We present our model behavior as a way to help readers to understand the model structure.

Preliminary insights focusing on the operation transition (resulting from the first four model sectors, work processes, knowledge, vulnerability and incident cost) have been reported in (Rich et al. 2007). Findings from the incident response capability part has been reported in (Qian et al. 2009).

6 Model Validation tests

This chapter focuses on model validation. First, we introduce theories on the subject. Unlike data-driven models whose validation mainly involves statistical tests, system dynamics models are causal descriptive. Their validation lies not only in reproducing behavior but in explaining the way it is generated and possibly in suggesting ways of changing the existing behavior as well. Barlas suggested three categories of tests: direct structure tests, structure-oriented behavior tests, and behavior pattern tests (Barlas 1996). Following his theory, we perform direct structure tests in the second part and structure-oriented behavior tests in the third part of this chapter. We do not have data for normal behavior pattern tests. Therefore, we decided to interview experts to obtain their opinion about the model behavior as alternative for behavior test. This will be reported in a separate chapter following this one.

6.1 Introduction to model validation

In relation to the notion of validity, Barlas argued that it is crucial to distinguish between models that are “causal descriptive” and those that are “correlational” (Barlas 1996).

Table 6-1 Comparison of causal and correlational models

	Causal models	Correlational models
Characteristics	Theory-like ⁸	Data-driven
Base of Mathematical expression	Postulated causal relations	Observed association
Model representation	How certain aspects of a real system function/ theories about that system	Statistical correlations among various elements of a real system
Purpose of the model	Prediction and explanation	Prediction only
Validation	Both qualitative and quantitative methods apply	Statistical testing
Examples	System dynamics model	Econometric models

⁸ A model that is based on causal relationship forms a theory about how certain aspects of the system function.

Since there is no claim of causality in structure, correlational models place a premium on the model output, which should match the “real” data within a certain range. Therefore, the most commonly utilized model validation method is the statistical test. However, causal models, being a “theory” for the real system, must not only reproduce behavior but also explain the way it is generated and possibly suggest ways of changing the existing behavior as well. System dynamics models fall within this category.

The validation of system dynamics models involves two aspects: tests of model structure and tests of model behavior. Model behavior tests, which compare the model-generated behavior with the observed reference behavior, are generally “weak” in the system dynamics context because they cannot separate spurious behavior accuracy (i.e., “right behavior for the wrong reasons”) from true behavior validity. Such tests provide no structural information (Barlas 1989). Validity of the model’s internal structure is crucial (Barlas 1996). Meanwhile, structure tests are “strong” tests because they directly evaluate the model structure. The essence of model validity lies in structural validity: “right behavior for the right reasons.”

However, judging the validity of a model’s internal structure is difficult and in most cases, qualitative and informal; hence, it is difficult to communicate. In papers discussing system dynamics model validation, one common criticism has emerged: the insufficient utilization of formal and impartial quantitative procedures for testing the quality of models (Grcic and Munitic 1996).

In response, Barlas proposed to distinguish between two types of structural testing: direct structure testing and indirect structure testing, also referred to as structure-oriented behavior testing (Barlas 1996; Barlas and Kanar 2000). Direct structure tests assess the model structure validity by direct comparison with knowledge on real system structures. There is no simulation involved, and these tests are qualitative in nature. Indirect structure tests, on the other hand, indirectly assess the structure’s validity by applying certain behavior tests on model-generated behavior patterns. These tests are quantitative and involve simulation. Structure-oriented behavior tests can provide information on potential structural flaws (Barlas 1989). Their main advantage over direct structure tests is that they are suitable

to formalize and quantify (Barlas and Kanar 2000). Barlas summarized the validation procedures for system dynamics models in three categories: direct structure tests, structure-oriented behavior tests, and behavior pattern tests (see Figure 6-1).

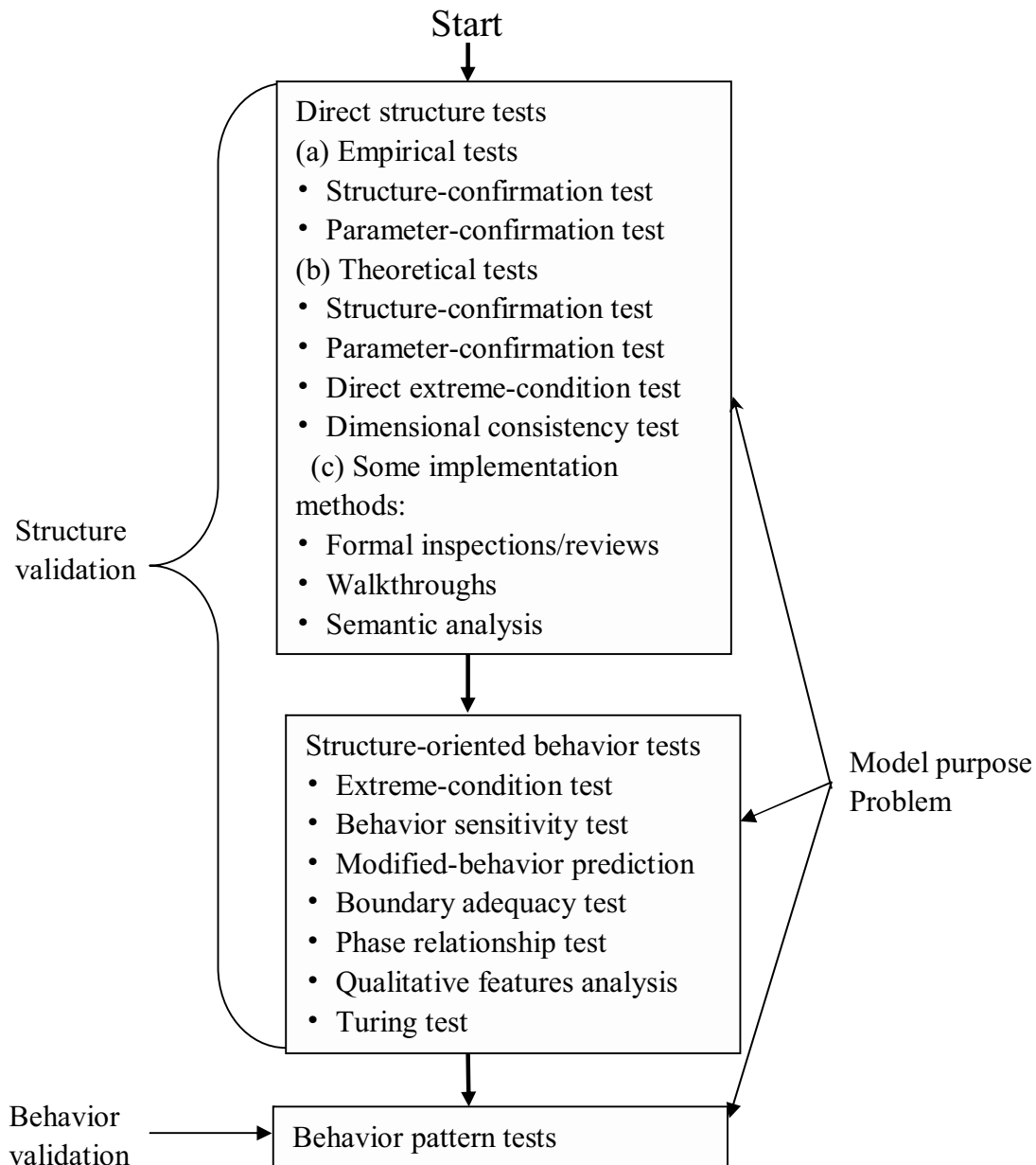


Figure 6-1 System dynamics model validation

Sources: Formal Aspects of Model Validity and Validation in System Dynamics (Barlas 1996)

All tests should be designed with respect to the model purpose. The sequence of the model validation is to first test the model structure validity and then the model behavior accuracy. Accuracy of model behavior reproduction is only meaningful after the model has passed structure tests.

6.2 Direct structure tests

Direct structure tests include assessments for structure, parameter, boundary, and dimension (Forrester and Senge 1980; Fang and Lim 2009). We summarize the purpose of these tests and the tools for these tests in Table 6-2.

Table 6-2 Direct structure tests

Test	What to Test	Common Tools and Procedures
Structure Assessment	Model structure is consistent with relevant descriptive knowledge of the system	Use causal diagrams, stock and flow maps, or direct inspection of model equations; Use interviews, workshops to solicit expert opinion, archival materials, and direct inspection in system processes
Parameter Assessment	Parameter values consistent with and reasonable to descriptive and numerical knowledge of the system	Use statistical methods to estimate parameters; Use judgmental methods based on interviews, expert opinion, focus groups, and direct experience
Boundary Adequacy	The important concepts for addressing the problem are endogenous to the model	Use model boundary charts, variable list, and/or causal loop diagram to explicitly present endogenous and exogenous variables for inspection
Dimension Consistency	Each equation dimensionally consistent without the use of parameters having no real world meaning	Use dimensional analysis software; Inspect model equations for suspect parameters.

Structural assessment is employed to examine the model structure validity via theoretical and empirical comparison with knowledge on the real system structure. Several factors add to our confidence on the model structure.

First, in this study, the model was conceptualized in two group model-building workshops that deeply involve the client. It was the client representatives who provided related information, created dynamics stories, which finally led to a consensus understanding of the problem definition. It was also the client representatives who elicited the model structure, adding variables to the model and pointing out the relationships between variables based on their knowledge of real system. In this way, we ensure that the model address the problem the client facing in reality.

Second, after the group model-building workshops, we further developed the model based on the basic model structure derived from the workshops. In this model development process, we had series of meetings with the client. During those meetings, we presented our model structure to our client representatives and consulted their opinion about it. The client representatives confirmed where they thought was correct, questioned where they felt uncertain, and suggested where to adjust and further improve. Thus, we further built the model. It was in this iterative process that we developed our model to the current stage. This process strongly suggests that the model portrays the real system as it is based on information from client. Besides, the clients' confirmation of the model structure during the meetings serves as direct structure validation of our model.

Finally, when the model was completed, we invited four experts from the IRMA team to review the model structure and behavior. They all agreed on the model structure (the model validation interview is documented in the next chapter). Through these efforts, we have developed confidence in the model structure.

Parameter assessment evaluates the constant variables against knowledge of the real system, both conceptually and numerically (Forrester and Senge 1980). We conducted an interview with the platform chief during model formalization. During the interview, we first discussed the definition of the key variables. We agreed on the meaning of the variables before trying to quantify them. Next, the platform chief assisted us in quantifying a number of parameters based on his experience and knowledge of the platform. The remaining parameters were based on experts' opinion, literature, and our estimation. We have summarized the model constants and their validity in Table 6-3.

Table 6-3 Model constants

Constants	Description and value	Unit	Validity
Operator resources for maturing each WP	Percentage of the operators' time needed to mature one work process (=4%)	%/process	Suggested by client
Total operator resources	Total percentage of the operators' time (=100%)	%	Valid by its definition
Minimum Operator resources	The minimum percentage of resource reserved for production	%	Decision variable

for production	(=90%)		
Time to mature new work processes	Time needed for immature new work processes to become mature ones given enough resources (=4)	Month	Suggested by client
Normal effectiveness of resources in developing new work processes	The average amount of processes a person could develop in an hour under normal condition (=0.006)	processes / (person*hour)	Model calibration
wt on new knowledge burden	The weight of new knowledge burden on the total new initiatives burden (=1)	Dimensionless	Modeler estimation
wt on new work process burden	The weight of new work process burden on the total new initiatives burden (=1)	Dimensionless	Modeler estimation
wt on mature WP	Weight of mature work process on the system resilience (=1)	Dimensionless	Modeler estimation
wt on mature knowledge	Weight of mature knowledge on the system resilience (=1)	Dimensionless	Modeler estimation
Operator resources for maturing each knowledge	Percentage of the operators' time needed to mature one set of knowledge (=4%)	%/knowledge	Input by client
Time to mature new knowledge	Time needed for immature new knowledge to become mature given enough resources (=8)	Month	Estimated based on literature
Normal effectiveness of resources in developing new knowledge	The average amount of knowledge a person could develop in an hour under normal condition (=0.006)	Knowledge / (person*hour)	Model calibration
Maximum vulnerability Index	Maximum fraction of hits creating incidents (=100%)	%	Valid by its definition
Initial frequency of events	Information security threats before the operation transition (=2)	event/Month	Estimated based on literature
Normal severity of incidents	The average total cost of incident before the operation transition =(500,000)	NOK/incident	Estimated based on literature
Time to learn from incidents	Time needed from incidents happening to learn from incidents (=3)	Month	Suggested by client
Normal learning per incident	The incident response (IR) knowledge people learn from normal severity of incidents (=1)	IR knowledge / incident	Reference point
Time to build up	Time needed from investment	Month	Suggested by

IR capability	decision made to IR capability ready (=3)		client
Time to change perception	Time needed for management to change their perception about frequency of incidents (=3)	Month	Estimated based on experience
Time to obsolete IR capability	Time needed for IR capability to become out-dated (=12)	Month	Estimated based on experience
Normal revenue	Average revenue of the Brage platform in traditional operation (=30,000,000)	NOK/Month	Suggested by client
Normal cost and expenditure	Average production cost and expenditure of the Brage platform in traditional operation (=26,000,000)	NOK/Month	Suggested by client
Average cost per incident response capability	Average cost for each incident response capability, including salary, training cost, etc. (=400,000)	(NOK/ Month) / (Incident / Month)	Estimated based on literature

The parameters listed above are model constants. They are suggested by the client or estimated based on literature or experience. The initial values of stocks are also model constants. We summarize them in Table 6-4.

Table 6-4 Initial value of stocks

Initial value of stocks	Description and value	Unit	Validity
Traditional work processes	The amount of traditional work processes to be changed (=20)	Work processes	Suggested by client
Immature new work processes	The amount of immature new work processes on the platform (=0)	Work processes	Suggested by client
Mature new work processes	The amount of mature new work processes on the platform (=0)	Work processes	Suggested by client
Traditional knowledge	The amount of traditional knowledge to be changed (=20)	Knowledge	Suggested by client
Immature new knowledge	The amount of immature new knowledge on the platform (=0)	Knowledge	Suggested by client
Mature new knowledge	The amount of mature new knowledge on the platform (=0)	Knowledge	Suggested by client
Incident response capability	The amount of incident could be handled in a month (=0.1)	Incident/ Month	Estimated based on experience
Perception of	Management's perception of the	Incident/	Estimated based

frequency of incidents	amount of incident happening in a month (=0.125)	Month	on experience
------------------------	--	-------	---------------

The initial value of work processes and knowledge is fixed based on the case. For incident response capability and perception of frequency of incident, their value is estimated based on experience.

Boundary adequacy test verifies if the important concepts for addressing the problem are endogenous to the model. As discussed in the literature review, Section 2.2.2, (p.22) Risk = Threat \times Probability that the threat exploits the vulnerability \times Potential impact. In this model, threat is represented by the “*frequency of events*”, which has the potential to develop into incidents. It is endogenously affected by the progress of operation transition. The probability that the threat exploits the vulnerability is represented by the “*vulnerability index*”, the fraction of events that become incidents. The “*vulnerability index*” is affected by new work processes and knowledge in the system and the knowledge gap generated by the operation transition. The potential impact is represented by the “*severity of incidents*”, affected by the operation transition and the incident response capability. The incident response capability, which has a big impact on the “*severity of incidents*”, is also an endogenous variable decided by the investment mechanism. Thus, we conclude that the most important variables are endogenous to the model.

Table 6-5 summarizes what is endogenous and exogenous to the model and what is excluded from the model for inspection.

Table 6-5 Model boundary

Endogenous	Exogenous	Excluded
<ul style="list-style-type: none"> - Mature new work processes - Mature new knowledge - Vulnerability index - Frequency of events - Frequency of incidents - Severity of incidents - Incident response capability - Revenue - Product cost and expenditure - Monthly profit 	<ul style="list-style-type: none"> - Management time to develop new work processes - Management time to develop new knowledge - Minimum operator resources for production - Average cost per incident response capability 	<ul style="list-style-type: none"> - Change of oil price - Change of production resources price - Effect of oil reserve on oil production - Human compliance - Under-reporting of incidents

Dimension consistency test assesses whether the dimensions of the right-hand side and left-hand side of the equation are internally consistent (Barlas 1996). Every variable contains a unit that identifies its meaning in reality and suggests ways to measure it. Every equation should be consistent in units. This ensures that the equation is in accordance with the physical or logical rules of reality. We are not adding apples to pears. For example:

$$\begin{aligned}
 \text{Expected incident cost} &= \text{Frequency of incidents} * \text{Severity of incidents} \\
 (\text{NOK/month}) &= (\text{incident/month}) * (\text{NOK/incident})
 \end{aligned}$$

Here, we will not present all the equations. The software Vensim (Ventana Simulation Environment), wherein the model is built, offers a dimension consistency check. The model passes the unit check using Vensim V5.7.

Above all, we have assessed model structure, parameter, boundary, and dimension with satisfactory result.

6.3 Structure-oriented behavior tests

Direct structure tests, although powerful in concept, are too qualitative and informal. Structure-oriented behavior tests combine the strength of structural orientation with the advantage of being quantifiable; thus, they become an important part of model validation. Structure-oriented behavior tests include extreme condition test, sensitivity test and integration error test. The purpose of these tests and their tools are summarized in Table 6-6.

Table 6-6 Structure-oriented behavior test

Test	What to Test	Common Tools and Procedures
Extreme Condition Test	How model responds when extreme policies apply	Test response to extreme values of each input, alone, and in combination
Sensitivity Test	How model responds when numerical values change	Test response to a set of varying numeric values and see if model-generated behavior is consistent with the real system
Integration Error	How model responds to the choice of time step	Cut the time step in half and test for changes in behavior

Extreme condition test involves assigning extreme values to selected parameters and comparing the model-generated behavior to the anticipated behavior of the real system under the same extreme condition (Barlas 1996). We have chosen those variables that are involved in feedback loops and set their value to zero, or extremely large (compare to the base scenario). Before simulating the model, we make a forecast of how the system will behave in reality under such extreme condition. Then we simulate the model and compare the model-simulated behavior with our expectation. If the model behavior fits our expectation, then, the extreme condition test is passed. If not, we will have to investigate the reasons that generate unexpected behavior and may need to improve the model structure.

Table 6-7 List of Extreme tests performed

Test name	Variable change		
	Variable name	Base run	Test
<i>Ex 1 – No operation transition</i>	Management time to develop new work processes	Time 0-12, 100, Time 13-120, 34	0
	Management time to develop new knowledge	Time 0-12, 100 Time 13-120, 34	0
<i>Ex 2 – No resources for new work processes and knowledge maturation</i>	Minimum operator resources for production	90%	100%
<i>Ex 3 – Extreme long time to mature new work processes</i>	Time to mature new work processes	4	40
<i>Ex 4 – Extreme long time to mature new knowledge</i>	Time to mature new knowledge	8	80
<i>Ex 5 – Extreme long time to</i>	Time to change perception	3	30

<i>change the management's perception of risk</i>			
<i>Ex 6 – Extreme long time to build incident response capability</i>	Time to adjust IR capability	3	30
<i>Ex 7 – Extreme long time for incident response capability to obsolete</i>	Time to obsolete IR capability	12	120
<i>Ex 8 – All resources available to mature new work processes and knowledge</i>	Minimum operators resources for production	90%	0

The Brage model has passed the above extreme tests. For detailed behavior of these extreme tests, please refer to Appendix III Extreme Tests (p. 275).

Sensitivity test determines the parameters to which the model is sensitive and verifies if the real system would exhibit similar sensitivity to the corresponding parameters (Barlas 1996). Sensitivity tests are performed on two types of variables: first, table functions; second, constants. Table functions are used to capture the nonlinear relationship of two variables. The table functions in the model are formulated based on empirical knowledge or theoretical information from literature. Both of these methods provide more qualitative information than quantitative information. In most cases, we have two reference points (the starting point and the end point of the curve for the table function), and other points in between are based on our estimation of the shape of the curve. In the sensitivity test, we will change the shape of the curve to see how model behavior changes. In this way we test the sensitivity of the table functions. For model constants, we differentiate them into three types: 1) initial level of stocks; 2) reference points; and 3) other constants. The initial levels of stocks are fixed in the Brage model. For example, there are 20 traditional work processes to be changed into new work processes. Therefore, the initial traditional work processes is 20. The initial level of immature new work processes and mature new work processes is 0. For this type of variables, sensitivity test is not needed. The reference points are also fixed. For example, the “Maximum vulnerability Index” is 100%, meaning in the worst situation, whatever could go wrong will go wrong. For this type of constants, sensitivity test is not needed either. The remaining constants are subject to sensitivity tests. We will run the model 200 times within certain range of the constant. We

inspect the distribution of the simulation results and investigate whether the sensitivity of model behavior is reasonable.

There are two kinds of sensitivity: behavior pattern sensitivity and numerical sensitivity. Behavior pattern sensitivity occurs when change of the variable value causes the model behavior pattern change. In cases when model behavior pattern does not change, and only the numerical value of the model variables change, we say it is numerical sensitivity. Normally, the value change of the model variable causes other variables to show numerical sensitivity. If behavior pattern sensitivity is observed, investigation should be made to see if there exists inappropriate model structure. Or otherwise, this variable presents a leverage point, which changes the dominance of loops and thus the model behavior pattern. If so, more research and investigation for this variable is needed to ensure its value, and this variable could be a good candidate as policy variables.

Table 6-8 List of sensitivity tests performed

Test name-variable	Sensitivity test
<i>S1- Effect of the new initiatives burden on maturing new work processes</i>	Three different shapes of table functions are tested
<i>S2 - Effect of mature new WP on maturing new WP</i>	Three different shapes of table functions are tested
<i>S3- Effect of new initiatives burden on maturing new knowledge</i>	Three different shapes of table functions are tested
<i>S4- Effect of mature knowledge on maturing new knowledge</i>	Three different shapes of table functions are tested
<i>S5- Effect of knowledge gap on vulnerability index</i>	Three different shapes of table functions are tested
<i>S6- Effect of immature new knowledge on vulnerability index</i>	Three different shapes of table functions are tested
<i>S7- Effect of immature new WP on vulnerability index</i>	Three different shapes of table functions are tested
<i>S8- Effect of resilience on severity</i>	Three different shapes of table functions are tested
<i>S9- Time to mature new work processes</i>	Base run value: 4 Test: Range: 3-5; Random Uniform; 200 Runs
<i>S10- Time to mature new</i>	Base run value: 8

<i>knowledge</i>	Test: Range: 6-10; Random Uniform; 200 Runs
<i>S11- Operator resources for maturing each WP</i>	Base run value: 4% Test: Range: 3%-5%; Random Uniform; 200 Runs;
<i>S12- Operator resources for maturing each knowledge unit</i>	Base run value: 4% Test: Range: 3%-5%; Random Uniform; 200 Runs;
<i>S13- Time to adjust IR capability</i>	Base run value: 3 Test: Range: 2-4; Random Uniform; 200 Runs;
<i>S14- Time to obsolete IR capability</i>	Base run value: 12 Test: Range: 10-14; Random Uniform; 200 Runs;
<i>S15- Extending the run time of the model</i>	Base run: run time=120 Test: run time=240

The Brage model has passed the above sensitivity test. For detailed behavior of these sensitivity tests, please refer to Appendix IV Sensitivity tests p. 291.

Integration error test is conducted to assess whether the results are sensitive to the choice of time step (Sterman 2000). System dynamics models are formulated in continuous time with integration method. The model behavior should not be sensitive to the choice of the time step. The way to test the integration error is to cut the time step in half and run the model again. If the result changes in ways that matter, the time step is too large. For this model, when cutting the time step into half, the model behavior remains consistent with the base run, thus passing the integration error test.

6.4 Behavior tests

Once enough confidence has been developed in the model structure validity, we can begin applying behavior tests — designed to measure how accurately the model can reproduce reality. In normal cases, the behavior test consists of comparing the model-generated behavior with historical data using statistics tools to assess the point-by-point fit. However, this research concerns information security risks during operation transition. Historical time series data are not always available. For example, the vulnerability index has not been evaluated. For some other variables that might have historical data, the data might not be precise. For example, there are historical data about frequency of incidents and severity of incidents. However, the incident reporting is not well regulated and most minor incidents are not recorded. Such data are not suitable to serve as a base for behavior tests. Therefore, the standard behavior test is not applicable in this case. Alternatively, we invited the experts from the IRMA team to review the model behavior. During the interview, several different scenarios

were presented to the experts. Their recognition of the model behavior increased the confidence in the model behavior validity. This model validation interview will be reported in the next chapter.

6.5 Closing remarks for chapter 6

Model validation is an ongoing process throughout the model building process. According to Sterman, “Testing begins as soon as you write the first equation.” He emphasized that testing involves far more than the replication of historical behavior, - every variable must correspond to a meaningful concept in the real world, and every equation must be checked for dimensional consistency. The sensitivity of model behavior and policy recommendations must be assessed in light of the uncertainty in assumptions, both parametric and structural (Sterman 2000).

With the group model-building workshops, validation starts even earlier. During the system conceptualizing stage, the modeller must start the validation by asking questions such as “Do we have the right person for the workshop?”, “Does the dynamic problem definition represent the reality?”, “Are we at the right level of aggregation?” and so on. The answers to such questions cannot be achieved by formal, objective validation process; they are social, judgment beliefs.

A wide range of tests help modellers to understand the robustness and limitations of the models. A wide range of data, both numerical and qualitative, provides opportunities for confirming or challenging the model. However, no model can be fully validated. Never ask whether a model is true or false, but ask whether the model is useful in relation to its purpose.

7 Model Validation Interviews

This chapter presents the interviews with information security experts from the IRMA project reviewing the Brage model simulation results. The first section of this chapter explains the goals for the interviews. The next section focuses on the interview design. It includes the rationale that led to the choice of a structured interview to obtain expert feedback and reflection, a description of the booklet for the structured interview, and the test of the booklet. The third section describes the administration of the interviews including the selection of informants and the arrangement of the interviews. Finally, the interview results are analyzed along with a summary of the indicated strengths and weaknesses of the Brage model.

7.1 Purpose of the Interviews

As discussed in chapter 6, the Brage model does not have historical time series data which we can compare with the model-simulated behavior. Hence, a standard behavior validation of the model is not possible. We thus have to find an alternative way to validate the model behavior. The plan is to use interviews with experts so as to seek their opinion on the model-simulated behavior. Their acceptance of the model-simulated behavior adds our confidence to model.

The foremost goal for the interviews is to determine if the model-generated behaviors are credible. Under the given assumptions of the model, would experts expect to see the behaviors generated by the model? If the behaviors are found to be in accordance with the expectations, they could provide support for the model's results and in part, for the underlying structure. If the behaviors are found to be in contrast with the expectation, they would stimulate discussions on how the results have been obtained and what changes should be considered (Rich 2002).

The second goal for the interviews is to check the soundness of the model structure. As mentioned, the recognition of the model behavior implied a support for model structure. Moreover, we also conducted direct inquiries about the model structure. Prior to the interviews, the model structure was presented to the chosen informants. During the interview, the informants were firstly asked about their opinions on the

model structure. Then we checked with them whether specific causal links and certain parts of the model were a good representation of the reality. Finally, we also asked whether there are any missing links. These are questions directly related to model structure. This process served as direct structure validation.

Third, the interviews could aid in the assessment of the model parameters. This was done in part, through the acceptance of the model behavior. At the same time, we directly queried the informants about some of the model parameters during the interviews. This was a process which served as the parameter assessment.

Another goal of the interview is to seek experts' advice on future model development. There were questions about additional model structure, variables, and scenarios. The answers to these questions helped us shape policy designs and future research direction.

7.2 Interview design

7.2.1 The rational for using a structured interview

Interview research is a frequently used method for data collection in the social science. Interviews can be conducted either in person or over the phone. These can either be structured (based on a carefully worded interview script) or unstructured (allowing the interviewee to tell stories and give examples). The former is often used as a means to collect data for specific questions, while the latter is often used as a means to unearth issues that the interviewer finds novel or counterintuitive.

Conducting interviews with experts has long been utilized in various stages of system dynamics model development. We summarize the following table based on a study conducted by Luna-Reyes and Andersen (Luna-Reyes and Andersen 2003).

Table 7-1 The objectives of using interviews during model development

Model development stage	Purpose of use interview
Model conceptualization	Used to identify problem and elaborate dynamic hypotheses
Model formulation	Used to obtain parameters and policies
Model testing	Used to obtain expert judgment about model structure and behavior

In most cases, the unstructured interview is more suitable for model conceptualization, while the structured interview is more suitable for model formulation and model testing. For model testing, Vennix described an approach based on “workbooks” to conduct model assessment with individuals or groups (Vennix 1996). The workbooks contain questions on causal relations and model behavior. Rich used interviews to validate the model behavior of knowledge management in his dissertation. Our foremost intention is also to validate the model behavior. Therefore, we follow the procedures taken by Rich (2002). A model review booklet was developed to facilitate the interview. We will introduce the booklet below.

7.2.2 The interview booklet

An interview booklet was prepared to support the interview for this study. It included three parts:

1. The first part presented the introduction and background information, and was required be read by the informants before the interview. The introduction contained interview instructions for the informants, while the section on background information presented the model structure, a brief summary of scenarios to be seen, and the key variables and their definitions. At the end of this part, an indicator pointed out that the informants should stop reading.
2. The second part was the main body of the interview. It showed the behavior of the key variables of six scenarios: 1) Base, 2) Focus on production, 3) Focus on knowledge, 4) Quicker to build IR capability, 5) Higher initial IR capability, and 6) Delay transition. For each scenario, the informants were asked to rate the key variables as plausible (P), uncertain (U), or not plausible (N), under the conditions of the scenario. When these terms were not used explicitly, we made judgments for the rate based on what is implied by the content of the informants’ comment. The informants were then asked to provide their reasons for the model behavior. After describing their own mental models of the scenario, they were then asked to evaluate a prepared analysis based on the causal constructs of the simulation. Again, they were asked to rate the analysis with plausible (P), uncertain (U), or not plausible (N). Since the informants provided their own mental model before learning of the simulation-based explanation, it became possible to consider how their mental models

differed from that of the simulation. The final questions for each scenario were to identify missing causal factors and policy actions.

3. The third part consisted of the closing questions. It compared related scenarios, asking the informants to evaluate the differences in the model-generated behavior. The outcome of the evaluation was rated as plausible (P), uncertain (U), or not plausible (N). This part also includes questions asking the informants about where the model could be extended through additional structure, variables, or scenarios. The full interview booklet was attached at Appendix V Model validation interview p.318.

7.2.3 Booklet testing

We conducted extensive testing of the booklet before releasing it to the informants. Nine volunteers participated in the booklet testing. They were consultants and researchers in universities (see Table 7-2). Four of them had experience with information security management.

Table 7-2 Volunteers who participated in the interview booklet testing

Occupation of the participants	Numbers
Consultants (from IBM, KPMG, Deloitte)	6
PhD students (in information security research)	2
Assistant Professor (in information system)	1

The first test interview provoked many changes in the booklet. The introduction part was shortened, eliminating the detailed information on model structure. The chosen key variables were also reduced from eight to six, because the interview took a much longer time than we expected.

The following several test interviews led to minor revisions, such as changing the scenario sequence, improving the wording, and adjusting the closing questions. After the first five test interviews, further suggestions for changes were seldom encountered, indicating that the interview booklet had achieved maturity.

Most volunteers agreed with the model behavior under different scenarios. Only a single respondent found the base run behavior difficult to understand, which led to a difficulty in giving opinion for different scenarios. The other eight persons showed

positive opinions to the model behaviors. Two of them explicitly mentioned that they had encountered cases in reality that corresponded to the model behavior. One volunteer reported an incident occurred in a company which was implementing an SAP system in the finance department. The company failed to allot sufficient resources to allow its employees to learn new the work processes and gain knowledge; thus, people were unable to work efficiently under the new system. This gave rise to numerous errors and unsettled accounting treatments that finally led to the resignation of the entire accounting team. The company had to temporarily outsource its accounting tasks to clean up the old unsettled treatments while recruiting a new team, costing the company millions of dollars in expenditures. This case was similar to what was presented in the second scenario – focus on production. The other volunteer had experience consulting on safety management for a big Chinese oil and gas company. She felt that the company has been in the loop presented in scenario 5: the management investment in safety was low, and fewer safety problems were detected leading to a misperception of being safe, leading to even lower investment in safety management. This underinvestment in safety is a latent danger for the company. Thus, she strongly agreed with the reinforcing loop in scenario 5 and thought it represented the reality very well. And she commented that it was crucial to bring the organization into the positive side of the reinforcing loop: more investment in safety, more safety problems detected and reported and even more investment in safety until the system become robust.

7.3 Interview Administration

7.3.1 Recruitment of subjects

The ideal informants should be persons from Hydro. However, Hydro's formal engagement in this project was terminated at the end of 2006. Moreover, at the end of 2006, Hydro merged with another big Norwegian oil and gas company, Statoil, forming the new company StatoilHydro. This led to organizational restructuring, and we could no longer obtain support from those who originally participated in our workshops. Alternatively, the IRMA team had expertise in incident response management in Hydro. They were thus good candidates for the model review interview. We contacted IRMA team in July 2008, and obtained their continued support for the project. Four experts from the IRMA were confirmed to participate in

the model validation interview. Each participant was asked to schedule two sections on the same day for the interview, with 90 minutes allotted for each section. Four consecutive days were scheduled for the four experts respectively.

7.3.2 The process of the interview

The interview booklet was sent to the IRMA experts when the testing of the booklet was completed, two weeks before the interview with them started. The informants were instructed to read the first part of the booklet before the interview. The interviews were structured in three blocks.

1. Background: The first block included confirming consent orally, asking permission for taping the interview, and verifying that the informants had read the background materials. All four informants had read the background material beforehand. We then asked the experts whether they agree with the model structure presented in background information. We discussed any questions the informants had about the interview, the model, the variables, and others.

2. Simulation Scenarios: The second block presented the model behavior of six scenarios (Base, Focus on production, Focus on knowledge, Quicker to build IR capability, Higher initial IR capability, and Delay transition). Each simulation was presented individually using a specific sequence of steps:

- Step 1: A short description of the situation was read to the interviewee. A graph of each of the behavior of the six variables was presented, after which a description of each was read aloud by the interviewer. The Base Run behavior for each variable was included in the other five scenarios to facilitate comparisons. The booklet contained both the graph and the text description to enable the interviewee to follow along.

- Step 2: After the description of the behaviors, the informants were asked if they believed the behavior of each individual variable was plausible (P), uncertain (U) or not plausible (N), within the constraint of each scenario. Comments and questions were encouraged.

- Step 3: The informants were then asked to craft an explanation of how the model behavior was generated. This explanation could include the causal factors in the model or additional factors deemed important to understanding the outcomes.

- Step 4: After describing their own mental model of the scenario, the informants were asked to consider a prepared analysis of the situation. This analysis was drawn from the causal constructs of the simulation model. They were asked to evaluate the plausibility of the prepared analysis and provide any other reactions to this alternative explanation, along with other factors that should be added. Care was taken in the wording of the questions and instructions to reduce any implications of correctness of the prepared analysis.

3. Closing questions: the final part of the interview included two types of questions. First, after going through six scenarios one by one, questions were raised to compare the behavior of relevant scenarios. Presented with the graph of the key variables in different scenarios, the informants were asked whether they thought the difference was reasonable, what were the reasons that generated the behavior, and whether such behavior was realistic. The second type of questions asked the informants to identify any model structures, variables, or scenarios that would be in the interest for future model development.

7.3.3 Data capture

With the consent of the subjects, all four interviews were taped. The tapes were not made into transcripts because we were not to make coding of the obtained information. We used tapes just to ensure informants' opinions and comments were correctly taken. After the interview, we listened to the tapes several times to collect the informants' opinions and comments, and to ensure a correct understanding of their ideas. The key messages are listed in the following section.

7.4 Result of the model review interview

The interviews were conducted in November 2008. In this section, we present the informants' response to the model behaviors presented to them.

7.4.1 Interview results—scenario review

Scenario 1. Base Run: Reactions to the behaviors of Base Run were mixed (see Table 7-3). Consent agreement was reached for two variables, namely, severity of incidents

and incident response capability. For other variables, at least one informant showed uncertainty or disagreements.

Table 7-3 Base Run

	A1	A2	A3	A4
Mature new work processes	U	P	P	P
Mature new knowledge	U	N	P	P
Monthly profit	P	P	P	N
Frequency of incidents	P	U	P	N
Severity of incidents	P	P	P	P
Incidents response capability	P	P	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* Three informants (A2, A3, A4) thought that the development of the mature new work processes was plausible. One of them commented that a period of four months for the new work processes to mature seemed long, but he could understand that it was because of the work swift on the oil platform. The other informant (A1) felt that she did not have enough knowledge about the Industry to be certain.
- *Mature new knowledge.* Two informants (A3, A4) believed that the model reflected the development of mature new knowledge. Of the two other informants (A1, A2), one felt that she did not have enough knowledge about the Industry to be certain, while the other respondent thought that the mature knowledge would follow the shape of mature new work processes more closely.
- *Monthly profit.* Three informants (A1, A2, A3) agreed with the pattern of the monthly profit—a drop at the beginning and then a gradual increase thereafter. Among them, one informant felt that the increase in the latter years seemed too big. She amended “Of course, it depends on the business. Maybe it could be that big and that is why they (Hydro) have invested so much on it.” The informant (A4) disagreed with the pattern of the monthly profit. He thought there would be no drop in the monthly profit. He argued that the benefits brought by Integrated Operations were so huge that from the beginning, the increase of revenue could off-set the negative effects of operation transition on production.
- *Frequency of incidents.* Two informants (A1, A3) agreed with the pattern of frequency of incidents. One of them pointed out, “It is likely to have more incidents at the beginning and stay there for a while and hopefully it will drop later as we know well about the new work processes.” For the two other informants (A2, A4), one felt

uncertain that frequency of incidents would stay at such a high level for so long. He thought it might drop sooner after reaching a high level. The other informant disagreed with the behavior because he learned from a survey about incidents on a platform adopting Integrated Operations that the number of incidents before and after the use of advanced ICT had not changed. He agreed that the system is more vulnerable in Integrated Operations, because it is much more complex than the traditional operation. Higher vulnerability meant higher probability of incidents happening. However, whether or not incidents really occurred in reality was affected by many other exogenous factors. We also thought that minor incidents might not be reported and included in the survey results. However, the informant disagreed with the sharp increase of frequency of incidents. He thought it could be that the company had prepared for increasing risks so that the frequency of incidents did not increase that much.

- *Severity of incidents.* All four informants agreed with the behavior of the severity of incidents. One informant commented, “Quite realistic. The increase in the beginning is because the increase of frequency of incidents, and the decrease is mainly because the increase of incidents response capability.”
- *Incident response capability.* All four informants indicated that the incident response capability was likely to gradually increase and then fall. One informant commented, “People will become more capable to respond to incidents, and when frequency of incidents drops, it (the capability) will drop too.”

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants were able to present a systematic explanation: when new work processes and knowledge were implemented, the frequency of incidents increased sharply as the system became more vulnerable and faced more threats. Later, when people learned to work with the new work processes, the frequency of incidents dropped. The severity of incidents increased at the beginning as there was not enough response capability. As the level of incident response capability gradually increased, the severity of incidents decreased. One reason that the informants could come up with such quality explanations could be that three of the four informants had participated in the group model-building workshops and had knowledge about the model.

Then, the prepared analysis of the scenario was read to the informants, which was similar to what they had explained. The prepared analysis also pointed out that the sharp increase of the frequency of incidents at the beginning was also due to the ambitious plan of changing five traditional work processes into new work processes in the first year. All the informants agreed that the causal explanation of the base run was plausible.

Scenario 2. Focus on production: The second scenario shown to the informants was named focus on production, where more resources were reserved for production, leaving fewer resources available to learn new work processes and knowledge. The reaction to the behavior of this scenario was still mixed (see Table 7-4). Compared to the base run, all of the informants agreed with the behavior of mature new work processes, but for the other variables, at least one informant had doubts on their plausibility.

Table 7-4 Focus on production

	A1	A2	A3	A4
Mature new work processes	P	P	P	P
Mature new knowledge	P	P	U	P
Monthly profit	P	P	U	N
Frequency of incidents	U	P	U	P
Severity of incidents	P	U	P	U
Incidents response capability	P	U	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* All four informants thought that the development of mature new work processes was plausible. They all felt that the development of mature new work processes should be slightly slower than the base run.
- *Mature new knowledge.* Three informants (A1, A2, A4) believed that the model reflected the development of mature new knowledge. One of them commented, “I agree with the behavior. When there is very little time spent on maturing new knowledge, it will mature very slowly.” The other informant (A3) thought the mature new knowledge dropped too much. He thought people could mature new knowledge by working with the new work processes.
- *Monthly profit.* Two informants (A1, A2) thought the behavior was plausible. The other two (A3, A4) had different opinion. One of them thought that the drop of the monthly profit in the later years was too big. The other thought that the monthly profit

should behave similar to the base run. He argued that although the operators had less productivity (because of less knowledge), more resources were focused on production. Therefore, the production should be similar to the base run and the monthly profit.

- *Frequency of incidents.* Two informants (A2, A4) agreed with the behavior of this variable. One of them commented, “This is surely true. People make more mistakes with less knowledge.” For the other two informants (A1, A3), one felt that the pattern was right but the difference seemed too big; the other one felt that the frequency of incidents would not increase to such a high level.

- *Severity of incidents.* Two informants (A1, A3) agreed with the behavior of the severity of incidents. One of them commented, “Under such a scenario, you will have more severe incidents at the beginning, and it takes more time to reduce severity.” The other two informants (A2, A4) thought the pattern was likely but that they both felt that the severity of incidents might even be higher as people did not have mature knowledge.

- *Incident response capability.* Three informants (A1, A3, A4) indicated that incident response capability was likely to increase as the frequency of incidents had been increasing throughout the simulation time. One informant (A2) thought that although the number of incidents increased, as their severity stabilized, investments in incident response capability might stop, and it might not increase in the latter years.

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants explained quite systematically: With less time available for learning, knowledge would mature very slowly. The monthly profits dropped less at the beginning as more resources were reserved for production. However, since it took longer to learn the new work processes, the monthly profits would be lower in the long run. The frequency of incidents increased because people did not have enough knowledge. The severity of incidents also increased. At the same time, IR capability increased due to the increased occurrence of incidents. All of them agreed with the prepared analysis of the scenario we read to them.

One informant made additional comments that this was a very realistic scenario. From his observation, the oil and gas company had been focusing on production optimization and not enough training had been conducted for the operators. He expressed concern about this production-orientated management view. If operators

were not trained to react to different situations, they would not know how to perform when deviation happens.

Scenario 3. Focus on knowledge: The third scenario shown to the informants was named focus on knowledge, where fewer resources were reserved for production, leaving more resources available for knowledge building. The reaction to the behavior of this scenario was improved (see Table 7-5). Compared to the base run, all of the informants agreed with the behavior of mature new work processes and mature new knowledge. The other variables are questioned by one or two informants.

Table 7-5 Focus on knowledge

	A1	A2	A3	A4
Mature new work processes	P	P	P	P
Mature new knowledge	P	P	P	P
Monthly profit	P	N	P	P
Frequency of incidents	P	P	U	P
Severity of incidents	P	P	P	U
Incidents response capability	P	U	P	N

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* All four informants thought that the development of mature new work processes was plausible. They all felt that the development of mature new work processes should not be greatly affected since it already had enough resources in the base run.
- *Mature new knowledge.* All four informants believed that the model reflected the development of mature new knowledge. One informant's comment was "the knowledge should be better than base run."
- *Monthly profit.* Three informants (A1, A3, A4) agreed with the model-simulated behavior of the monthly profit, which they deemed worse than the base run at the beginning but better than the base run in the latter years. The other informant (A2) thought the monthly profit should increase quicker in the later years so that "It reaches 14M earlier and stays there."
- *Frequency of incidents.* Three informants (A1, A2, A4) agreed with the model-simulated behavior of frequency of incidents. One of them pointed out that "You will have fewer incidents with more knowledge, and in the end, it will converge with the base run." Although the other informant (A3) agreed with the pattern, he felt that the difference should not be so big.

- *Severity of incidents.* Three informants (A1, A2, A3) agreed with the behavior of the severity of incidents. One of them commented, “I think it will reduce severity of incidents as you have more knowledge.” The other informant (A4) thought the pattern was likely but he felt that the severity of incidents might be reduced to an even lower level.
- *Incident response capability.* Two informants (A1, A3) indicated that incident response capability was likely to be lower as the frequency of incidents became reduced. For the other two (A2, A4), one thought “It will follow the shape of the base run more closely.” The other was of the opinion that “Having more mature knowledge could lead to high IR capability”.

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants explained quite systematically that with extra resources, the knowledge matured quicker. The profit was lower in the beginning because of the extra effort to mature knowledge, and the profit was higher in the later years as people have more knowledge of the new operation. There would be fewer incidents due to more knowledge people have. The severity of incidents would be reduced for the same reason, and the incident response capability would be lower because of the reduced frequency of incidents. All of them agreed to the prepared analysis of the scenario we read to them.

Scenario 4. The fourth scenario shown to the informants was named quicker to build IR capability, where time to build IR capability is reduced from three months to two months. Among the six scenarios, the reaction to the behavior of this scenario was the best. Two informants totally agreed with the behavior of six variables, and the other two had doubts with one variable (see Table 7-6).

Table 7-6 Quicker to build IR

	A1	A2	A3	A4
Mature new work processes	P	P	P	P
Mature new knowledge	P	P	P	P
Monthly profit	U	P	P	P
Frequency of incidents	P	N	P	P
Severity of incidents	P	P	P	P
Incidents response capability	P	P	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* All four informants thought that the development of the mature new work processes was plausible. The policy for this scenario will not affect the maturation of new work processes. Therefore, it was easy to understand that mature new work processes behave exactly the same as the base run.
- *Mature new knowledge.* All four informants believed that the model reflected the development of mature new knowledge. For the same reason as mature new work processes, the behavior of mature new knowledge was the same as the base run.
- *Monthly profit.* Three informants (A2, A3, A4) agreed with the model-simulated behavior of the monthly profit, which is a little better than the base run. The other informant (A1) thought that “If you increase a reasonable amount on incident response capability, and spend the money wisely, then it is beneficial. But if you spend a lot on the incident response capability, it probably will not be cost effective.”
- *Frequency of incidents.* Three informants (A1, A3, A4) agreed with the model-simulated behavior of frequency of incidents. The other informant (A2) thought that the frequency of incidents should be different considering the side efforts of this change.
- *Severity of incidents.* All informants agreed with the behavior of the severity of incidents. One of them commented, “The severity of incidents should be lower than the base run.”
 - *Incident response capability.* All informants indicated that incident response capability was likely to be higher than the base run. One of them commented, “There will be more incident response capability because of more investments made.”

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants explained quite systematically: with a shorter time to build up incident response capability, you have more incident response capability that reduces severity of incidents; thus, the management will gain more than they lose. All of them agreed with the prepared analysis of the scenario we read to them.

Scenario 5. Higher initial IR capability: The fifth scenario shown to the informants was named higher initial IR capability, where the initial incident response capability was raised from 0.1 to 0.3. The reaction to the behavior of this scenario was quite good. One informant totally agreed with the behavior of the six variables, and the other three had doubts on one variable (see Table 7-7).

Table 7-7 Higher initial risk awareness

	A1	A2	A3	A4
Mature new work processes	P	P	P	P
Mature new knowledge	P	P	P	P
Monthly profit	U	P	U	P
Frequency of incidents	P	N	P	P
Severity of incidents	P	P	P	P
Incidents response capability	P	P	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* All four informants thought that the development of the mature new work processes was plausible, and that the policy for this scenario would not affect the maturation of new work processes. Therefore, it was easy to understand that mature new work processes behave exactly the same as the base run.
- *Mature new knowledge.* All four informants believed that the model reflected the development of mature new knowledge. For the same reason as mature new work processes, the behavior of mature new knowledge was the same as the base run.
- *Monthly profit.* Two informants (A2, A4) agreed with the model-simulated behavior of the monthly profit, which is a little better than the base run. The other two informants (A1, A3) felt uncertain as to whether the incident cost reduced would be more than the investment in incident response capability. According to the general economic theory on diminishing marginal return, one informant thought that there should be a point before which the investment in incident response capability would be cost effective and after which the investment in it would not be cost effective.
- *Frequency of incidents.* Three informants (A1, A3, A4) agreed with the model-simulated behavior of the frequency of incidents. The other informant (A2) thought that considering the side efforts of this change, the frequency of incidents should be different.
- *Severity of incidents.* All informants agreed with the behavior of the severity of incidents. One of them commented, “You will have less severe incidents because you are able to handle them better.”
- *Incident response capability.* All four informants indicated that incident response capability was likely to be higher than the base run. One of them commented, “There will be more incident response capability since more investment is made.”

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants explained quite systematically: with more investments on incident response capability, the incident response capability will increase and then the severity of incidents will be reduced.

We further explained the mechanism that the increase in incident response capability at the beginning helped detect more incidents, which could then lead to more investment in later years. That is the reason why the incident response capability had been higher than the base run for several years until the frequency of incidents began to drop. All the informants agreed to this line of reasoning.

Scenario 6. Delay transition: The sixth scenario shown to the informants was named delay transition. In this scenario, additional structure was added to the model: when the incidents cost reached five times higher than the initial level, the transition speed will be reduced to half, and when the incidents cost reaches 10 times higher than the initial level, the operation transition will stop. The reaction to the behavior of this scenario was mixed. One informant totally agreed with the behavior of the six variables, while the other three had doubts on some of the variables (see Table 7-8).

Table 7-8 Delay transition

	A1	A2	A3	A4
Mature new work processes	P	U	P	P
Mature new knowledge	P	U	U	P
Monthly profit	P	P	U	U
Frequency of incidents	P	U	P	P
Severity of incidents	P	P	P	P
Incidents response capability	P	N	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

- *Mature new work processes.* Three informants (A1, A3, A4) thought that the development of the mature new work processes was plausible. The mature new work processes was delayed in this scenario. The other informant (A2) thought the delay seemed too small.
- *Mature new knowledge.* Two informants (A1, A4) believed that the model reflected the development of mature new knowledge. One of them pointed out, “As you do not implement new work processes that fast, you have more time to build knowledge at the beginning. But in the long run, still it is behind schedule.” For the other two

informants (A2, A3), one thought the pattern of mature new knowledge was likely, but that the crossing of the two lines might occur earlier. The other thought that the difference between mature new knowledge in this scenario and in the base run should be bigger: “since the implementation of new work processes was delayed, more knowledge should be able to mature.”

- *Monthly profit.* Two informants (A1, A2) agreed with the model-simulated behavior of the monthly profits. The two other informants (A3, A4) felt uncertain. One of them thought the monthly profits should be reduced more, while the other thought the lowest point of the monthly profits should be delayed too.
- *Frequency of incidents.* Three informants (A1, A3, A4) agreed with the model-simulated behavior of the frequency of incidents. The other informant (A2) thought that frequency of incidents should be reduced but not that much. He felt it should still be at a relatively high level.
- *Severity of incidents.* All informants agreed with the behavior of the severity of incidents. They all thought that it should be lower than the base run scenario at the beginning and approach the same level in the end.
 - *Incident response capability.* Three informants (A1, A3, A4) indicated that incident response capability was likely to be higher than the base run. The other informant (A2) thought that it should be more similar with the base run.

Scenario Reviews. When asked to analyze the underline mechanism that caused these results, all the informants explained quite systematically: the slower implementation of new work processes gave people more time to acquire knowledge, resulting in fewer incidents and less severe incidents. Moreover, the incidents response capability did not need to be very high. The profit behaved similar as the base run in the beginning, but as the IO had been slowed down, it became far less in the latter years. All of them agreed with the prepared analysis of the scenario we read to them.

7.4.2 Interview results—closing questions

There were two types of questions in the closing section. Questions 1 to 5 still focused on model structure and behavior, while Questions 6 to 8 asked informants for additional model structure, variable, and scenarios.

Questions 1 to 5 summarized the counterintuitive behavior results in the above scenarios (e.g., “more focus on production, less the monthly profit” and “higher

incident response capability, more incident cost”) and asked the informants whether such counterintuitive behavior was surprising to them (a “no” answer would be coded as the model behavior was plausible). They were then asked to explain the reasons for their answers and relate the model behavior to reality. The reactions of the informants to these five questions are summarized in Table 7-9.

Table 7-9 Closing questions

	A1	A2	A3	A4
Q1	P	P	P	P
Q2	P	P	P	P
Q3	P	P	P	P
Q4	P	P	P	P
Q5	P	P	P	P

Legend: P: Plausible, U: Uncertain, N: Not Plausible

None of the informants thought the counterintuitive model behaviors were surprising. When asked to explain, they gave the right reasons for the behaviors difference. One reason of such consensus would be that after previously going through the six scenarios, the informants had already gained an understanding of the model structure that caused the model behavior. The experts’ answers gave support for the model behavior and structure.

Questions 6 to 8 asked informants for additional model structure, variable, and scenarios that they felt necessary for future model development. Below, we summarize their responses.

- Human compliance. Two informants mentioned that the model might consider adding more human factors in such a way that “When people get used to new work processes, they could start to look for short cuts.” They hoped this piece of structure could be developed in future modeling work.
- Preventive efforts from incident response capability. One informant stated that some of the incident response capability might be allocated to work on incident prevention, which could reduce the frequency of incidents. In the current situation, on Brage, the incident response team was ad hoc, gathering only when an emergency arose, and preventive function did not exist. However, it would be good if the model could show the effect of preventive work.

- Incident reporting. Two informants declared that incidents were not properly reported. One informant pointed out, “Top management has no idea of small incidents that were happening; they only knew about those incidents that disrupted production.” This could lead to misperception of risks and underinvestment in incident response capability. The other informant commented that incidents happening in one part of the system were not typically shared with other parts of the system. There had been no learning from incidents and similar incidents could still occur. If the model could show the benefit of incident reporting and learning from incident, it would be of great interest.
- Investment in incident response capability. One informant mentioned that the decision to make investments in incident response capability might not be based on frequency of incidents, but on the severity of incidents. The top management team did not show concern about small incidents; they only knew about severe incidents. Another informant suggested that the incident cost might affect decision on incident response capability. These two types of decision rules on investment in incident response capability are tested in chapter 8.
- Learning from incidents. One informant thought that learning from incidents could help people build mature new work processes and mature new knowledge. Although learning from incidents was quite limited in reality, if the model could show its effects, it would encourage the management to promote learning from incidents.

7.5 Closing remarks for chapter 7

This chapter presented the review of the Brage model. Four experts from the IRMA team reviewed six different scenarios. The base run scenario produced a great deal of discussions of the model structures that supported it. Understanding this scenario helped the informants to analyze the other scenarios. Some scenarios (such as scenario 4 and 5) were easier than other scenarios (such as scenario 1 and 6), and had more consensus. In general, the informants agreed to most of the patterns generated by the model. They had some uncertainty about the amount of increase/decrease for some variables. Only nine disagreements arose from the total 164 evaluations (Table 7-3 to Table 7-9). Over all, the interview results serve as indicators that the model passed its behavior tests. It also implied that the feedback structure of the model was plausible. In this manner, we completed our model validation. In the next chapter, the model will be used to analyze different scenarios for policy formulation.

8 Policies

Based on the validated Brage model, we investigate different policies to seek answers to our research questions, listed in Chapter 1 Section 1.3 (p. 13): (1) What is an appropriate speed for the transition to Integrated Operations on oil and gas platform considering the trade off between financial gains and information security risks? (2) How does resource allocation during operation transition affect the effective use of new technology and information security risks during the operation transition? (3) How do management decision rules on investment in incident response capability affect information security risks?

In the first part of this chapter, we address each of these questions separately. The Brage model is used to simulate different policy settings. The simulation results are compared and analyzed. Based on the insights from such analyses, we identify the best policies. In the second part, we simulate the Brage model combining these individual policies. The analysis of individual policies leads to insights on how these policies can complement each other to best mitigate information security risks during operation transition. In the final section, we add the link that incident cost will affect the operation transition speed to the Brage model. In such a way, it is possible to study how management's response to increasing incident cost will influence the operation transition and information security risks.

The policies tested in this chapter all come from the model-based interventions: Some are introduced by our client in the group model-building workshops while others are suggested by the informants in the model validation interviews.

8.1 Single Policy

In this section, we address each of the three research questions separately using the Brage model. We first analyze the model behavior of several different policy settings, and end with a summary of the rule to achieve a sound policy.

8.1.1 Transition speed

There are twenty new work processes to be introduced for the transition to Integrated Operations. Management desires a fast operation transition in order to reap the benefits from Integrated Operations as soon as possible. However, a fast introduction of many new work processes and knowledge might cause trouble. We make a comparison between four policies with different transition speeds, the settings of which are listed in Table 8-1.

Table 8-1 Transition speed policies

Base run (Policy 1)	Implement five new work processes in the first year, and afterwards, two new work processes each year until twenty new work processes are completed
Fast transition (Policy 2)	Implement five new work processes each year, until twenty new work processes are completed
Slow transition (Policy 3)	Implement two new work processes every year, until twenty new work processes are completed
Slow then fast (Policy 4)	Implement two new work processes in the first year, and afterwards, three new work processes each year until twenty new work processes are completed

The base run policy is formulated based on the real plan for the operation transition on Brage. Policy 2, “fast transition” is based on the idea that emerged in the second group model building workshop. One team of experts thought new work processes could be implemented at a relative stable speed in 3-4 years (see Figure 8-1) Therefore, we test the policy that five new work processes are introduced per year, - implying 4 years to complete the implementation of twenty new work processes.

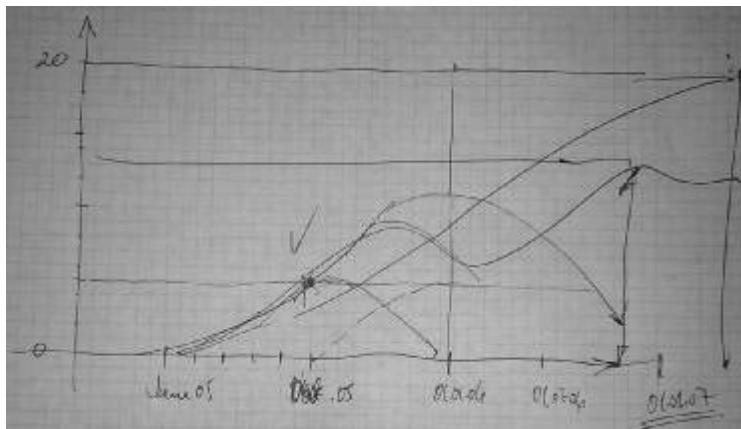


Figure 8-1 Experts opinion on the new work processes implementation

During our communication with the client, we often heard concerns about too fast transition to Integrated Operations. That is the reason we investigate the third policy—to see what would happen if we slow down the speed of operation transition. The introduction of twenty new work processes are evenly distributed in the course of 10 years time, which means two new work processes be implemented in one year.

During our model validation interview, one informant noticed that the “frequency of incidents” and “severity of incidents” both increased sharply in year 1. This led the informant to ask how the situation would be in case of a slow transition speed at the beginning and an increased speed in later years. Thus, we investigate a fourth policy, implementing two new work processes in the first year and then three new work processes per year thereafter.

8.1.1.1 Simulation results analysis

In this section, we present the model-simulated results of these four policies along with the analysis of the model behavior. The base run (policy 1) is represented by the blue line numbered as 1; the fast transition (policy 2) is represented by the red line numbered as 2; the slow transition (policy 3) is represented by the green line numbered as 3; and the slow then fast (policy 4) is represented by the purple line numbered as 4 (see below).

Base Run — 1 — 1 — 1 — 1 — 1 — 1
Fast transition — 2 — 2 — 2 — 2 — 2 — 2
Slow transition — 3 — 3 — 3 — 3 — 3 — 3
Slow then fast — 4 — 4 — 4 — 4 — 4 — 4

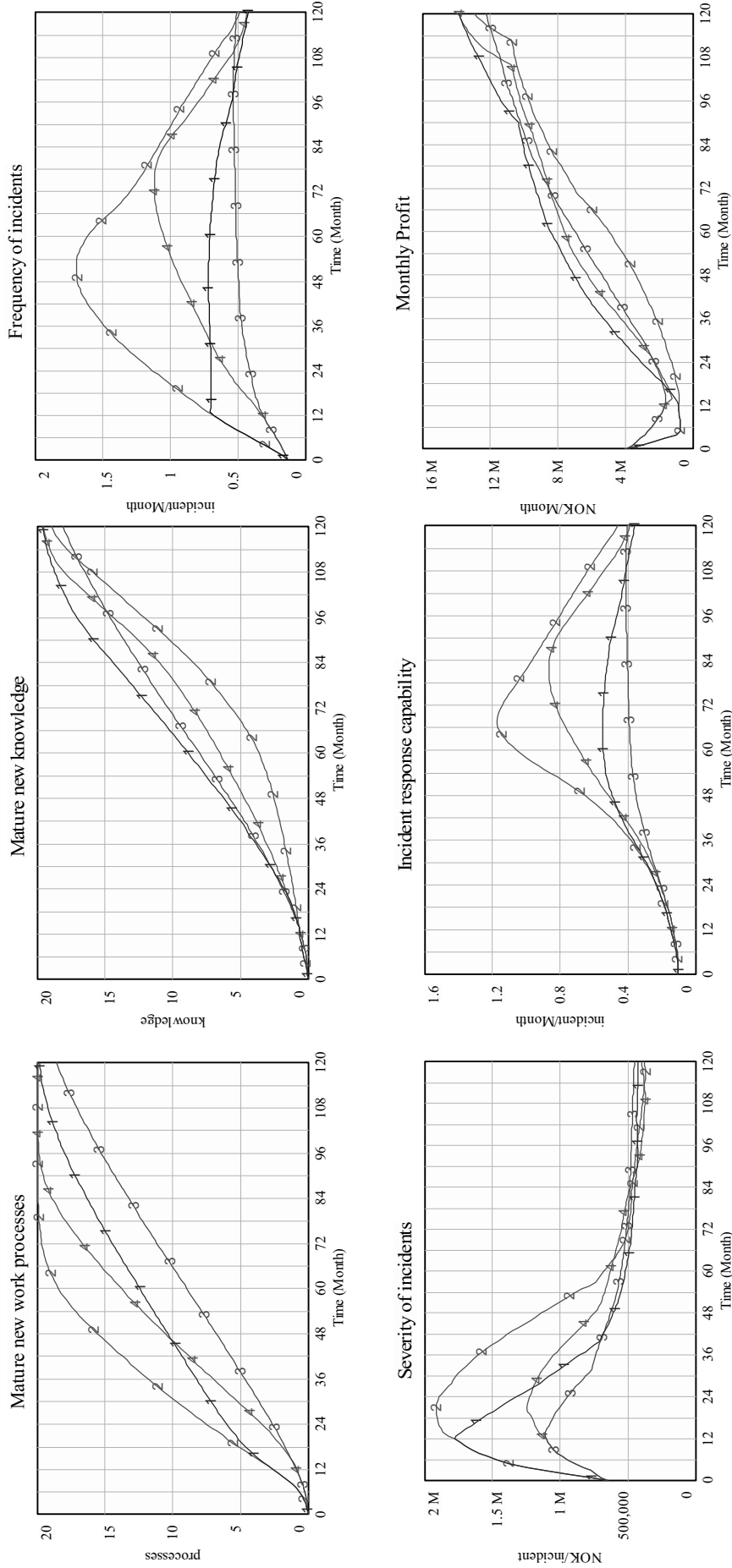


Figure 8-2 Simulation results for different transition speed policies

Base run: (blue line, with number 1) - Implementing five new work processes in the first year and two new work processes each year after.

Five new work processes and related knowledge are introduced in the first year. There are not enough resources to mature all of them. In resource conflicts, resources are first allocated to mature new work processes. Therefore, new knowledge matures only very slowly in the beginning. From year 2 on, two new work processes are implemented each year. The amount of mature new work processes increase steadily. And the amount of mature new knowledge gradually picks up. Both new work processes and new knowledge approach twenty at the end of the simulation. The *"frequency of incidents"* increases sharply in the beginning because the quick operation transition during the first year introduces more threats to the platform and the platform is highly vulnerable mainly due to the accumulation of immature knowledge and the big knowledge gap. The *"frequency of incidents"* stays at the high level as new work processes and knowledge are introduced on a continuous basis. The *"frequency of incidents"* starts to decrease in year 8 since most new work processes and knowledge have been introduced already by then. Since the *"incidents response capability"* is low in the traditional operation, with a sudden sharp increase in the occurrence of incidents, there is not enough capability to handle them. Therefore, the *"severity of incidents"* increases. It takes time to realize the inadequacy of incident response capability, to make investment, and to build up incidents response capability. As the *"incidents response capability"* builds up, the *"severity of incidents"* starts to drop from year 2. The *"incidents response capability"* starts to decrease in year 6 as fewer incidents occur. Thus the *"severity of incidents"* stabilizes. The *"monthly profit"* drops in the first year for two reasons: First, resources are allocated to mature new work processes and knowledge, - which leads to reduction of production output and, thus, to a drop in revenues. Second, the benefit of Integrated Operation is small at the beginning. As more new work processes are implemented, the increased productivity and reduced cost improve the *"monthly profit"*. The *"monthly profit"* increases after year 2, and exceeds the original level in year 3. After year 6, the *"monthly profit"* increases faster than before since most new work processes and knowledge have matured so that resources are released to address production.

Policy 2: Fast transition (red line with number 2) – Implementing five new work processes each year

The number of mature new work processes builds up more quickly than in any other of the policies since five new work processes are implemented each year. Under such circumstance, the operators' are kept busy being trained in new work processes and thus having little time to acquire new knowledge. Moreover, a fast introduction of new work processes creates high "*new initiatives burden*" which reduces the operators' learning efficiency. As a result, the amount of mature new knowledge remains quite low during the first 5 years. After that, as most new work processes are matured, more resources are allocated to mature new knowledge. When knowledge maturation increases, the "*new initiatives burden*" is reduced. That further accelerates the maturation of new knowledge. A reinforcing loop generates increasing growth of mature new knowledge during the last 5 years, reaching around 19 sets of mature new knowledge in the end. Among all four policies, knowledge maturation in policy 2 is the slowest during the first 5 years. Thus in this policy, the amount of immature new knowledge accumulates to its highest level and the knowledge gap is its largest. The widened knowledge gap makes the system most vulnerable and thus causes most incidents. The "*frequency of incidents*" peaks around 1.7 incident/month in year 5. It decreases thereafter as the knowledge maturation picks up. With the highest "*frequency of incidents*", the "*severity of incidents*" is also the highest among all policies. Yet the "*severity of incidents*" is only a little bit higher than in the base run, because more "*incident response capability*" has been built to handle the increasing number of incidents. The "*incident response capability*" is also the highest among all the policies. The "*monthly profit*" drops in the first year and exhibits at that time a behavior similar to the one in the base run. Thereafter, the "*monthly profit*" increases slowly, the slowest in all four policies. This is because the operation transition speed is so fast that the operators could not learn how to work effectively in the new operation. Therefore, the benefit of new operation could not be fully achieved. This policy keeps up with the old saying that "haste makes waste."

Policy 3: Slow transition (green line with number 3) – Implementing two new work processes each year

The number of mature new work processes and amount of knowledge accumulate relatively slowly in this policy and end both at the lowest value among the four policies. This is mainly due to the slow operation transition speed. The “*frequency of incidents*” is lowest because the platform is less vulnerable with a slow operation transition. Operators can take time to learn the new work processes and acquire new knowledge, reducing the immature new work processes and knowledge and the knowledge gap. With least incidents occurrence, the “*severity of incidents*” is also the lowest and the “*incident response capability*” is not as high as in other policies. The “*monthly profit*” does not drop as sharply as in policies 1 and 2 at the beginning, and reaches the lowest point by month 12. Then it starts to pick up. The “*monthly profit*” is not as high as that in policy 1 because the slow operation transition delayed the realization of the benefit of the new technology. But the “*monthly profit*” is higher than that in policy 2 as operators have learnt how to work effectively with the new technology.

Policy 4: Slow then fast (purple line with number 4) – Implementing two new work processes in the first year and three new work processes each year after

Because of the modest operation transition schedule, there are fewer mature new work processes during the first 4 years in this policy than in the base run. Subsequently, the number of mature new work processes in this policy exceeds that in the base run. The amount of mature new knowledge is lower than in the base run, because, from the second year on, the operation transition speed is faster in this policy than in the base run. Less operators’ time is available for maturing new knowledge. The “*frequency of incidents*” is lower than in the base run at the beginning as fewer new work processes and less knowledge are introduced. However, the “*frequency of incidents*” continues to increase until year 6, reaching a higher level than in the base run. The “*severity of incidents*” is much lower than in the base run, because there is no sharp increase in the “*frequency of incidents*” at the beginning. Though the “*frequency of incidents*” keeps increase until year 6, reaching a higher level than in policy 1, the “*incident response capability*” has been built up to handle incidents. Therefore, the “*severity of incidents*” is never higher than in the base run. The “*monthly profit*” behaves similar

to that in policy 3. It does not drop as sharply as in policies 1 and 2, and reaches the lowest point by month 12, when it starts to pick up. The “*monthly profit*” is not as high as that in policy 1, but higher than that in policy 2.

8.1.1.2 Policy evaluation

We have studied the key model outputs in the case of four policies. Here, we provide an overall evaluation and a direction for a sound policy.

For a business unit, whether a retail store or an oil platform, an important goal is to make profit. Therefore, the monthly profit is a crucial indicator for the policy evaluation. Moreover, specific to an oil platform, the management is keen to avoid severe incidents that might cause production disruption or even threaten health, safety, and environment (HSE). Therefore, the severity of incidents is another key indicator used in the evaluation of the policies. Originally, we planned to include the frequency of incidents as an indicator. However, in the model validation interview most informants mentioned that the management does not consider minor incidents. Therefore, the frequency of incidents is not the key concern of the management. This variable is not included as a policy evaluation indicator.

With our emphasis on the severity of incidents and the monthly profit, it is clear that policy 2 is not a good choice. In this policy, the monthly profit is the lowest and the severity of incidents is the highest among all policies. This shows that a fast operation transition, with little time for the operators to be trained in the new work processes and acquire new knowledge, is not only dangerous but also less profitable, because the amount of immature new knowledge prevents the effective use of new technology. In the other three policies, we identify conflicts in the two indicators: A fast transition generates more profit, but it also causes incidents to be of high severity (such as in the base run policy). In contrast, a slow transition reduces the severity of incidents while it generates less profit (such as policy 3). What policy is considered the best depends on the range of what is considered acceptable values for each of the indicators as well as the weight assigned to each of them. For example, if an incident over 2 million NOK must be prevented, then the transition speed in policy 1 (base run) is not acceptable since the severity of incidents reaches more than 1.5 million NOK at the end of year 1. Because the severity of incidents simulated by the Brage model

represents the average severity of incidents, 1.5 million NOK average severity of incidents means that among all incidents, those more severe ones could be well above 2 million NOK. Policy 3, “slow transition” and policy 4 “slow then fast transition” are better choices in this respect. Comparing policies 3 and 4, the monthly profit for the latter is slightly higher, but its severity of incidents is marginally higher. Considering the scale of the monthly profit, a slight increase in monthly profit could result in large absolute amount, policy 4 might be a better one. So far, the speed of implementing two new work processes during the first year and three new work processes each year in the succeeding years is the best among the four tested policies. In cases wherein severe incidents over 2 million NOK is acceptable, policy 1 might be considered as the best since it generates the most monthly profit.

Although the choice of transition speed depends on the management’s judgment of the two key indicators, the “*monthly profit*” and the “*severity of incidents*”, some basic rules may be followed in order to determine the best transition speed policy.

In the case where four months are needed to mature new work processes, and eight months to mature new knowledge during the operation transition, implementing more than three new work processes a year will lead to the accumulation of immature new work processes, immature new knowledge, and a widened knowledge gap (when the operators do not have enough time to mature new work processes, less time will be allocated to mature knowledge). In this case, implementing two new work processes a year might be a quite safe approach. Herein, all new work processes can mature and 1.5 sets of corresponding new knowledge can mature, thus leaving only a half-set of new knowledge remaining to mature thereafter. Implementing fewer than two new work processes a year is an unnecessarily slow transition of operations. Such a slow transition will only result in slightly lower severity of incidents, but in a much less monthly profit. Therefore, a sound policy could be to implement two to three new work processes each year, depending on the level of risk that the management is willing to take and the pressure to make profit.

In more general terms, for any major operation transition project, the management should plan the implementation of new work processes with time-steps that offer time for employees to mature not only their new work processes but also their new knowledge. If the only focus is on immediately reaping benefits from new technology

and implementing many new work processes in a short period of time, the project might face risks wherein employees feel burdened with novelties and where the learning efficiency is reduced, resulting in the improper use of new technology. This might lead to a situation where operators work in the “old way” with new technology. The expected benefits from new technology will not be realized while great vulnerabilities will be introduced into the system.

8.1.2 Resource allocation during operation transition

There are limited resources on a platform. The operators work 12 hours a day, seven days a week. During operation transition, apart from their routine production task, the operators have to be trained in new work processes and acquire new knowledge, - a disruption in routine work. Given the limited resources, if more operators’ time is set aside for new work processes and acquiring new knowledge, less of their time is available for production, and vice versa. Here, we will investigate how different resource allocation policies affect the operation transition and information security risks. Three policies are simulated: 1) “base run,” (the same as the policy 1 in section 8.1.1), 2) “fewer resources for maturation,” and 3) “more resources for maturation.”

Table 8-2 Resource allocation policies

Base run (Policy 1)	This policy implies that 90% of the operators’ time is reserved for production, (10% of the operators’ time is available for maturing new work processes and knowledge)
Fewer resources for maturation (Policy 2)	This policy implies that 95% of the operators’ time is reserved for production, (5% of the operators’ time is available for maturing new work processes and knowledge)
More resources for maturation (Policy 3)	This policy implies that 85% of the operators’ time is reserved for production (15% of the operators’ time is available for maturing new work processes and knowledge)

In the base run, we set the “minimum operators resources for production” to 90% of the total operators’ working time. During the model validation interview, the informants suggested that there was always a strong focus on production and that management could not afford major drop of production performance. As a result, we test what if less time is provided for training and learning by setting the “minimum operators resources for production” to 95%, leaving only 5% of operators working

time for the operation transition. During the workshops, the group members came up with policies for more training, which means more time is provided for the operators to mature new work processes and knowledge. We test this policy by setting the “minimum operators’ recourses for production” to 85%, leaving 15% of the operators’ working time for training and learning.

8.1.2.1 Simulation results analysis

In this section, we will present the results and an analysis of the behavior resulting from model-based simulations when applying the three policies. The base run (policy 1) is represented in figure 8-3 by the blue line numbered as 1; “less time for learning” (policy 2) is represented by the red line numbered as 2; and “more time for learning” (policy 3) is represented by the green line numbered as 3.

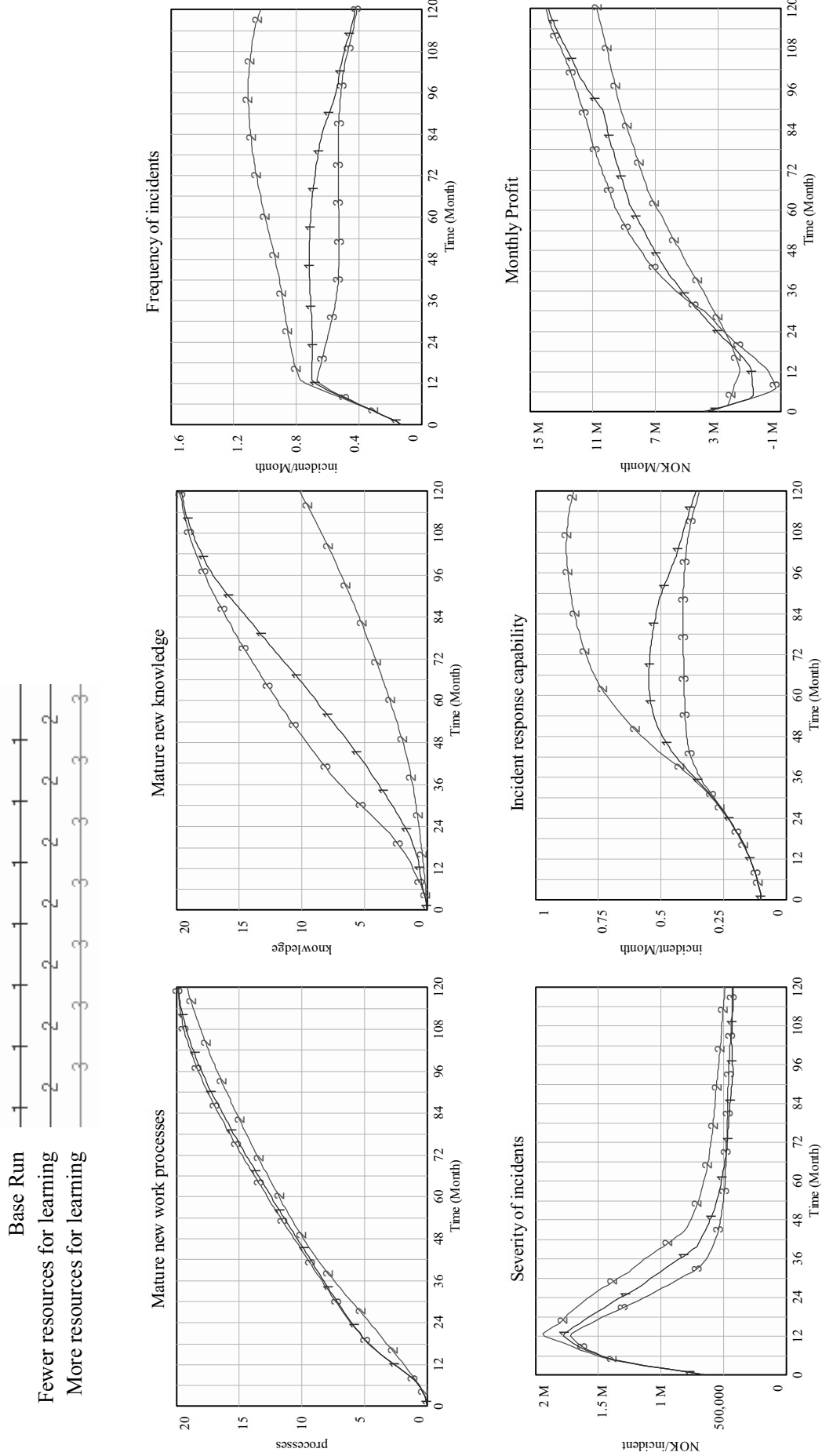


Figure 8-3 Simulation results of different resources allocation policies

Here, we will not repeat the base run analysis, but focus on the other two policies.

Policy 2: Fewer resources for learning (red line, number 2) – 95% operators' time is reserved for production, leaving 5% operators' time for learning new work processes and knowledge

Under this policy, less operators' time is available for new work processes and knowledge maturation. As the time is first allocated to mature new work processes, the time to mature new work processes is almost the same in policy 2 as in policy 1. However, the time to mature new knowledge, the remaining amount of time after what is used for new work process maturation, is much less in policy 2 than in policy 1. As a result, the mature new work processes are only slightly lower than that in the base run, but the mature new knowledge is much less than in the base run. Working with new work processes without mature new knowledge makes the platform very vulnerable, causing the “*frequency of incidents*” to continuously increase until year 8. It reaches a much higher level than that in the base run. The “*severity of incidents*” is only slightly higher because the “*incident response capability*” is built higher to properly handle the incidents. The “*monthly profit*” doesn't drop as much as the base run in the beginning since more time is reserved for production. However, the “*monthly profit*” increases slowly later. In the end, it only approaches 11 million NOK, almost 30% lower than in the base run (reaching around 14 million NOK in the end). This is because the operators do not have sufficient knowledge to work with the new work processes. The benefit of the new technology could not be fully realized.

Policy 3: More resources for learning (green line, number 3) –85% operators' time is reserved for production, leaving 15% operators' time for learning new work processes and knowledge

Under this policy, more operators' time is made available for new work processes and knowledge maturation. Having already enough time to mature new work processes in the base run, additional time does not make a difference. The mature new work processes are almost the same as that in the base run. Yet, in need of more time for new knowledge maturation, additional time fastens the knowledge maturation. With more mature new knowledge, the platform is less vulnerable and has fewer incidents. The “*severity of incidents*” is also slightly lower than in the base run. The incident response capability is lower in this policy. The “*monthly profit*” drops deeper at the

beginning in this policy, even reaching negative figure. This is because more resources are allocated to learning and fewer resources are left for production. However, as the operators quickly learn to work with new technology, the “*monthly profit*” increases faster later, exceeding the level in the base run in year 3.

8.1.2.2 Policy evaluation

We have studied the key model output for the three resource allocation policies and will provide an overall evaluation of the results and a direction for a sound resource allocation.

For the monthly profit, policy 3 is the best in the long run. At the same time, policy 3 produces fewer incidents and less severe incidents. The disadvantage of policy 3 is that the monthly profit-drop in the short-term is more severe. With a long-term perspective, however, policy 3 is found to be the best of the three.

Thus the allocation of resources during operation transition is a matter of short-term versus long-term benefits. People tend to consider short-term benefits more than long-term ones. During the model validation interviews, many experts mentioned that the management’s main focus is on production, and big profit drops are unacceptable. For that reason policy 2 may well be preferred to policy 3. Yet simulation results show that policy 3 generates more profit in the long-term and the severity of incidents under this policy is low.

Overall, the basic rule is that when new work processes are to be implemented and new knowledge thus introduced, the management should expect and allow for a production drop over a short period of time to allow for people to adapt. Such activities are distractions from routine tasks. Under such circumstances, short-term benefits often conflict with the long-term ones. If more time is given for people to learn new work processes and knowledge, their short-term performance will drop more severely. In the long run, however, the benefit of the new technology could be fully realized at an earlier stage. If less time is given for people to be trained in new work processes and acquire new knowledge, their short-term performance might not drop so much, but in the long run, the benefit of the new technology could take a longer time to realize. Based on the empirical evidence that management mostly

focuses on short-term benefits, we would like to emphasize the need to sacrifice some short-term benefits in exchange for more long-term benefits, as illustrated by the simulation results resulting from the policies tested.

It might be wise to notify the operators of the expected short-term performance drop before the start of operation transition. When trying to motivate people for a new operation method, the management often focuses on the benefit that the new method will bring. However, when people start to use it, complaints about the new method often surface. People cannot complete their work as quickly and as smoothly as they are used to, and they make mistakes, yet they do not know whom to contact when deviation occurs. All the unfamiliarity generates negative feelings about the new method, delaying the adoption process or even making it fail. Plenty of cases exist wherein a new system is implemented, but people still work in the traditional way. It is sometimes difficult for the operators to see that it is not the new method of operations that causes the productivity drop, but their unfamiliarity with the new method. By continuously using and learning of the new system, workers can regain and even improve the productivity with the new operation method. Therefore, in order to smoothly get over the operation transition period one may make people aware of upcoming difficulties during the transition period and encourage them to overcome the difficulties by using and learning the new method.

8.1.3 Management policy on investment in incident response capability

Most organizations view security control as an overhead factor and adopt a reactive security management approach, that is, they only address security concerns after actual incidents happen. A proactive approach requires action before incidents happen. For those who are responsible for security, it is often difficult to persuade senior executives and board members to implement information security in a systemic way (Allen 2005). The difficulty in selling proactive investment lies in the paradox of information security management: if investment is made proactively, the frequency of incidents and severity of incidents will be reduced, leading to a low perception of risks and making it difficult to justify the investment in information security management. This reasoning is best embodied by the statement, “Nobody ever gets credit for fixing problems that never happened”.

The same situation is reflected in the Brage case. During the group model-building workshop, we have identified that the investments in incident response capability is based on the frequency of incidents. When more incidents occur, management will feel the need to make investments in incident response capability. Later, during the model validation interview, experts thought that this assumption remains to be too optimistic. Two out of four informants mentioned that the top management, people who make investment decisions, does not know of any of the minor incidents taking place in work place. They only recognize and are concerned about severe incidents that cause production disruption. One informant thought that top management might make an investment only when the incident cost is high.

The Brage model is based on the structure elaborated from the group model-building workshop, that is, the investments in incident response capability is based on the frequency of incidents. We will first test this policy rule. Then, we will adjust the Brage model in order to test the other two policy rules, that is, investments in incident response capability based on severity of incidents and investments in incident response capability based on incident cost.

8.1.3.1 Invest when more incidents happen

In this part, we will use the Brage model to simulate two policies. The first one represents a reactive policy, in which investment in incident response capability is made when more incidents happen. The second policy is a proactive one, in which investment is made before the operation transition starts.

Table 8-3 Response capability investment policies:

Policy 1: Invest when more incidents happen (base run)	Keep the initial incident response capability at 0.1 incident / month.
Policy 2: Raise initial incident response capability	Raise the initial incident response capability from 0.1 incident / month to 0.3 incident/month.

In traditional operations, the incident response capability is quite low. There is no need for high incident response capability with the limited use of ICT. The average incident cost per month in traditional operation is only around 80,000 NOK. Normal

severity of incidents is 500,000 NOK. Therefore, incident response capability in traditional operation is only 0.1 incident/month. In accordance with the first policy, the management keeps the incident response capability level despite their concern about increasing information security risks. Following the second policy, on the other hand, the management raises the incident response capability to 0.3 incident/month before the start of the operation transition. The increase is significant (200%), but small in absolute terms (0.2 incident/month), as the management would not raise the incident response capability to a very high level considering the tight cost control.

Now, in Figure 8-4 and 8-5, we will present the model-simulated results of the two policies along with an analysis of the model behavior. The behavior resulting from the “invest when more incidents happen” policy is represented by the blue line numbered as 1; the behavior resulting from the “raise initial incident response capability” policy is represented by the red line numbered as 2.

Invest when more incidents happen — 1 — 1 — 1 — 1 — 1 — 1 — 1 —
 Raise initial incident response capability — 2 — 2 — 2 — 2 — 2 — 2 — 2 —

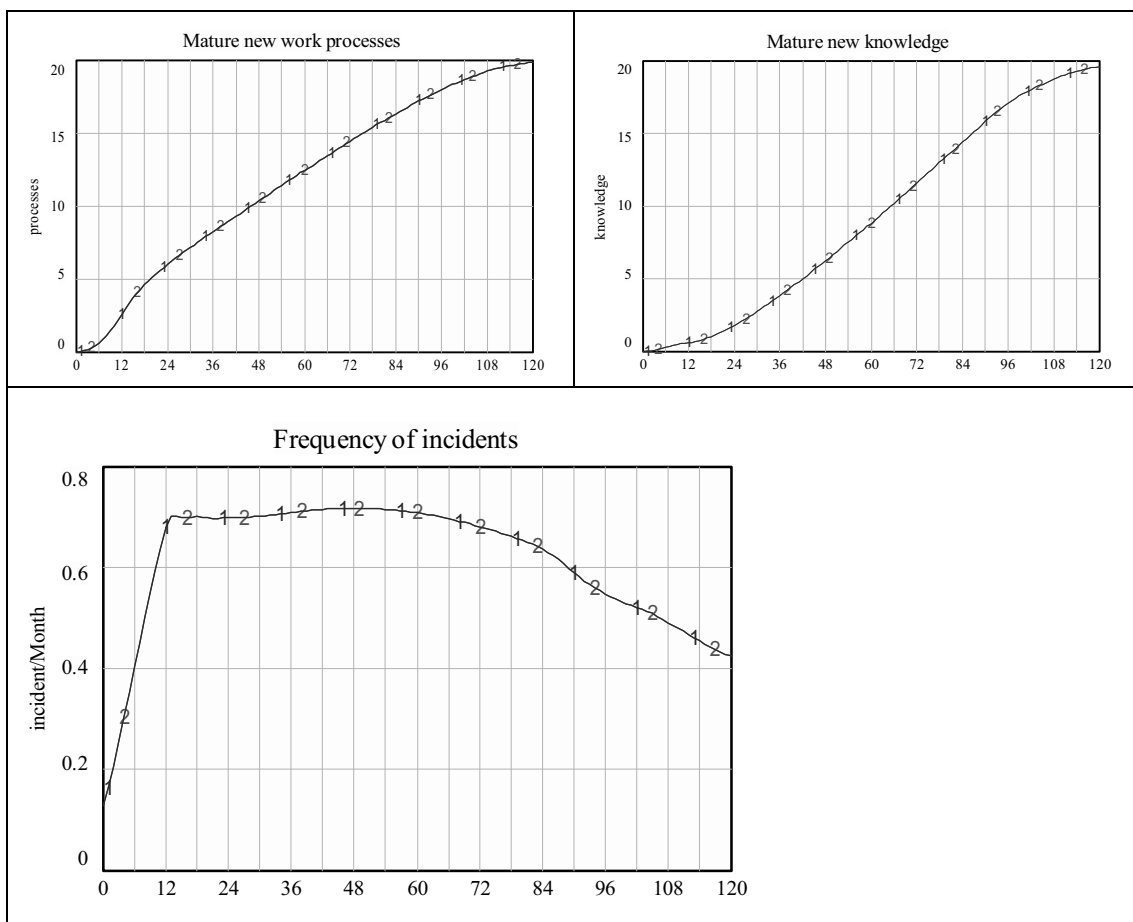


Figure 8-4 Mature new work processes and knowledge and frequency of incidents resulting from a reactive vs. a proactive investment policy

As shown in Figure 8-4, changing the initial incident response capability will not affect the operation transition. Therefore, mature new work processes, mature new knowledge, vulnerability index, and frequency of incidents remain the same for the two policies.

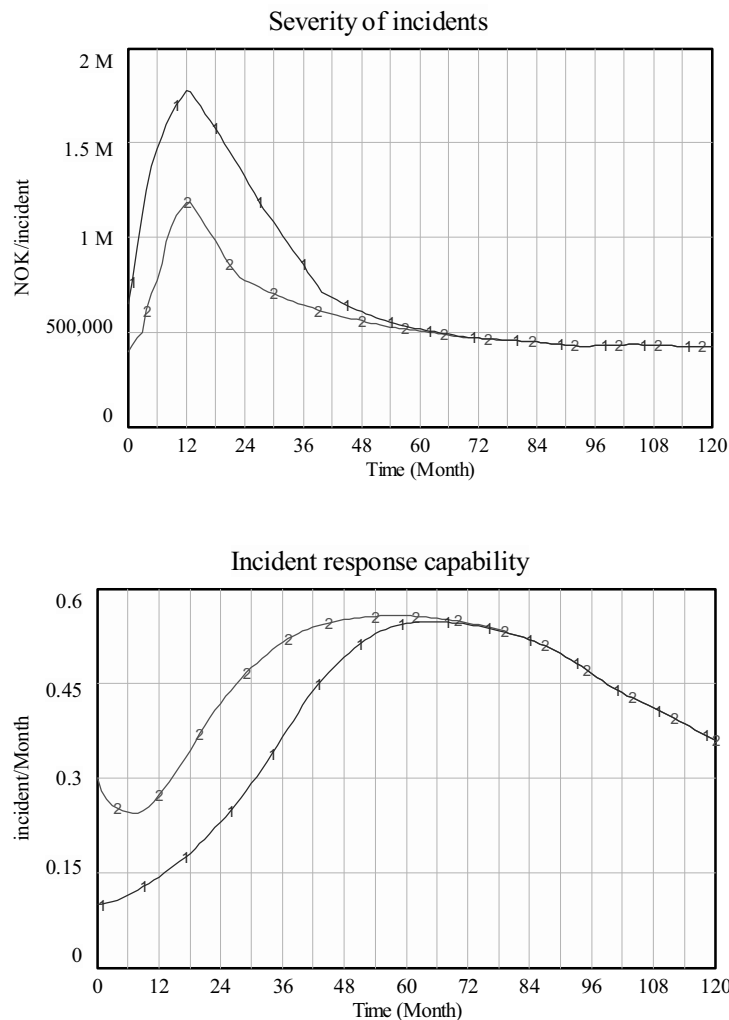


Figure 8-5 Severity of incidents and Incident response capability resulting from a reactive vs. a proactive investment policy

The “*severity of incidents*” is greatly affected by the incident response capability. Under policy 2, the severity of incidents peaks around 1.2 M NOK / incident, while in the base run, it peaks to around 1.7 M NOK / incident. In comparison, the “*severity of incidents*” reduces by around 35% under policy 2.

For these two policies, the “*frequency of incidents*” is exactly the same. The different behavior of the “*severity of incidents*” is solely caused by the difference in the

“*incident response capability*” under the two policies. Why does incident response capability build up so slowly in base run? Why doesn’t management invest more as many incidents happen? It is because the management does not know that so many incidents are in fact happening. With a low incident response capability, only a small fraction of incidents is detected, leaving a large fraction of incidents undetected. Therefore, the management’s perception of the frequency of incidents is much lower than the actual frequency. This causes underinvestment in incident response capability, which results in the high severity of incidents. As seen in Figure 8-6, policy 2 causes the incident detection rate to be much larger than in the base run.

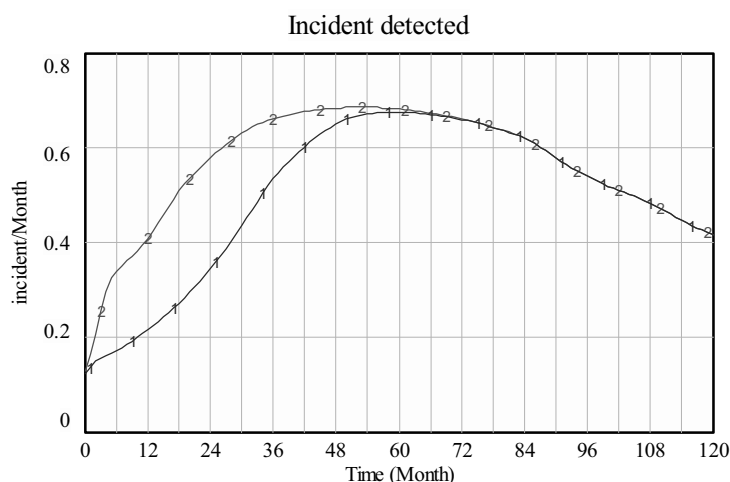


Figure 8-6 Incident detected resulting from a reactive vs. a proactive investment policy.

This is what people call the “*capability trap*” during the group model-building workshop. Herein, a low incident response capability leads to a small fraction of incidents detected, resulting in the low perception of risks and underinvestment in incident response capability. This feedback loop traps incident response capability from achieving the real desired level. One real example given by the experts in IRMA is on a virus-stricken computer that kept on shutting down by itself after working for several hours. The operators felt annoyed by the work disruption, but no one really knew that it was caused by a computer virus. Months passed before people finally found that it was a virus causing the problem. If this virus contaminated the production system, and the production system shut down during production, it would have caused severe incidents. This case reflects that low incident response capability cause low incident detection. Moreover, undetected incidents are of great danger and could eventually have severe consequences.

Policy conclusions

The results from the policy tests support proactive investments in incident response capability. As suggested by the information security experts from the IRMA team, any incident cost from 100 K NOK -2 M NOK is labeled as “dangerous”, ranked level 3 (level 5 for most serious incident) and incident cost from 2 M NOK-20 M NOK is labeled as “critical;” ranked level 4. The variable severity of incidents represents the average cost of incidents, which implies that among all incidents in the base run, those more severe ones are critical incidents. Under policy 2, most incidents are still within a dangerous level.

However, investing in incident response capability is not always cost-beneficial. Whether additional investment in incident response capability is efficient depends on the adequacy of incident response capability. If the incident response capability is already adequate, further investment will be in vain. During the operation transition, when the original incident response capability is deemed inadequate, the management should consider proactive investments. Based on the simulation, we can see that with low incident response capability, fewer incidents are being detected. Thus, a reactive policy will trap the management into being unable to discover an increasing number of incidents and into under-investment in incident response capability. Besides, building incident response capability takes time. It might be too late to invest when the signs of an increasing number of incidents show up. Overall, during the operation transition, the policy to make investments only after recognizing that more incidents happen, will lead to high probabilities for severe incidents.

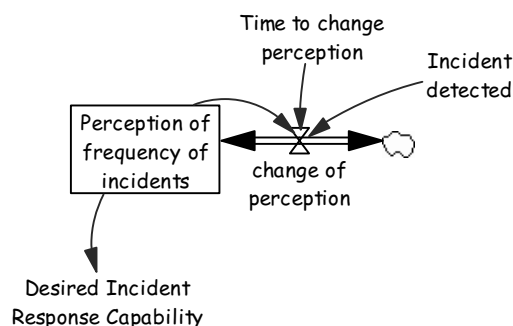
The above model not only applies to oil and gas companies during the operation transition but also to other high-risk organizations under normal operations. The number of Internet users is ever-increasing and the tools for attacks are quickly evolving. Even without any operation transition, companies constantly face a changing environments and increasing threats. If a company only observes a few incidents, the management should not simply draw the conclusion that the company is in low risk condition. In fact, there are two possibilities: it could be that the company has managed its information security risks very well, or that the incident response capability is so low that only few incidents are being detected and reported. In the latter case, the company is actually under great risk. An audit program for information

security would be necessary to investigate the real information security condition of any company.

8.1.3.2 Invest when severe incidents happen

From the model validation interview, we learned from the informants that those who make investment decisions do not seem to be aware of the minor incidents occurring in the workplace. “They only care about those severe incidents that disrupt production,” one informant claimed. As such, we changed the model structure to capture this observation. In the original Brage model, the investment in incident response capability (based on the “*desired incident response capability*”) is affected by the perception on the frequency of incidents (see left of Figure 8-7). Now the model is adjusted in that the investment in incident response capability is affected by the severity of incidents (right of Figure 8-7). There is a threshold level, under which no investment is made. In such way, the model represents the decision rule that investment decisions are made only when severe incidents happen.

The Original Brage model



The Adjusted Brage model

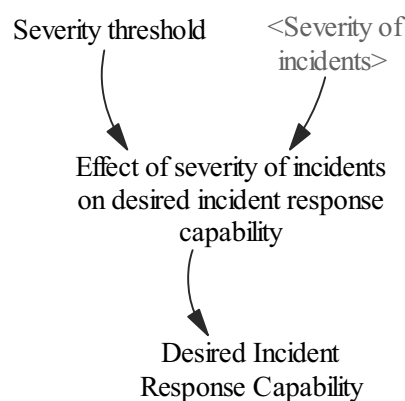


Figure 8-7 Structure adjustment for severity based policy

We simulate two policies, - both of them designed to avoid severity of incidents exceeding the level of 1 M NOK/incident. Under the first policy, when severity of incidents is under 1 M NOK/incident, management does not make investments in incident response capability because of lack of concern. If the severity of incidents is above 1 M NOK/incident, then management will make a significant investment (increase the incident response capability by 30%) to make sure that the severity of incidents be controlled under 1 M NOK / incidents. Under the second policy, already when the severity of incidents reaches 0.7 M NOK/incident, management starts

investing preemptively in incident response capability. Yet the investment is not as much as under the first policy. Management only invests 10% of the current incident response capability.

Policy setting:

Policy 1: Invest when severe incidents happen	When the severity of incidents is over 1 M NOK/incident, invest to make incident response capability increase 30%.
Policy 2: Invest earlier	When the severity of incidents is over 0.7 M NOK/incident, invest to make incident response capability increase 10%.

Result analysis:

Below we present the results of the two policies along with an analysis of the model behavior. In the diagram below, the “invest when severe incidents happen” policy is represented by the blue line numbered as 1; the “invest when we seem to approach a severe incident” policy is represented by the red line numbered as 2 (see below).

Invest when severe incidents happen — 1 — 1 — 1 — 1 — 1 —
 Invest when we seem to approach a severe incident 2 — 2 — 2 — 2 — 2 — 2

The change in this model structure does not affect the operation transition. As a result, the mature new work processes, mature new knowledge, vulnerability index, and frequency of incidents all remain the same as in the original Brage model (see Figure 8-8).

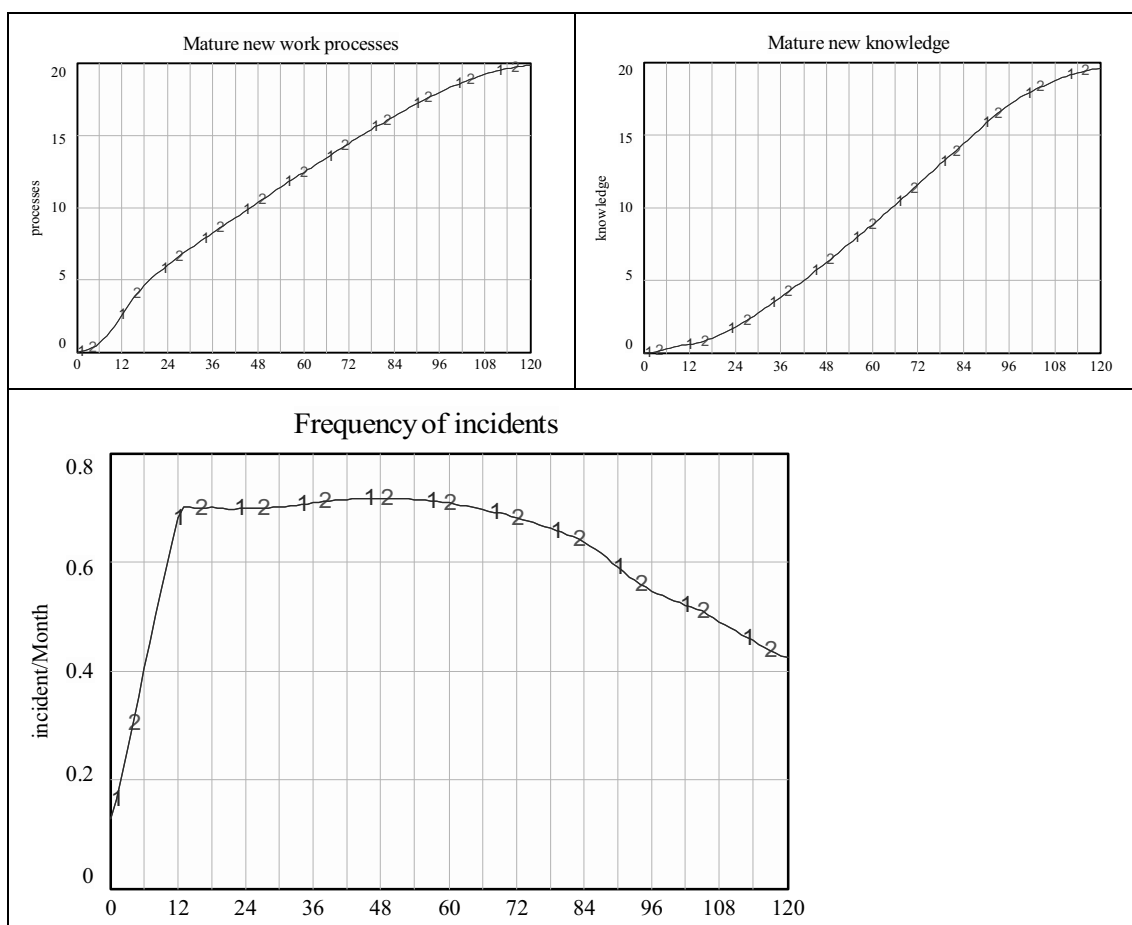


Figure 8-8 Mature new work processes and knowledge and frequency of incidents resulting from policies on severity of incidents

The severity of incidents oscillates under both policies (see Figure 8-9). Under the first policy, even though the management invest a lot (30% of the current incident response capability) to prevent incidents higher than 1 M NOK/incidents from happening, the severity of incidents often reaches well above 1 M NOK/incident. When incident response capability is high, the severity of incidents is low. However, the incident response capability obsolesces over time, and the severity of incidents gradually increases. Yet, the increasing severity of minor incidents is ignored by the management. When the incident response capability becomes so low that incidents are not detected and handled properly, severe incidents eventually will occur. When investment is made at that time, there is time delay for capacity building. And during the time delay, the organization is under risk of having even more severe incidents. As indicated by the simulation results, the severity of incidents in policy 1 will not stop increase when it reaches 1 M NOK/incident, rather, it gets to higher than 1.1 M NOK/incident, and it stays over 1M for more than 3 months time.

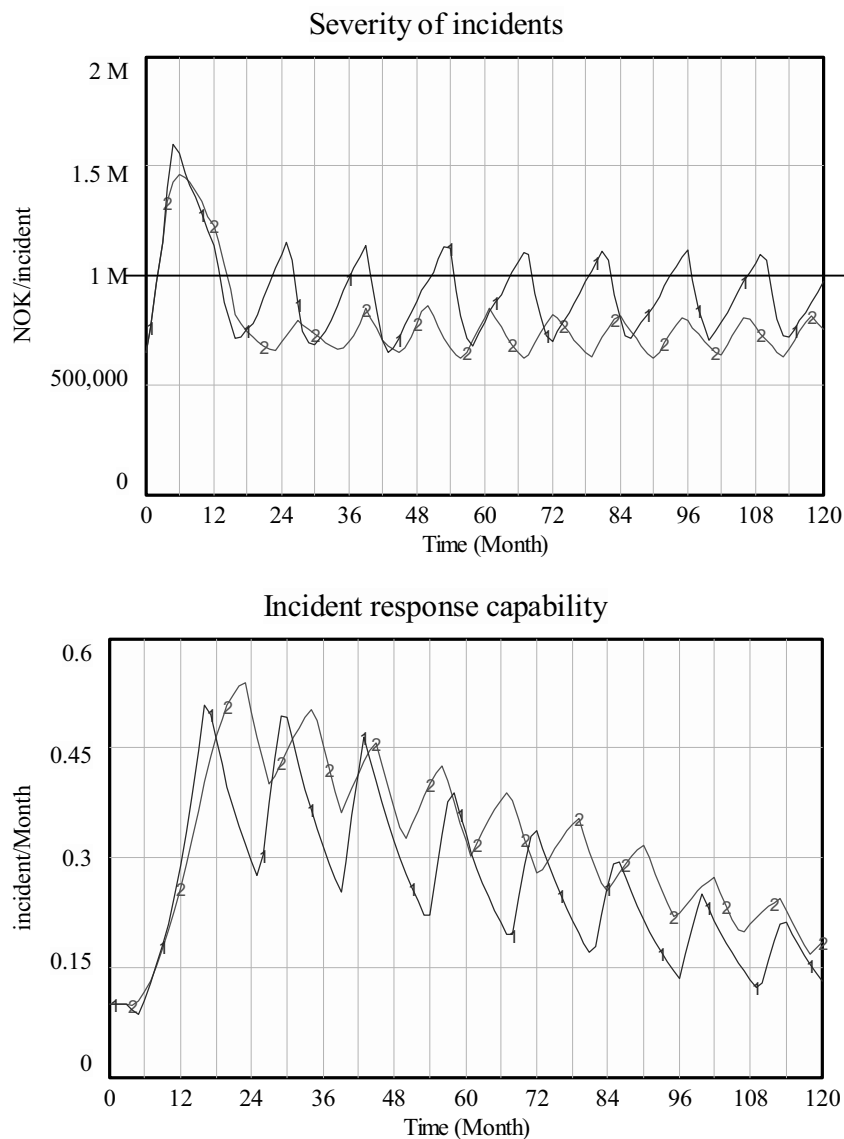


Figure 8-9 Severity of incidents and incident response capability resulting from policies on severity of incidents

In many investigation reports on severe incidents, researchers found that before major incidents happen, there are signs of increasing number/severity of minor incidents happening (Hopkins 2008). However, the management did not notice these small signs. Our simulation result illustrates such kind of behavior. Under the second policy, the management is aware of less severe incidents: When severity of incidents reaches 0.7 M NOK/incident, management starts investing in incident response capability. Even though they invest a less amount, the severity of incidents is well controlled within a small range, thus avoiding any severe incidents. We can see that, - except for the first year of operation transition, when the incident response capability is inadequate and the severity of incidents reaches a high level, for the remaining years

the severity of incidents is controlled between 0.6 M NOK and 0.8 M NOK throughout.

From Figure 8-9, we see that under the first policy, the incident response capability drops to a relatively low level, while it does not do so under the second policy. Noticing the increasing severity of incidents and investing earlier helps prevent the incident response capability from dropping much under the second policy. Hence, the severity of incidents is well controlled under less than 1 M NOK/incident. Of course, as the new work processes and knowledge mature, the system is becoming less vulnerable with fewer incidents happening. Therefore, the need for incident response capability is, in general, decreasing.

While this part of the thesis was under development, a comparative case of car accidents took place in China. In three consecutive weeks, three car drivers, driving after drinking, killed three pedestrians, one in each car accident. There was a heated discussion about how such tragedies could happen. Some experts pointed out that one reason is that the authorities do not take minor traffic accidents seriously. Drivers under the influence of alcohol or drugs will not receive a serious punishment, unless they cause a severe accident. The authorities have not invested a great effort aimed at detecting and punishing offenders in such minor accidents. As a result, lots of people tend to drive under the influence of alcohol or drugs. Consequently, the risk of severe accidents happening is very high.

Policy conclusions

Ignoring minor incidents and caring only about severe incidents is a reactive approach. This approach ignores increasing risks, thus, actually increases the possibility of severe incidents happening. In general, a reactive approach is not preventive. It is necessary to be proactive, to take care of less severe incidents and make investment in incident response capability earlier. As shown in the case of the two policies, if management investigates less severe incidents (when the severity reaches no more than 0.7 M NOK / incident), and makes investments to improve incident response capability, then it is less likely that incidents of a severity reaching over 1 M NOK will occur. On the contrary, in the case of a reactive approach, investments are made after a severe incident has happened, as there is delay in capability building, the

severity of incidents may well climb much higher than expected. During the time of the delay, potential incidents might materialize and lead to severe consequence.

The threshold level 0.7 M NOK is used here as an example. The management has to decide on its own threshold level based on the company's characteristics. For example, if the company could build up incident response capability quite quickly, the level of threshold may be high. On the contrary, if it takes a long time to build up incident response capability, the threshold level may well be low. Another factor to consider is the consequence of a severe incident. The high hazardous industry such as oil and gas production, nuclear plant, chemical plant, wherein severe incidents could lead to a disaster to people and the environment, the threshold should be at a low level. In other industries, such as in retail companies, where the consequence of incident is less severe, the threshold may remain relatively high. There are other factors to consider as well. Here, we will not list all. The key point is that it will not be very effective to care only about those severe incidents. A more effective approach will be to prevent severe incidents by dealing effectively with less severe incidents and make proactive investment before a severe incident actually happens.

8.1.3.3 Invest when the incident cost is high

In the model validation interview, one informant mentioned that the decision to invest in incident response capability might well depend on the incident cost. This kind of decision rule is financially easy to justify. Since the incident cost is high, it will be worthwhile to make investments in incident response capability to reduce incident cost. We now change the model structure to capture this decision rule. In the original Brage model, the investment in incident response capability is affected by the perception on the frequency of incidents (see left of Figure 8-10). In present model, the investment in incident response capability is affected by the expected incident cost, which is the product of "frequency of incidents" and "severity of incidents." There is a threshold level, under which no investment is made (see right of Figure 8-10). In such way, the model represents the decision rule that investment decisions are only made when incident cost are high.

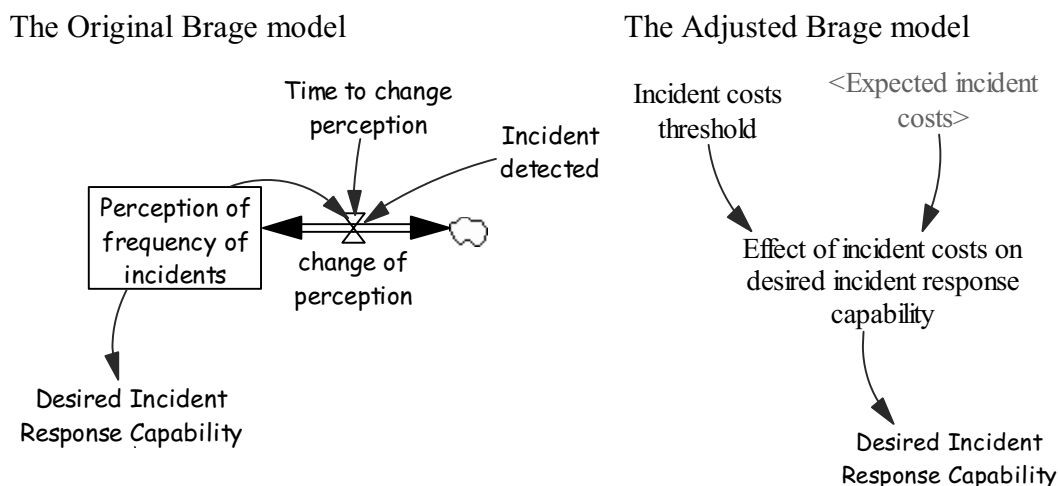


Figure 8-10 Structure adjustment for cost based policy

Two policies are evaluated by way of simulation. Under the first policy, if the expected incident cost is less than 0.5 M NOK/month, no investment will be made; when it is more than 0.5 M NOK/month, the management will invest significantly (to increase the incident response capability by 30%) in order to reduce incident cost. Under the second policy, the management makes an earlier (preemptive) investment. When the expected incident cost reaches 0.3 M NOK/month, the management starts investing, but by an amount less than one invested under the first, - to increase the incident response capability only by 10%.

Policy setting:

Policy 1: Invest when the incident cost is high	When the expected incident cost is over 0.5 M NOK / month, increase 30% of the incident response capability in order to reduce the incident cost.
Policy 2: Invest earlier	When the expected incident cost is over 0.3 M NOK / month, increase 10% of the incident response capability to reduce the incident cost.

Below we present the model behavior resulting from the two policies along with an analysis of the model behavior. The “invest when incident cost is high” policy is represented by the blue line numbered as 1; the “invest when we seem to approach high cost” policy is represented by the red line numbered as 2 (see below).

Invest when incident cost high — 1 — 1 — 1 — 1 — 1 — 1 — 1 —
 Invest when we seem to approach high cost — 2 — 2 — 2 — 2 — 2 — 2 — 2 —

The change in the model structure will not affect the operation transition. As a result, the mature new work processes, mature new knowledge, vulnerability index, and frequency of incidents all remain the same as in the original Brage model.

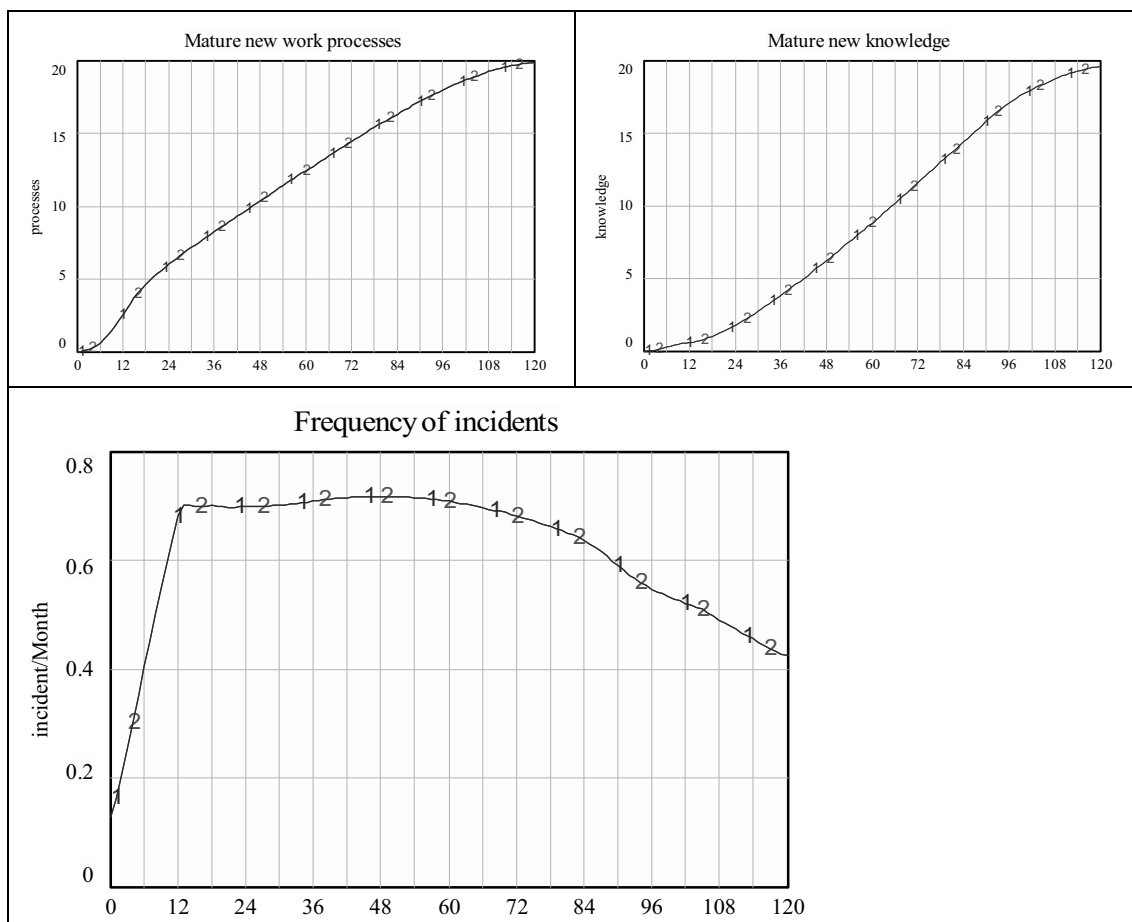


Figure 8-11 Mature new work processes and knowledge and frequency of incidents resulting from policies on incident cost

The incident cost oscillates under both policies (see Figure 8-12). Under the first policy, it exceeds 0.5 M NOK/month periodically. This is because when the incident cost reaches 0.5 M NOK/month, the management starts investing in response capability. However, building such a capability takes time. In the meantime, the incident cost exceeds 0.5M NOK/month. If management wishes to prevent incident cost from exceeding 0.5 M NOK/month, it must invest before the incident cost actually reaches that level. Under the second policy, the incident cost oscillates around 0.3 M NOK / month. The amplitude is considerably less than under the first policy due to the fact that investment is made preemptively and there is no need to invest large amount. The incident response capability will not go up much and it will not drop too low as well.

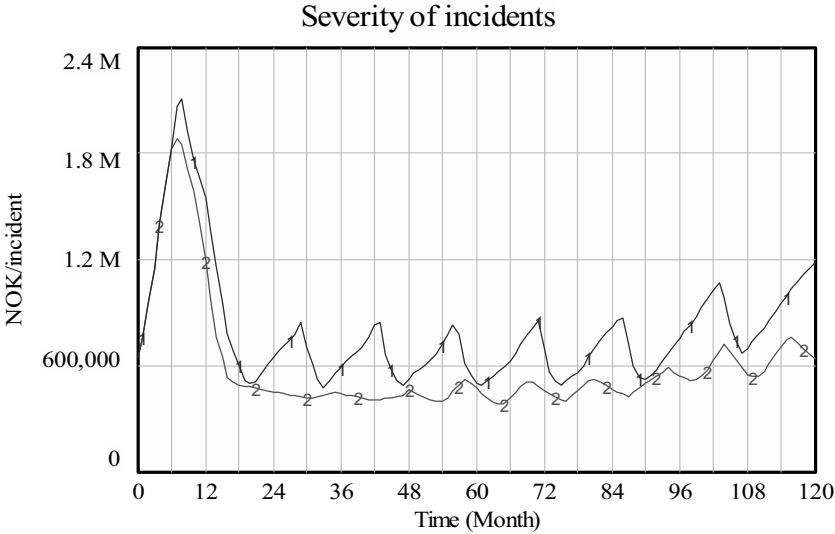
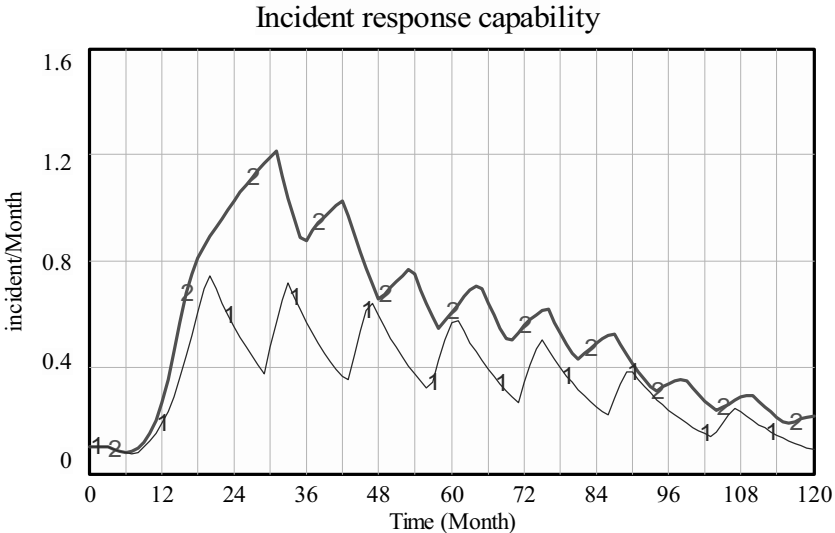
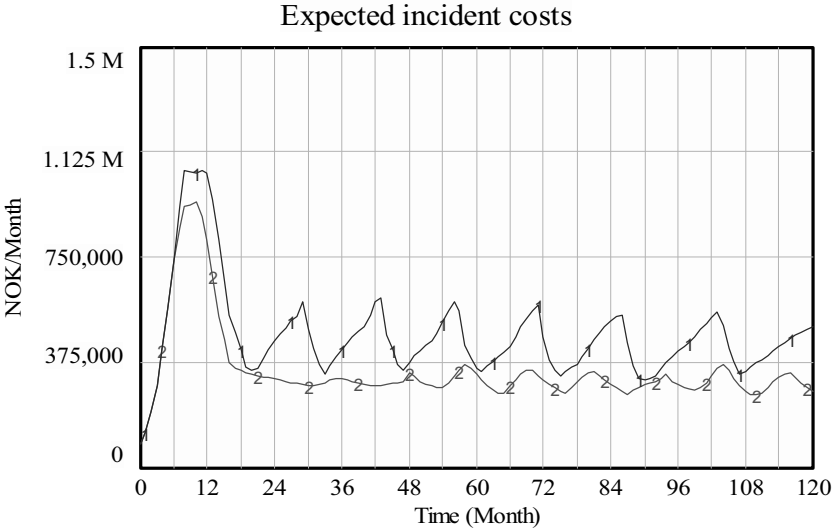


Figure 8-12 Incident cost, Severity of incidents and incident response capability resulting from policies on incident cost

There is a decreasing trend of incident response capability under both policies. The incident response capability is higher under the second policy, as compared to the first one. As fewer incidents occur when new work processes and knowledge mature, investments in incident response capability is being reduced. Under both policies, the incident response capability reaches a relatively low level.

There is another potential problem associated with this decision rule. In the long run, the severity of incidents exhibits an increasing trend under both of these policies. Under the first policy, the severity of incidents reaches a level higher than 1M NOK/incident by the end of simulation. This is because when new work processes and knowledge matures, frequency of incidents is reduced. As a result, incident cost will be low, and thus the investment in incident response capability is reduced correspondingly. The incident response capability diminishes by way of obsolescence over time. When incidents do occur, they will be severe incidents because the capability is inadequate and they may therefore not be handled effectively.

Policy conclusions

Investing in incident response capability solely based on the incident cost will not prevent the low-probability, high-impact incidents. Rather, it merely works to reduce high probability incidents. Most incidents arise with a high frequency, but also with low impact. However, it is the low frequency, high impact incidents that have the most severe consequences. The oil and gas companies are in a hazardous industry that seeks to prevent such kind of incidents. Thus, making investment in incident response capability based on incident cost alone is not a proper decision rule. If this method is used for decision making, the management should, in addition, pay special attention to signs of the increase in severity of incidents and keep the incident response capability at a reasonable level in order to avoid severe incidents.

8.2 Mixed Policy

We have studied the implications of individual policies above. In reality these policies could be used together (synthesized) to achieve a more desirable result. For example, when a high transition rate is desired, then more of the operators' resources could be allocated to learn new work processes and acquire new knowledge. A fast transition of operations might generate high information security risks. In that case, it is better to

raise incident response capability to a higher level preemptively, i.e. before the transition of operations takes place. Below, we study the combination of the three individual policies using the Brage model. Note that this means the investment in incident response capability is based on frequency of incidents. For what discussed in section 8.1.3.2 and 8.1.3.3, the Brage model has been adjusted. We have gained insights about these two decision rules during the previous discussion. Now, we will return to work on the Brage model in the following study. We seek a combination of policies that best mitigate information security risks during the operation transition.

Two combinations of policies will be compared to the policy governing the base case (base run). Insights from the investigation of individual policy lead to the settings of the combined policies. Fast operation transition is desirable. However, we have learnt that fast operation transition will lead to high immature new work processes and knowledge, and enlarged knowledge gap. All of these cause high information security risks. Allocating more resources (operators' time) to learn new work processes and acquire new knowledge helps to reduce immature new work processes and knowledge, reducing knowledge gap. At the same time, preemptively investment in incident response capability can control the severity of incidents and thus, control the information security risks. Based on such general rules, we set up the second combination of policies with a transition speed corresponding to the introduction of three new work processes and the associated knowledge per year (faster than the base run), with 85% of resources reserved for production (more resources allocated for learning), and the initial incident response capability set to 0.3 incident / month (higher initial incident response capability). In the third combination of policies we operate with a transition speed of four new work processes and the associated knowledge per year (even faster than policy combination 2), with 80% of resources reserved for production (even more resources allocated for learning than policy combination 2), and the initial incident response capability raised at 0.5 incident / month (even higher than policy combination 2). The three policy combinations are summarized in Table 8-4.

Table 8-4 Policy combination set-up

	Transition speed	Minimum resources for production	Initial incident response capability
Policy combination 1 base run	five work processes the first year and two work processes each year after	90% of the total the operators' time	0.1 incident/month
Policy combination 2	three work processes a year	85% of the total the operators' time	0.3 incident/month
Policy combination 3	four work processes a year	80% of the total the operators' time	0.5 incident/month

Below is a presentation of the results of the three policy combinations along with an analysis of that model behavior. The base run policy combination is represented by the blue line numbered as 1, the result of policy combination 2 is represented by the red line numbered as 2, and the result of policy combination 3 is represented by the green line numbered as 3.

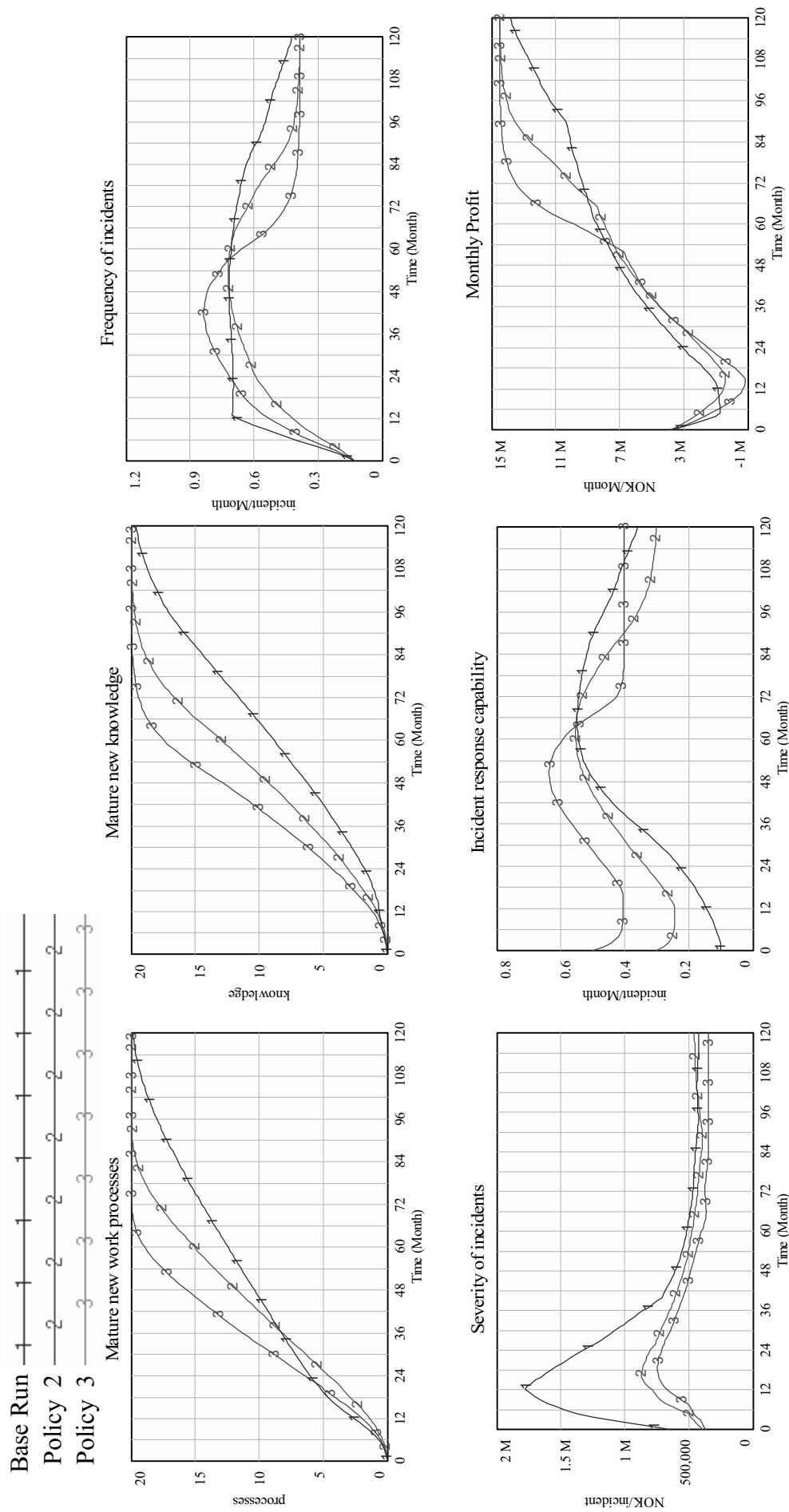


Figure 8-13 Simulation results for mixed policy

Here, we will not repeat the discussion of the base run, but focus on the other two policy combinations.

Policy combination 2: Implementing three new work processes per year (red line, number 2)

Due to the slack in operation transition schedule at the beginning of policy combination 2, less mature new work processes accumulate initially compared to the result of the base run. After year 3, however, the cumulative matured new work processes under policy combination 2 exceeds the level attained in the base run. Mature new knowledge builds up quicker under policy combination 2 than that in the base run because: a) more resources have been made available for knowledge maturation; and b) more new work processes and knowledge are introduced in policy combination 2 after year 3 (the transition speed for the base run is five new work processes in the first year and two new work processes each year after and the transition speed for policy combination 2 is three new work processes per year). The “*frequency of incidents*” gradually increases as the fast transition of operations introduces threats and vulnerability to the platform. When most new work processes and knowledge have been matured, i.e. after year 5, the “*frequency of incidents*” starts to decrease. The “*severity of incidents*” is much lower mostly because that high “*initial incident response capability*” keeps incident response capability at a higher level in policy 2. The “*monthly profit*” drops deeper in the beginning. It picks up from year 2 of, but is, for several years, lower than that in the base run. After year 5, there is a period of rapid increase in the “*monthly profit*” and it exceeds the level in base run at year 5.5. The reason why the “*monthly profit*” is lower during the first couple of years is mainly because more resources are used to mature new work processes and knowledge, which leads to a lower production output and, thus, lower revenues. After year 6, when most of the new work processes and knowledge have been matured, resources are released from learning activities to focus on production. That is why the “*monthly profit*” subsequently increases fast.

Policy combination 3: Implementing four new work processes per year (green line, number 3)

This policy combination is similar to the former one (policy 2), but incorporates a faster transition of operations. After year 2, the level of mature new work processes exceeds the level of that in the base run. There is more mature new knowledge,

because the transition of operations is faster and more of the operators' time has been made available to mature new knowledge. The "*frequency of incidents*" follows the same pattern as the one resulting under policy combination 2, but reaches, eventually, a higher level. This is because the faster transition of operations brings more threats and vulnerability to the platform. When most new work processes and the associated knowledge have matured, the "*frequency of incidents*" is quickly reduced to the same level as under policy 2. The "*severity of incidents*" is the lowest among all the three combinations. This is because the "*initial incident response capability*" under this policy 3 is the highest, 0.5 incident/month. The "*monthly profit*" drops even lower, reaching almost -1M NOK/month at the end of year 1. It increases from year 2 to 4 to the same level as in policy combination 2. As new work processes and the associated knowledge mature earlier, the increase of "*monthly profit*" starts earlier than under policy combination 2, reaching the top level earlier as well.

Policy conclusion

Policy combination 3 has the fastest operation transition speed, while the severity of incidents is the lowest of the all policy combinations. This is because the incident response capability has been raised to 0.5 incident/month before the operation transition is initiated. That way, incidents could be readily detected and handled, so as to control the severity of incidents. From our analysis, we conclude that it is possible to carry out a fast and smooth transition of operations so long as the management is prepared in advance for information security risks. Needless to say, with a fast transition of operations, more of the operators' time is required for maturing new work processes and assimilating the associated knowledge. This will lead to severe, fall in production and, thus, revenue and profit. The monthly profit under policy combination 3 drops to negative level for several months during the years 1 and 2, while, in the long run, the monthly profit under policy combination 3 is the best. It is not easy for the top management and shareholders to support this policy combination because, in view of uncertainties, the future outcome is typically discounted compared to the current outcome. It is difficult to accept a worse-before-better scenario. This model could help them understand that the small short-term profit drop will enable the company to gain considerably larger earnings and profit in the mid- to long-term future. That may well add confidence in such a conclusion and lead to investments of the operators' time for learning. However, if the management still cannot commit

resources to mature new work processes and the associated knowledge, than it is better to reduce the operation transition speed. As we have argued before, without enough knowledge, the monthly profit will be lower in the mid and long term and the platform will be much more vulnerable (see section 8.1.2).

8.3 Model extension

The Brage model describes how operation affects information security risks—changes in the vulnerability index, frequency of incidents, severity of incidents, and incident cost during operation transition. However, the model has not included how security incidents could affect the speed of operation transition. During the group model-building workshops, representative from the top management of Hydro expressed that should a severe incident occur, the operation transition might be delayed, or even stopped. The reason for not including such linkage in the current Brage model is that this managerial decision remains vague. Even to Hydro’s management, it is not clear what kind of incident could trigger a decision to slow down or stop operation transition. Here, we add such a feedback to investigate how the model behavior changes for different policies.

8.3.1 Extended causal loop diagram

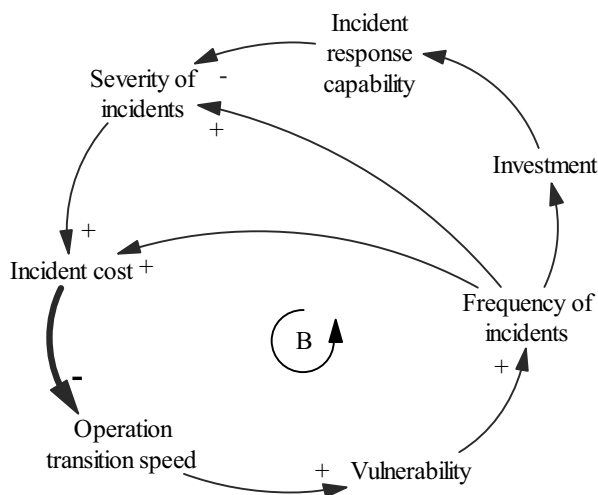


Figure 8-14 Causal loop diagram of feedback from a major incident

The bolded link is added for the current policy analysis. Adding this link creates a new balancing loop: When the incident cost reaches certain high level, the

management will perceive that the transition to Integrated Operations is risky and thus decide to reduce the speed of this operation transition. Slower operation transition generates fewer immature new work processes and less immature knowledge on the platform and will reduce vulnerability and thus lower the frequency of incidents. Under a certain incident response capability, fewer incidents imply that more response capability is made available to handle each incident, which will then lead to better incident handling and reduced severity of incidents. Reduced severity of incidents and reduced frequency of incidents both lower the incident cost.

8.3.2 Policies under the model extension

In addition to the base run, where incident cost does not affect the transition speed, two more policies are made subject to investigation using this extended Brage model. In both of these cases, the incident cost affects the transition speed, yet with different starting points - different level of incident cost. For details on settings see Table 8-5.

Table 8-5 Policy settings for extended Brage model

Policy 1: Base run	The incident cost does not affect the transition speed.
Policy 2: Reduce transition speed when the incident cost is high	When the incident cost reaches a level 5 times higher than its initial value, then the transition speed will be reduced to half. When the incident cost reaches 10 times higher than the initial level, the operation transition will be stopped. When the incident cost is lower than twice the initial level, the management will make an effort to catch up with the schedule.
Policy 3: Reduce transition when the incident cost is moderate	When the incident cost reaches a level 3 times higher than its initial value, then the transition speed will be reduced to half. When the incident cost reaches 10 times higher than the initial level, the operation transition will be stopped. When the incident cost is lower than twice the initial level, the management will make an effort to catch up with the schedule.

Below, we present the results produced by the three policies along with an analysis of that model behavior. The base run policy is represented by the blue line numbered 1, the “reduce transition speed when incident cost is high” is represented by the red line numbered as 2, and the “reduce transition speed when incident cost is moderate” is represented by the green line numbered as 3.

We can see in Figure 8-15 that the mature new work processes are delayed in policy 2 and even more delayed in policy 3. In policy 2, it reaches around 19 mature new work processes at the end of the simulation; in policy 3, it only reaches around 17.

Here, we will not repeat the base run policy analysis, but focus on policies 2 and 3.

Policy 2: Reduce transition speed when the incident cost is high (red line, number 2)

The maturation of new work processes is delayed under policy 2. This delay actually releases some of the operators' time to mature new knowledge. Therefore, in the beginning, the mature new knowledge builds up more quickly under policy 2. Later, however, as the transition is delayed, the mature new knowledge is lower than in the base run. With more mature knowledge under policy 2, the platform is less vulnerable, and fewer incidents occur. This also reduces the "severity of incidents" and the "incident response capability". The "monthly profit" is slightly lower than that in the base run.

Policy 3: Reduce transition speed when the incident cost is moderate (green line, number 3)

The behavior pattern under policy 3 is similar to the one under policy 2. The maturation of new work processes is, however, even more delayed in this case. In the beginning, new knowledge matures to a somewhat larger extent, compared to what happens in the base run, but much less in later years. The "frequency of incidents" is lower than in the base run, and so are the "severity of incidents" and the "incident response capability". The "monthly profit" is much lower in this policy than in the base run because the operation transition is delayed so much that the benefit of the new technology has not been fully realized at the end of the simulation.

Policy conclusion.

Overall, the policy to delay operation transition when incident cost is high can help reduce the severity of incidents at the expense of lower monthly profit in the long run. In some cases, it is worthwhile to delay the operation transition to avoid severe incidents. For example, under policy 2, the monthly profit is slightly reduced, while

the peak of severity of incidents is 20% lower than that in the base run. This may be an acceptable choice. However, if we delay the operation transition relatively early, such as under policy 3, then the severity of incidents is only a somewhat lower than under policy 2, yet the monthly profit is much lower. And this is probably not an acceptable policy.

The management should realize that there are information security risks during the operation transition. The increase in the frequency of incidents and severity of incidents should be expected and, to some extent, be tolerated. If the operation transition is delayed in cases of a small increase in severity of incidents, then this will delay the realization of the benefits from Integrated Operations. The result is not only the reduced profitability, as demonstrated under the various policies, but also the loss of competitive advantage of the firm. In fact, during the operation transition, after the harsh startup phase, one may note that the frequency and severity of incidents will drop as a consequence of the new work processes and knowledge eventually having matured, as shown in the base run simulation. Of course, it is important to ensure that, in the meantime, no incidents with a devastating impact occur. When incident cost reaches high levels, it might be wise to slow down the operation transition and give the operators more time to absorb the new work processes and knowledge. The management should also consider the negative impact of the severe incidents on the operators' perception about Integrated Operations. The operators might feel insecure and resistant to use the advanced technology associated with Integrated Operations. Therefore, implementing proactive policies could be a better option than delaying the operation transition when severe incidents happen. The proactive policies include allocating more resources for operators to learn new work processes and knowledge, and building up a stronger incident response capability prior to operation transition.

8.4 Closing remarks for chapter 8

In the chapter, we used the validated Brage model to investigate the model behaviors under different policy and reached some insights on how to mitigate information security risks during the transition to Integrated Operations. Some insights are specific for the Brage platform, e.g. the transition speed should be between two new work processes per year and three new work processes per year. Some insights are applicable to other organizations, for example, the short-term performance drop during the operation transition is the expense for realizing the benefits of new

technology in the long-term; the reactive approach in investment in incident response capability would lead to high probability of severe incidents. These insights will be summarized in chapter 9 conclusion.

9 Conclusion

In this final chapter, first, we recapitulate the research and its findings. Then, we discuss the contribution of this work, not only to our client Hydro but also to the information security management and the system dynamics field at large. Third, we critique our work, mostly on the underachieved client relationship: what were the problems we encountered?; what could we have done better to improve the situation? Finally, we point out the direction of our future research.

9.1 Recapitulation of the research and its findings

9.1.1 Model development

This project spans over more than five years, from March 2005 to present.⁹ According to the standard modeling process, the research can be divided into four stages:

Modeling process	Time period	Activities
Model Conceptualization	Mar 2005- Oct 2005	Two group model building workshops
Model Formulation	Oct 2005 - Feb 2007	Meetings and interview
Model Testing	Feb 2008 – Dec 2008	Interview with experts
Implementation & Documentation	Jan 2009 – present	Write thesis

The summary of the activities and achievements in each of these stages is as follows.

Stage 1 Model Conceptualization: Two Group Model-building Workshops

The first group model-building workshop articulated the client's problem. Before the workshop, Hydro's concerns on and fears in operation transition and information security risks were vaguely stated.

⁹ This study had a one-year maturity leave from February 2007 to February 2008.

In the first workshop, it was acknowledged that the operation transition not only includes the introduction and maturation of new work processes, but also the introduction and maturation of new knowledge. Knowledge-building takes longer time and is often overlooked, leading to unappreciated knowledge gap, which causes a suboptimal operation transition to result higher information security risks. All the participants reached consensus that the information security concerns Hydro had was specifically on the immature new work processes, immature new knowledge and the knowledge gap during the operation transition that make the platform vulnerable (more prone to incidents). Severe incidents on an oil platform could cause huge finance losses and even threaten HSE (Health, Safety and Environment). The critical factors are the speed of the operation transition, the speed of maturation (related to resources allocation), and how investments in incident response capability could help control the severity of incidents.

The second workshop formed the reference mode of the operation transition schedule and articulated the general model structure. The Brage model is by and large in line with this model structure, as analyzed in section 5.1.1.

Stage 2 Model formulation: Meetings and Interview

After the second workshop, we had series of teleconferences with Hydro and IRMA. Such conferences usually started with a presentation of the model we had developed, -both model structure and model behaviour. The recognition of the model structure and behaviour from the client (Hydro) and the experts (IRMA) add confidence to the model. Then discussions about the definition of variables, their terminology, value, and other concerns followed. Many of the questions raised by the client pointed out further model development direction. The information and data we obtained from the conferences helped us to further improve the model.

Stage 3 Model Testing: Model Review Interview

When the Brage model was completed, we performed the direct structure tests and the behavior oriented structure tests (see chapter 6). However, due to the unavailability of historical time series data, the normal behavior pattern tests were deemed inapplicable.

As an alternative, we invited the IRMA team to review the model behavior. Detailed interview results are presented in section 7.4. Experts' recognition of the model behavior increased the confidence in the model's validity.

Stage 4 Implementation: Interactive learning environment

To disseminate the model insights to a more general audience, we proposed using the story-telling method. Stefanie Hillen, a member of our research project team, developed a framework for authoring such dynamic stories for interactive learning. Based on our model, dynamic stories were developed and tested with Students in University of Agder and Gjøvik University College. We hope to get Hydro's collaboration in the implementation of these dynamic stories as part of our future research.

9.1.2 Model insights

The validated Brage model was used to simulate different policies to seek answers to our research questions. The model insights are summarized below:

I. Considering the trade off between financial gains and information security risks, what is an appropriate speed for the transition to integrated operation?

For an operation transition to be successful, the operators need to learn not only what to do (new work processes) but also how to do and why to do in a particular way (new knowledge), i.e. to have sufficient knowledge about the new work processes. It takes longer time to build knowledge than to learn the new work processes. When planning the operation transition speed, the management should consider the time needed for new knowledge to mature. The following Figure 9-1 shows how various operation transition speeds affects the operation transition (accumulated profit, at the left hand side, purple line with square label) and information security risks (peak severity of incidents, at the right hand side, blue line with round label).

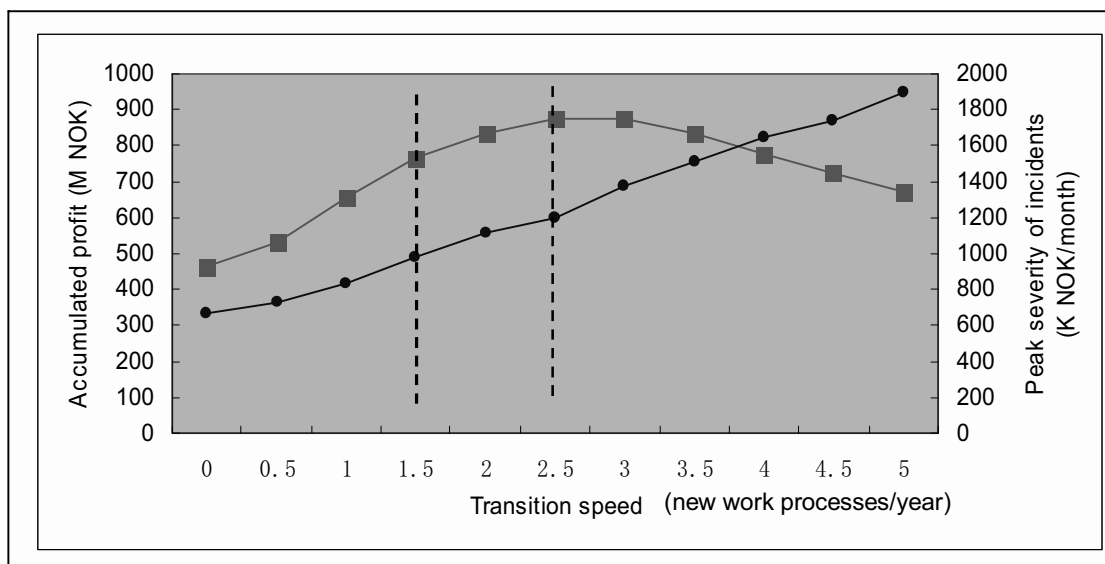


Figure 9-1 Transition speed

We can divide the transition speed into three categories. First, transition speed below 1.5 new work processes implemented per year (three new work processes per two years) is categorized as “slow.” Under such a transition speed, the accumulation of immature new work processes and knowledge is not high and the knowledge gap is not big. Thus, information security risks are not high. From Figure 9-1, we can see that by increasing the operation transition speed in this range, the accumulated profit increases faster than the peak security of incidents. Therefore, the decision to increase the transition speed within this range is mostly beneficial and desirable.

Second, transition speed between 1.5 and 2.5 new work processes implemented per year is categorized as “medium.” Under such a transition speed, the accumulation of immature new work process is low, yet the accumulation of immature new knowledge is relatively high, and the knowledge gap is significant. Therefore, the platform is more vulnerable and information security risks are relatively high. Increasing the transition speed in this range, the accumulated profit increases at a similar pace as the peak of severity of incidents. The judgment as to what constitutes the optimal transition speed depends on the acceptance range of both of these variables and the relative weight assigned to each of them as well.

Finally, transition speed over 2.5 new work processes implementer per year is categorized as “fast.” Under such a transition speed, the accumulation of immature new work process is high, leaving no time to mature new knowledge. The accumulation of immature new knowledge is even higher, and the knowledge gap is

larger. Therefore, the platform is most vulnerable and the information risks are higher. When the transition speed increases in this range, the accumulated monthly profit will decrease because the operators cannot work effectively without the knowledge about how to work effectively with new work processes. As we often say, haste makes waste. It is not a wise decision to increase transition speed within this range if there are no additional resources available to help mature new work processes and knowledge.

One of the difficulties in implementing this model insight is identifying how long time is needed for new work processes and knowledge to mature. This is especially difficult in the case of knowledge, most of which is tacit. The management should carefully observe how people work with the new work processes, the kinds of comments they give, and the difficulties they have working with new work processes. Sometimes, surveys and interviews may help investigate whether knowledge has matured or not.

II How does resource allocation during operation transition affect the effective use of new technology and the security risks during the operation transition?

There are limited resources on the platform. Policy simulations demonstrate that the introduction of new work processes and knowledge will generate a short-term production drop for around 2 years. This is because the operators need to learn the new work processes and knowledge. The learning activities are distractions from routine production tasks. As the operation transition continues, the effect of the new technology on productivity will exceed the effect of reduced resources for production. And the monthly profit will be higher than its original level. The pattern of profit change (first drop then increase) was expressed by the group members in the first group model-building workshop (see Figure 9-2).

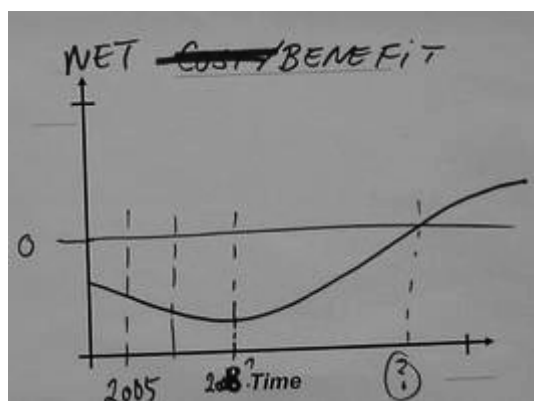


Figure 9-2 Net Benefit from group model-building workshop

From the model validation interview, the IRMA experts suggested that the management of Hydro has the focus to meet the production target. The simulation results shows that if the management strives towards meeting the production target during the operation transition, the operators are encouraged or forced to work on the production task and left with little time to learn new work processes and knowledge. This may lead to the operators working in the old ways under the cover of the new work processes, or finding out short-cut to get work done. The former way will hinder the realization of the benefits of the new technology. The latter way makes the platform more vulnerable.

This research question is related to the first research question raised. When the transition speed is slow, there will be fewer new work processes and less new knowledge that need to mature. Thus, fewer resources are needed for learning activities and the production drop will not be that significant. If, on the other hand, the transition speed is fast, more new work processes and knowledge need to mature. Under such condition, the management should set aside more time for the operators to learn the new work processes and acquire the new knowledge. In the short term, this will lead to a deeper drop in production output. However, when the operators have learned what to do and how to perform effectively with the new operation, the production output will sharply increase. Considering the long-term benefit, it is worthwhile to sacrifice one or two years' profit in exchange for high profit during the latter eight or nine years. However, most people focus on the short-term benefit so that policies endure short-term loss, but long-term benefit is more difficult to implement. For example, a CEO who endures short-term performance drop might be fired before the realization of long-term benefit. The “worse before better” situation is not widely understood. Decisions on the long-term benefit produce a higher yield if

more people understand the distinction between the “better before worse” and the “worse before better” situation better.

The Brage chief estimated that, on average, to mature one new work process, 4% of the operators’ working time is needed, and to mature one set of knowledge, 4% of the operators’ working time is needed. In reality, the resources needed for maturing each specific new work processes and related knowledge are not the same. It depends on how difficult the new work processes are. If the new work process is difficult, then more resources will be needed for learning. Again, the management should carefully observe how the operators are working with the new work processes. If the operators show signs of discomfort working with the new work processes, the management should consider setting aside more time for the operators to learn the new work processes and acquire new knowledge.

III. How do management decision rules on investment in incident response capability affect the security risks?

We have identified three types of management decision rule regarding investments in incident response capability from the group model-building workshop and the model validation interview: (1) invest when more incidents happen; (2) invest when severe incidents happen; and (3) invest when incident cost is high.

Invest when more incidents happen. In a traditional operation, the incident response capability is low because the limited use of ICT technology has incurred very few information security incidents. When operation transition starts, the management is aware of the increasing information security risks. But it is not willing to invest in incident response capability until more incidents occur. It is difficult to justify investments without real signs of increasing incidents. However, when incident response capability is low, only a small fraction of incidents can be detected. That results in a perception of low risk and underinvestment in incident response capability. This feedback prevents incident response capability from quickly achieving its real desired level. Inadequate incident response capability may lead to untimely detection of incidents and improper handling of them, which might lead to truly more severe incidents.

This was referred to as the “capability trap” in the first group model-building workshop. The model simulation shows that the proactive approach, raising incident response capability before the operation transition starts, is effective in reducing the severity of incidents during operation transition. (See simulation results in Section 8.1.3.1)

Invest when severe incident happens. Experts have reported during the model validation interview that the top management does not know the minor incidents occurring in the workplace. They only care about severe incidents that disrupt production. Thus, we modified the Brage model to capture this decision rule. The simulation results show an oscillation of the severity of incidents. Severe incidents that the management is keen on preventing do happen once in a while primarily because the management does not notice the signs of increasing risk and the need for investing in incident response capability. When the severity of incidents reaches their warning line, they start to make investment. However, as there is delay in building incident response capability, the severity of incidents continues to increase before the incident response capability is ready in place. As a result, the severity of incidents reaches higher than the accepted level repeatedly.

The proactive approach is to care about the less severe incidents and make investments on incident response capability when signs of increasing risks are observed, such as increasing number of minor incidents or increasing severity of minor incidents. (See simulation results in Section 8.1.3.2) In this way, it is possible to prevent severe incidents from happening.

Invest when high incident cost occur. This kind of decision rule is financially easy to justify. As incident cost is high, it will be worthwhile to make investment in incident response capability and reduce incident cost. This decision rule works effectively in reducing incidents with high frequency. When the frequency of incidents is low, incident cost will also be low, and thus no investment will be made in incident response capability. Incident response capability becomes obsolete over time. If an incident occurs, expectedly, it will be severe because there is not enough capability to handle the incident properly (see the simulation result in section 8.1.3.3).

This decision rule is not a good choice for the management who is keen on preventing severe incidents. If this decision rule is used in reality, the management should also pay special attention to the increase in severity of incidents. The severity of incidents should be an additional indicator for investment in incident response capabilities.

9.2 Research contribution

The research presented in this thesis is grounded on the case of operation transition in Hydro. It specifically focuses on the change in information security during operation transition. The research utilizes system dynamics to build simulation model and elicit information using model-based interventions. This research contributes not only to our client (Hydro), but to the information security field and system dynamics field at large as well.

9.2.1 Contributions to the client

The contribution of this research to our client Hydro is twofold.

First, the group model-building workshop helped our client clarify the problem it is facing and the mechanism that causes the problem. Trond Lilleng, the person in charge of the operation transition in Hydro, expressed the following during the first group model-building workshop: *“Brage faces risks that Hydro does not really understand. The management does not know whether it is right to make the transition. They fear intruders will come to the network.”* Through the first group model-building workshop, it became clear to all the participants that the operation transition not only includes the introduction of new work processes, but also related new knowledge. Knowledge building takes longer time and is often overlooked. The immature new work processes, immature new knowledge and the knowledge gap will cause the platform to be vulnerable, increasing the probability of incidents happening.

In the second group model-building workshop, after having identified the feedback loops in a discussion with the participants, the platform chief and the chief information security office in Hydro realized the importance of knowledge maturation during the operation transition. A discussion ensued on how to reduce time for knowledge maturation. One idea was to adopt a technical device that could allow the operators on vacation to obtain data and updates from the operators working on the

platform. That way, the operators would more likely remember what they had learned when they come back to work on the platform after vacation.

Second, we provided Hydro with a validated model that gave rise to insights into how the operation transition speed, the resource allocation during operation transition, and the management decision rule on investment in incident response capability affect information security risks. Many other platforms were to be moved into Integrated Operations, following Brage's experience. These model insights could help the management in Hydro to improve the operation transition schedule by better planning. Moreover, the model served as a vehicle by which we could study how various policies play out in the long run. One of the challenges in policy design is caused by the uncertainty of the long-term effect. Statistics tools may be useful for short-term forecasts, but it is difficult to evaluate the long-term effect. The system dynamics simulation model, represents causal structure, provides a vehicle by which we may investigate various scenarios. It facilitates the search for a robust policy that fosters a successful (smooth and fast) operation transition, i.e. one that will work successfully under a wide variety of possible circumstances (scenarios).

9.2.2 Contributions to information security management

Research on information security management has a tradition of merely focused on the technology aspect. Research has, however, recently given more attention to human and organizational factors. This thesis contributes to the field of information security management in three different ways.

First, the change of information security risks during the operation transition (new technology adoption) period has not been subject to model-based studies before. It has been well recognized that new technology adoption is a complex and difficult process. A substantial amount of research has been conducted to examine the various factors that affect successful adoption of new technology (Attewell 1992; Fichman 2001; Burnes 2003; Lee and Kim 2007). The factors identified includes, but are not limited to, the following ones: characteristics of the user community (education, job tenure, resistance to change), characteristics of the organization (centralization, formalization, specialization), characteristics of the technology being adopted (complexity), characteristics of the task to which the technology is being applied (task autonomy, variety, and uncertainty), and the organizational environment (uncertainty,

interdependence) (Lee and Kim 2007). However, information security risks have not been considered. In the literature of information security, research has focused on user interfaces of security-related systems, on counterproductive computer usage and human compliance study (from human aspect), and on information security checklist and standards and various methods for risk assessment (from organizational aspect) (see section 2.3.2 and section 2.3.3). The change of information security risks during the operation transition period has not been studied in depth before. We are now in a fast changing society. Information security risks are deemed to be higher during those changes. How we manage information security risks in this fast changing environment, is an important issue. This research is among the first attempts to address this issue.

Second, we introduce a dynamic view with the long-term perspective on information security management. Although information security incidents happen in an eruptive manner, the underlying mechanism that leads to such incidents often exists for a relatively long period of time. Understanding such mechanism helps us reduce information security risks.

Last, but not least, this thesis illustrates how formal modeling and simulation could enhance our theory building on the dynamics of information security management. The Brage model demonstrated how key information security indicators, such as frequency and severity of incidents and incident cost, could be included in a simulation model. Moreover, the model can be used to identify important information security variables, such as incident response capability and risk perception, which may be considered as key information security indicators later. Information security management involves not only “hard” knowledge, such as work processes and technology, but also “soft” knowledge, which includes people’s awareness, people’s perception, and the culture of the organizational environment. These soft aspects are actually the key factors that affect information security risks. Identifying changes in “soft” variables, such as risk perception, is important in order to improve information security management.

9.2.3 Contributions to the field of system dynamics

It is well acknowledged that system dynamics models are used to help the client seek solutions for their problems. “The modeling process should be placed in the context of the ongoing activities of the people in the system” (Sterman 2000 p. 27). Unlike other

mathematical models, which mainly rely on numerical data, system dynamics models are based on the causal structure of the system, which means understanding the client's system is critical to model building. To understand that client system, proper communication is necessary. Therefore, utility of the system dynamics modeling process relies heavily on the quality of our communication with client.

Some of the research efforts have been devoted to establish best practice for communication with a group of client representatives for model conceptualization, named group model-building workshop. (Vennix, Andersen, and Richardson 1997; Vennix 1999; Vennix 1996; Richardson, Andersen, and Luna-Reyes 2005; Richardson and Andersen 1995; Andersen et al. 2007; Andersen, Richardson, and Vennix 1997; Andersen and Richardson 1997; Luna-Reyes et al. 2006). Though a number of standard procedures have been developed, the researchers also agree that the communication with client is still more art than science. The group model-building process is sometimes compared to a football match or an improvisation jazz concert. Though much could be planned beforehand, the outcome relies heavily on the interactive process. Therefore, documenting and reflecting on different cases is an important step towards the accumulation of knowledge in group model-building (Luna-Reyes et al. 2006).

In this study, we used two group model-building workshops in a series: first to articulate the client's problem and secondly to conceptualize the dynamic model. In this thesis, we fully documented these two group model-building workshops. This adds to the knowledge accumulation on group model-building cases. Many group model-building workshops are conducted with a clear problem definition in mind. Therefore, concept models are prepared in advanced and shown to the client at very early stage of the workshop. In our case, however, we did not have a clear problem definition as a point of departure during the first group model-building workshop. Therefore, the exercises were designed in such a way as to extract information first (divergence) and then converge on a clarification of the problem. The schedule designed for the first workshop was mostly divergent exercises to obtain information related of the problem. The divergent exercises were followed by convergent exercises that allowed the real problem to emerge. As a result, the concept model, based on the problem, was built and presented to the group. This process included obtaining information from the client, making information converge and feed the

converged information back to client in modeling language. In the second group model-building workshop, instead of presenting the concept model, we did an exercise asking the group members to experiment with the concept model. This exercise triggered group members great interest to the model. Also, it helped them to think about the relationship between model structure and model behavior, and to link the model with the reality. Such experience is important for group model-building practice.

Group model-building techniques have received much attention in research as a model-based communication method, while communication with clients during other model building stages, e.g. model validation is less studied. Experts in system dynamics seem all to agree that direct structure validation of a model is a qualitative process, that includes a discussion with client to confirm that the model addresses the client's problem and that the model structure is in agreement with the client's and / or the major stakeholders' perception of the problem at hand. However, there is little literature about how such communication should be conducted. In case where historical data do not exist for behavior test, interview with experts to confirm that the model behavior conforms with reality could be used as an alternative method. Literature on this issue is also scarce. We refer to what Dr. Rich did in his dissertation and conducted structured interview with experts for behavior test. We hope that such case accumulation would lead to further research effort to standardize the best practice of communication in model validation.

9.3 Critique on the model-building process

Based on our research design of various model-based interventions with client, it was expected that Hydro would be highly involved in the model-building processes. However, Hydro's participation in this project was not as comprehensive as expected in the initial stage. Though the situation improved during the model-building process, we lost opportunities to elicit more information in the beginning. In retrospect, we have looked into the reasons why we encountered such initial difficulties in the beginning. That may help other researchers when using tools such as the model-based interventions with client in their studies.

Finding the right person. As we mentioned in Section 4.2, only one person in Hydro, Trond Lilleng, the leader of the Integrated Operations project, attended the first group

model-building workshop. It is important to obtain support from the high level management in the beginning. However, meeting with only one high level person is not sufficient to undertake a model-building exercise of this kind. We found that Trond Lilleng, focusing on the strategy level of the operation transition, can express the overall picture of the whole Operation Integration very well, but couldn't provide a detailed picture on the operational level. Using divergent and ranking exercise, the group members identified who the important stakeholders are. In our second workshop, we successfully involved a variety of people with high influence and high impact that constituted the major stakeholders. From these people we obtained more detailed information about new work processes implementation and related organizational changes. For future research, when planning for a model-based intervention with a client, an ideal structure is to interact with one person, representing the top management and three to four mid-level managers.

Meeting place. While Hydro is located in Bergen, our research cell is located in another city, Grimstad. Though, the two cities are less than 200 miles apart, however, and a trip from Bergen to Grimstad takes at least four hours, in total. The first workshop was organized in Grimstad. We assume this was one of the reasons why only Trond Lilleng attended this first group model-building workshop. It was difficult for the platform chief and other management personnel to leave the control center at the same time for a two-day period. We held the second workshop in one of the training rooms in Hydro, Bergen. Five key persons participated, all of whom became interested in the system dynamics method, which is a key success factor. For only that way we may be able to obtain the information necessary to build the Brage model. We conclude from our experience that location is very important for an effective model-based intervention to take place. If possible, a place convenient for clients' participation is always preferred.

Client contact. Only IRMA had an agreement with OLF for the collaboration with Hydro. AMBASEC also work with Hydro because of its collaboration with IRMA required by the Norwegian Research Council. Therefore, AMBASEC didn't have direct contact with Hydro. The meetings we wanted to have with Hydro were organized through IRMA. This complicated the matter and was not efficient. Sometimes, it was difficult for IRMA to argue for the necessity/time with Hydro contacts when they excused themselves amid their busy schedules. Much time has

been wasted in the process of negotiation and communication. It is important to have a direct channel of communication with client to ensure efficiency.

Language. The IRMA team was able to participate in many of the OLF's meeting on operation transition and information security. These meetings provided information relevant to the research and were opportunities to present our primary research result, obtain feedback, and keep contact with Hydro. However, as these meetings were in Norwegian and the two main researchers in the AMBASEC team, Ying Qian and Stefanie Hillen, did not understand Norwegian, we could not participate in such meetings. Our inability to understand Norwegian proved to be a disadvantage when working with our client, since the meetings, documents, and language at work were all in Norwegian. Though English is the working language in academia, a research project that closely works with client has to consider the local language applied.

9.4 Future research direction

The current Brage model is at a highly aggregated level. It is possible to disaggregate the model to include more details about work processes and knowledge. At the same time, the model can be extended to include more sectors. The model can likewise link with the risk matrix developed by IRMA. In the remainder of this section, we detail some of the specific extensions of our work that we propose be undertaken in the future.

9.4.1 Disaggregate the model

In the current version of the model, work process and knowledge are aggregated concepts, and we did not differentiate one work process from the others. Every work process takes four months to mature, while the corresponding knowledge takes eight months to mature. The impact of new work processes and knowledge on vulnerability is identical. We also did not distinguish how much benefit each new work process brings to the platform and only assumed that earlier implemented work processes would bring more benefit because management would eventually implement those higher impact work processes earlier to harvest the benefits of Integrated Operations as early as possible.

In reality, the 20 new work processes to be implemented on the Brage platform are all different from each other. Some may be easier to implement than the others, implying a shorter maturation time for this new work process and new knowledge. Some work processes could have a large impact on information security, bringing more threats or vulnerabilities into the system. Some work processes bring more improvement by increasing productivity, while some others have a larger impact on cost reduction.

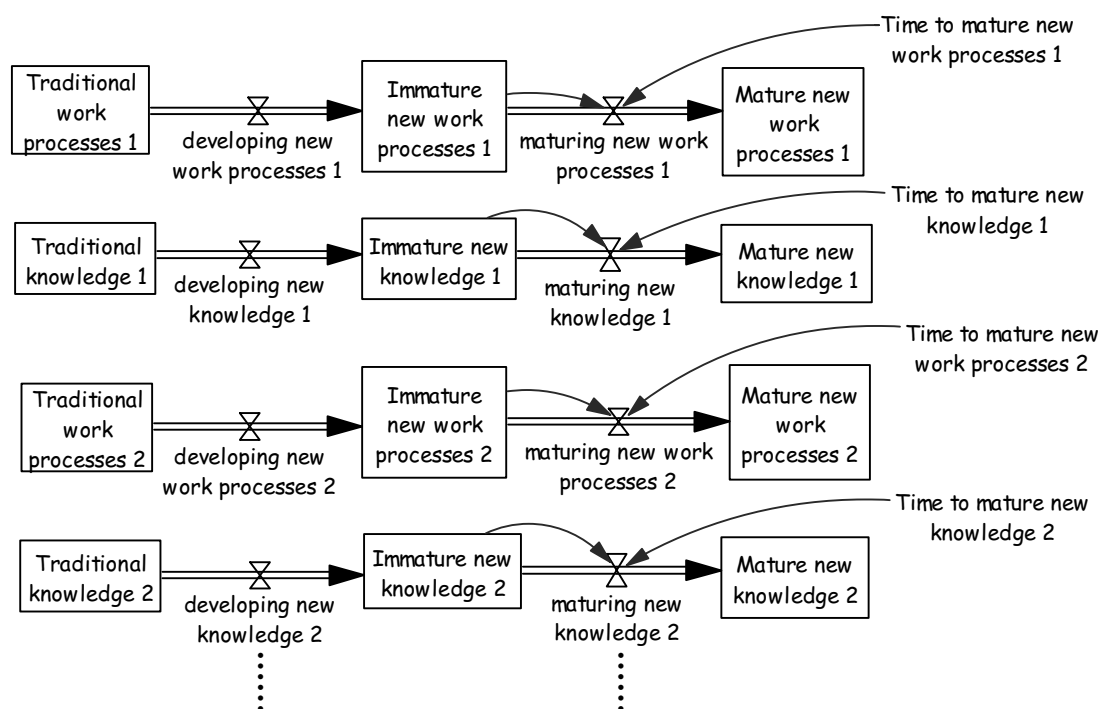


Figure 9-3 Disaggregate work processes and knowledge

If provided with detailed information about each new work processes, the model can be disaggregated from abstract new work processes into specific *new work processes 1*, *new work processes 2*, ..., and *new work processes 20*. Accordingly, new knowledge can also be disaggregated into *new knowledge 1*, *new knowledge 2*, ..., and *new knowledge 20*. In doing so, the model could be used not only to investigate transition speed in general, but also to form a detailed transition schedule: when to implement what. Such an operation transition schedule takes into account the desire for a fast realization of the benefit of new technology and low information security risks as well.

9.4.2 Extend the model

The Brage model describes the operation transition and the change of information security risks during this process. Additional sectors could be added to the Brage model to tackle various questions.

One example is the issue of human compliance. During the model validation interview, the experts mentioned that when people are new to the work processes, they tend to follow the instructions carefully and obey the rules. However, as soon as they get used to new operations, they tend to find ways to cut corners. Some may ignore security rules, which will lead to more vulnerability. This theory sounds reasonable, but it requires more research efforts to be solidified and adding it to the model.

Another example is on the expectation regarding the effects of the new operations. During our discussion with the client, the representatives mentioned that the operators form an expectation of the effects of the new technology before it is implemented. However, upon implementation, the operators often find that their expectations are not met. To motivate the operators for new operations, the management often focuses on the benefits of the new technology, thereby setting high expectations. However, when the operators start to use new technology, its effectiveness cannot be fully realized, because the operators are not familiar with that new technology. Therefore, an expectation gap is generated. This gap, if large, will reduce the operators' willingness to make use of and learn to use the new technology effectively. Thus, the effectiveness of the new technology will remain low. This will trap the effectiveness of using new technology at a low level (see Figure 9-4). On the other hand, if the expectation gap is not large, the operators are willing to use it and to learn about the new technology. This will improve the effectiveness of using new technology and further reduce the expectation gap, - which make the new technology adoption successful.

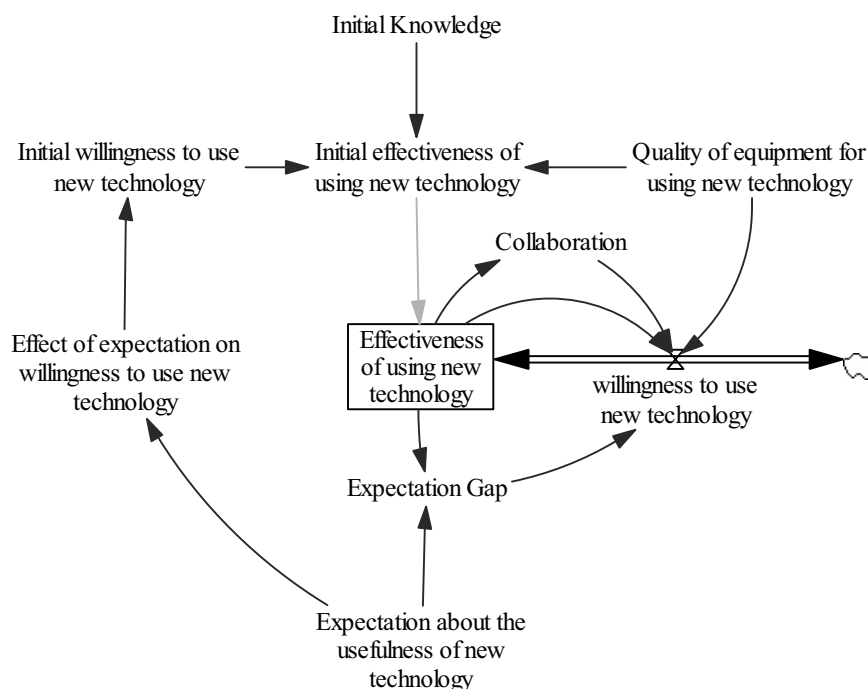


Figure 9-4 Expectation has an impact on the effectiveness of using new technology

We formed our theory about the expectation gap, as shown in Figure 9-4. We were not able to further contact Hydro for a validation of this theory. If validated, this theory could also be included in the Brage model to investigate how different expectation levels affect the operation transition.

9.4.3 Link to the risk matrix developed by IRMA

In the current Brage model, the severity of incidents and frequency of incidents are both highly aggregated: They are the average for all kinds of incidents. In this way, we observe the general trend of how, on average, the information security indicators develop over time. But we are not able delve into various types of incidents.

The IRMA team developed a risk matrix for the Brage platform, presenting the frequency and severity of various kinds of incidents. It is possible to incorporate the IRMA's risk matrix into our model and to disaggregate the average frequency and severity of incidents using the data in the risk matrix. By doing so, we may see the trend in the development of each type of incidents.

For example, if we disaggregate the incidents into five types, say “Terror attacks”, “DOS attacks”, “Illegal insider activities”, “Viruses” and “Human errors”. Then we will have the frequency and severity incidents for each category. The cost of each type of incidents could be calculated as the product of the frequency and severity of this type of incidents. And the total incident cost is the sum of incident cost of the five types of incidents (see Figure 9-5).

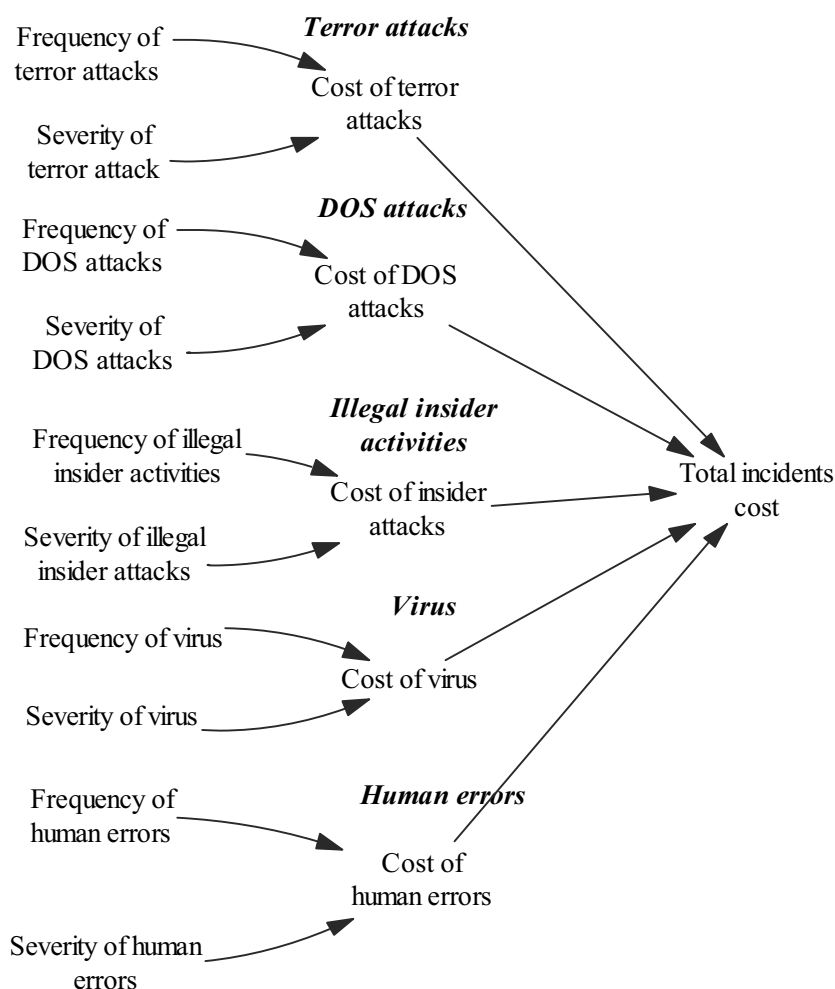


Figure 9-5 Link risk matrix in the Brage model

Operation transition affects various types of incidents differently. For example, it will definitely have a major impact on the frequency of human errors, but it will not have such an impact on the frequency of terrorist attacks. With these detailed data for different kinds of incidents, the model simulation can, then, show how the risk matrix will change over time. For example, the forecasted risk matrix in 2010 and 2015 could be as following:

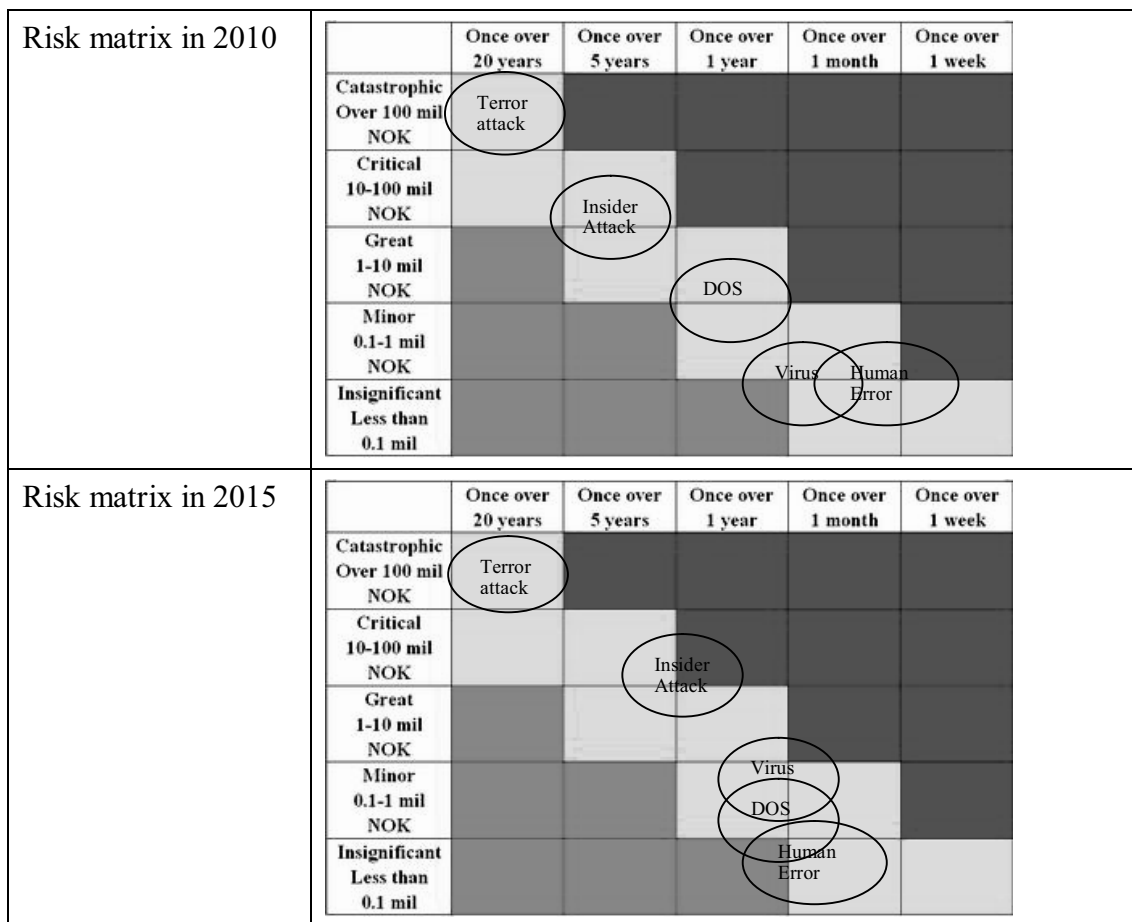


Figure 9-6 Sample future risk matrix

Such a forecast will help the management for their decision-making on what kind of investment is needed for in information security.

However, the difficulty of linking current risk matrix into the model is associated with in several factors. First, until now, there is no widely accepted classification of incidents. It is very difficult, if not impossible, to form a complete and exclusive list of incidents. For example, some terror attacks also utilize insiders. Many really successful attacks are the result of the collaboration of outsiders and insiders. Another example, some viruses are intentionally planted into the client ICT system, while others are spread around unintentionally and resulting from human error. Sometimes, it is difficult to identify to which category an incident belongs. Second, the current risk matrix for Brage is based on the historical data about incidents that have occurred on Brage. Incidents that have not occurred are not presented in the risk matrix. Such a risk matrix is not a complete representation of information security risks. Forecasts based on such risk matrix could be misleading. A maturation of the risk matrix is the pre-requirement for linking it into the Brage model.

9.5 Closing remarks for chapter 9

This chapter revisits the model-building process and the model insights. The model-building process is a two-way communication centered on system dynamics modeling, including group model-building workshops, model-development meetings and interview, and the model validation interview. The two-way communication process helped us gather qualitative information and quantitative data for model development. It also helped our client understand the current problem and the system structure causing the problem. Through this two-way communication process, we have built consensus with client, which facilitated our model development and our client's model apprehension.

The work contributes to helping our client to clarify the problems it is facing and providing a vehicle (the validated system dynamics model) for policy investigation. To the information security field, this research addresses the issue (the change of information security risks during operation transition) that has never been address by modeling method. This study introduces a dynamic view with the long-term perspective on information security management and illustrates how formal modeling and simulation could enhance our theory building on the dynamics of information security management. This work also contributes to system dynamics field in the accumulation of experience in model-based interventions.

In this chapter, we also critically reflect our communication with client. Several issues, from the selection of meeting place to the communication channels utilized, have been discussed where improvement could be made to obtain better results in future research. Finally, we pointed out three directions for future research efforts.

Reference

- Allen, Julia. 2005. *Governing for Enterprise Security*: Software Engineering Institute.
- Andersen, David, Dawn Cappelli, Jose J. Gonzalez, Mohammad Mojtahedzadeh, Andrew Moore, Eliot Rich, Jose Maria Sarriegui, Timothy J. Shimeall, Jeffrey M. Stanton, Elise Weaver, and Aldo Zagonel. 2004. Maps of the Insider Cyber-threat Problem. Paper read at The 22nd International Conference of the System Dynamics Society, at Oxford, UK.
- Andersen, David, and George Richardson. 1997. Scripts for group model building. *System Dynamics Review* 13 (2):107-129.
- Andersen, David, George Richardson, and Jac. A. M. Vennix. 1997. Group model building: Adding more science to the craft. *System Dynamics Review* 13 (2):187-201.
- Andersen, David, Nancy H. Roberts, Ralph M. Deal, Michael S.Garet, William A. Shaffer, Tanette Nguyen, and Marian N. Steinberg. 1983. An Introductory Curriculum in System Dynamics. *Dynamica* 8 (2).
- Andersen, David., Jac. A. M. Vennix, George Richardson, and Etienne A. J. A. Rouwette. 2007. Group Model Building: Problem Structuring, Policy Simulation and Decision Support. *Journal of Operational Research Society* 58 (5):691-694.
- Andersen, Ross, and Tyler Moore. 2006. The Economics of Information Security. *Science* 314 (5799):610-613.
- Anderson, Ross. 2001. Why Information Security is Hard—An Economic Perspective. Paper read at 17th Annual Computer Security Applications Conference.
- Arce, Iván. 2003. The weakest link revisited. *Security & Privacy, IEEE* 1 (2):72-76.
- Askildsen, Annette-Helen. 2004. Remote Control and Co-operation of Offshore Installations Department of Industrial Economics and Technology Management, NTNU, Trondheim.
- Attewell, Paul. 1992. Technology Diffusion and Organizational Learning: The Case of Business Computing. *Organization Science* 3 (1):1-19.
- August, Terrence, and Tunay I. Tunca. 2008. Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions. *Information Systems Research* 19 (1):48-70.
- Barlas, Yaman. 1989. Tests of Model Behavior that Can Detect Structural Flaws: Demonstration with Simulation Experiments. Paper read at Computer-Based Management of Complex Systems: International System Dynamics Conference, at Stuttgart.
- . 1996. Formal Aspects of Model Validity and Validation in System Dynamics. *System Dynamics Review* 12 (3):1-28.
- Barlas, Yaman , and Korhan Kanar. 2000. Structure-Oriented Behavior Tests in Model Validation. Paper read at 18th International Conference of the System Dynamics Society, August 6-10, at Bergen, Norway.

- Brown, John Seely , and Paul Duguid. 1991. Organizational Learning and Communities of Practice: Toward a Unified View of Working, Learning, and Innovation. *ORGANIZATION SCIENCE* 2 (1):40-57.
- Brown, John Seely, and Paul Duguid. 2001. Knowledge and Organization: A Social-Practice Perspective. *Organization Science* 12 (2):198-213.
- Burnes, Bernard. 2003. Managing change and changing managers from ABC to XYZ. *Journal of Management Development; Volume: 22; Issue: 7; 2003* 22 (7):627-642.
- Cappelli, Dawn M., and Andrew P. Moore. 2008. Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks: CERT Program – Software Engineering Institute Carnegie Mellon University.
- Caralli, Richard A. , and William R. Wilson. 2004. The Challenges of Security Management: Carnegie Mellon University Software Engineering Institute.
- Caralli, Richard A., James F. Stevens, Lisa R. Young, and William R. Wilson. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process: Carnegie Mellon Cert Program.
- Chuvakin, Anton. 2006. Five mistakes of vulnerability management.
- Clarke, Lee, and James F Jr. Short. 1993. Social Organization and Risk: Some Current Controversies. *Annual Review of Sociology* 19:375-399.
- Davis, Jason P., Kathleen M. Eisenhardt, and Christopher B. Bingham. 2007. Developing Theory Through Simulation Methods. *Academy of Management Review* 32 (2):480-499.
- Facts: The Norwegian Petroleum Sector. 2005. edited by T. Larstad and Ø. Dretvik. Oslo, Norway: Ministry of Petroleum and Energy Norwegian Petroleum Directorate.
- Facts: The Norwegian Petroleum Sector. 2007. Oslo, Norway: Ministry of Petroleum and Energy Norwegian Petroleum Directorate.
- Fang, Yulin, and Kai H. Lim. 2009. System Dynamics Modeling – The Case of E-commerce Resource Endowment and Sustainable Performance in a Click-and-Mortar Firm.
- Fichman, Robert. G. 2001. The role of aggregation in the measurement of IT-related organizational innovation. *MIS Quarterly* 25 (4):427-456.
- Forrester, Jay Wright. 1961. *Industrial Dynamics*. Cambridge MA: Productivity Press.
- . 1992. Policies, Decisions and Information Sources for Modeling. *European Journal of Operational Research* 59 (1):42-63.
- Forrester, Jay Wright, and Peter Senge. 1980. Tests for building confidence in system dynamics models. *TIMS Studies in the Management Sciences* 14:209.
- Gifford, Eric Allan. 1998. Hectronic information security. *Potentials, IEEE* 7 (4):26-30.
- Gonzalez, Jose J, and Agata Sawicka. 2002. A Framework for Human Factors in Information Security. Paper read at WSEAS International Conference on Information Security (ICIS'02), at Rio de Janeiro, Brazil.

- Gonzalez, Jose J., Ying Qian, Finn Olav Sveen, and Eliot Rich. 2005. Helping Prevent Information Security Risks in the Transition to Integrated Operations. *Teletronikk*:29-37.
- Gonzalez, Jose J., and Agata Sawicka. 2003. The Role of Learning and Risk Perception in Compliance. In *From Modeling to Managing Security: A System Dynamics Approach*, edited by J. J. Gonzalez. Kristiansand, Norway: Norwegian Academic Press.
- Grcic, Branko, and Ante Munitic. 1996. System Dynamics Approach to Validation. Paper read at 1996 International System Dynamics Conference, at Cambridge, Massachusetts.
- Gutmann, Peter. 2008. Security Usability.
- Hopkins, Andrew. 2008. *Failure to Learn: the BP Texas City Refinery Disaster*. Sydney: CCH Australia Limited.
- Integrated Work Processes: Future work processes on the Norwegian Continental Shelf. 2005. Norwegian oil industry association (OLF).
- Jaatun, Martin Gilje, Stig Johnsen, Maria B. Line, Odd Helge Longva, Inger Anne Taondel, Eirik Albrechtsen, and Irene Waerao. 2007. Incident Response Management in the oil and gas industry. Thronheim, Norway: SINTEF.
- Johnsen, Stig, Maria. B. Line, and Annette-Helen Askildsen. 2006. Towards more secure virtual organizations by implementing a common scheme for incident response management. Paper read at Eight International Conference on Probabilistic Safety Assessment and Management (PSAM8), at New Orleans, US.
- Lee, Sangjae, and Kyoung-jae Kim. 2007. Factors Affecting the Implementation Success of Internet-based Information System. *Computers in Human Behavior* 23 (4):1853-1880.
- Line, Maria B., Eirik Albrechtsen, Martin Gilje Jaatun, Inger A. Toondel, Stig Johnsen, Odd Helge Longva, and Irene Waerao. 2007. A Structured Approach to Incident Response Management in the Oil and Gas Industry.
- Lipson, Howard F. 2002. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. In *Special Report CMU/SEI-2002-SR-009*. Pittsburgh, PA, USA.
- Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. 1992. Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly* 16 (2):173-186.
- Luna-Reyes, Luis Felipe, and Deborah Lines Andersen. 2003. Collecting and Analyzing Qualitative Data for System Dynamics: Methods and Models. *System Dynamics Review* 19 (4):271-296.
- Luna-Reyes, Luis Felipe., Ignacio J. Martinez-Moyano, Theresa A. Pardo, Anthony M. Cresswell, David F. Andersen, and George P. Richardson. 2006. Anatomy of a group model-building intervention: building dynamic theory from case study research. *System Dynamics Review* 22:291-320.
- NIST. 2006. Glossary of Key Information Security Terms, edited by R. Kissel: National Institute of Standards and Technology.

- Peltier, Thomas R. 2005. *Information Security Risk Analysis (second edition)*. FL: Auerbach Publications.
- Protecting What Matters: The 6th Annual Global Security Survey. 2008.
- Qian, Ying, Yulin Fang, Eliot Rich, Martin Gilje Jaatun, and Stig. O. Johnsen. 2009. Managing emerging information security risks during transitions to Integrated Operations. Paper read at The Hawaii International Conference on System Sciences, at Hawaii, USA.
- Qian, Ying, and Jose J. Gonzalez. 2006. Adapting Group Model Building Methods to Improve Information Security Data. Paper read at 24th International Conference of the System Dynamics Society, at Nijmegen, The Netherlands.
- Qian, Ying, Jose J. Gonzalez, and Finn Olav Sveen. 2005. Defining Complex Problems Using Group Model Building and System Archetypes. Paper read at The Multi-Conference on the Application of System Dynamics and the Disciplines of Management, at Shanghai, China.
- Randers, Jergen. 1980. Guidelines for Model Conceptualization. In *Elements of the System Dynamics Method*, edited by J. Randers. Cambridge MA: Productivity Press.
- Rasmussen, Jens. 1982. Human Errors. A taxonomy for Describing Human Malfunction in Industrial Installations. *Journal of Occupational Accidents* 4:311-333.
- . 1987. Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models. *IEEE Transactions on Systems, Man, and Cybernetics* 13 (3):291 - 300.
- Reason, James, Dianne Parker, and Rebecca Lawton. 1998. Organizational controls and safety: The varieties of rule-related behaviour. *Journal of Occupational and Organizational Psychology* 71:289-304.
- Repenning, Nelson P. 1999. A Simulaton-based Approach to Understanding the Dynamics of Innovation Implementation. Cambridge, Massachusetts.
- Repenning, Nelson P., and John D. Sterman. 2001. Nobody Ever Gets Credit for Fixing Problems that Never Happened: Creating and Sustaining Process Improvement. *California Management Review* 43 (3):64-88.
- Rich, Eliot. 2002. Modeling the Dynamics of Organizational Knowledge School of Information Science and Policy, University at Albany, Albany, NY.
- Rich, Eliot, David Andersen, and George Richardson. 2005. OLF-IRMA-AMBASEC Group Model Building Technical Report I 25-26 May 2005. New York: University at Albany.
- . 2005. OLF-IRMA-AMBASEC Group Model Building Technical Report II 7-8 September 2005. New York: University at Albany.
- Rich, Eliot, Ignacio J. Martinez-Moyano, Stephen Conrad, Dawn M. Cappelli, Andrew P. Moore, Timothy J. Shimeall, David. F. Andersen, Jose J. Gonzalez, Robert J. Ellison, Howard F. Lipson, David Mundie, Jose Maria Sarriegui, Agata Sawicka, Thomas R. Stewart, Jose Manuel Torres, Elise A. Weaver, and Johannes Wiik. 2005. Simulating Insider Cyber-Threat Risks: A

- Model-Based Case and a Case-Based Model. Paper read at The 21st International Conference of System Dynamics Society, at New York.
- Rich, Eliot, Finn Olav Sveen, Ying Qian, Stefanie Hillen, Jaziar Radianti, and Jose J. Gonzalez. 2007. Emergent Vulnerability in Integrated Operations: A Proactive Simulation Study of Risk and Organizational Learning. Paper read at The 40th Hawaii International Conference on System Sciences, at Hawaii, U.S.A.
- Richardson, George, and David Andersen. 1995. Teamwork in Group Model-Building. *System Dynamics Review* 11 (2):113-137.
- Richardson, George, David Andersen, and Luis Felipe Luna-Reyes. 2005. Join Minds: Group modeling to link people, process, analysis, and policy design.
- Roberts, Nancy H., David Andersen, Ralph M. Deal, Michael S. Grant, and William A. Shaffer. 1981. *Introduction to Computer Simulation*. Waltham, MA: Pegasus Communications.
- Ryan, Julie J.C.H., and Daniel J. Ryan. 2008. Performance Metrics for Information Security Risk Management. *Security & Privacy, IEEE* 6 (5):38-44.
- Sawicka, Agata. 2004. Dynamics of Security Compliance: Case of IT-based Work Environment, Department of Information Science and Media Studies, University of Bergen, Bergen.
- Schneier, Bruce. 2000. *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley Computer Publishing, John Wiley & Sons, Inc.
- . 2008. Why Computer Security is Fundamentally an Economic Problem. In *Schneier on Security*. Indianapolis: Wiley.
- Schou, Corey, and Dan Shoemaker. 2007. *Information Assurance for the Enterprise: A Roadmap to Information Security*. New York: McGraw-Hill/Irwin.
- Siponen, Mikko T. 2005. An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. *European Journal of Information Systems* 14:303-315.
- Stephenson, Peter. 2004. Risk and Incident Management - Getting Started. *Computer Fraud & Security* (11):17-19.
- Sterman, John D. 2000. *Business Dynamics : Systems Thinking and Modeling for a Complex World*. Boston: Irwin/McGraw-Hill.
- . 2001. System Dynamics Modeling: Tools for Learning in a Complex World. *California Management Review* 43 (4):8-25.
- . 2002. All Models are Wrong: Reflections on Becoming a Systems Scientist. *System Dynamics Review* 18:501-531.
- Stoneburner, Gary, Alice Goguen, and Alexis Feringa. 2002. Risk Management Guide for Information Technology Systems: National Institute of Standards and Technology.
- Vennix, Jac A. M. 1996. *Group model building : facilitating team learning using system dynamics*. Chichester ; New York: J. Wiley.
- Vennix, Jac. A. M. 1999. Group model-building: tackling messy problems. *System Dynamics Review* 15 (4):379-401.

- Vennix, Jac. A. M., David Andersen, and George Richardson. 1997. Group model building, art, and science - Foreword. *System Dynamics Review* 13 (2):103-106.
- Wang, Jingguo, Aby Chaudhury, and Raghav H. Rao. 2008. A Value-at-Risk Approach to Information Security Investment. *Information Systems Research* 19 (1):106-120.
- Wantanakorn, D., M. J. Mawdesley, and W. H. Askew. 1999. Management errors in construction. *Engineering, Construction and Architectural Management* 6 (2):112-120.
- Werlinger, Rodrigo, Kirstie Hawkey, and Konstantin Beznosov. 2009. An Integrated View of Human, Organizational, and Technological Challenges of IT Security Management. *Information Management & Computer Security* 17 (1).
- West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, and Mark Zajicek. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs). Pittsburgh: Carnegie Mellon Software Engineering Institute.
- Winch, Graham W. 1997. The Dynamics of Process Technology Adoption and the Implications for Upgrade Decisions. *Technology Analysis & Strategic Management* 9 (3):317-328.
- Wolstenholme, Eric F. 2004. Using Generic System Archetypes to support thinking and modeling. *System Dynamics Review* 20 (4):341-356.
- Wolstenholme, Eric. F. 2003. Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review* 19 (1):7-26.

Appendix

Appendix I Model Equations

NB: This format of this document is:

```
*****
.Section name
*****
```

Equation: variable name = formula or value

- ~ Unit of the variable
- ~ Definition of the variable

```
*****
.Work processes
*****
```

maturing new work processes = Immature new work processes / Time to mature new work processes * Effect of new initiatives burden on maturing new WP * Effect of mature new WP on maturing new WP * Effect of resources on maturing new work processes

- ~ processes/Month
- ~ The new work processes matured in a month

Fraction of changed work processes = Fraction of immature work processes + Fraction of mature new work processes

- ~ Dmnl
- ~ Fraction of work processes that are new, no matter mature or immature

Operator resources available for maturing new WP and knowledge = Total operator resources - Minimum operator resources for production

- ~ fraction of working time
- ~ The percentage of operators' time available for maturing new work processes. It depends on how much time is reserved for production.

Operator resources to mature new WP = min(Operator resources required to mature new WP, Operator resources available for maturing new WP and knowledge)

- ~ fraction of working time
- ~ The percentage of time devoted to mature new work processes

Effect of resources on maturing new work processes = $0.1 + 0.9 * (\text{Operator resources to mature new WP} / \text{Operator resources required to mature new WP})$

~ Dmnl

~ The effect of resource adequacy on new work processes maturation

Effect of incident cost on transition to IO = WITH LOOKUP (Expected incident cost/Initial average incident cost, $([(0,0)-(20,10)],(0,1),(20,1))$)

~ Dmnl

~ There is a possible policy that when the incident cost is high, the management might reduce the operation transition speed. This variable reflects the policy. It is set to 1 in the base model. And it will be assigned with different value when to test the policy.

Initial average incident cost = 83346

~ NOK/Month

~ Average incident cost (per month) at the beginning of operation transition.

Effect of new initiatives burden on maturing new WP = WITH LOOKUP (New initiatives burden,

$([(0,0)-(1,1)],(0,1),(0.1,0.97),(0.18,0.9),(0.27,0.72),(0.37,0.57),(0.5,0.43),(0.7,0.35),(1,0.3))$)

~ Dmnl

~ New initiatives burden hinders people from maturing new work process. This variable ranges from 0.3 to 1. When there is no new initiatives burden, the new work processes will be matured at full speed. When everything in the system is new, new initiatives burden reach 1, the speed of maturing new work processes will be reduced to 0.3.

Effect of mature new WP on maturing new WP = WITH LOOKUP (Fraction of mature new work processes,

$([(0,0)-(1,1)],(0,0.5),(0.05,0.62),(0.1,0.72),(0.25,0.86),(0.5,0.96),(0.8,1),(1,1))$)

~ Dmnl

~ Mature new work processes represent experience for maturing new work processes. When more experience accumulate, as more new work processes are matured, it will facilitate the further maturation of new work processes. This variable ranges from 0.5 to 1. When no experience, the effectiveness of new work processes maturation is only 50% of maximum effectiveness. It increases as new work processes are matured and when 80% of the work processes have been matured, people are so experienced that they mature new work processes at maximum effectiveness.

Effectiveness of resources in developing new work processes = Normal effectiveness of resources in developing new work processes*Effect of traditional WP on new WP

development * Effect of changed WP on new WP development * Effect of new initiatives burden on new WP development

- ~ processes/hour
- ~ The productivity of work processes development

Minimum operator resources for production = 0.9

- ~ fraction of working time
- ~ The minimum percentage of operators' time reserved for production

Effect of changed WP on new WP development = WITH LOOKUP (Fraction of changed work processes,

([(0,0)-(1,1)],(0,0.5),(0.05,0.62),(0.1,0.72),(0.25,0.86),(0.5,0.96),(0.8,1),(1,1)))

- ~ Dmnl
- ~ New work processes represent experience for developing new work processes. When more experience accumulate, as more new work processes are developed, it will facilitate the further development of new work processes. This variable ranges from 0.5 to 1. When no experience, the effectiveness of new work processes development is only 50% of maximum effectiveness. It increases as new work processes are developed and when 80% of the work processes have been developed, people are so experienced that they develop new work processes at maximum effectiveness.

Effect of new initiatives burden on new WP development = WITH LOOKUP (New initiatives burden, [(0,0)-(1,1)], (0,1), (0.1,0.97), (0.25,0.87), (0.3,0.78), (0.4,0.65), (0.5,0.57), (0.6,0.53), (1,0.5)))

- ~ Dmnl
- ~ Seeing much burden in the system holds people back from developing new work processes. This variable ranges from 0.5 to 1. When there is no new initiatives burden, the new work processes will be developed at full speed. When everything in the system is new, new initiatives burden reach 1, the speed of developing new work processes will be reduced to 0.5.

Management time to develop new work processes = WITH LOOKUP (Time, [(0,0)-(200,120)], (0,100), (12,100), (13,34), (120,34)))

- ~ hour/Month
- ~ Management personnel's time devoted to develop new work processes\!\!

Effect of traditional WP on new WP development = WITH LOOKUP (Fraction of traditional WP, [(0,0)-(1,1)], (0,0), (0.015,0.24), (0.045,0.47), (0.14,0.71), (0.27,0.83), (0.422018,0.92), (0.55,0.96), (0.8,1), (1,1)))

- ~ Dmnl
- ~ Traditional work processes offer potential for developing new work processes. When this potential decrease, as the traditional work processes developing into new work processes, it will make the further developing of new work processes

more difficult. This variable ranges from 0 to 1. When all the work processes are traditional, it is 1. When there is no traditional work processes, it becomes 0.

Fraction of traditional WP = Traditional work processes/Total work processes in place

- ~ Dmnl
- ~ Fraction of work processes that are traditional.

Normal effectiveness of resources in developing new work processes = 0.006

- ~ processes/hour
- ~ The maximum amount of processes a person could develop in an hour.

Operator resources required to mature new WP = Operator resources for maturing each WP*(Immature new work processes)

- ~ fraction of working time
- ~ The amount of resources required to mature all the new work processes in the system

Operator resources for maturing each WP = 0.04

- ~ fraction of working time/processes
- ~ Percentage of operators' time needed to mature one work process

Time to mature new work processes = 4

- ~ Month
- ~ Time needed to mature one new work process given enough resources

Fraction of mature new work processes = Mature new work processes/Total work processes in place

- ~ Dmnl
- ~ Fraction of work processes that are matured new work processes

developing new work processes = Management time to develop new work processes * Effectiveness of resources in developing new work processes * Effect of incident cost on transition to IO

- ~ processes/Month
- ~ The new work processes developed in a month

New initiatives burden = (Fraction of immature knowledge*wt on new knowledge burden + Fraction of immature work processes * wt on new work process burden)/(wt on new knowledge burden + wt on new work process burden)

- ~ Dmnl
- ~ Immature new work processes and immature new knowledge are burden to people in the sense of handling changes in what to do, how to do, who to contact and in our case, also how to contact.

Total work processes in place = Immature new work processes + Mature new work processes + Traditional work processes

- ~ processes
- ~ Total work processes on the platform

Fraction of immature work processes = Immature new work processes / Total work processes in place

- ~ Dmnl
- ~ Fraction of work processes that are immature new

Mature new work processes = INTEG (maturing new work processes, 0)

- ~ processes
- ~ Mature new work processes are those new work processes that operators could work unassisted.

Immature new work processes = INTEG (developing new work processes-maturing new work processes, 0)

- ~ processes
- ~ Immature new work processes are those newly implemented work processes. Operators still need management guidance to work with them.

Traditional work processes = INTEG (-developing new work processes, 20)

- ~ processes
- ~ Traditional work processes are those work processes that need to be changed during the operation transition.

wt on new knowledge burden = 1

- ~ Dmnl
- ~ The weight of new knowledge burden on the total new initiatives burden

wt on new work process burden = 1

- ~ Dmnl
- ~ The weight of new work process burden on the total new initiatives burden

.Knowledge

*****~

maturing new knowledge = Immature new knowledge/Time to mature new knowledge*Effect of resources on maturing new knowledge * Effect of new initiatives burden on maturing new knowledge * Effect of mature knowledge on maturing new knowledge

- ~ knowledge/Month
- ~ The new knowledge matured in a month

Effect of resources on maturing new knowledge = $0.1+0.9*(\text{Operator resources to mature new knowledge}/\text{Operator resources required to mature new knowledge})$

- ~ Dmnl
- ~ The effect of resource adequacy on new knowledge maturation

Operator resources available for maturing new knowledge = Total operator resources - Minimum operator resources for production - Operator resources to mature new WP

- ~ fraction of working time
- ~ The percentage of time available to mature new knowledge

Effect of mature knowledge on maturing new knowledge = WITH LOOKUP

(Fraction of mature new knowledge,

$[(0,0)-(1,1)],(0,0.5),(0.05,0.62),(0.1,0.72),(0.25,0.86),(0.5,0.96),(0.8,1),(1,1))$)

- ~ Dmnl
- ~ Mature new knowledge represents experience for maturing new knowledge. When more experience accumulate, as more new knowledge is matured, it will facilitate the further maturation of new knowledge. This variable ranges from 0.5 to 1. When no experience, the effectiveness of new knowledge maturation is only 50% of maximum effectiveness. It increases as new knowledge is matured and when 80% of the knowledge has been matured, people are so experienced that they mature new knowledge at maximum effectiveness.

Effect of new initiatives burden on maturing new knowledge = WITH LOOKUP

(New initiatives burden, $[(0,0)-(1,1)], (0,1), (0.1,0.97), (0.18,0.9), (0.27,0.72),$

$(0.37,0.57), (0.5,0.43), (0.7, 0.35), (1,0.3))$)

- ~ Dmnl
- ~ New initiatives burden hinders people from maturing new knowledge. This variable ranges from 0.3 to 1. When there is no new initiatives burden, the new knowledge will be matured at full speed. When everything in the system is new, new initiatives burden reach 1, the speed of maturing new knowledge will be reduced to 0.3.

Operator resources required to mature new knowledge = Operator resources for maturing each knowledge unit * Immature new knowledge

- ~ fraction of working time

Normal effectiveness of resources in developing new knowledge = 0.006

- ~ knowledge/hour
- ~ The average amount of knowledge a person could develop in an hour under normal condition

Effect of new initiatives burden on new knowledge development = WITH LOOKUP
 (New initiatives burden, $[(0,0)-(1,1)]$, (0,1), (0.1,0.97), (0.25,0.87), (0.3,0.78),
 (0.4,0.65), (0.5,0.57), (0.6,0.53), (1,0.5))

~ Dmnl

~ Seeing much burden in the system holds people back from developing new work processes and knowledge. This variable ranges from 0.5 to 1. When there is no new initiatives burden, the new knowledge will be developed at full speed. When everything in the system is new, new initiatives burden reach 1, the speed of developing new knowledge will be reduced to 0.5.

Effect of changed knowledge on new knowledge development = WITH LOOKUP
 (Fraction of changed knowledge, $[(0,0)-(1,1)]$, (0,0.5), (0.05,0.62), (0.1,0.72),
 (0.25,0.86), (0.5,0.96), (0.8,1), (1,1))

~ Dmnl

~ New knowledge represents experience for developing new knowledge. When more experience accumulate, as more new knowledge is developed, it will facilitate the further development of new knowledge. This variable ranges from 0.5 to 1. Without any experience, the effectiveness of new knowledge development is only 50% of maximum effectiveness. It increases as new knowledge is developed and when 80% of the knowledge has been developed, people are so experienced that they develop new knowledge at maximum effectiveness.

Effect of traditional knowledge on new knowledge development= WITH LOOKUP (Fraction of traditional knowledge, $[(0,0)-(1,1)]$, $[(0,0)-(1,1)]$, (0,0), (0.015,0.24),
 (0.045,0.47), (0.14,0.71), (0.27,0.83), (0.422018,0.92), (0.55,0.96), (0.8,1), (1,1)))

~ Dmnl

~ Traditional knowledge offers potential for developing new knowledge. When this potential decreases, as the traditional knowledge developing into new knowledge, it will make the further developing of new knowledge more difficult. This variable ranges from 0 to 1. When all the knowledge is traditional, it is 1. When there is no traditional knowledge, it becomes 0.

Fraction of changed knowledge = Fraction of immature knowledge + Fraction of mature new knowledge

~ Dmnl

~ Fraction of knowledge that is new, no matter mature or immature

Effectiveness of resources in developing new knowledge = Normal effectiveness of resources in developing new knowledge * Effect of new initiatives burden on new knowledge development * Effect of changed knowledge on new knowledge development * Effect of traditional knowledge on new knowledge development

~ knowledge/hour

~ The productivity of new knowledge development

Management time to develop new knowledge = WITH LOOKUP (Time,
 ((0,0)-(200,100)], (0,100), (12,100), (13,34), (120,34)))

- ~ hour/Month
- ~ Personnel's time devoted to develop new knowledge

Fraction of traditional knowledge = Traditional knowledge / Total knowledge in place

- ~ Dmnl
- ~ Fraction of knowledge that is traditional.

Operator resources for maturing each knowledge unit = 0.04

- ~ fraction of working time/knowledge
- ~ Percentage of operators' time needed to mature one set of knowledge

Time to mature new knowledge = 8

- ~ Month
- ~ Time needed to mature one new work process given enough resources

Operator resources to mature new knowledge = min (Operator resources available for
 maturing new knowledge, Operator resources required to mature new knowledge)

- ~ fraction of working time
- ~ The percentage of time devoted to mature new knowledge

developing new knowledge = Management time to develop new knowledge *

Effectiveness of resources in developing new knowledge * Effect of incident cost on
 transition to IO

- ~ knowledge/Month
- ~ The new knowledge developed in a month

Total knowledge in place = Immature new knowledge + Mature new knowledge +
 Traditional knowledge

- ~ knowledge
- ~ Total knowledge on the platform

Mature new knowledge = INTEG (maturing new knowledge, 0)

- ~ knowledge
- ~ Knowledge related to mature new work processes

Immature new knowledge = INTEG (developing new knowledge-maturing new
 knowledge, 0)

- ~ knowledge
- ~ Knowledge related immature new knowledge.

Traditional knowledge = INTEG (-developing new knowledge, 20)

- ~ knowledge
- ~ Knowledge that related to traditional work processes

Fraction of mature new knowledge = Mature new knowledge / Total knowledge in place

- ~ Dmnl
- ~ Fraction of knowledge that is mature new knowledge

Fraction of immature knowledge = Immature new knowledge / Total knowledge in place

- ~ Dmnl
- ~ Fraction of knowledge that is immature

.Vulnerability

*****~

New work processes = Fraction of changed knowledge * Total work processes in place

- ~ processes
- ~ Immature new work processes plus mature new work processes

Desired mature new knowledge = New work processes * Mature knowledge per work process

- ~ knowledge
- ~ Mature new knowledge required for the already mature new work processes

Knowledge gap = (Desired mature new knowledge - Mature new knowledge)

- ~ knowledge
- ~ The gap between the required mature new knowledge and the actual mature new knowledge

Mature knowledge per work process = 1

- ~ knowledge/processes
- ~ The knowledge required for each new work process

Effect of knowledge gap on Vulnerability Index = WITH LOOKUP (Knowledge gap, ((0,0)-(20,1)], (0,0.4), (20,0.8))

- ~ Dmnl
- ~ The effect of knowledge gap on vulnerability. When there is no knowledge gap, the 60% of the vulnerability will be reduced. When the knowledge gap is 20 (maximum), only 20% of the vulnerability will be reduced.

Effect of immature new WP on Vulnerability Index = WITH LOOKUP (Fraction of immature work processes, ((0,0)-(1,1)], (0,0.4), (0.05,0.47), (0.15,0.56), (0.26,0.63), (0.4,0.7), (0.6,0.77), (1,0.9)))

- ~ Dmnl
- ~ The effect of immature new work processes on vulnerability. When there is no immature new work processes, 60% of the vulnerability will be reduced. When the fraction of immature work processes reach 1, meaning all the new work processes are new, only 10% of the vulnerability will be reduced.

Effect of immature new knowledge on Vulnerability Index= WITH LOOKUP (Fraction of immature knowledge, ((0,0)-(1,1)], (0,0.4), (0.05,0.48), (0.13,0.56), (0.25,0.62), (0.4,0.67), (0.6,0.72),(1,0.8)))

- ~ Dmnl
- ~ The effect of immature new knowledge on vulnerability. When there is no immature new knowledge, 60% of the vulnerability will be reduced. When the fraction of immature work processes reach 1, meaning all the new knowledge is new, only 20% of the vulnerability will be reduced.

Maximum Vulnerability Index = 1

- ~ Dmnl
- ~ The theoretical maximum fraction of events turning into incidents, which is 100%.

Vulnerability Index = Maximum Vulnerability Index * Effect of knowledge gap on Vulnerability Index * Effect of immature new knowledge on Vulnerability Index * Effect of immature new WP on Vulnerability Index

- ~ Dmnl
- ~ The actually fraction of events that become incidents

.Incidents

*****~

Normal severity of incidents = 500000

- ~ NOK/incident
- ~ The average total cost of incident before the operation transition

Effect of new initiatives burden on severity of incidents= WITH LOOKUP (New initiatives burden, ((0,0.5)-(1,1.5)], (0,1), (0.1,1), (0.2,1.04), (0.3,1.1), (0.5,1.2), (0.6,1.24), (0.8,1.28), (1,1.3)))

- ~ Dmnl
- ~ The new initiatives burden hinders the incident response. It ranges from 1 to 1.3. When there is no new initiatives burden, the incident cost will be as

usual. When the new initiatives burden reaches 1, which means that everything in the model is new, the severity of incidents will increase 30%.

Frequency of events = Initial frequency of events * Effect of new work processes on events

- ~ event/Month
- ~ The average number of events happening every month

Effect of new work processes on events= WITH LOOKUP (Fraction of changed work processes, (((0,0)-(1,5)], (0,1), (0.05,1.4), (0.1,1.75), (0.2,2.1), (0.3,2.3), (1,3)))

- ~ Dmnl
- ~ As the operation transition goes on, it affects the threats the system face

Effect of adequacy of IR capability on severity of incidents= WITH LOOKUP (Incident response capability / Frequency of incidents, (((0,0)-(10,10)], (0.1,5), (0.2,3.5), (0.3,2.8), (0.6,1.5), (1,1), (2,0.8), (10,0.5))))

- ~ Dmnl
- ~ The adequacy of IR capability affects the severity of incidents. When it is very inadequate (0.1), the severity of incidents could be 5 times as high as normal severity of incidents. When it is very adequate (10), the severity of incidents could be reduced to 50% of normal severity of incidents.

Severity of incidents = Normal severity of incidents * Effect of resilience on severity * Effect of adequacy of IR capability on severity of incidents * Effect of new initiatives burden on severity of incidents

- ~ NOK/incident
- ~ Average total incident cost per month

Frequency of incidents = Vulnerability Index * Frequency of events

- ~ incident/Month
- ~ Average number of incidents happening every month

Expected incident cost = Frequency of incidents * Severity of incidents

- ~ NOK/Month
- ~ Average incident cost per month

Effect of resilience on severity = WITH LOOKUP ((wt on mature knowledge * Fraction of mature new knowledge + wt on mature WP * Fraction of mature new work processes) / (wt on mature knowledge + wt on mature WP), (((0,0.6)-(1,2)], (0,1), (0.098,0.99), (0.2,0.95), (0.3,0.9), (0.4,0.83), (0.5,0.78), (0.6,0.73), (0.8,0.71),(1,0.7)))

- ~ Dmnl
- ~ The effect of resilience on average severity of incidents. When resilience is 0, the severity of incidents will not be reduced. When the resilience is 1, meaning all

the new work processes and knowledge have been matured, the severity of incidents will be reduced to 70% of its original level.

Fraction of incidents detected = 0.4

- ~ Dmnl
- ~ The percentage of incidents that are detected

Frequency of detected incidents = Frequency of incidents * Fraction of incidents detected

- ~ incident/Month
- ~ How many detected incidents per month

Initial frequency of events = 2

- ~ event/Month
- ~ Information security threats before the transition to Integrated Operations

wt on mature knowledge = 1

- ~ Dmnl
- ~ Weight of mature knowledge on the system resilience

wt on mature WP = 1

- ~ Dmnl
- ~ Weight of mature work process on the system resilience

.Learning from incidents

*****~

Effect of severity on learning= WITH LOOKUP (Severity of incidents/Normal severity of incidents, ([[0,0)-(10,10)],(0,0),(1,1),(10,10)))

- ~ Dmnl
- ~ The effect of severity of incident on learning from incidents. The severe the incident is, the more people learn from it.

Learning per incident = Normal learning per incident * Effect of severity on learning

- ~ IR knowledge/incident
- ~ Incident response knowledge people learn from incident

learning from incidents = SMOOTH(Learning per incident*Incident detected, Time to learn from incidents)

- ~ IR knowledge/Month
- ~ Incident response knowledge people learn from incidents every month

Time to learn from incidents = 3

- ~ Month
- ~ Time needed from incidents happening to learn from incidents

Normal learning per incident = 1

- ~ IR knowledge/incident
- ~ Given normal condition, the amount of incident response knowledge people learn from one incident

.Incident Response Capability

change of perception = (Incident detected - Perception of frequency of incidents) /
Time to change perception

- ~ incident/(Month*Month)
- ~ Change of perception of frequency of incidents in a month

Adequacy of incident response capability = Incident response capability / Frequency
of incidents

- ~ Dmnl
- ~ The number of incidents handled over the number of incidents need to be handled.

Effect of adequacy of IR capability on incident detected = WITH LOOKUP
(Adequacy of incident response capability, ((0,0)-(1,1)], (0,0.2), (0.08,0.2), (0.2,0.3),
(0.3,0.45), (0.4,0.6), (0.5,0.74), (0.7,0.92), (0.8,0.97), (0.9,1), (1,1))

- ~ Dmnl
- ~ The effect of adequacy of IR capability on incident detected. When there is no IR capability, 20% of incidents will still be detected. When the IR capability is adequate, all the incidents will be detected.

Desired Incident Response Capability = Perception of frequency of incidents

- ~ incident/Month
- ~ The desired number of incidents that could be handled in a month

obsolete of IR capability = Incident response capability/Time to obsolete IR capability

- ~ incident/(Month*Month)
- ~ Decrease of incident response capability in a month

Time to obsolete IR capability = 12

- ~ Month
- ~ Average time for incident response capability to obsolete

Effect of learning from incidents on Incident response capability = learning from incidents / 100

- ~ 1/Month
- ~ The effect of learning from incidents on increasing incident response capability

Time to change perception = 3

- ~ Month
- ~ Time needed to change perception

Perception of frequency of incidents= INTEG (change of perception, 0.1246)

- ~ incident/Month
- ~ Management's perception of the amount of incident happening in a month

increase of IR capability = (Desired Incident Response Capability - Incident response capability) / Time to adjust IR capability

- ~ incident/(Month*Month)
- ~ Increase of incident response capability in a month

Incident detected = Frequency of incidents * Effect of adequacy of IR capability on incident detected

- ~ incident/Month
- ~ The amount of incident detect in a month

Incident response capability = INTEG (increase of IR capability - obsolete of IR capability + Effect of learning from incidents on Incident response capability * Incident response capability, 0.1)

- ~ incident/Month
- ~ The amount of incident could be handled in a month

Time to adjust IR capability = 3

- ~ Month
- ~ Time needed from making investment decision to incident response capability ready on board.

.Production and Profit

*****~

Revenue = Normal revenue * Fraction of resources for production * (1 + Effect of new work processes on productivity * Effect of knowledge adequacy on productivity)

- ~ NOK/Month
- ~ Monthly revenue from oil production

Effect of new work processes on cost reduction = WITH LOOKUP (Fraction of mature new work processes, $[(0,0)-(1,0.4)]$, (0,0), (0.08,0.01), (0.2,0.05), (0.3,0.1), (0.4,0.15), (0.5,0.2), (0.6,0.23), (0.8,0.27), (1,0.3))

~ Dmnl

~ The effect of mature new work processes on cost and expenditure for production. The Integrated Operations is expected to reduce cost and expenditure by 30%. It will gradually achieve this target as new work processes are implemented and matured

Effect of new work processes on productivity = WITH LOOKUP (Fraction of mature new work processes, $[(0,0)-(1,0.2)]$, (0,0), (0.09,0.035), (0.22,0.06), (0.42,0.083), (0.61,0.093), (1,0.1))

~ Dmnl

~ The effect of mature new work processes on productivity. The Integrated Operations is expected to increase productivity by 10%. It will gradually achieve this target as new work processes are implemented and matured

Cost for incident response capability = Average cost per incident response capability

* Incident response capability

~ NOK/Month

~ The amount of money used for having incident response capability. The amount mainly represents salary of the personnel.

Monthly Profit = Revenue - Product cost and expenditure - Expected incident cost - Cost for incident response capability

~ NOK/Month

~ Revenue minus product cost and expenditure minus cost of incident and cost for incident response capability

Average cost per incident response capability = 400000

~ NOK/incident

~ Average cost for having one incident response capability

Fraction of resources for production = Total operator resources - Operator resources to mature new WP - Operator resources to mature new knowledge

~ fraction of working time

~ The percentage of operators' time devoted to production

Effect of knowledge adequacy on cost reduction= WITH LOOKUP (Adequacy of mature new knowledge, $[(0,0)-(1,1)]$, (0,0), (0.05,0.18), (0.1,0.33), (0.2,0.55), (0.4,0.79), (0.55,0.87), (0.75,0.95), (1,1))

~ Dmnl

~ The effect of having enough knowledge on cost and expenditure of production

Adequacy of mature new knowledge = Mature new knowledge / Mature new work processes

- ~ knowledge/processes
- ~ Mature knowledge over mature new work processes

Effect of knowledge adequacy on productivity = WITH LOOKUP (Adequacy of mature new knowledge, ((0,0)-(1,1)], (0,0), (0.05,0.18), (0.1,0.33), (0.2,0.55), (0.4,0.79), (0.55,0.87), (0.75,0.95), (1,1))

- ~ Dmnl
- ~ The effect of having enough knowledge on productivity

Normal cost and expenditure = 2.6e+007

- ~ NOK/Month
- ~ Average monthly cost and expenditure related to oil production before the operation transition. Here the cost of incident and cost for incident response capability is not included

Product cost and expenditure = Normal cost and expenditure * (1-Effect of new work processes on cost reduction*Effect of knowledge adequacy on cost reduction)

- ~ NOK/Month
- ~ Monthly cost and expenditure related to oil production. Here the cost of incident and cost for incident response capability is not included

Total operator resources = 1

- ~ fraction of working time
- ~ Total percentage operators' time

Normal revenue = 3e+007

- ~ NOK/Month
- ~ Average Monthly revenue from oil production before the operation transition

.Control

*****~

Simulation Control Parameters

FINAL TIME = 120

- ~ Month
- ~ The final time for the simulation.

INITIAL TIME = 0

- ~ Month
- ~ The initial time for the simulation.

SAVEPER = 1

~ Month [0,?]

~ The frequency with which output is stored.

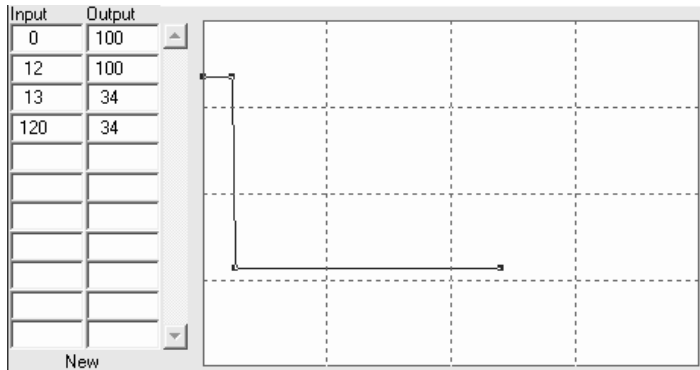
TIME STEP = 0.0625

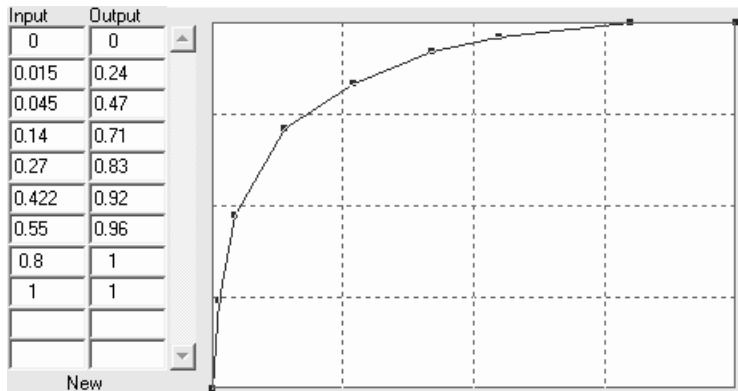
~ Month [0,?]

~ The time step for the simulation.

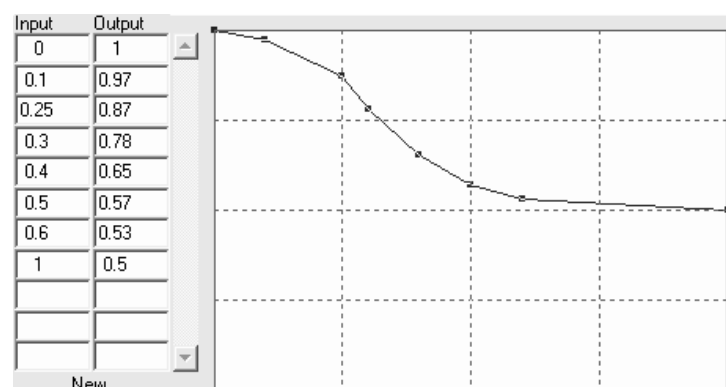
Appendix II List of look up functions

Work processes section:

<u>Management time to develop new work processes</u>		<u>Definition:</u> Management personnel's time devoted to develop new work processes
		<p><u>Base for this function:</u> This is a policy variable. The input for the base run is according the information from the Brage platform chief.</p>
<u>Range</u> >=0	<u>Reference point</u> None	<u>Shape</u> Irregular
		<u>Unit</u> hour/Month

<u>Effect of traditional WP on new WP development</u>		<u>Definition:</u> The effect of traditional work processes (as potential for developing new work processes) on the effectiveness of developing new work processes
		<p><u>Base for this function:</u> Estimated by modeler Agreed by client and model validation experts</p>
<u>Range</u> 0-1	<u>Reference point</u> (0,0), (1,1)	<u>Shape</u> Goal seeking
		<u>Unit</u> Dimensionless

Effect of new initiatives burden on new WP development



Definition: The effect of new initiatives burden (extra work load caused by the communication difficulty) on the effectiveness of developing new work processes

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-1

Reference point

(0,1)

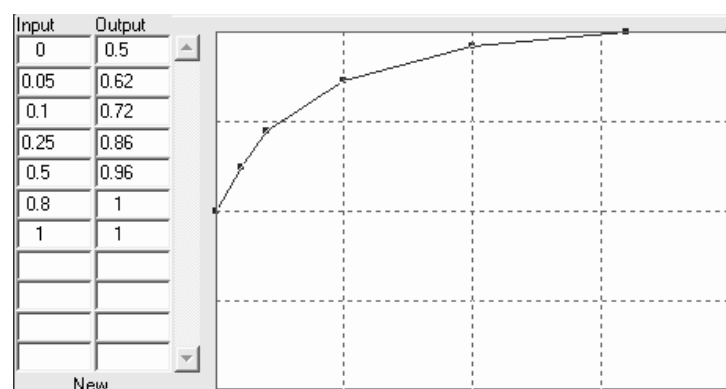
Shape

S-shape

Unit

Dimensionless

Effect of changed WP on new WP development



Definition: The effect of changed work processes (experience of developing new work processes) on the effectiveness of developing new work processes

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-1

Reference point

(1,1)

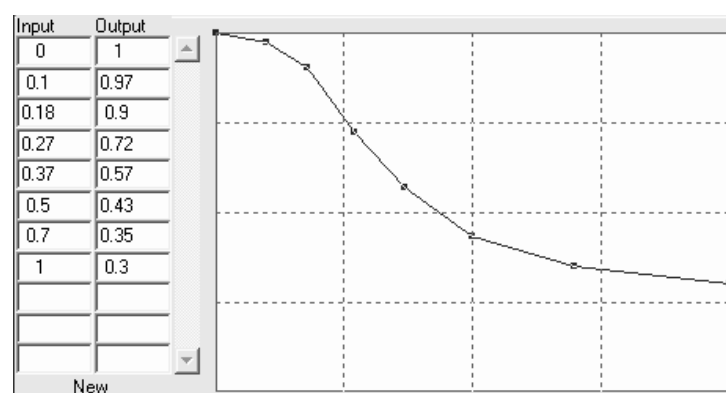
Shape

Goal seeking

Unit

Dimensionless

Effect of new initiatives burden on maturing new WP



Definition: The effect of new initiatives burden on the effectiveness of maturing new work processes

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-1

Reference point

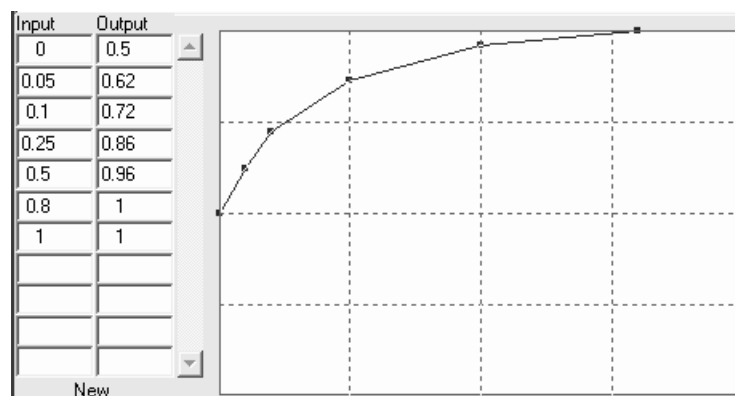
(0,1)

Shape

Goal seeking

Unit

Dimensionless

Effect of mature new WP on maturing new WP

Definition: The effect of mature new work processes (experience of new work processes maturation) on the effectiveness of maturing new work processes

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-1

Reference point

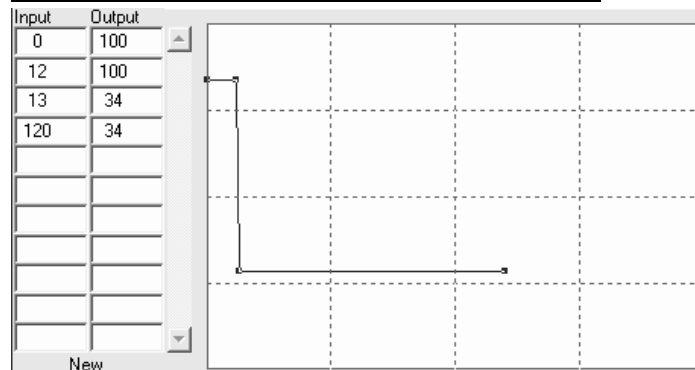
(0,1)

Shape

Goal seeking

Unit

Dimensionless

Knowledge section:**Management time to develop new knowledge**

Definition: Management personnel's time devoted to develop new knowledge

Base for this function:
This is a policy variable. The input for the base run is according to the information from the Brage platform chief.

Range ≥ 0 **Reference point**

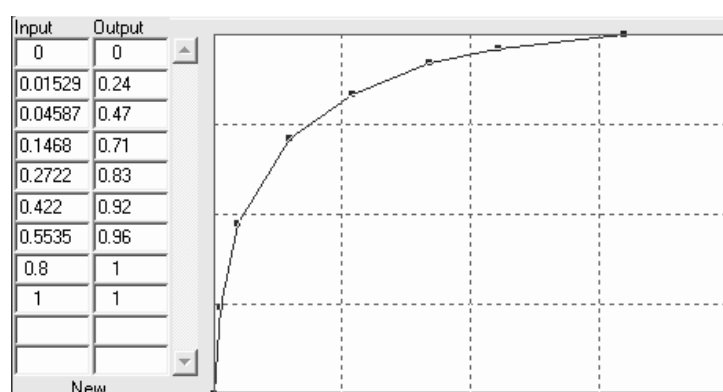
None

Shape

Irregular

Unit

hour/Month

Effect of traditional knowledge on new knowledge development

Definition: The effect of traditional knowledge (as potential for developing new knowledge) on the effectiveness of developing new knowledge

Base for this function:
Estimated by modeler
Agreed by client and model validation experts

Range

0-1

Reference point

(0,0), (1,1)

Shape

Goal seeking

Unit

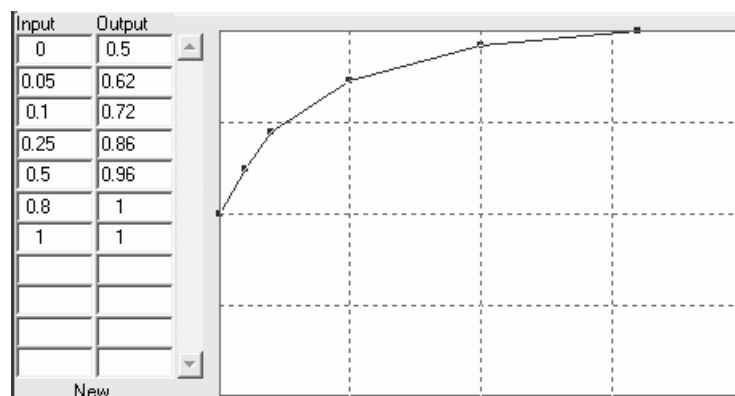
Dimensionless

<p><u>Effect of new initiatives burden on new knowledge development</u></p> <table border="1"> <thead> <tr> <th>Input</th> <th>Output</th> </tr> </thead> <tbody> <tr><td>0</td><td>1</td></tr> <tr><td>0.1</td><td>0.97</td></tr> <tr><td>0.25</td><td>0.87</td></tr> <tr><td>0.3</td><td>0.78</td></tr> <tr><td>0.4</td><td>0.65</td></tr> <tr><td>0.5</td><td>0.57</td></tr> <tr><td>0.6</td><td>0.53</td></tr> <tr><td>1</td><td>0.5</td></tr> </tbody> </table>		Input	Output	0	1	0.1	0.97	0.25	0.87	0.3	0.78	0.4	0.65	0.5	0.57	0.6	0.53	1	0.5	<p><u>Definition:</u> The effect of new initiatives burden (extra work load caused by the communication difficulty) on the effectiveness of developing new knowledge</p> <p><u>Base for this function:</u> Qualitatively suggested by client Estimated by modeler</p>
Input	Output																			
0	1																			
0.1	0.97																			
0.25	0.87																			
0.3	0.78																			
0.4	0.65																			
0.5	0.57																			
0.6	0.53																			
1	0.5																			
<p><u>Range</u> 0.5-1</p>	<p><u>Reference point</u> (0,1)</p>	<p><u>Shape</u> S-shape</p>	<p><u>Unit</u> Dimensionless</p>																	

<p><u>Effect of changed knowledge on new knowledge development</u></p> <table border="1"> <thead> <tr> <th>Input</th> <th>Output</th> </tr> </thead> <tbody> <tr><td>0</td><td>0.5</td></tr> <tr><td>0.05</td><td>0.62</td></tr> <tr><td>0.1</td><td>0.72</td></tr> <tr><td>0.25</td><td>0.86</td></tr> <tr><td>0.5</td><td>0.96</td></tr> <tr><td>0.8</td><td>1</td></tr> <tr><td>1</td><td>1</td></tr> </tbody> </table>		Input	Output	0	0.5	0.05	0.62	0.1	0.72	0.25	0.86	0.5	0.96	0.8	1	1	1	<p><u>Definition:</u> The effect of changed knowledge (experience of developing new knowledge) on the effectiveness of developing new knowledge</p> <p><u>Base for this function:</u> Qualitatively suggested by client Estimated by modeler</p>
Input	Output																	
0	0.5																	
0.05	0.62																	
0.1	0.72																	
0.25	0.86																	
0.5	0.96																	
0.8	1																	
1	1																	
<p><u>Range</u> 0.5-1</p>	<p><u>Reference point</u> (1,1)</p>	<p><u>Shape</u> Goal seeking</p>	<p><u>Unit</u> Dimensionless</p>															

<p><u>Effect of new initiatives burden on maturing new knowledge</u></p> <table border="1"> <thead> <tr> <th>Input</th> <th>Output</th> </tr> </thead> <tbody> <tr><td>0</td><td>1</td></tr> <tr><td>0.1</td><td>0.97</td></tr> <tr><td>0.18</td><td>0.9</td></tr> <tr><td>0.27</td><td>0.72</td></tr> <tr><td>0.37</td><td>0.57</td></tr> <tr><td>0.5</td><td>0.43</td></tr> <tr><td>0.7</td><td>0.35</td></tr> <tr><td>1</td><td>0.3</td></tr> </tbody> </table>		Input	Output	0	1	0.1	0.97	0.18	0.9	0.27	0.72	0.37	0.57	0.5	0.43	0.7	0.35	1	0.3	<p><u>Definition:</u> The effect of new initiatives burden on the effectiveness of maturing new knowledge</p> <p><u>Base for this function:</u> Qualitatively suggested by client Estimated by modeler</p>
Input	Output																			
0	1																			
0.1	0.97																			
0.18	0.9																			
0.27	0.72																			
0.37	0.57																			
0.5	0.43																			
0.7	0.35																			
1	0.3																			
<p><u>Range</u> 0.5-1</p>	<p><u>Reference point</u> (0,1)</p>	<p><u>Shape</u> Goal seeking</p>	<p><u>Unit</u> Dimensionless</p>																	

Effect of mature new knowledge on maturing new knowledge



Definition: The effect of mature new knowledge (experience of new knowledge maturation) on the effectiveness of maturing new knowledge

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-1

Reference point

(0,1)

Shape

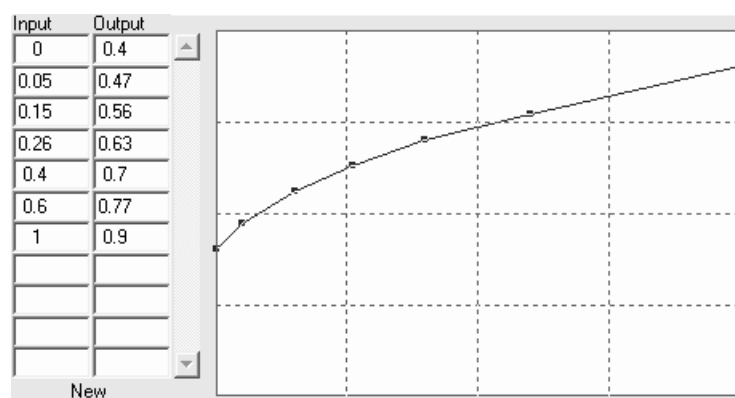
Goal seeking

Unit

Dimensionless

Vulnerability section:

Effect of immature new WP on Vulnerability Index



Definition: The effect of immature new work processes (not knowing what to do in the new work processes) on vulnerability

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.4-0.9

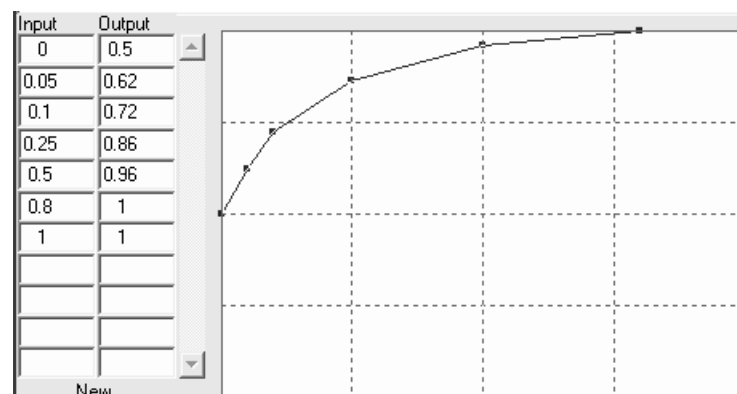
Reference point

Shape

Goal seeking

Unit

Dimensionless

Effect of immature new knowledge on Vulnerability**Index**

Definition: The effect of immature new knowledge (not knowledge how to do in the new work processes) on vulnerability

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

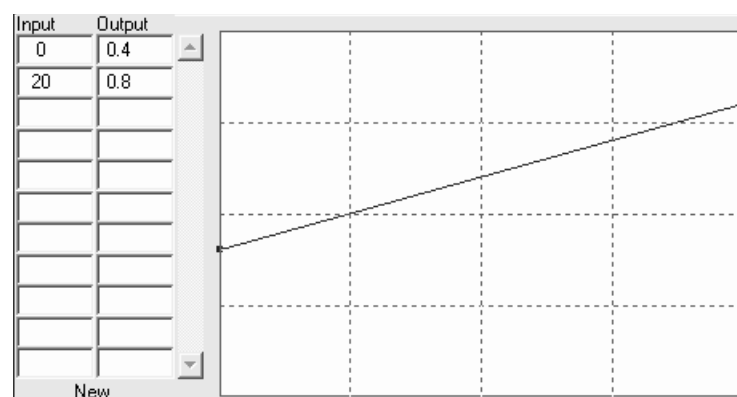
0.4-0.8

Reference point**Shape**

Goal seeking

Unit

Dimensionless

Effect of knowledge gap on Vulnerability Index

Definition: The effect of knowledge gap (not knowing why to work in the specific way) on the vulnerability index.

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

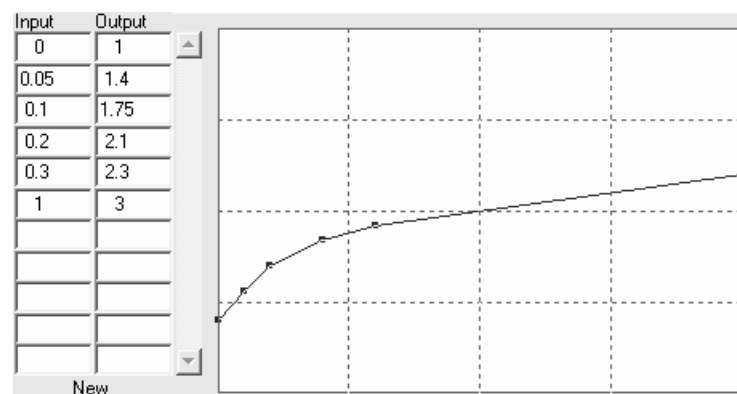
0.4-0.8

Reference point**Shape**

linear

Unit

Dimensionless

Incident cost section:**Effect of new work processes on events**

Definition: The effect of new work processes (continue of operation transition) on events (those that has the potential to become incidents).

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

1-3

Reference point

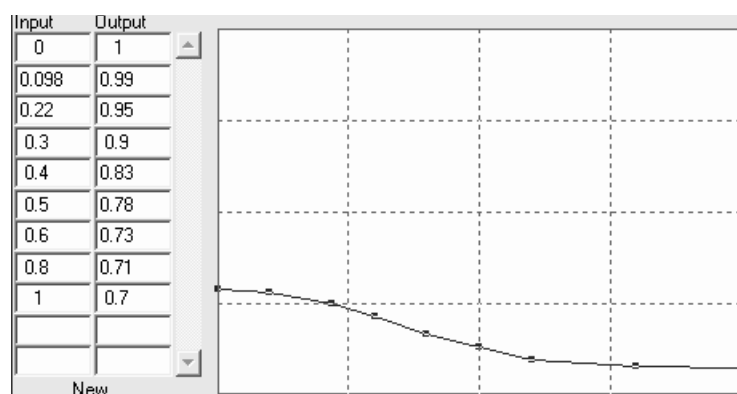
(0,1)

Shape

Goal seeking

Unit

Dimensionless

Effect of resilience on severity

Definition: The effect of resilience (related to mature new work processes and mature new knowledge) on severity of incidents

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

1-0.7

Reference point

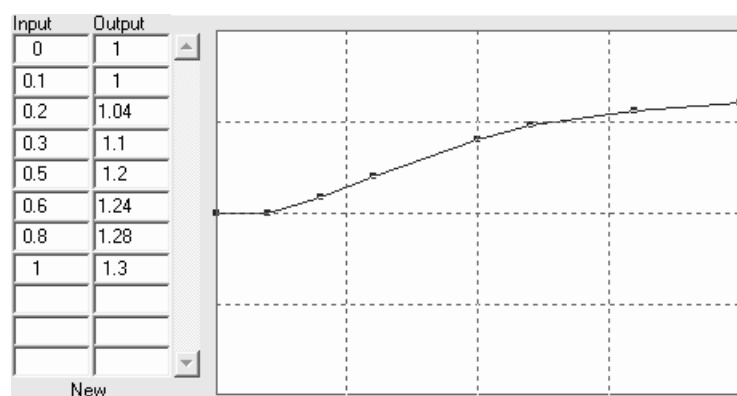
(0,1)

Shape

S-shape

Unit

Dimensionless

Effect of new initiatives burden on severity of incidents

Definition: The effect of new initiatives burden (having communication difficulties) on severity of incidents

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

1-1.3

Reference point

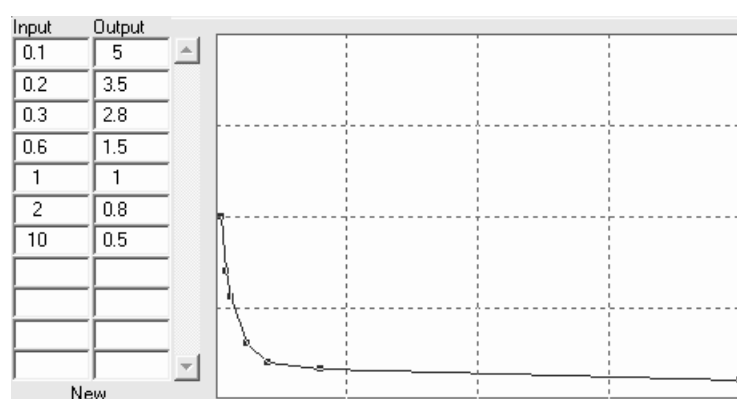
(0,1)

Shape

S-shape

Unit

Dimensionless

Effect of adequacy of IR capability on severity of incidents

Definition: The effect of adequacy of incident response capability (compare to frequency of incidents) on severity of incidents

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.5-5

Reference point

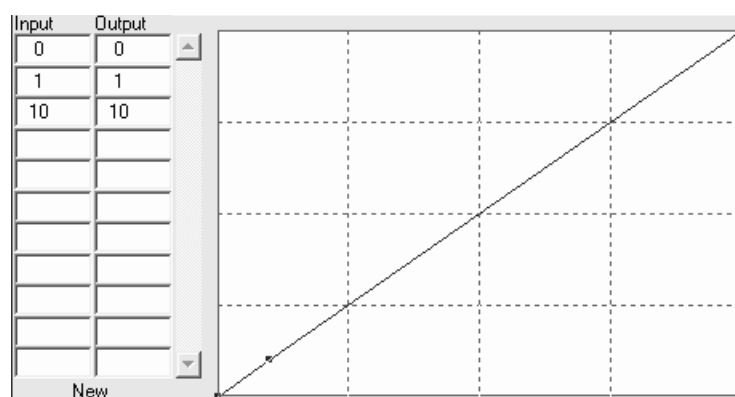
(1,1)

Shape

Goal seeking

Unit

Dimensionless

Learning from incidents section:**Effect of severity on learning**

Definition: The effect of severity (severity of incidents / normal severity of incidents) on learning from incidents

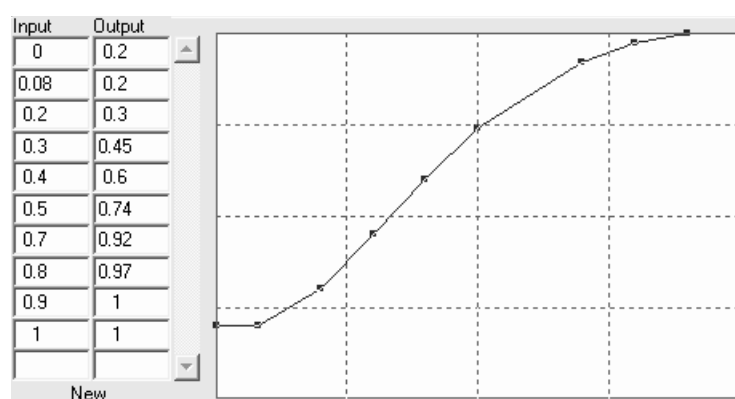
Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range
0-10

Reference point
(0,0), (1,1)

Shape
Linear

Unit
Dimensionless

Incident response capability section:**Effect of adequacy of IR capability on incident detected**

Definition: The effect of adequacy of incident response capability (compare to the frequency of incidents) on incident detected

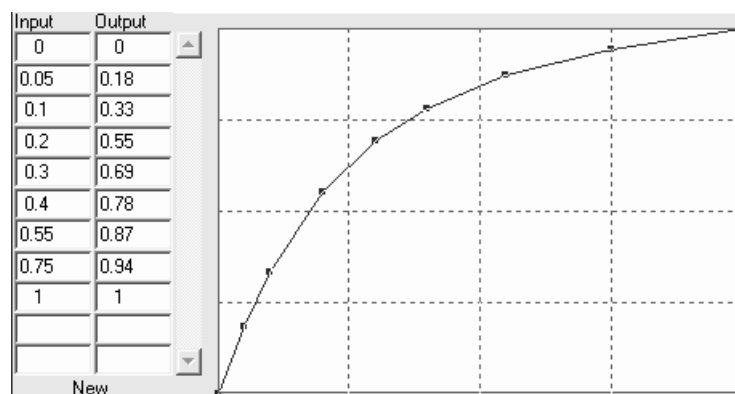
Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range
0.2-1

Reference point
(1,1)

Shape
S-shape

Unit
Dimensionless

Production and profit section:**Effect of knowledge adequacy on productivity**

Definition: The effect of knowledge adequacy (mature new knowledge / mature new work processes) on productivity

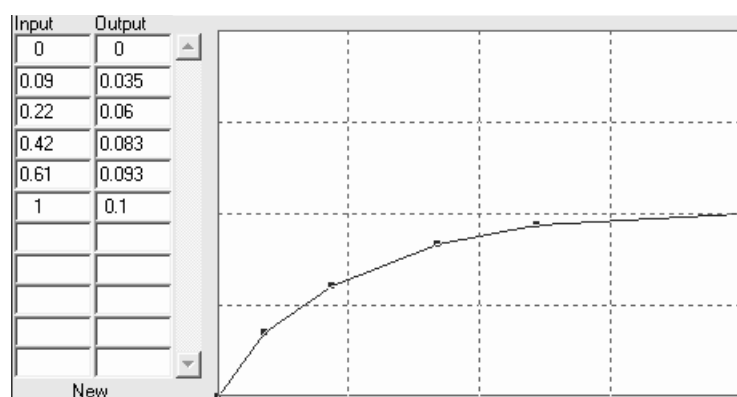
Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range
0-1

Reference point
(0,0), (1,1)

Shape
Goal seeking

Unit
Dimensionless

Effect of new work processes on productivity

Definition: The effect of new work processes (and the new technology embedded in them) on productivity

Base for this function:
Reference point suggested by client
Shape estimated by modeler

Range

0- 0.1

Reference point

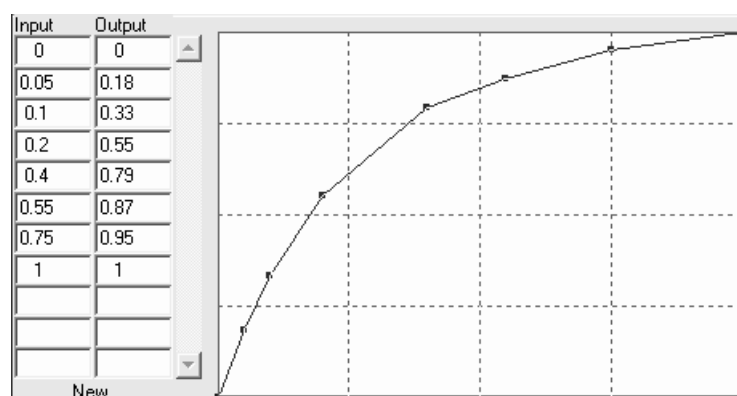
(0, 0) (1, 0.1)

Shape

Goal seeking

Unit

Dimensionless

Effect of knowledge adequacy on cost reduction

The effect of knowledge adequacy (mature new knowledge / mature new work processes) on cost reduction

Base for this function:
Qualitatively suggested by client
Estimated by modeler

Range

0.2-1

Reference point

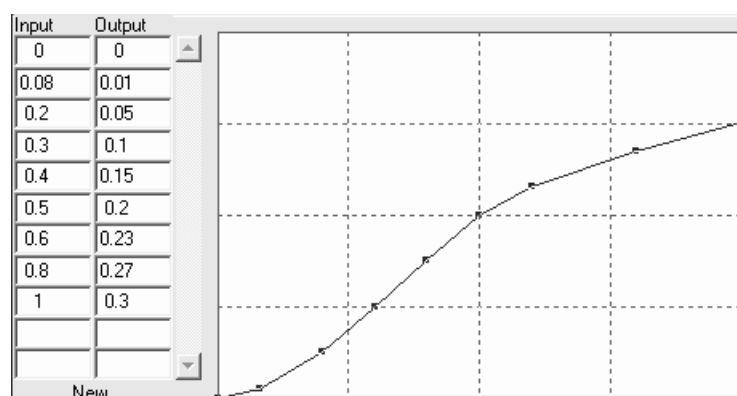
(0, 0) (1, 1)

Shape

Goal seeking

Unit

Dimensionless

Effect of new work processes on cost reduction

Definition: The effect of new work processes (and the new technology embedded in them) on productivity

Base for this function:
Reference point suggested by client
Shape estimated by modeler

Range

0.2-1

Reference point

(1,1)

Shape

Linear

Unit

Dimensionless

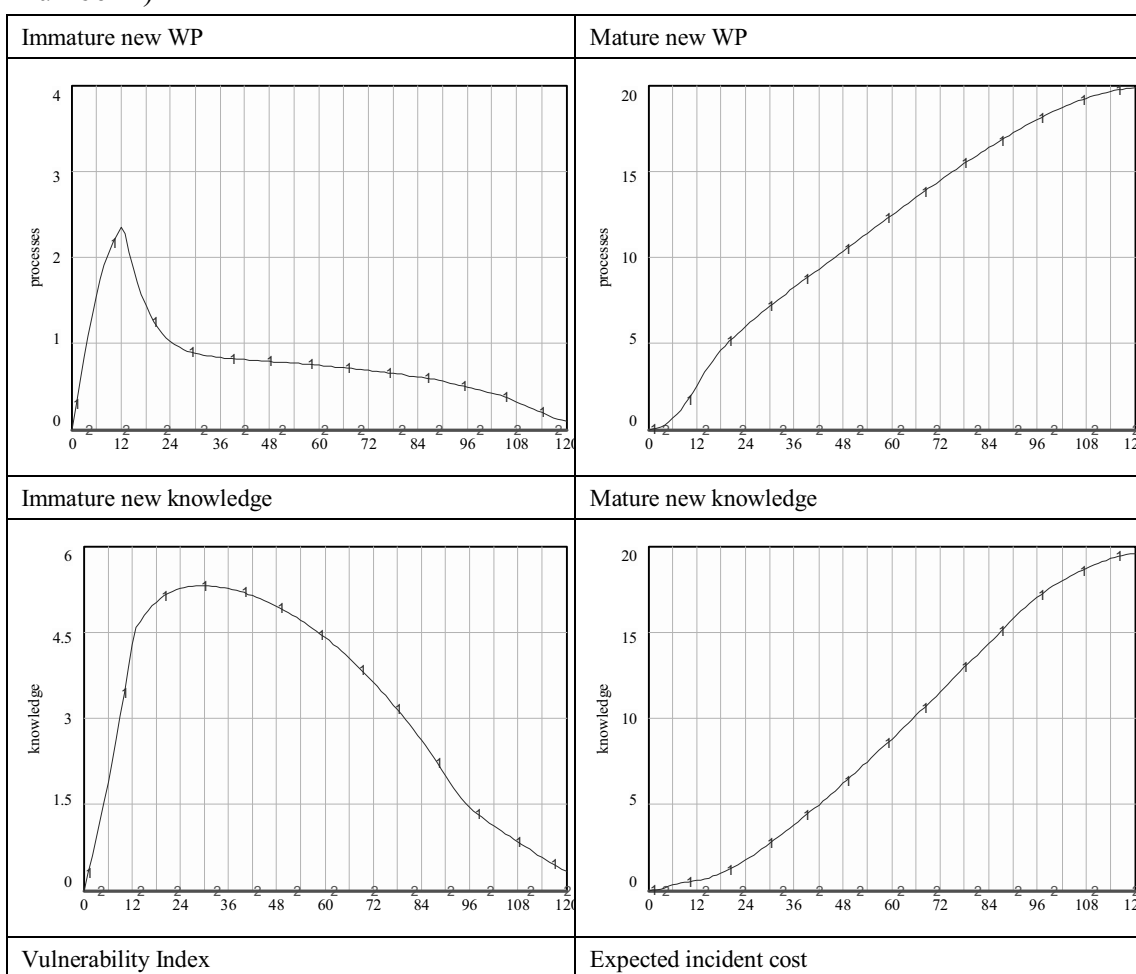
Appendix III Extreme Tests

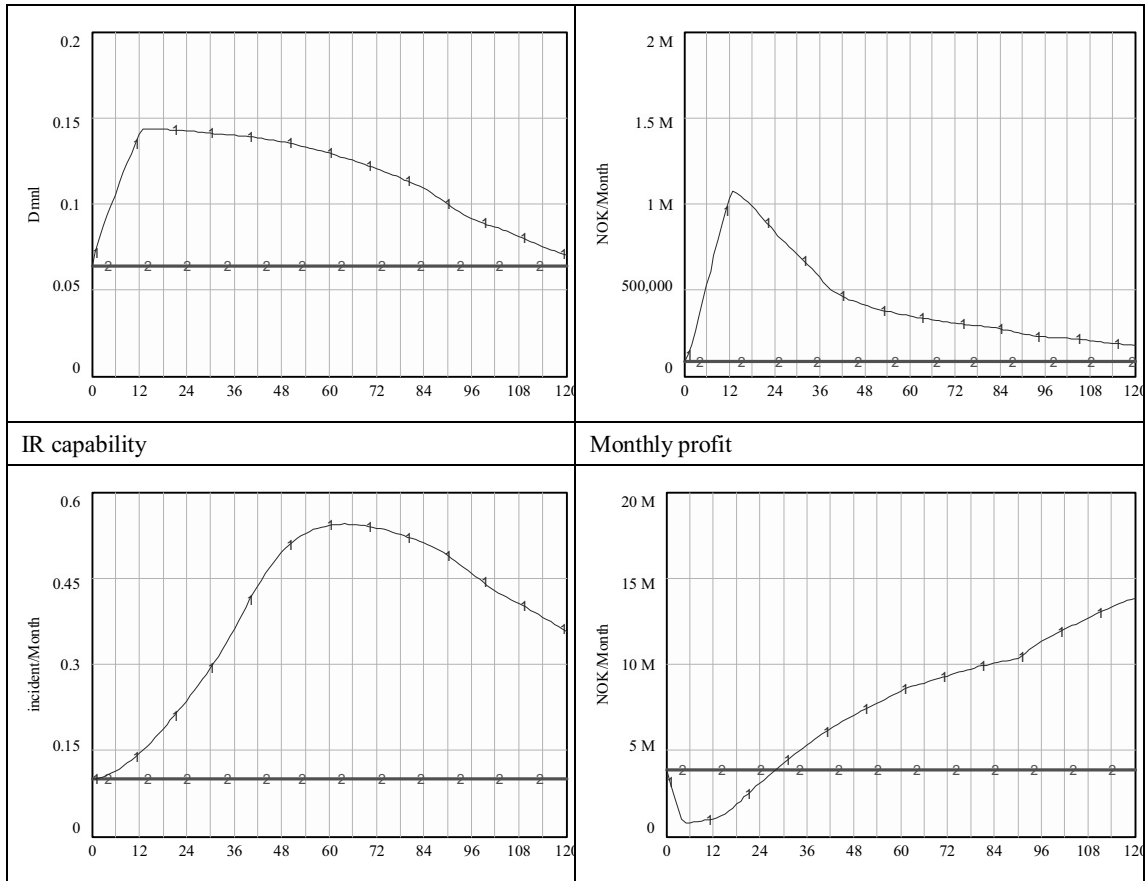
Ex 1 – No operation transition

Variables change: Management time to develop new work processes (=0),
 Management time to develop new knowledge (=0)

Expectation: No immature new work processes and knowledge; No mature new work processes and knowledge; Other variables are stable.

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





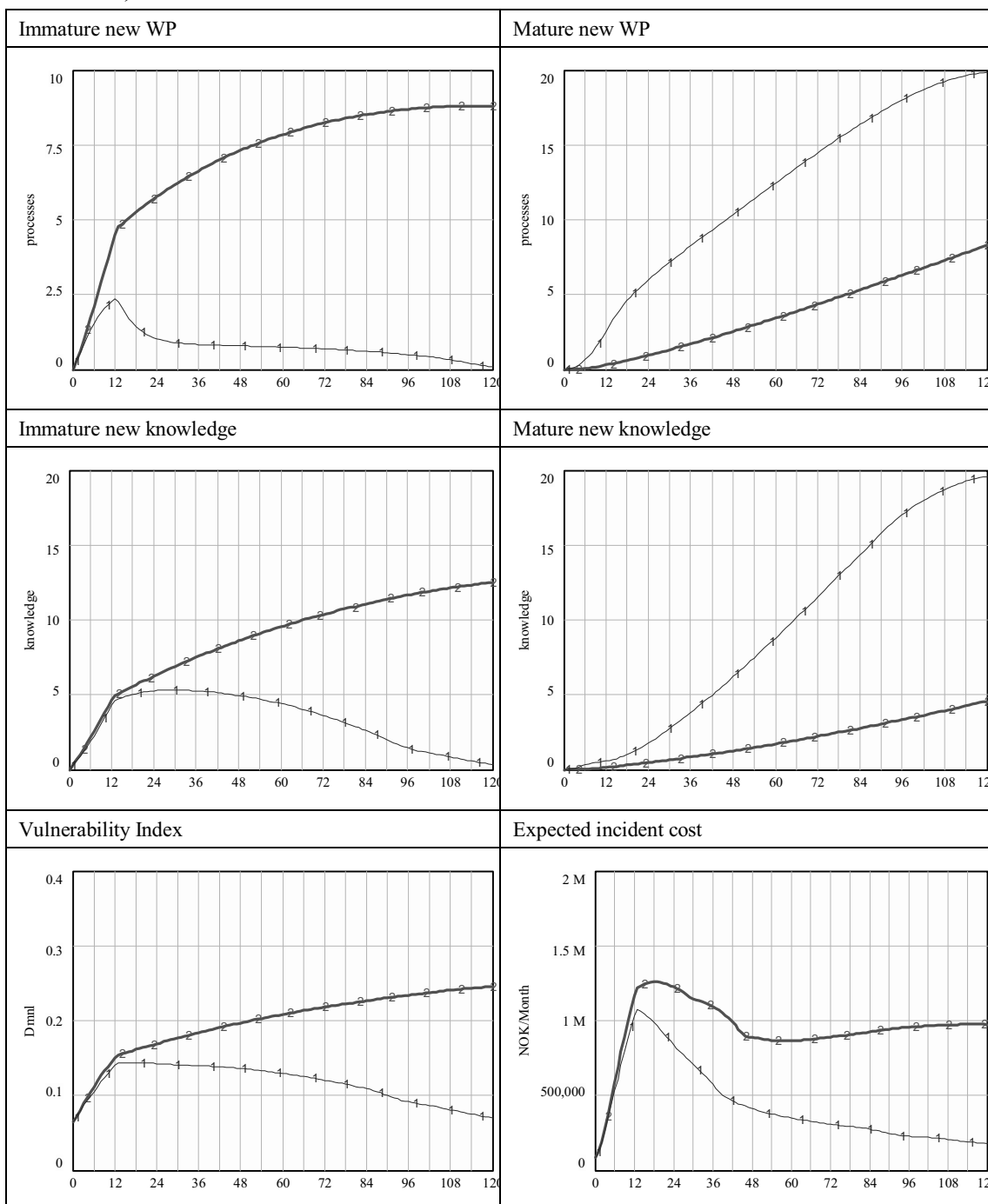
Result: Model simulated results fit the expectation. Extreme test passed.

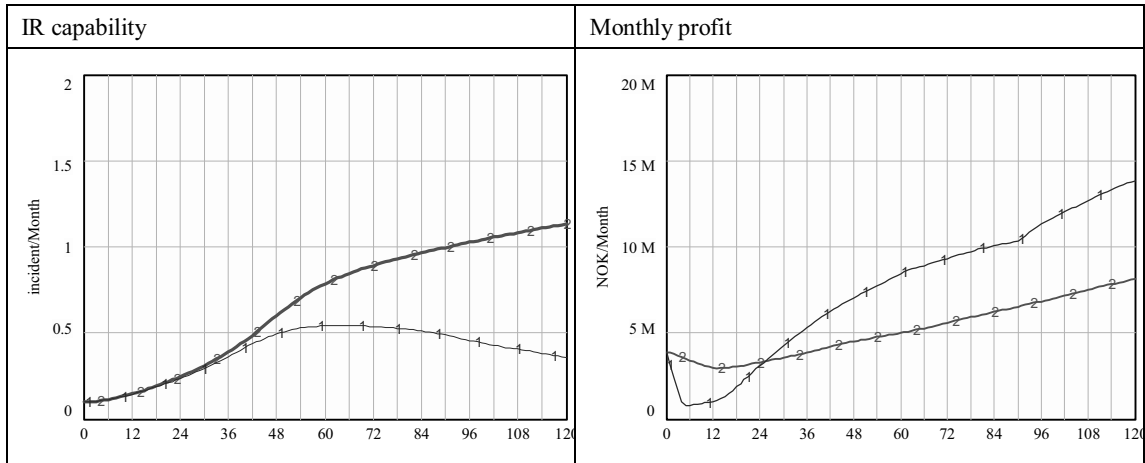
Ex 2 – No resources set aside for new work processes and knowledge maturation

Variables change: Minimum operator resources for production (=100%)

Expectation: Immature new work processes and knowledge will be higher; Mature new work processes and knowledge will be lower; Vulnerability keep increasing; Monthly profit higher at the beginning but lower in the end.
(All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





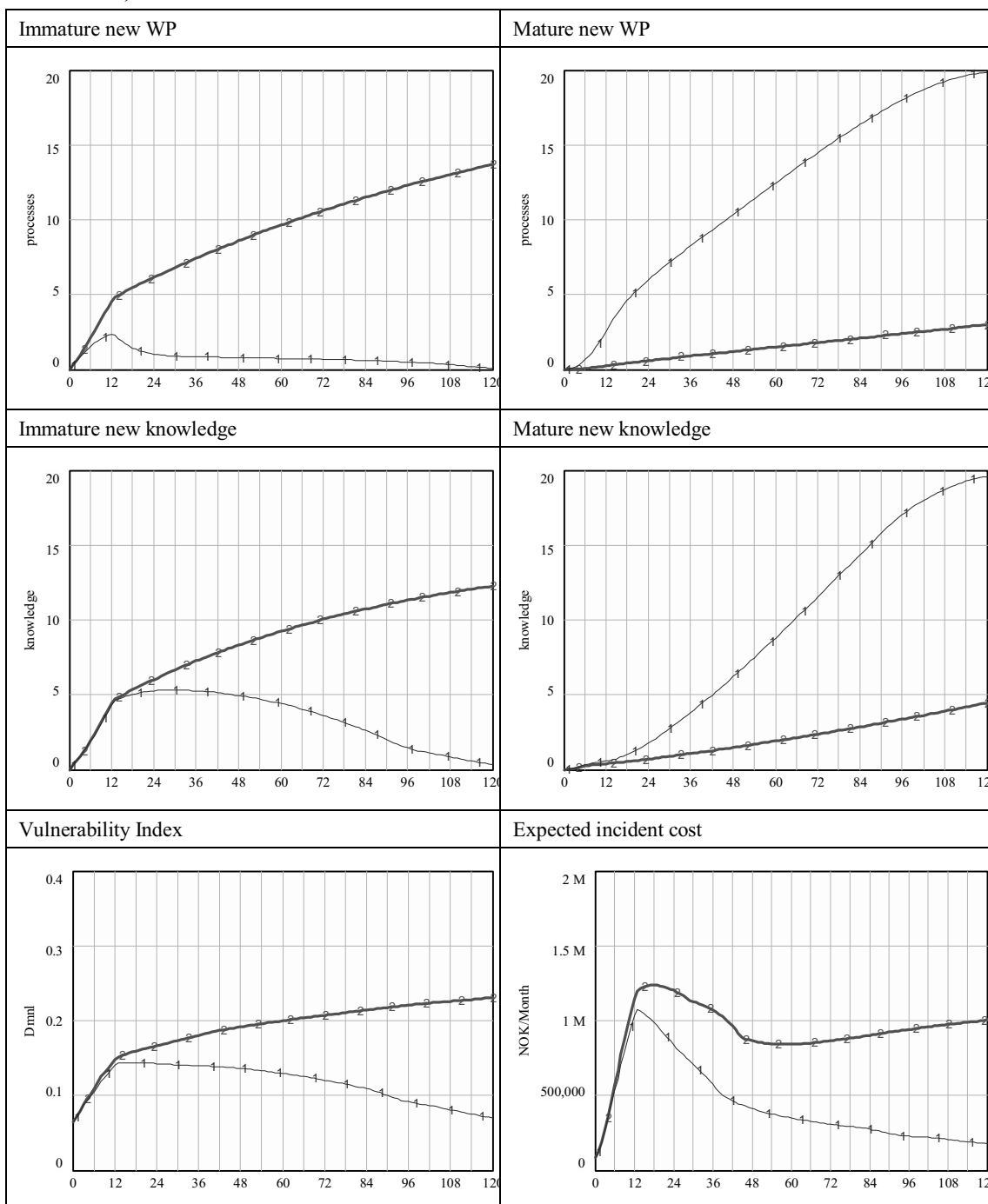
Result: Model simulated results fit the expectation. Extreme test passed.

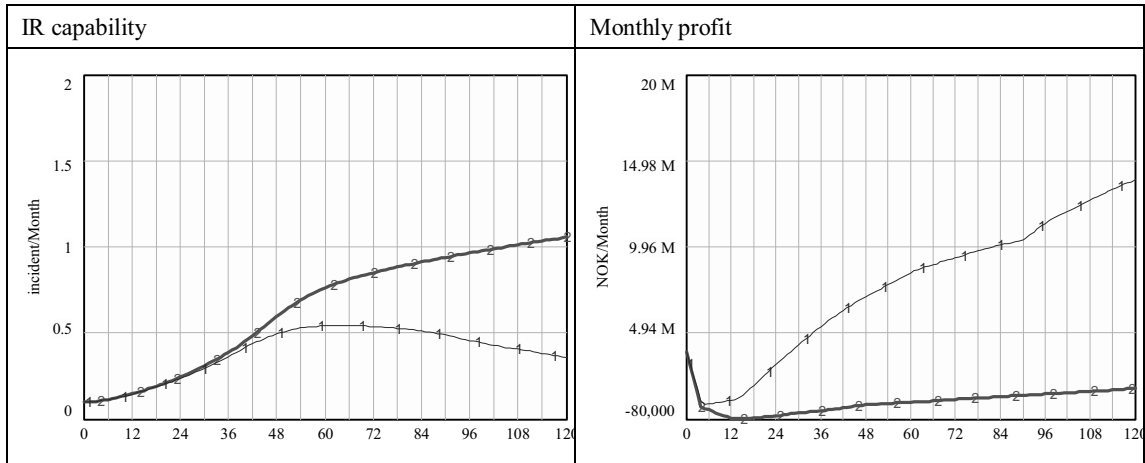
Ex 3 – Extreme long time to mature new work processes

Variables change: Time to mature new work processes (=40 month)

Expectation: Immature new work processes and knowledge will be higher and mature new work processes and knowledge will be lower. Vulnerability keeps increasing; Monthly profit always lower. (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





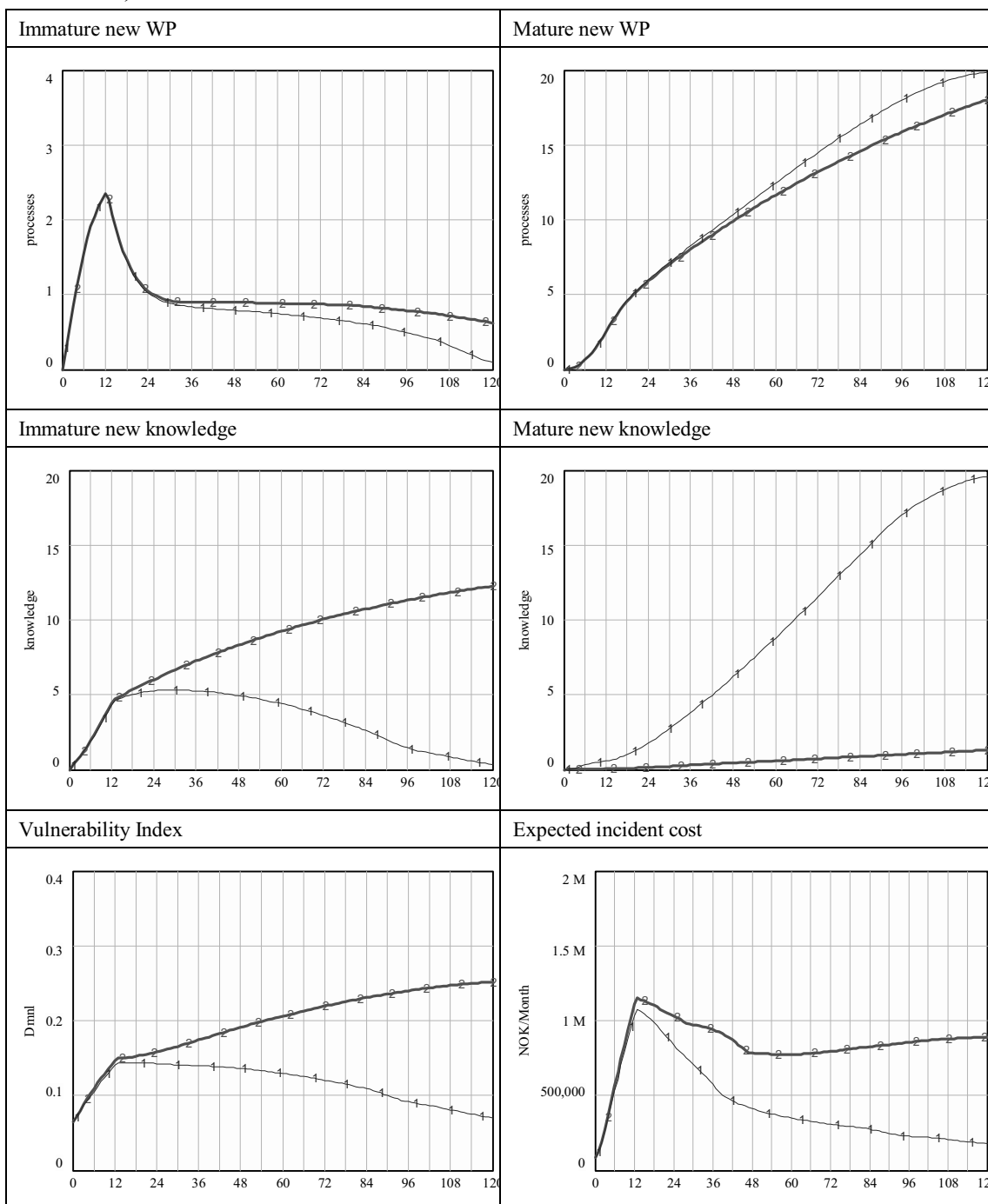
Result: Model simulated results fit the expectation. Extreme test passed.

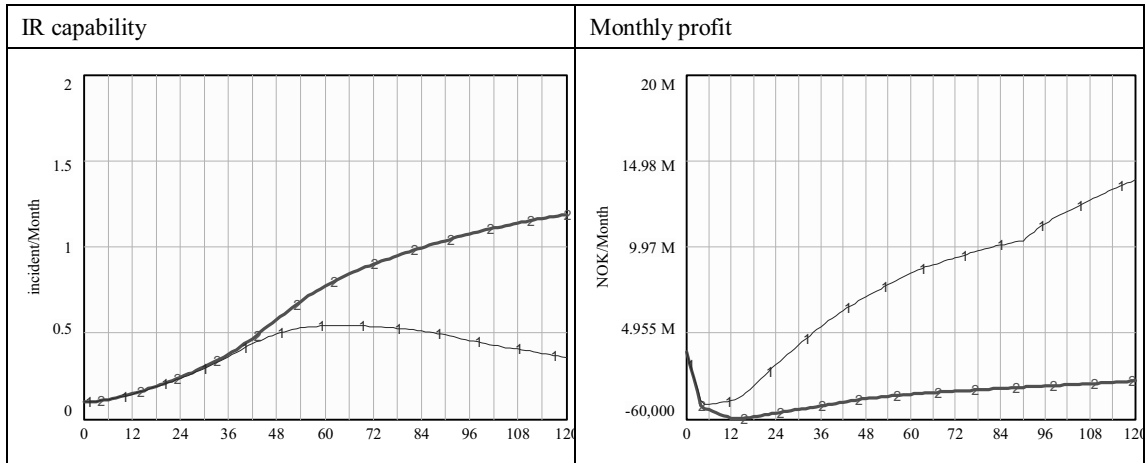
Ex 4 – Extreme long time to mature new knowledge

Variables change: Time to mature new knowledge (=80 month)

Expectation: Immature/mature new work processes will be affected slightly. Immature knowledge will be much higher and mature new knowledge will be much lower. Vulnerability keeps increasing; Monthly profit lower. (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





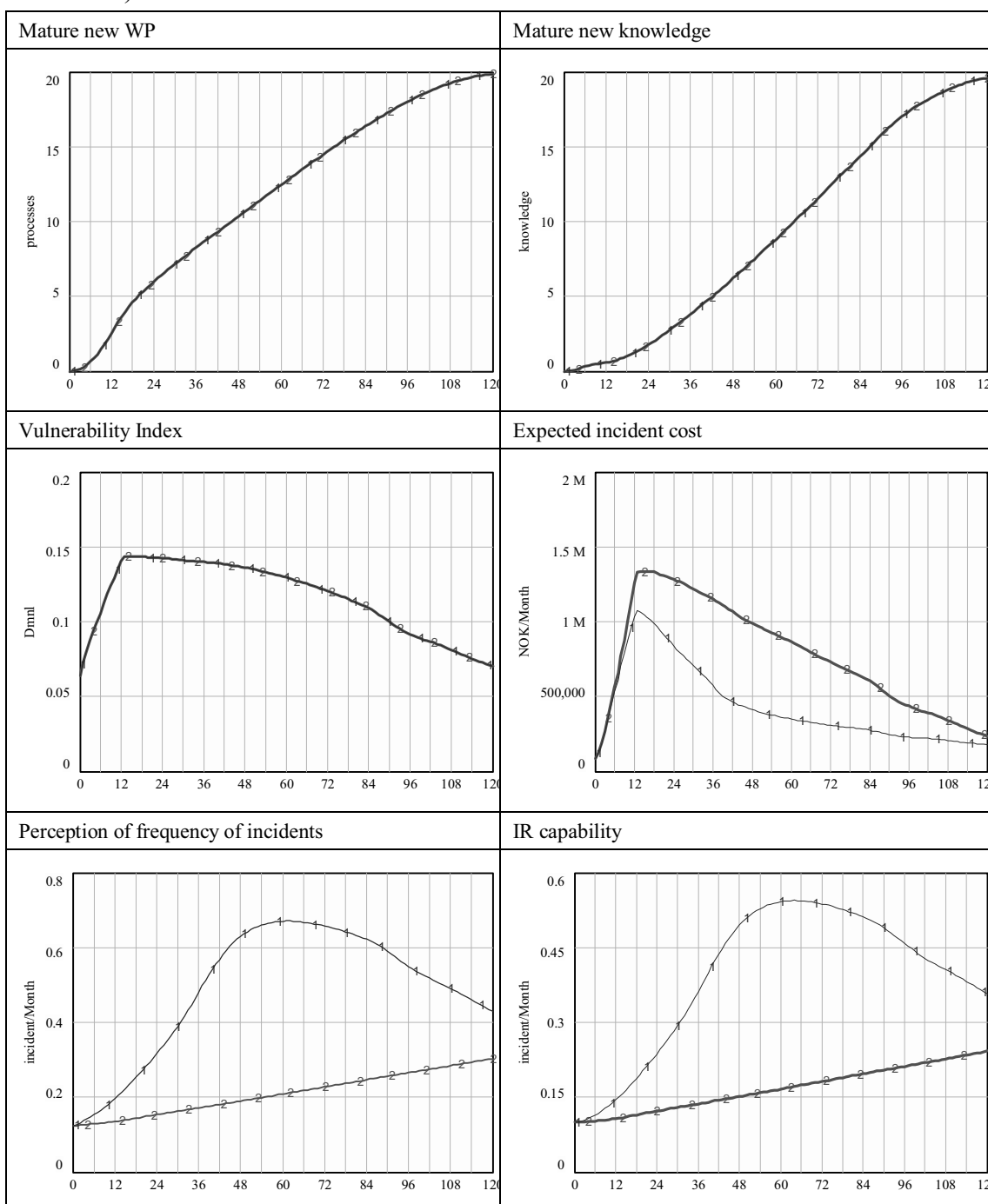
Result: Model simulated results fit the expectation. Extreme test passed.

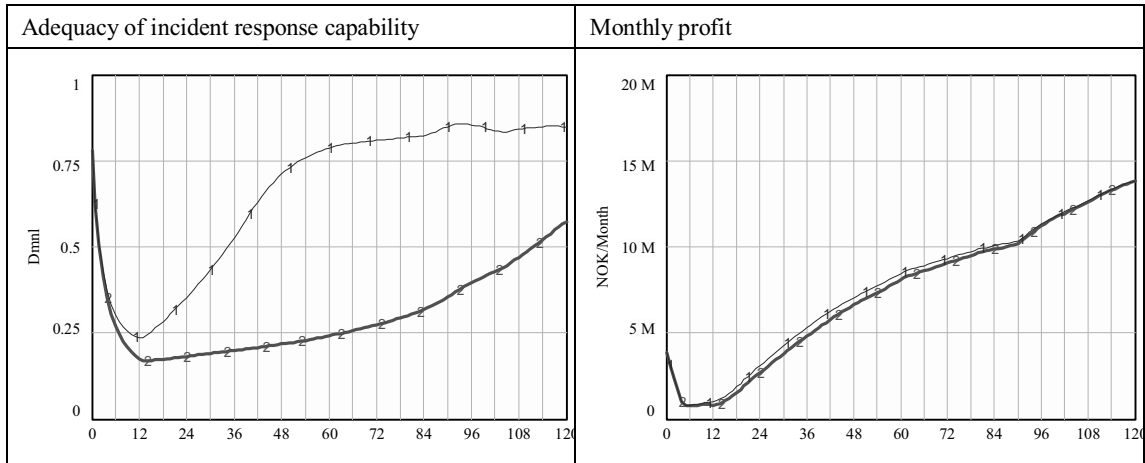
Ex 5 – Extreme long time to change the management’s perception of risk

Variables change: Time to change perception (=30 month)

Expectation: Operation transition will not be affected. The vulnerability index and the frequency of incidents stay the same as base run. Expected incident cost will be higher because the IR capability will be lower with lower perception of risk (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





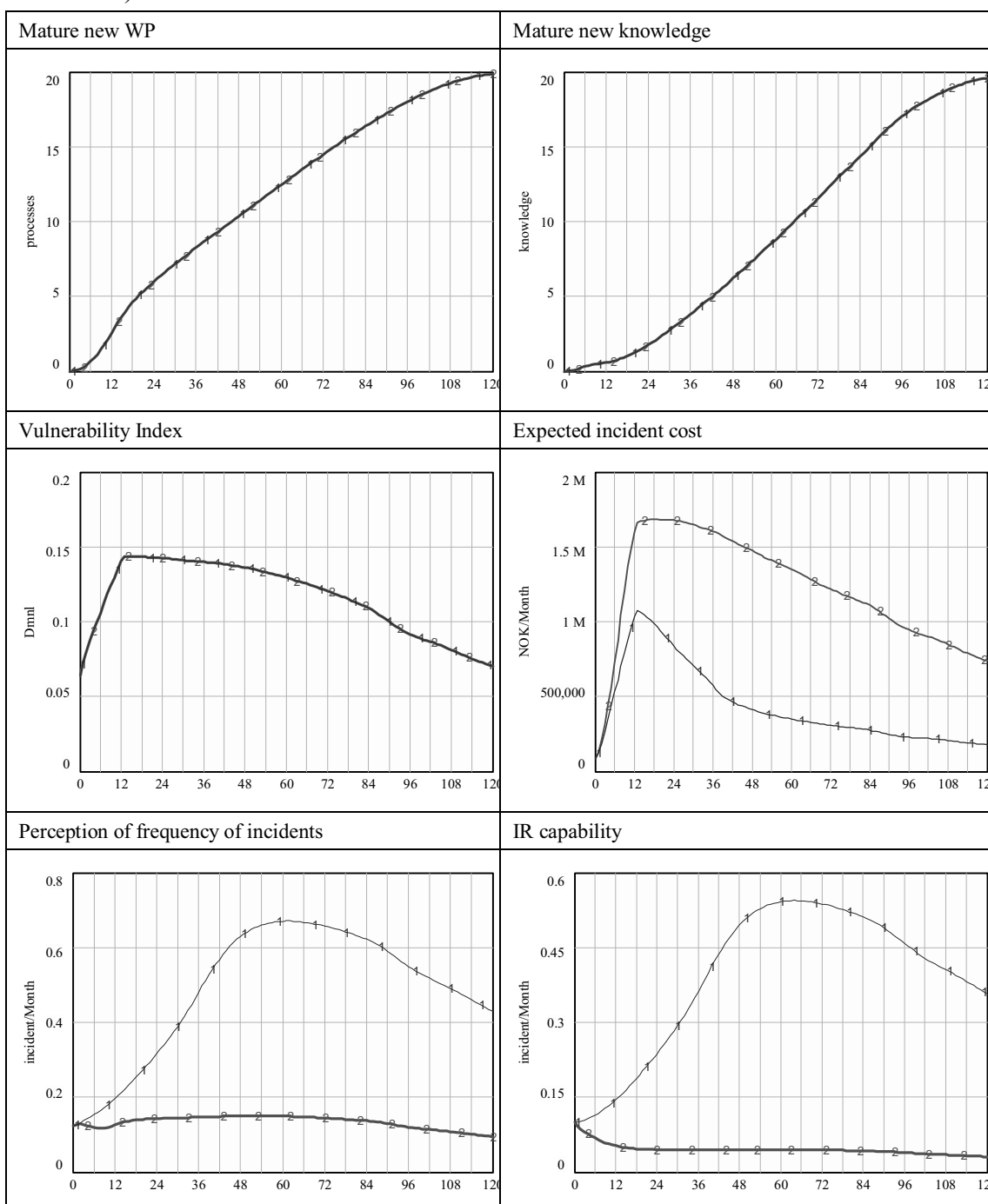
Result: Model stimulated results fit the expectation. Extreme test passed.

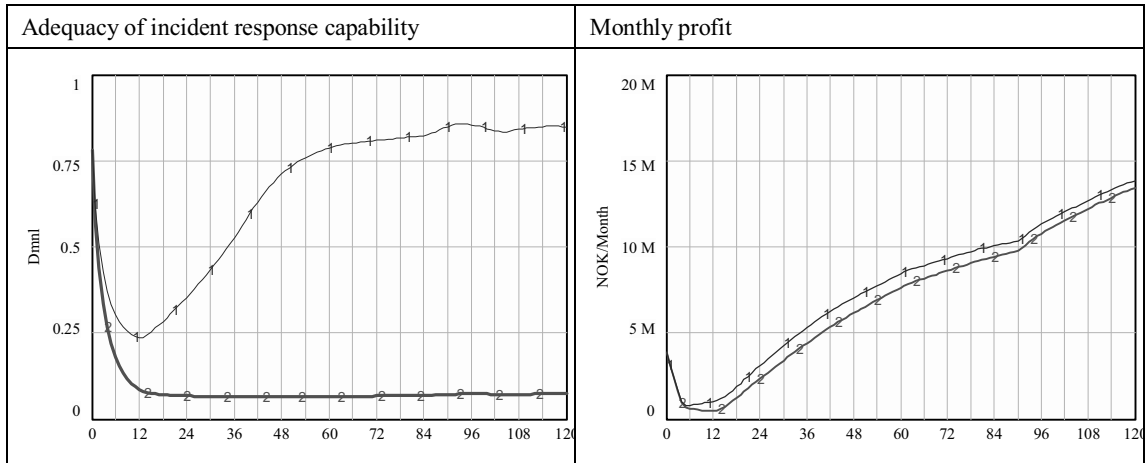
Ex 6 – Extreme long time to adjust incident response capability

Variables change: Time to adjust IR capability (=30 month)

Expectation: Operation transition will not be affected. The vulnerability index and the frequency of incidents stay the same as base run. Expected incident cost will be higher because the IR capability will be lower with long time to build capability (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





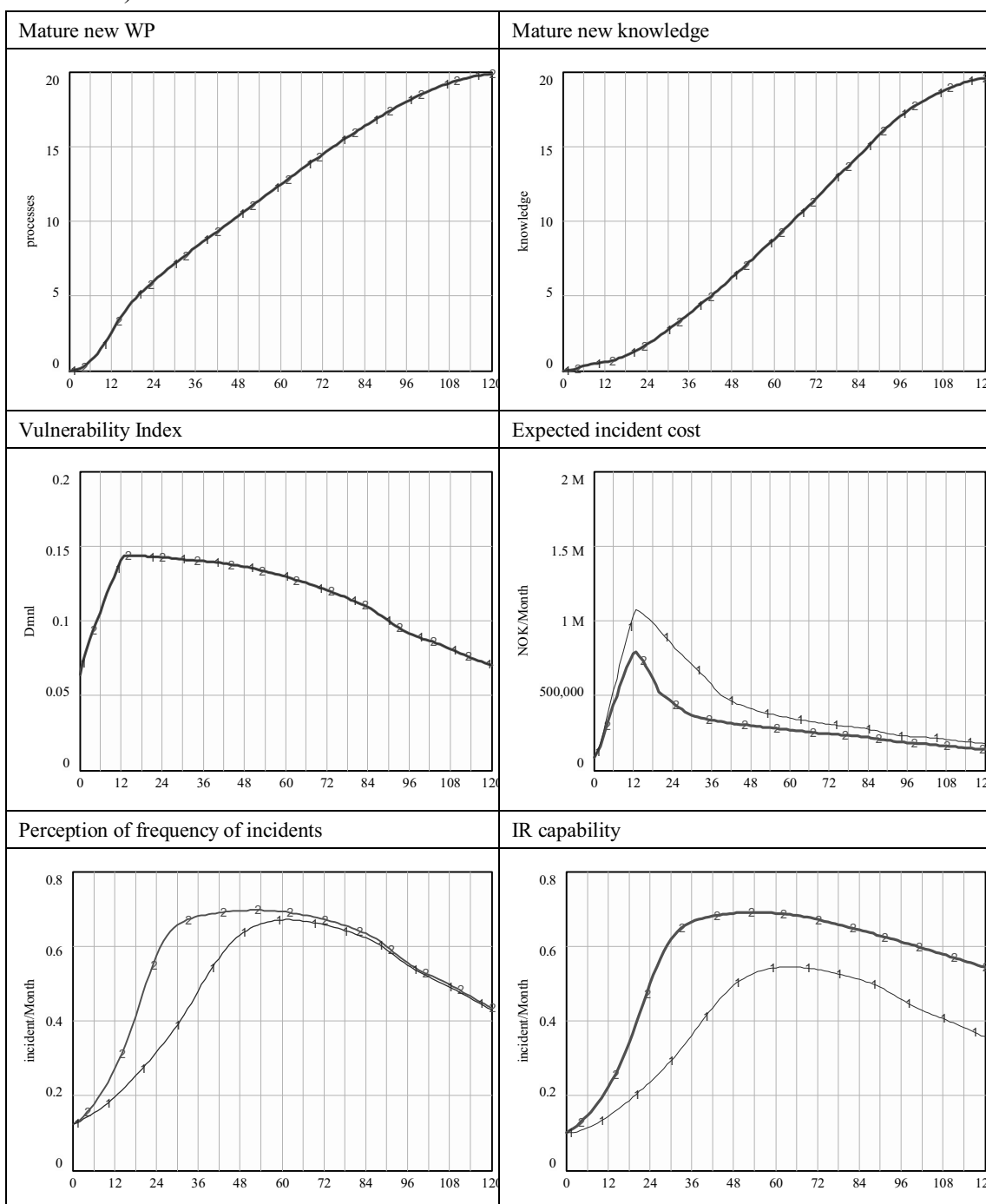
Result: Model stimulated results fit the expectation. Extreme test passed.

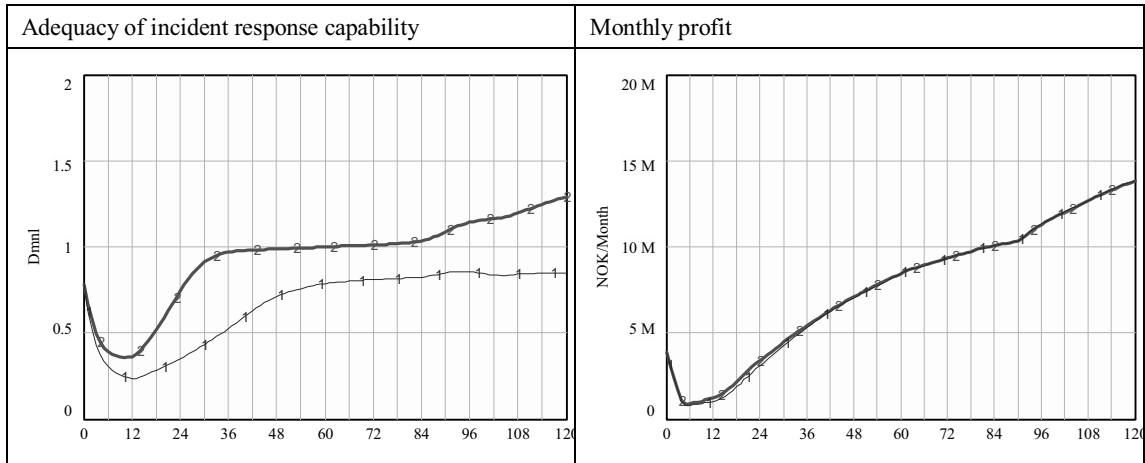
Ex 7 – Extreme long time for incident response capability to deplete

Variables change: Time to obsolete IR capability (=120 month)

Expectation: Operation transition will not be affected. The vulnerability index and the frequency of incidents stay the same as base run. Expected incident cost will be lower because the IR capability will be higher with long time to deplete capability (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)





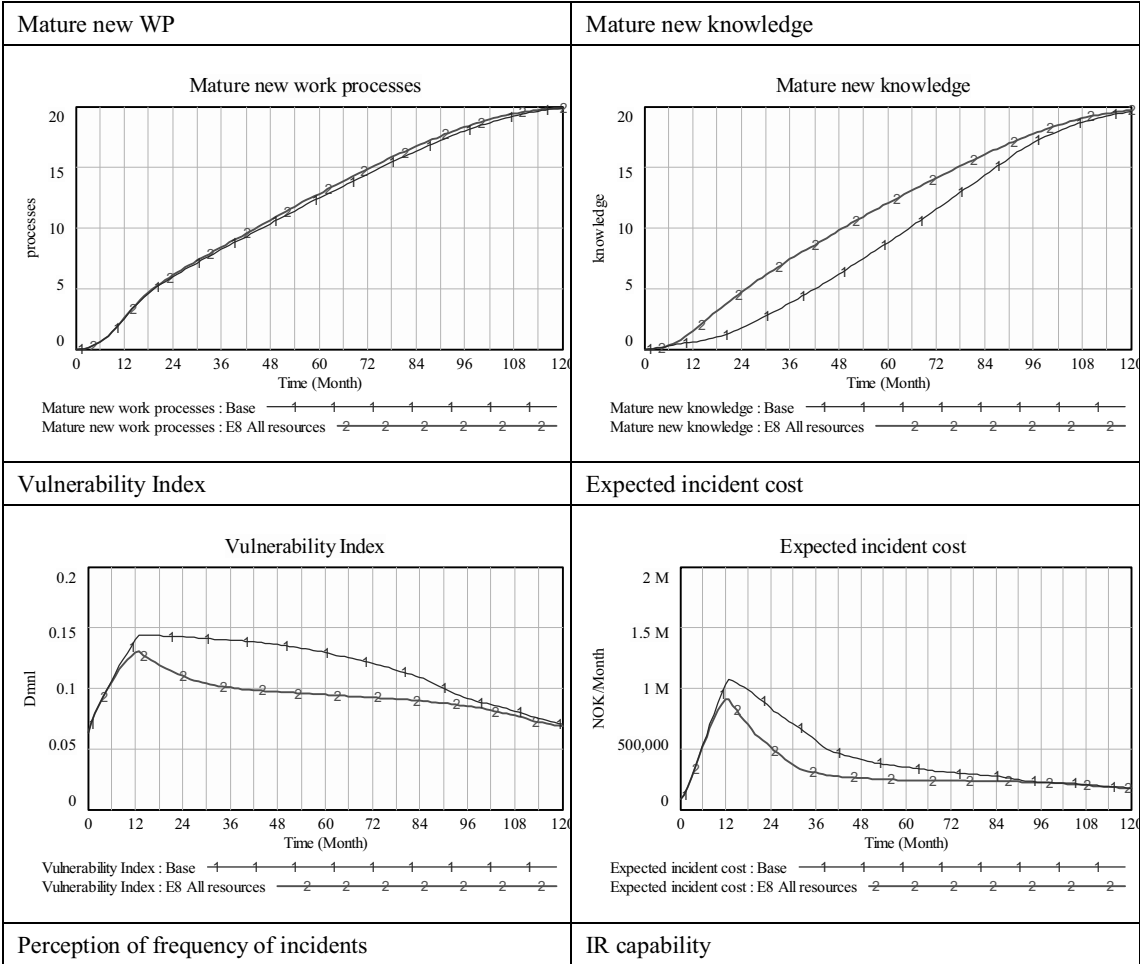
Result: Model stimulated results fit the expectation. Extreme test passed.

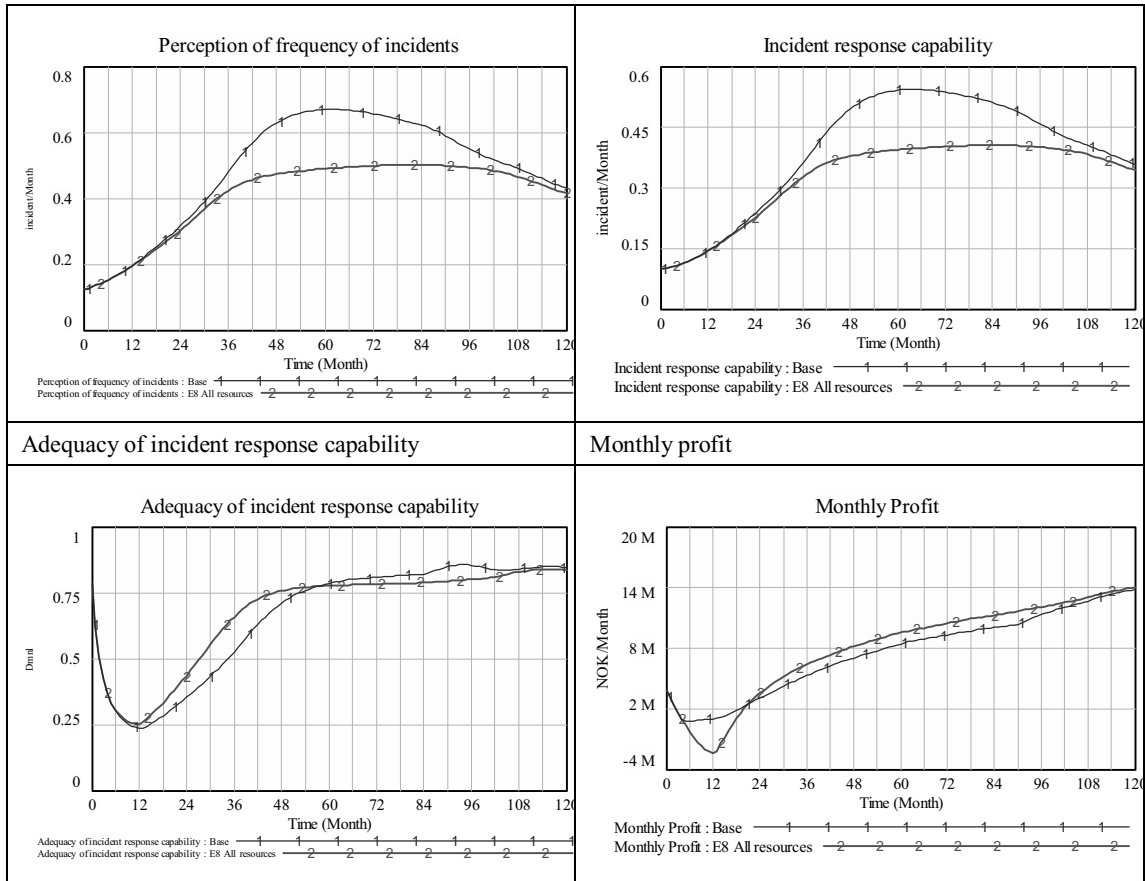
Ex 8 – All resources available to mature new work processes and new knowledge

Variables change: Minimum operator resources for production (=0%)

Expectation: The mature new work processes will be slightly higher but the mature new knowledge will develop much quicker. Vulnerability index will be lower as knowledge matures faster. Thus, the expected incident cost and the perception of frequency of incidents will both be lower, leading to less incident response capability. Monthly profit drop to lower level at beginning and later will be higher than the base run. (All compare to base run)

Model behavior: (Base: Blue line, with number 1; Extreme test: Red line, with number 2)

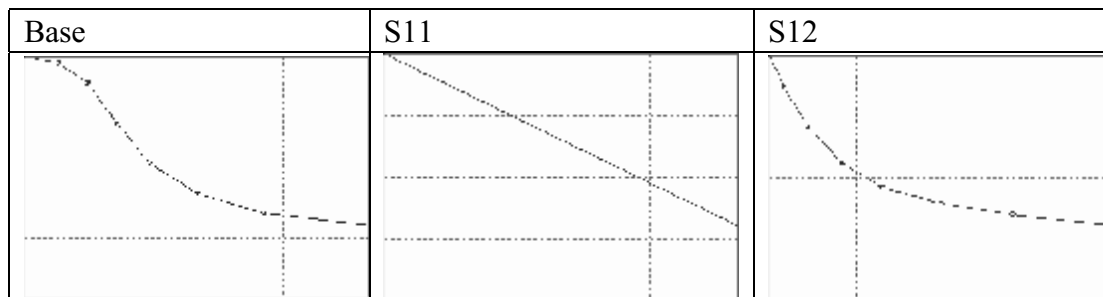




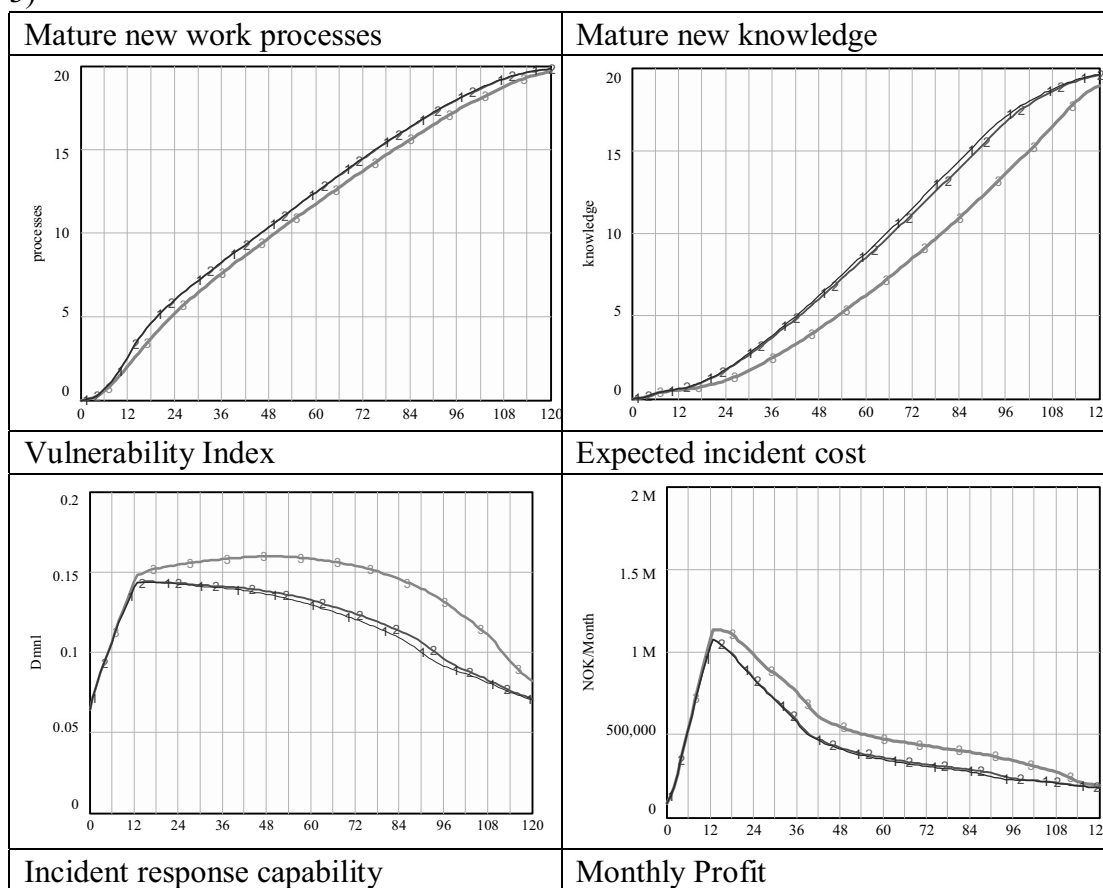
Result: Model simulated results fit the expectation. Extreme test passed.

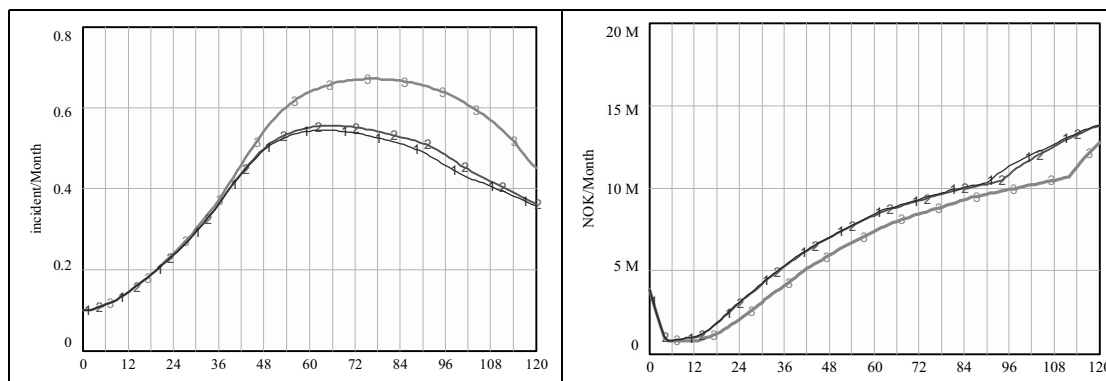
Appendix IV Sensitivity tests

S1- Effect of the new initiatives burden on maturing new work processes



Simulation behavior (Base: blue line, No. 1; S11: red line, No. 2; S12: green line, No. 3)





Analysis:

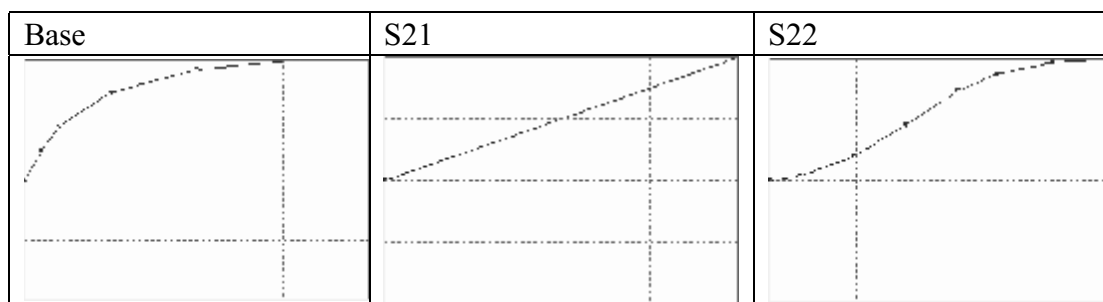
When the table function of “Effect of the new initiatives burden on maturing new knowledge” shifts from an inverted S shape into a linear shape (from base to S11), the model simulation behavior exhibits a modest difference. When the curve table function changes into a goal-seeking curve (S12), which rapidly decreases at the beginning, the simulation behavior exhibits difference to a certain degree. The behavior of “Mature new work processes” does not change significantly, as the effect of change is offset by other loops: when it is extra difficult for new work processes to mature, additional resources will be allocated. This leaves fewer resources for maturing new knowledge, forcing “Mature new knowledge” to become lower than the base run.

This generates a greater knowledge gap, which leads to higher vulnerability. The expected incident cost is only slightly higher as more incident response capability is built to control the cost of incident. With less mature knowledge, the benefits of integrated operations can be fully realized. The monthly profit is lower in S12.

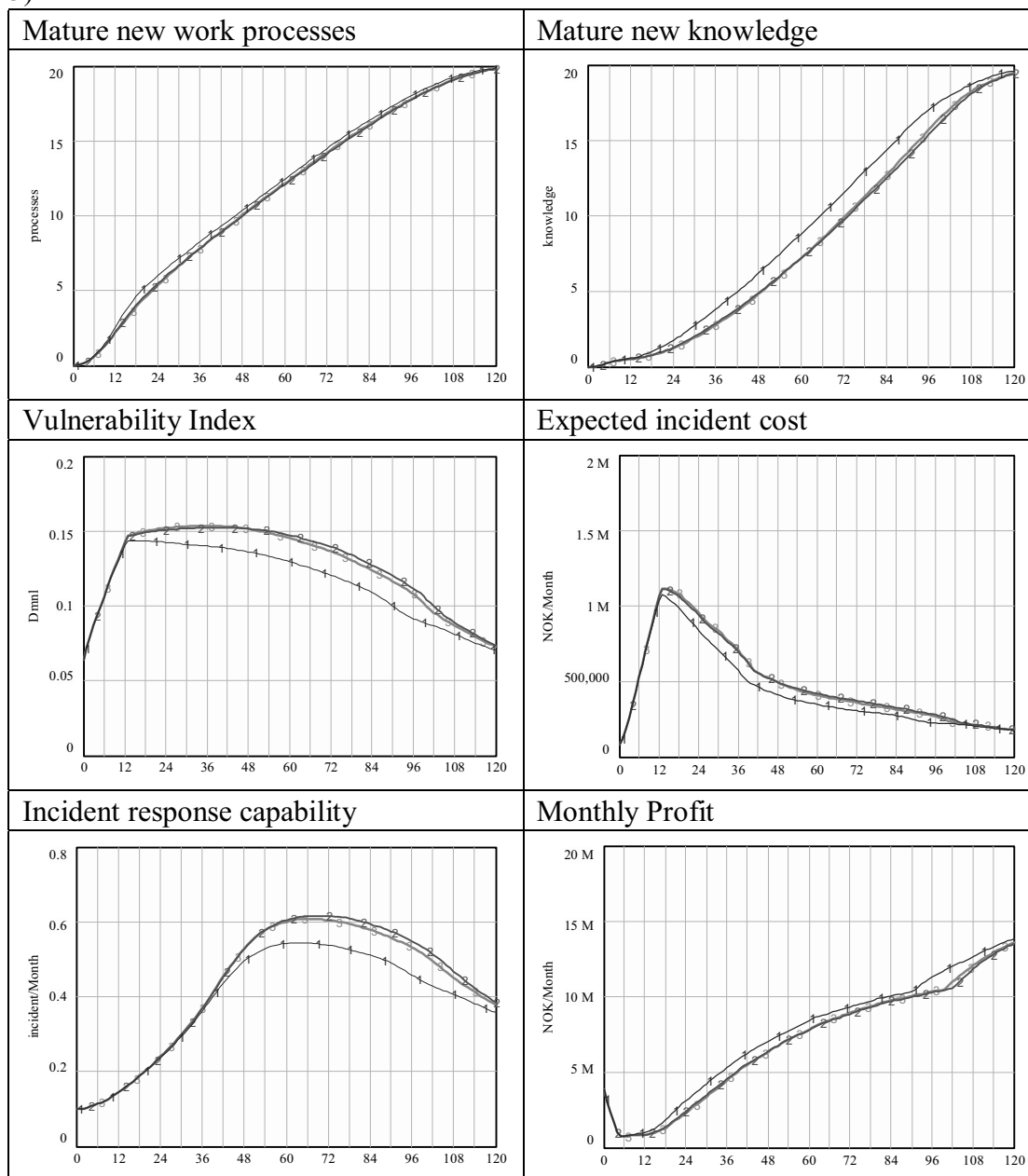
The sensitivity demonstrated in this test is reasonable. Empirically, when people are faced with a small amount of burden from new things, they are able to respond without affecting their performance. When the new burdens are high, their performance can be significantly affected. The curve in the base run becomes increasingly reasonable.

Result: Pass

S2 - Effect of mature new WP on maturing new WP



Simulation behavior (Base: blue line, No. 1; S21: red line, No. 2; S22: green line, No. 3)

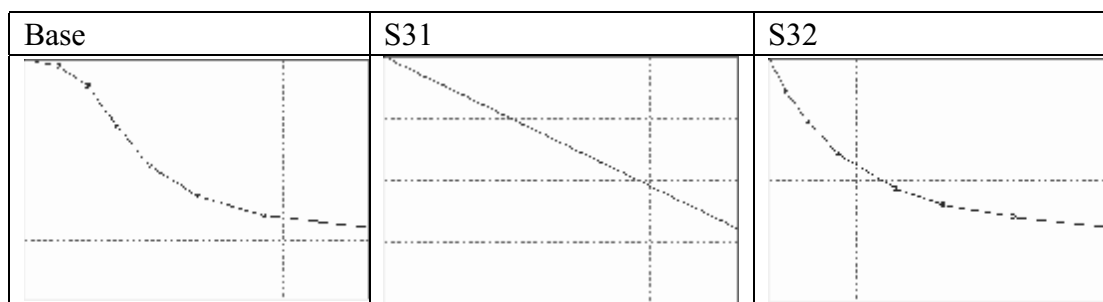


Analysis:

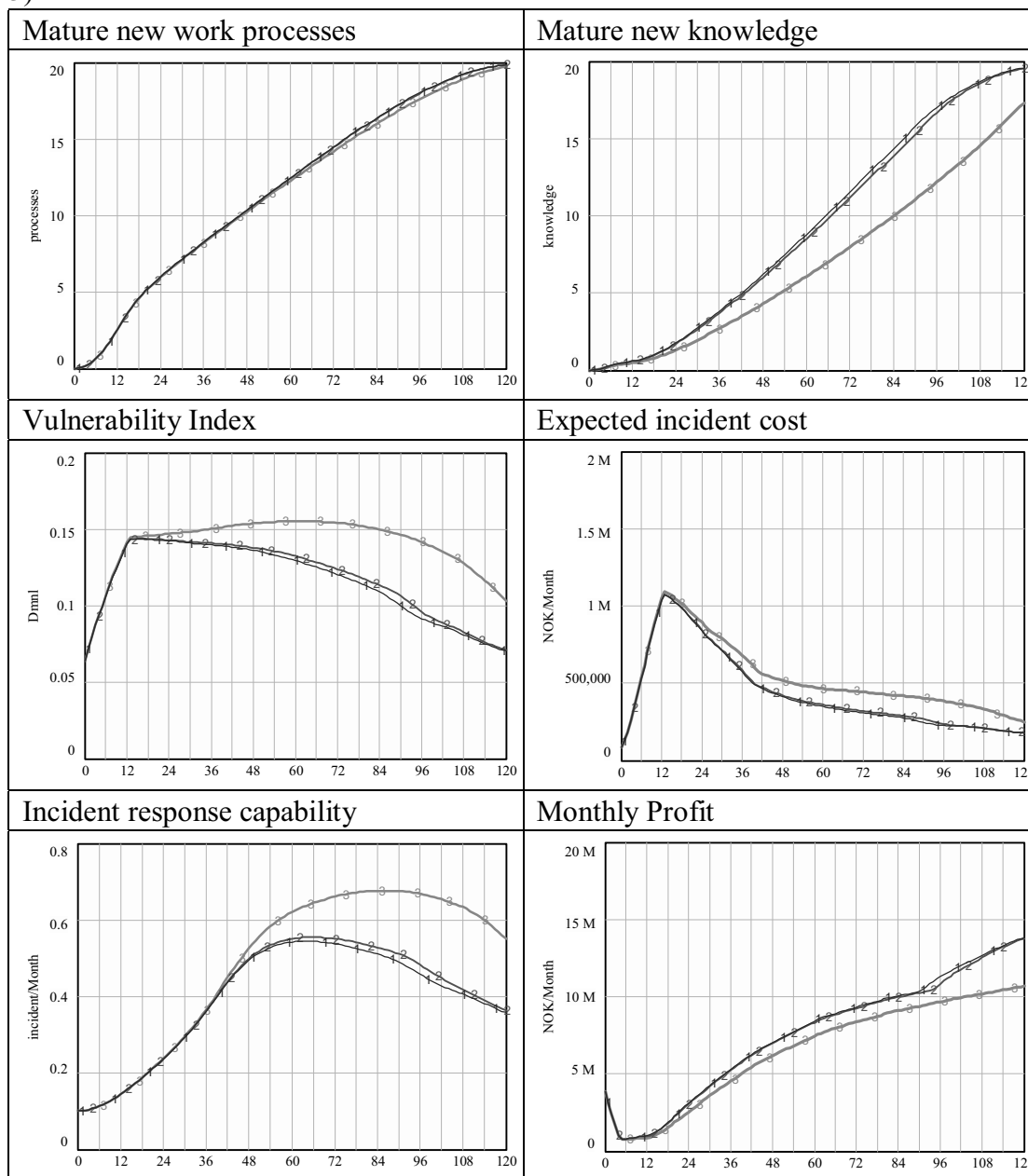
The “mature new work processes” behaves similarly for the three runs because the effect of change in this table function is offset by other loops. The effect is passed onto “mature new knowledge,” which likewise leads to behavioral change in the “vulnerability index” and “incident response capability.” The behavior of “expected incident cost” does not change significantly because the increasing “incident response capability” offsets the effect of increasing vulnerability. “Monthly profit” is slightly affected because less knowledge matures in S21 and S22. The behavior of S21 and S22 are fairly similar because their two table functions are quite similar as well.

Result: Pass

S3- Effect of new initiatives burden on maturing new knowledge



Simulation behavior (Base: blue line, No. 1; S31: red line, No. 2; S32: green line, No. 3)

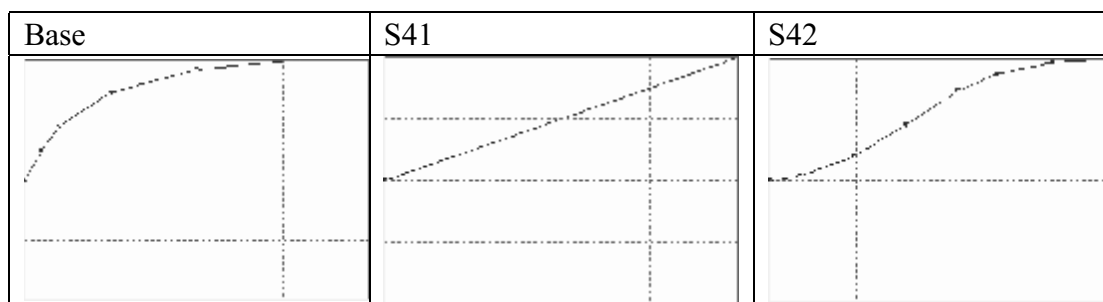


Analysis:

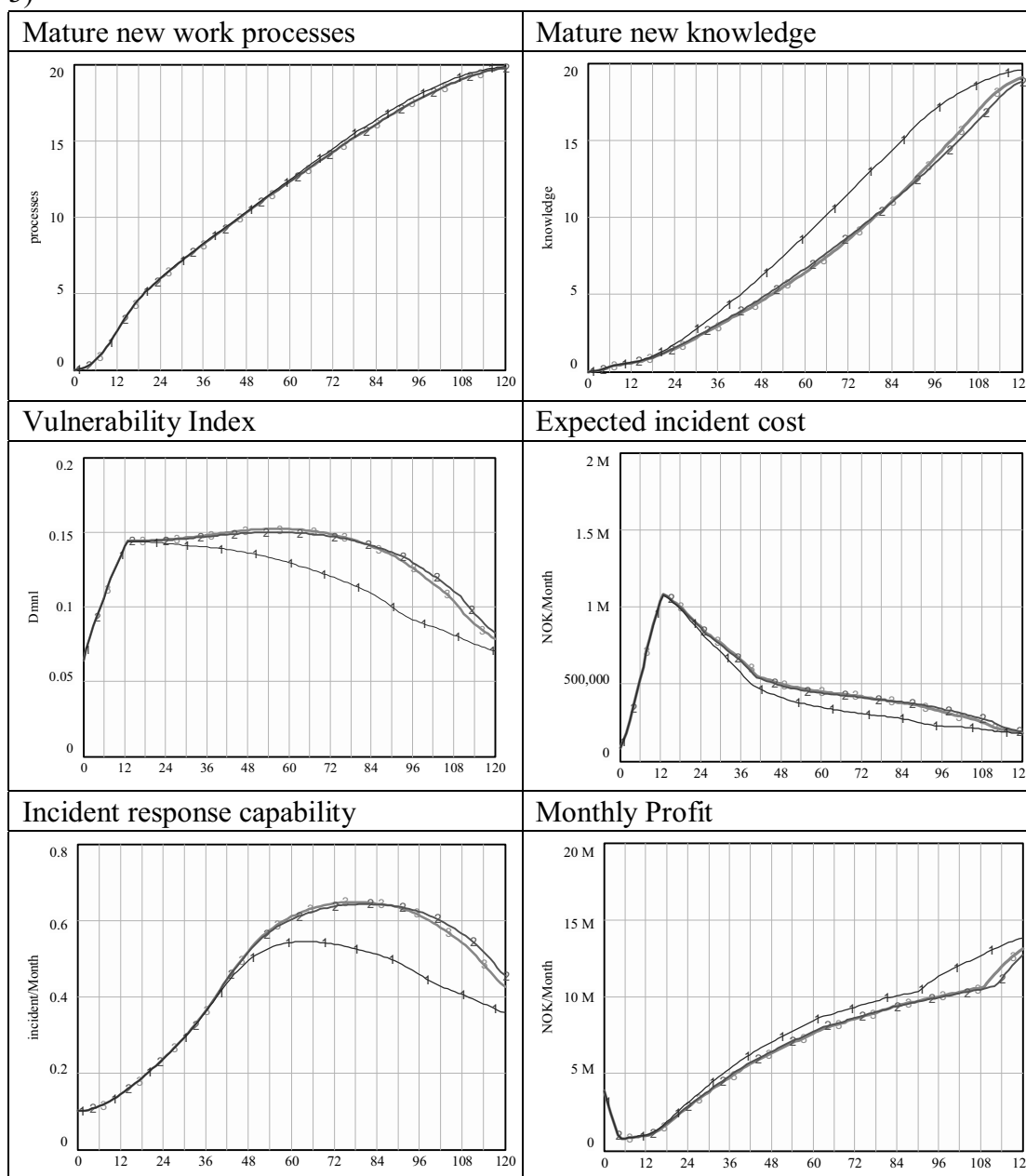
Compared with *S1- Effect of new initiatives burden on maturing new work processes*, *S3-Effect of new initiatives burden on maturing new knowledge* possesses similarities and differences. Like S1, the base run behavior and the S31 behavior exhibit a modest difference, and the S32 behavior displays greater difference. However, the difference in S32 is higher than the difference in S12. This may be explained by the fact that knowledge requires additional time to mature, and new initiatives present a higher burden that affects it more.

Result: Pass

S4- Effect of mature knowledge on maturing new knowledge



Simulation behavior (Base: blue line, No. 1; S41: red line, No. 2; S42: green line, No. 3)

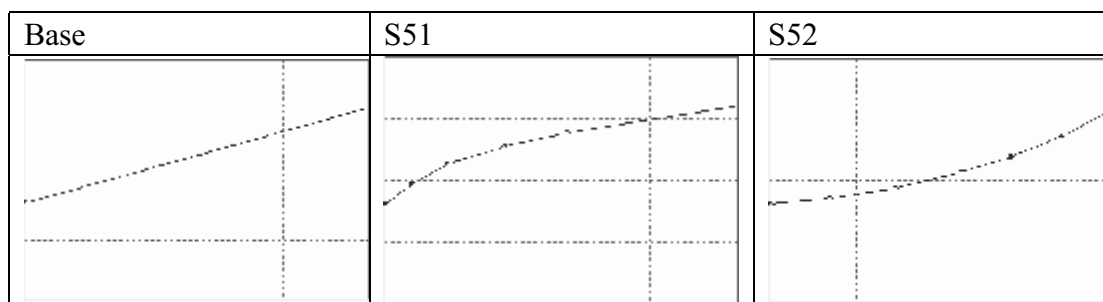


Analysis:

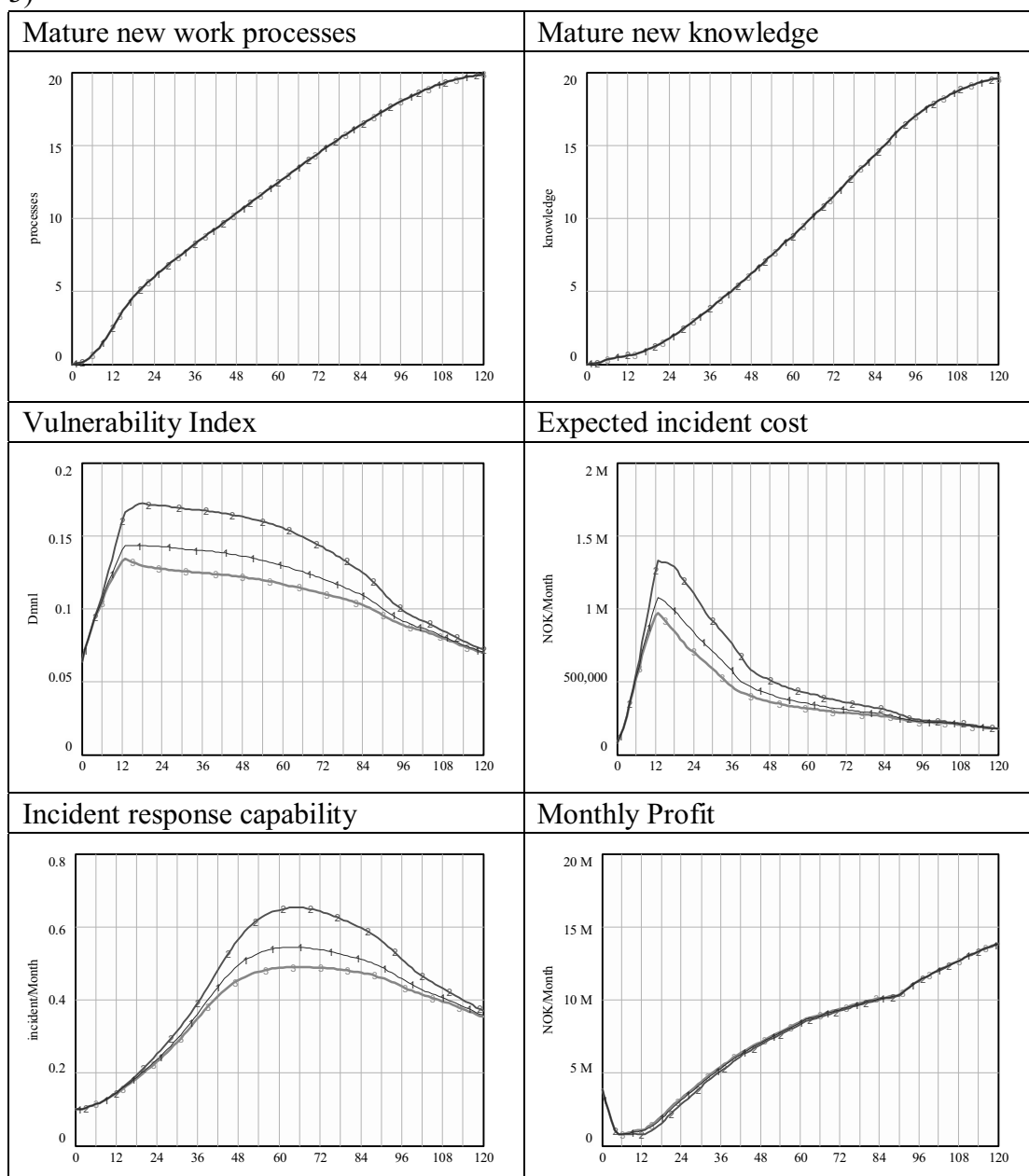
Compared with *S2 - Effect of mature new WP on maturing new WP*, the results of *S4 - Effect of mature knowledge on maturing new knowledge* are similar. However, the impact of S41 and S42 is bigger compared with the impact of S21 and S22. Considering that knowledge requires a longer time to mature, it is reasonable that S4 creates a bigger impact.

Result: Pass

S5- Effect of knowledge gap on Vulnerability Index



Simulation behavior (Base: blue line, No. 1; S51: red line, No. 2; S52: green line, No. 3)



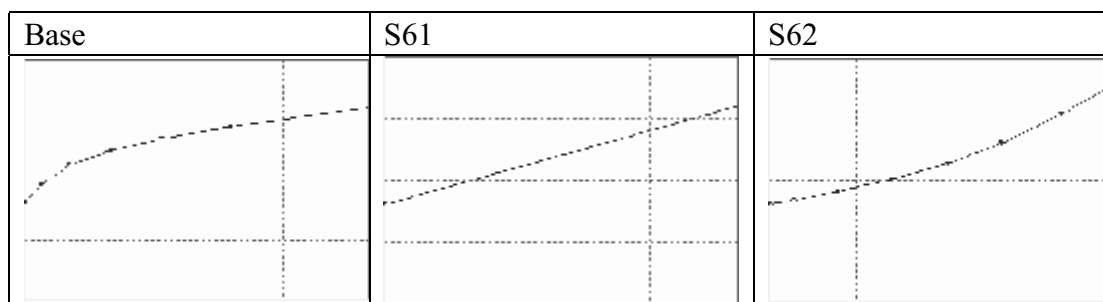
Analysis:

Change in the “Effect of knowledge gap on vulnerability index” will not affect the maturation of new work processes and knowledge, as demonstrated in the results. This variable holds a direct linkage to the “vulnerability index;” therefore, the change in this variable has an impact on the “vulnerability index.” This also leads to the corresponding change in “expected incident cost” and “incident response capability.” The impact on “monthly profit” is small.

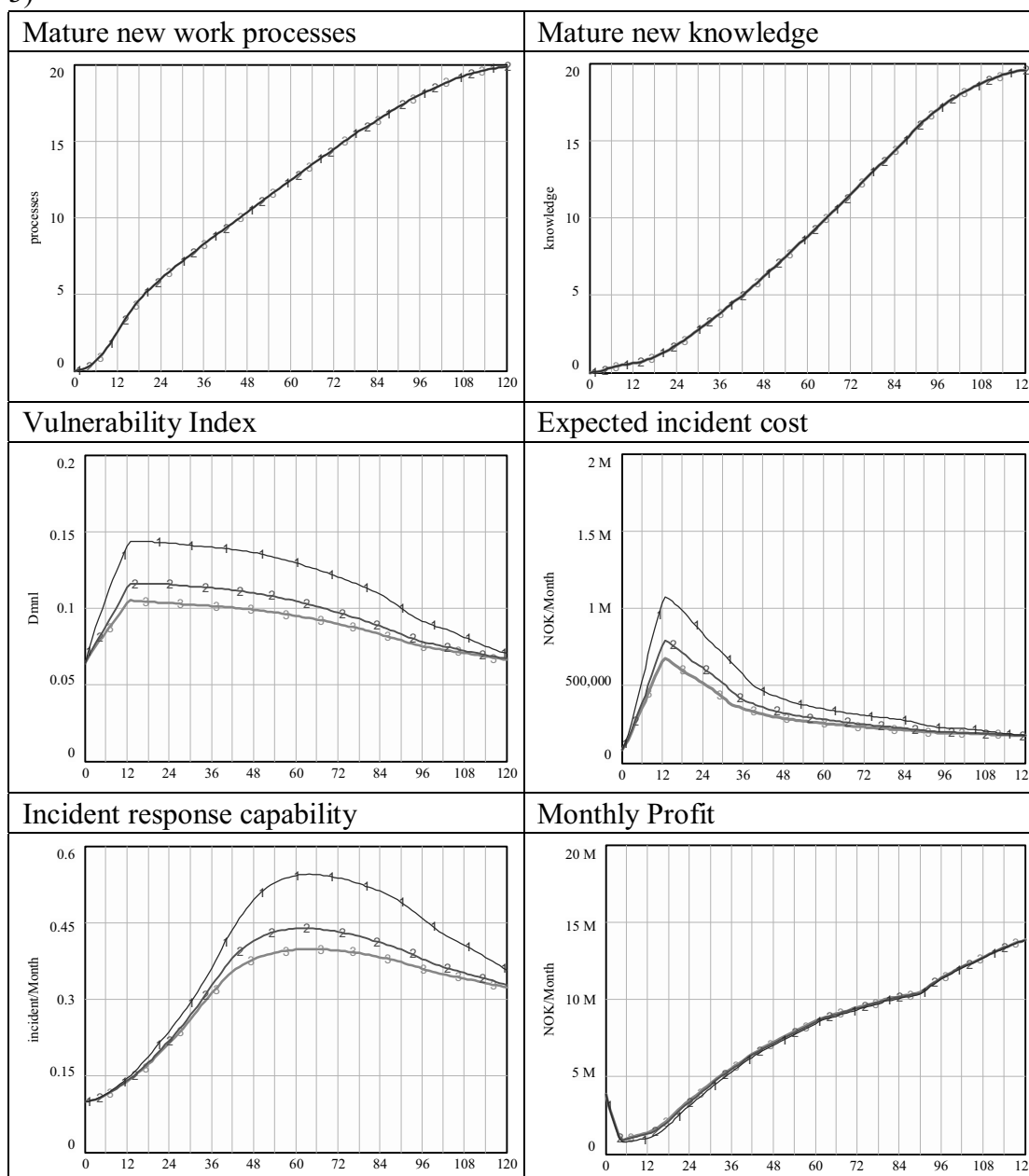
The sensitivity displayed in the model behavior is reasonable.

Result: Pass

S6- Effect of immature new knowledge on Vulnerability Index



Simulation behavior (Base: blue line, No. 1; S61: red line, No. 2; S62: green line, No. 3)



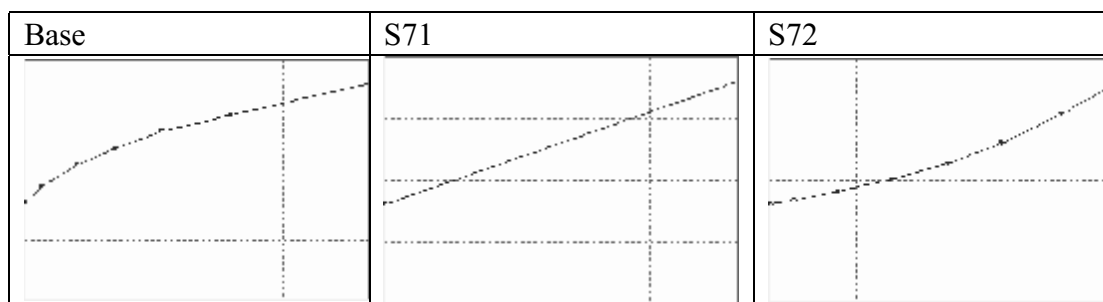
Analysis:

Change in the “Effect of immature new knowledge on vulnerability index” will not affect the maturation of new work processes and knowledge, as demonstrated in the results. This variable holds a direct linkage to the “vulnerability index;” therefore, the change in this variable has an impact on the “vulnerability index.” This also leads to the corresponding change in “expected incident cost” and “incident response capability.” The impact on “monthly profit” is small.

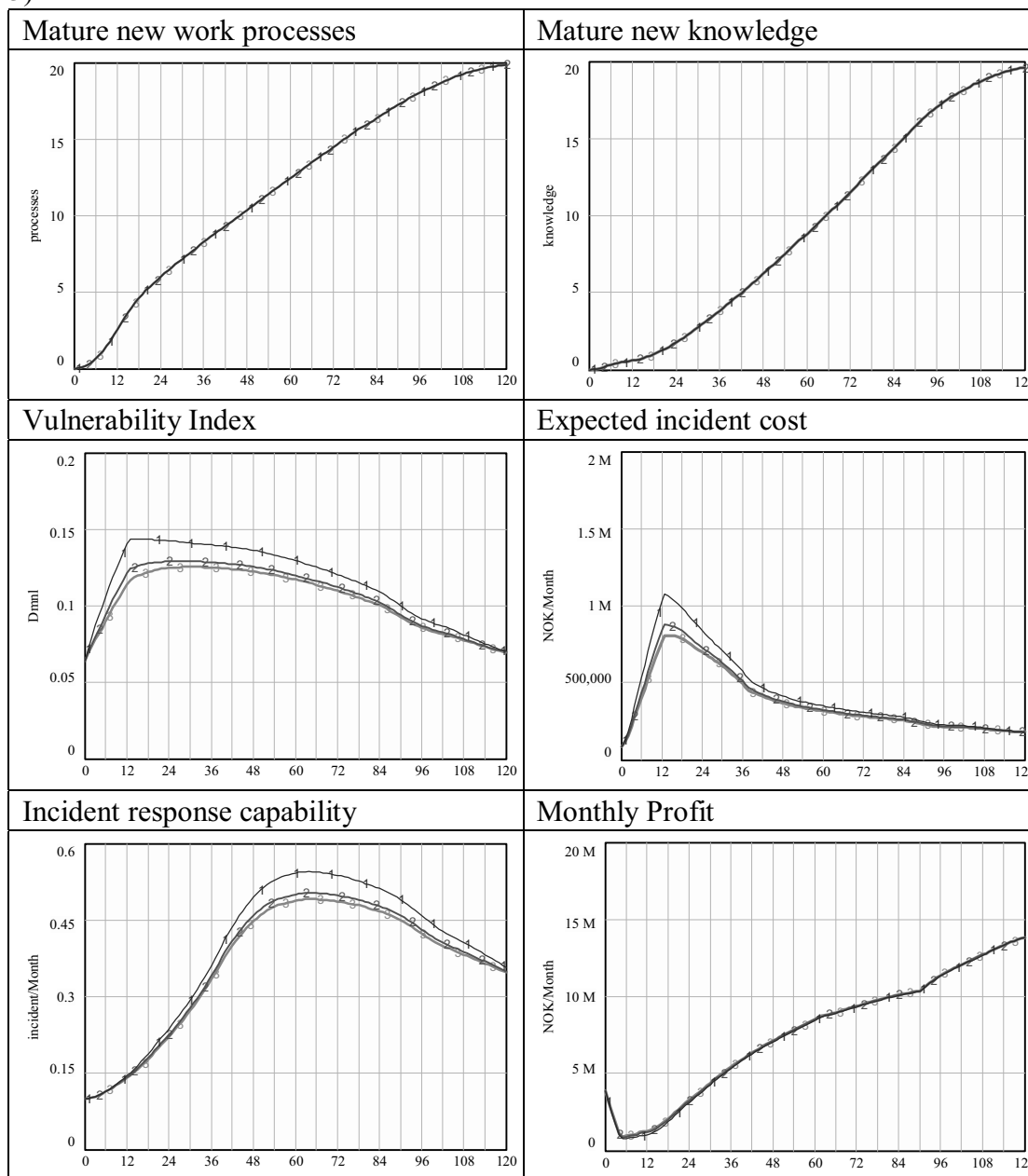
The sensitivity displayed in the model behavior is reasonable.

Result: Pass

S7- Effect of immature new WP on Vulnerability Index



Simulation behavior (Base: blue line, No. 1; S71: red line, No. 2; S72: green line, No. 3)



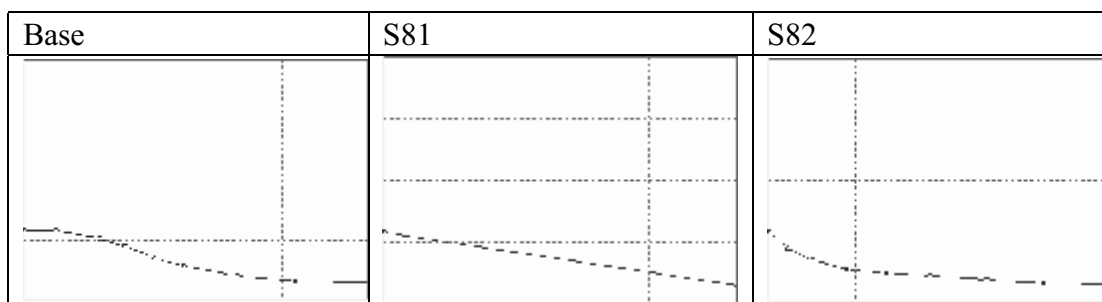
Analysis:

Change in the “Immature new WP on vulnerability index” will not affect the maturation of new work processes and knowledge, as demonstrated in the results. This variable holds a direct linkage to the “vulnerability index;” therefore, the change in this variable has an impact on the “vulnerability index.” This also leads to the corresponding change in “expected incident cost” and “incident response capability.” The impact on “monthly profit” is small.

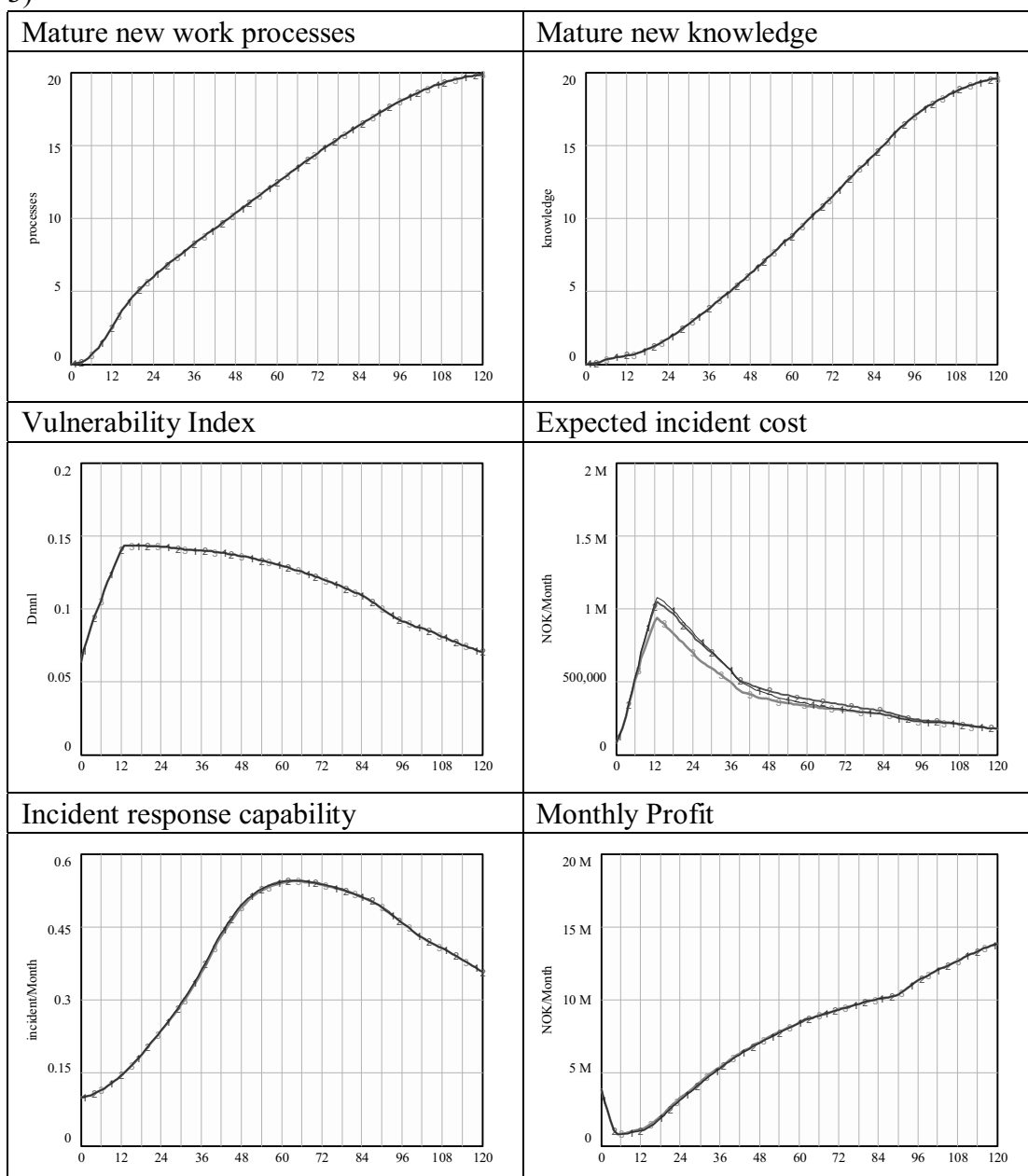
The sensitivity displayed in the model behavior is reasonable.

Result: Pass

S8- Effect of resilience on severity



Simulation behavior (Base: blue line, No. 1; S21: red line, No. 2; S22: green line, No. 3)



Analysis:

Change in the “Effect of resilience on severity” will not affect the maturation of new work processes and knowledge. Neither will it affect the “vulnerability index”. This variable holds a direct linkage to the “severity of incidents,” therefore the change in this variable has an impact on the “expected incident cost,” which slightly impacts the “monthly profit”.

The sensitivity displayed in the model behavior is reasonable.

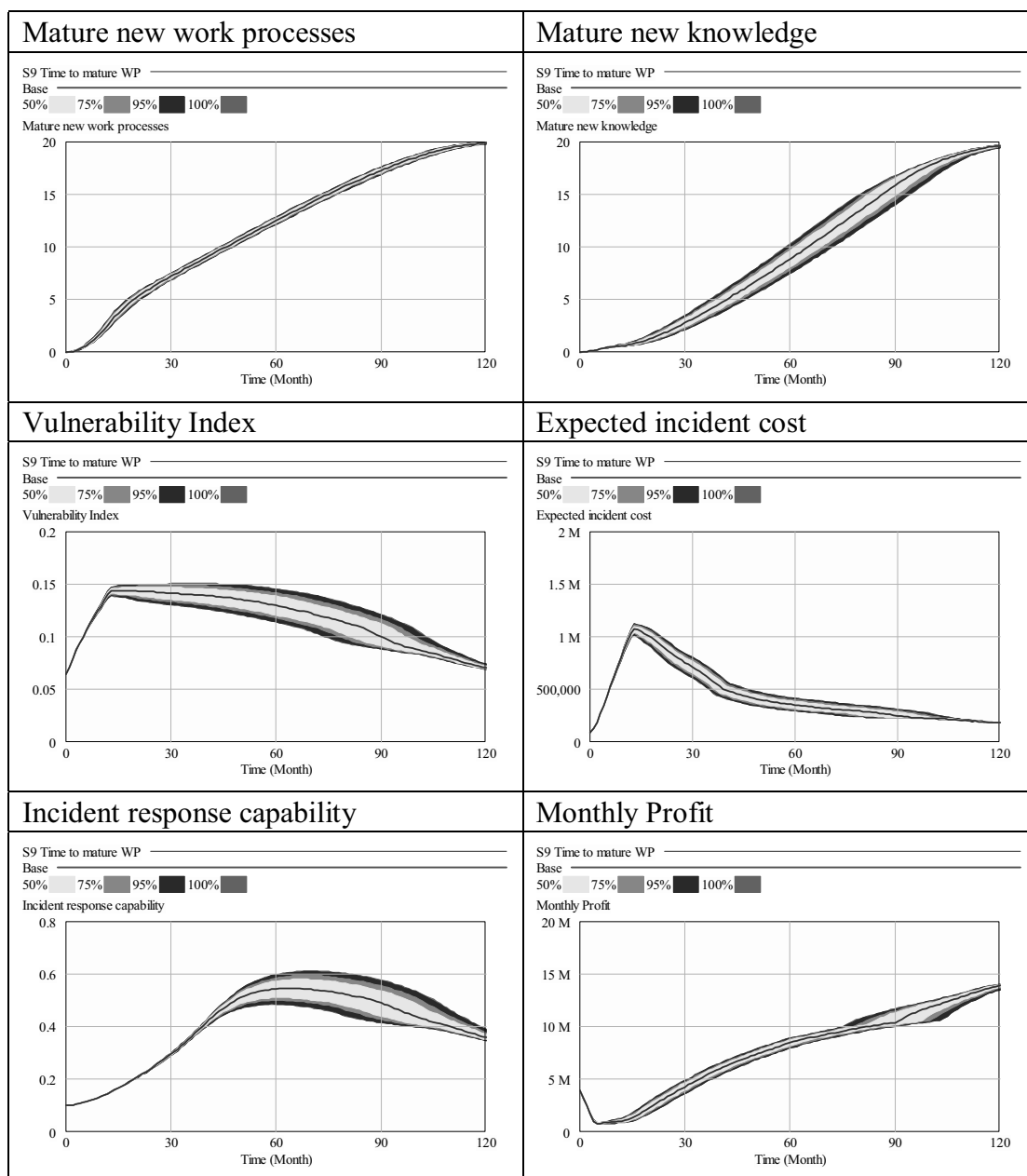
Result: Pass

S9- Time to mature new work processes

Base run: Time to mature new work processes = 4

Sensitivity test: Range: 3-5; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The “mature new work processes” does not change much. When the “time to mature new work processes” is long/short, more/fewer resources will be allocated to work on

the maturation of new work processes. Thus, the change of time to mature new work processes will not greatly affect mature new work processes. Yet when more/fewer resources are allocated to mature new work processes, fewer/more resources are left to mature knowledge. Therefore, the change time to mature new work processes has a bigger impact on “mature new knowledge” than on “mature new work processes”. Different mature knowledge level affects vulnerability level. Therefore, the “vulnerability index” also varies in a certain range. The impact passes onto “expected incident cost”, “Incident Response Capability” and “monthly profit”.

Numerical sensitivity is observed in “mature new knowledge”, “vulnerability index”, “expected incident cost”, “incident response capability” and “monthly profit”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

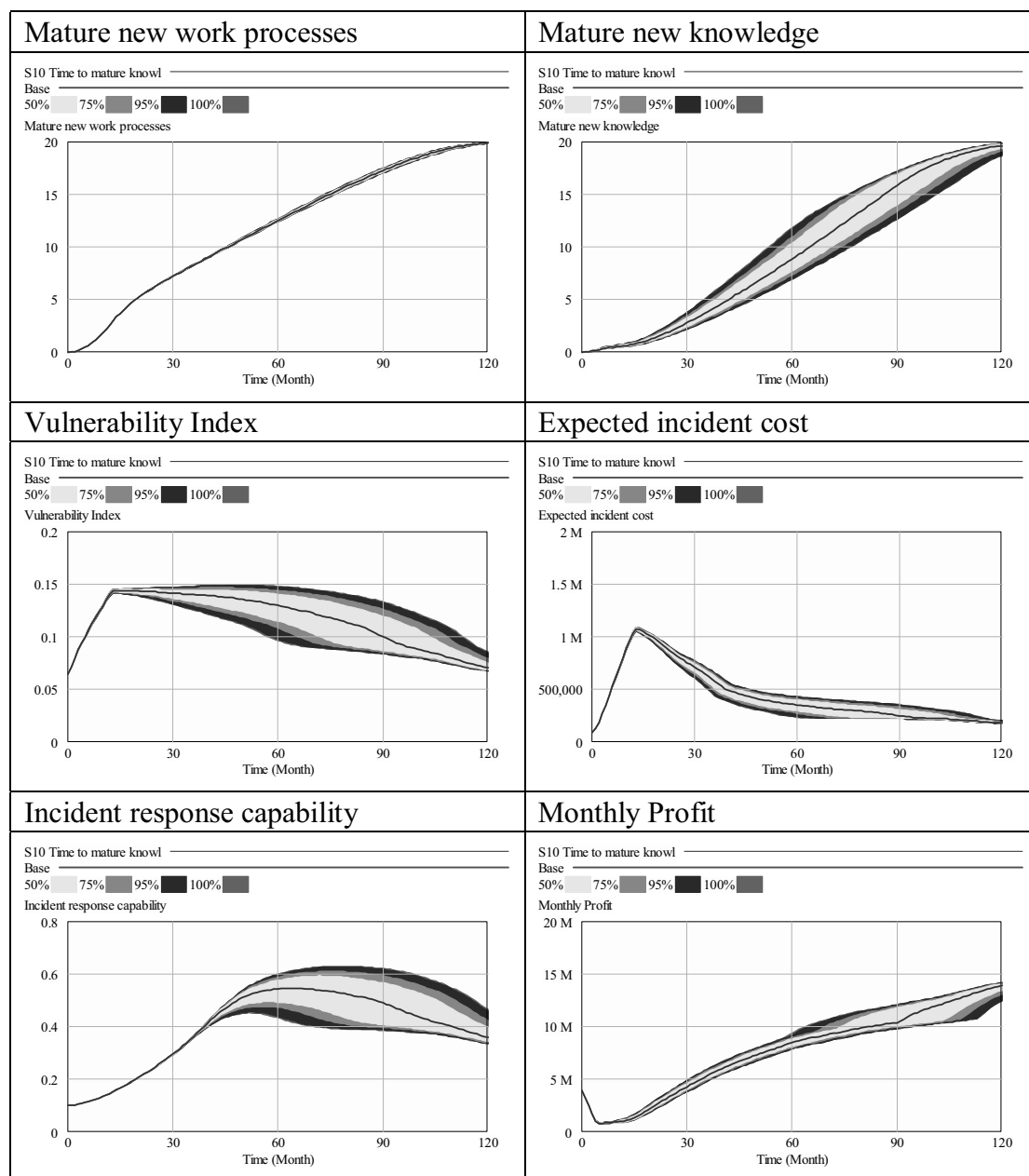
Result: Pass

S10- Time to mature new knowledge

Base run: Time to mature new knowledge = 8

Sensitivity test: Range: 6-10; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The change of “time to mature new knowledge” has little impact on “mature new work processes”. Yet it has direct impact on “mature new knowledge”. If the time to

mature new knowledge is longer/shorter, the mature new knowledge develops slower/faster. Thus, the behavior of mature new knowledge is in certain range. Different mature knowledge level affects vulnerability level. Therefore, the “vulnerability index” also varies in a certain range. The impact passes onto “expected incident cost”, “Incident Response Capability” and “monthly profit”.

Numerical sensitivity is observed in “mature new knowledge”, “vulnerability index”, “expected incident cost”, “incident response capability” and “monthly profit”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

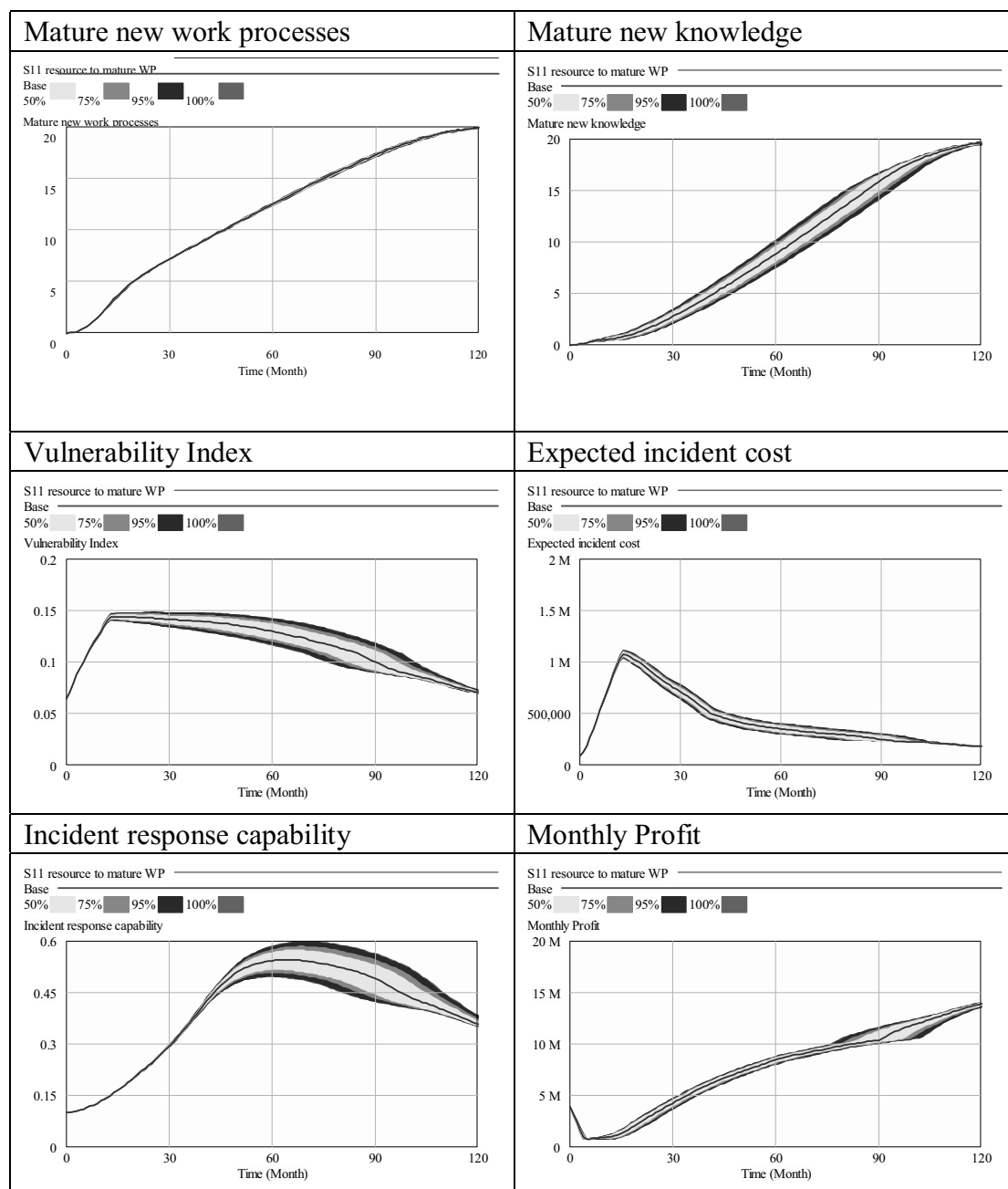
Result: Pass

S11- Operator resources for maturing each WP

Base run: Resources for maturing each WP = 0.04 (4% of the operator’s time)

Sensitivity test: Range: 0.03-0.05; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The change of “Resources for maturing each WP” has little impact on the “mature new work processes,” because no matter how many resources are needed for maturing each WP, enough resources will be allocated to mature new work process. But it affects “mature new knowledge”. When more/fewer resources are allocated to mature new work processes, fewer/more resources are left to mature knowledge, therefore, the mature new knowledge will develop slower/faster. Different mature knowledge level affects vulnerability level. Therefore, the “vulnerability index” also varies in a certain range. The impact passes onto “expected incident cost”, “Incident Response Capability” and “monthly profit”.

Numerical sensitivity is observed in “mature new knowledge”, “vulnerability index”, “expected incident cost”, “incident response capability” and “monthly profit”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

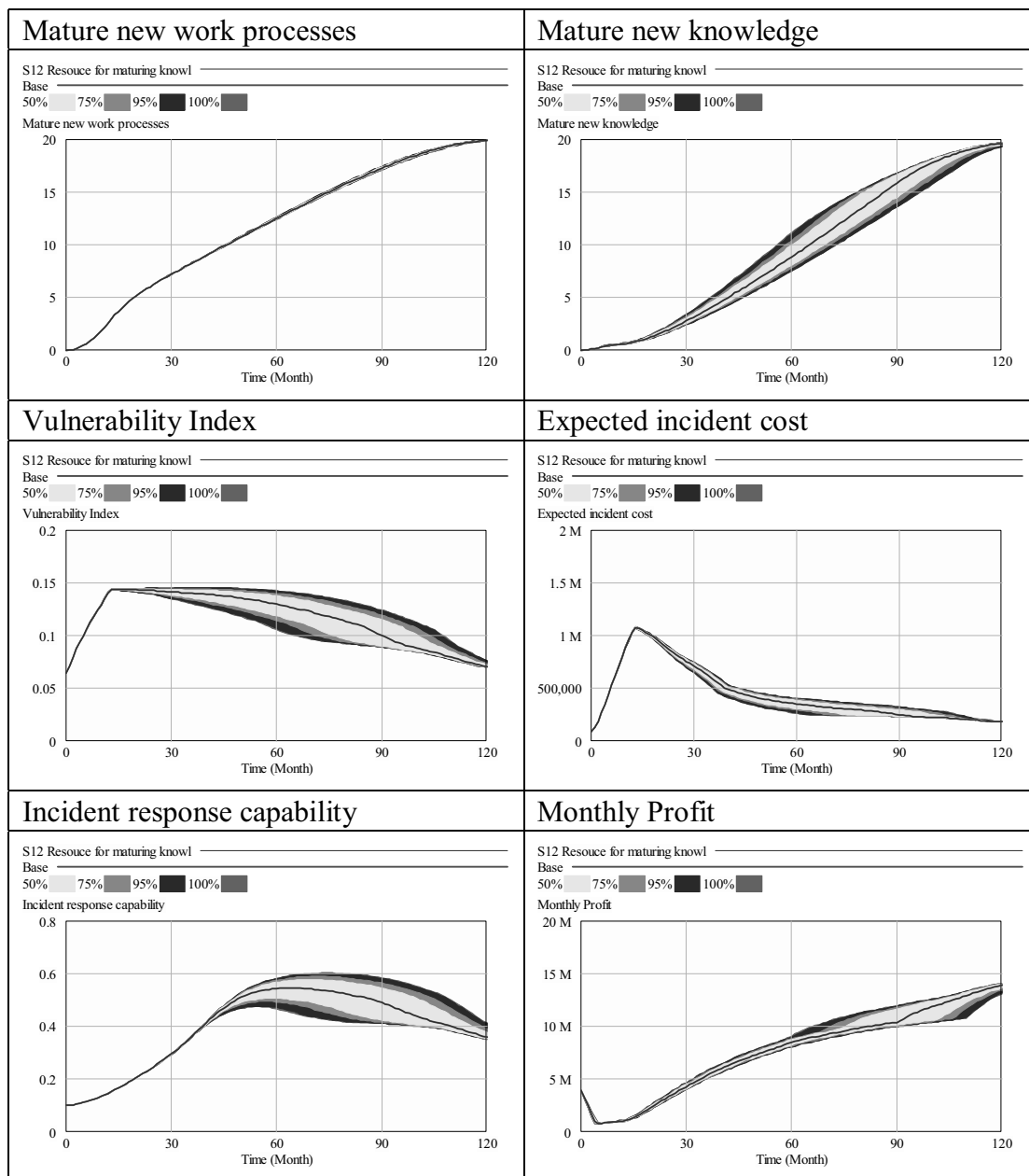
Result: Pass

S12- Operator resources for maturing each knowledge unit

Base run: Resources for maturing each knowledge = 0.04 (4% of the operator’s time)

Sensitivity test: Range: 0.03-0.05; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The change of “resources for maturing each knowledge unit” has little impact on “mature new work processes”. Yet it has direct impact on “mature new knowledge”. If the resources for maturing each knowledge unit are larger/smaller, the mature new knowledge develops slower/faster. Thus, the behavior of mature new knowledge is in certain range. Different mature knowledge level affects vulnerability level. Therefore, the “vulnerability index” also varies in a certain range. The impact passes onto “expected incident cost”, “Incident Response Capability” and “monthly profit”.

Numerical sensitivity is observed in “mature new knowledge”, “vulnerability index”, “expected incident cost”, “incident response capability” and “monthly profit”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

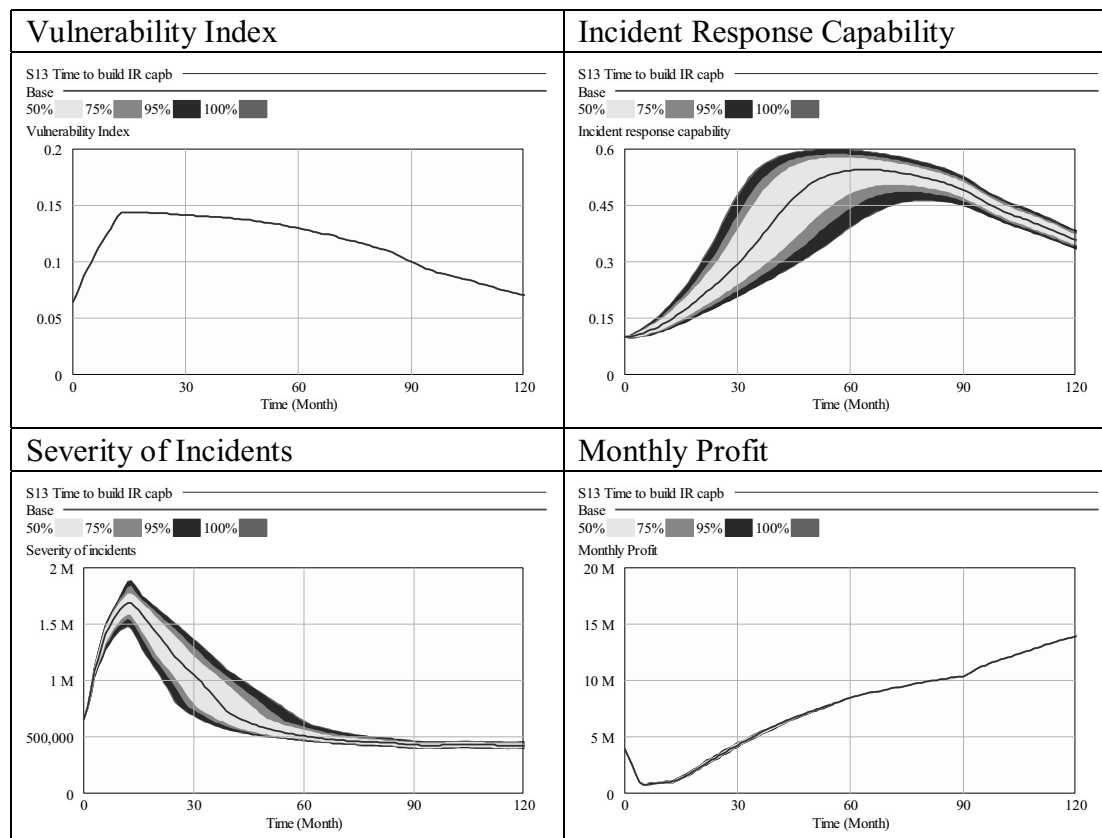
Result: Pass

S13- Time to adjust IR capability

Base run: Time to build up IR capability = 3 (month)

Sensitivity test: Range: 2-4; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The change of “time to build up IR capability” does not affect the operation transition. Mature new work processes and mature new knowledge do no change. As a result, the vulnerability index does not change either. Yet the “time to build up IR capability” has a direct impact on the incident response capability. If time to build up IR capability is longer/shorter, the incident response capability will be lower/higher. When the incident responds capability is lower/higher, the frequency of incidents will be higher/lower. We can see both of these variables, “incident response capability” and “severity of incidents” vary in certain range. The monthly profit is only slightly affected because the change of expected incident cost.

Numerical sensitivity is observed in “incident response capability” and “severity of incident”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

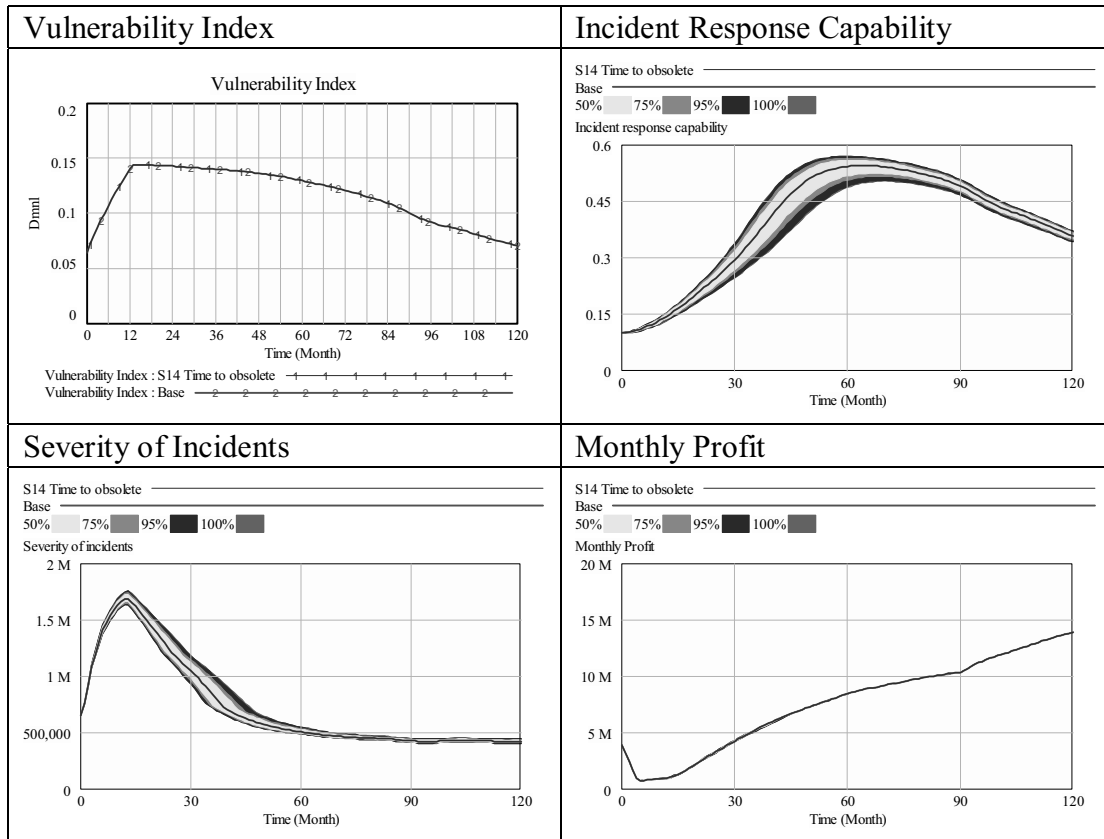
Result: Pass

S14- Time to obsolete IR capability

Base run: Time to obsolete = 12 (month)

Sensitivity test: Range: 10-14; Distribution: Random Uniform; Runs: 200;

Simulation behavior:



Analysis:

The change of “time to obsolete” does not affect the operation transition. Mature new work processes and mature new knowledge do no change. As a result, the vulnerability index does not change either. Yet the “time to obsolete” has a direct impact on the incident response capability. If time to build up IR capability is longer/shorter, the incident response capability will be higher/lower. When the incident responds capability is higher/lower, the frequency of incidents will be lower/higher. We can see both of these variables, “incident response capability” and “severity of incidents” vary in certain range. The monthly profit is only slightly affected because the change of expected incident cost.

Numerical sensitivity is observed in “incident response capability” and “severity of incident”. But no pattern sensitivity found. The numerical sensitivity is reasonable regarding the structure of the system.

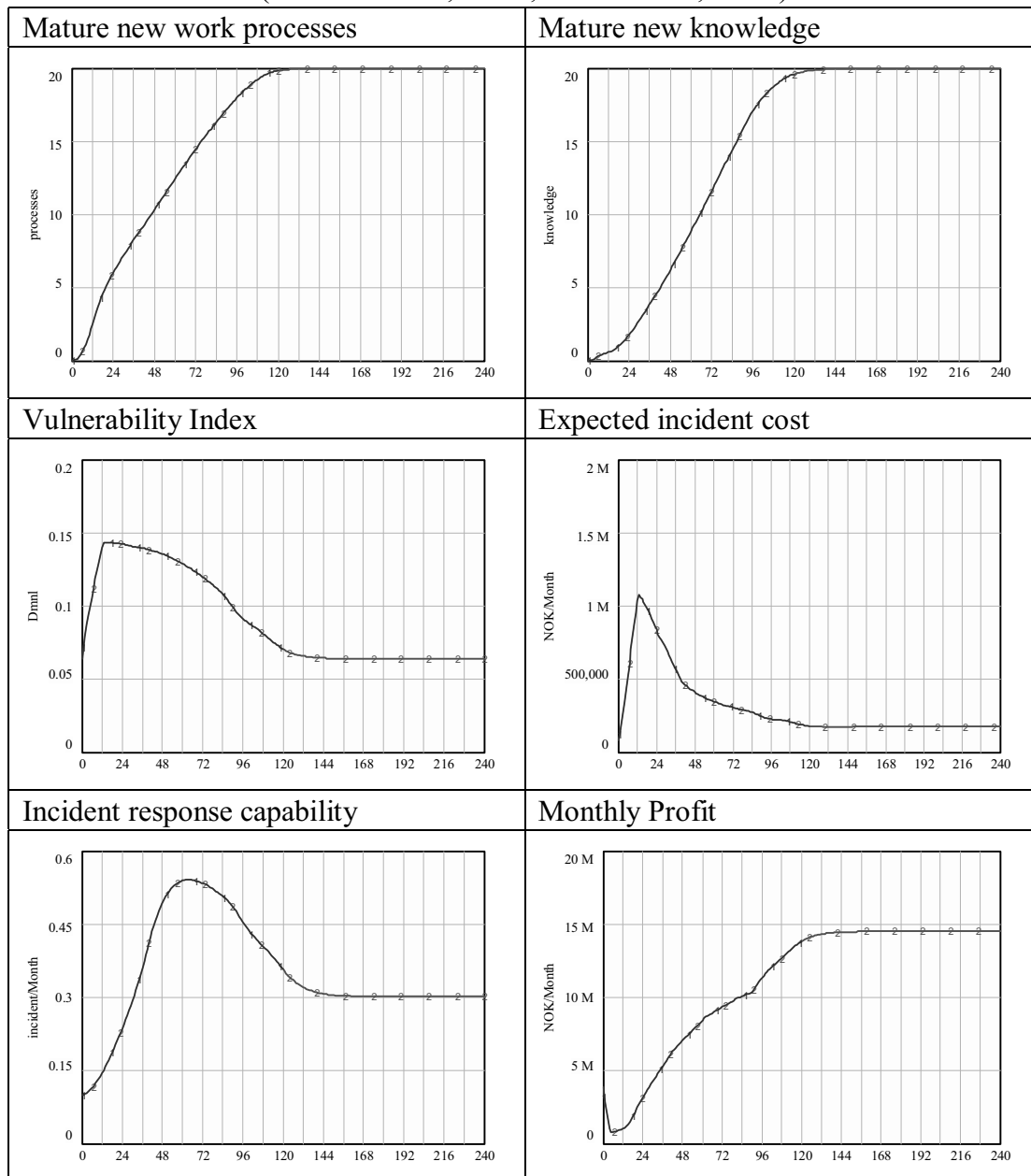
Result: Pass

S15- Extending the run time of the model

Base run: run time=120 (month)

Sensitivity test: run time=240 (month)

Simulation behavior (Base: blue line, No. 1; S15: red line, No. 2)



Analysis:

As the operation transitions is completing in 10 years time, we expect that the behavior in month 120-240 will be mostly stabilized.

Result: Pass

Appendix V Model validation interview booklet

Introduction

The purpose of this research project is to look for policies to mitigate information security risks during transition to Integrated Operations (IO) in the Norwegian Oil and Gas Industry. IO applies advanced information communication technology to increase remote onshore operation. The transition from traditional offshore operation to IO covers a long time span (10-12 years), evolves many work processes and has a perplex impact on information security risks. We have developed a system dynamics model to investigate this complicated process.

The model is grounded on the information from one pilot platform implementing IO, related experts and literatures. We need your help to review and comment on model behaviors. We will perform face-to-face interviews. (In case of unable to meet in person, telephone interview will be conducted.) The expected length of the interview is 3 hours.

Before the interview, please review section 1—background information (P 2-5). There is an indicator where to stop. We will talk through the remaining part of this booklet. When we speak, I will show you some model behaviors and ask your reaction to them.

There are no right or wrong answers – your comments and questions about what you see are the important data for the project.

Thank you for your participation. If you have any questions about this research, please feel free to contact me at ying.qian@uia.no

Ying Qian

Section 1 Background information

1. Transition to Integrated Operations

Integrated Operations (IO) adopts advanced computer control and communications technology to optimize production and reduce costs. Thus, it can extend the life time of mature platform and generate huge financial benefits. Yet changing from separated offshore operation to connected remote operation introduces information security risks. Oil and Gas Companies are in the hazardous Industry. Incidents could cause huge damage, not only financial loss but also threatening health, safety and environment (HSE). Therefore, the Norwegian Oil and Gas Company is cautious in moving into IO. One pilot platform started transition to IO in 2005.

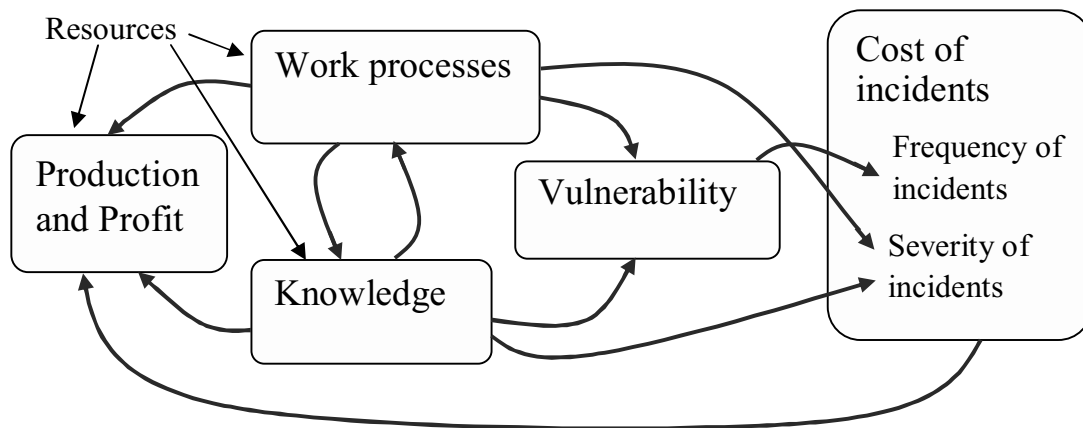
On this platform, there are 20 new work processes to be implemented. Each new work process has a set of new knowledge related to it¹⁰. The plan is to implement 5 new work processes related to production in the first year. Afterwards, new work processes related to maintenance, vendors and suppliers will be implemented at the pace of 2 new work processes every year. New work processes with advanced technology provide potentials to improve performance. New knowledge ensures the realization of these potentials. New work processes and related knowledge work together to improve production, reduce cost and make the platform more profitable.

When work processes and related knowledge are newly implemented, they are immature. It takes time to mature new work processes and knowledge. (An example explaining immature new work processes and immature knowledge, mature new work processes and mature knowledge at footnote¹¹) The maturation of new work processes and knowledge are interacting. The quicker the immature work processes matures, the quicker the immature new knowledge matures and vice versa. However, there is also

¹⁰ 'Work process' is the abstracted procedures, about what to do. 'Knowledge' is the detailed routines to perform the work, about how to do. For example, "8am-8:30am, offshore control center and onshore control center have a videoconference to make daily production plan" is a work process. How each participants work cooperatively in the meeting is knowledge.

¹¹ Example: Operation transition could be seen as asking people to go a new way to some place. You need to give people a map (new work process) and tell them how to go (new knowledge). On the first trip, they check frequently with the map to see where to go (new work process is immature) and think about your instructions of how to go (new knowledge is immature). It takes much more efforts to reach the place than necessary. (These efforts are used to mature new work processes and knowledge.) After several trips, people are able to go without a map (work process is mature). However, they still need to cautiously think about how to go, checking out the signs and etc. After some trips, they become so familiar with the new way that it seems they reach there without using their brain (knowledge is mature).

resource conflict. Resources (in terms of the operator's working hour) will be allocated to production, maturation of new work processes, and maturation of new knowledge. The resources needed to meet production target has the first priority. The remaining resources will be used to mature new work processes and then the remaining resources will be used to mature new knowledge. The following figure briefly summarizes these relationships.



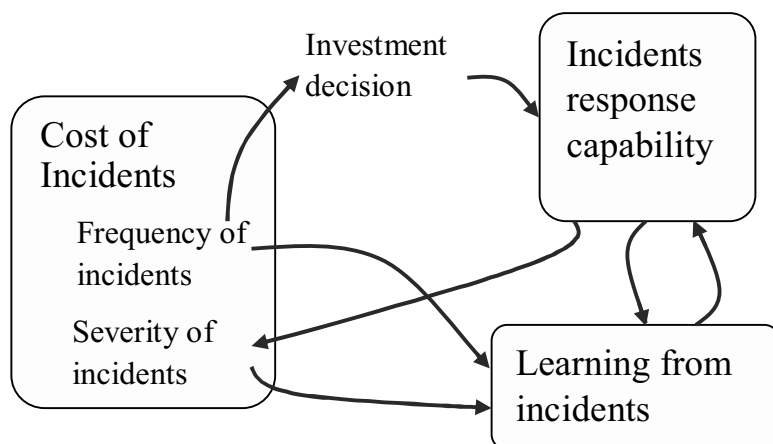
Many literatures point out that it takes longer time to mature knowledge than to mature work process. (See the example at Footnote 2 Page 2) Therefore, a knowledge gap will be generated when new work processes are implemented. This knowledge gap makes the system vulnerability increase. Things are more likely to go wrong when we do not know them well. The system is more vulnerable when a lot of immature new work processes and immature new knowledge are in place. High vulnerability leads to more incidents, increasing cost of incidents and reducing profit.

The IO will make the system more resilient. When new work processes and knowledge are mature, the severity of incidents will decrease. However, when new work processes and knowledge are immature, the severity of incidents will increase. The change of the severity of incidents impacts the cost of incidents and the profit too.

2. Incidents response capability

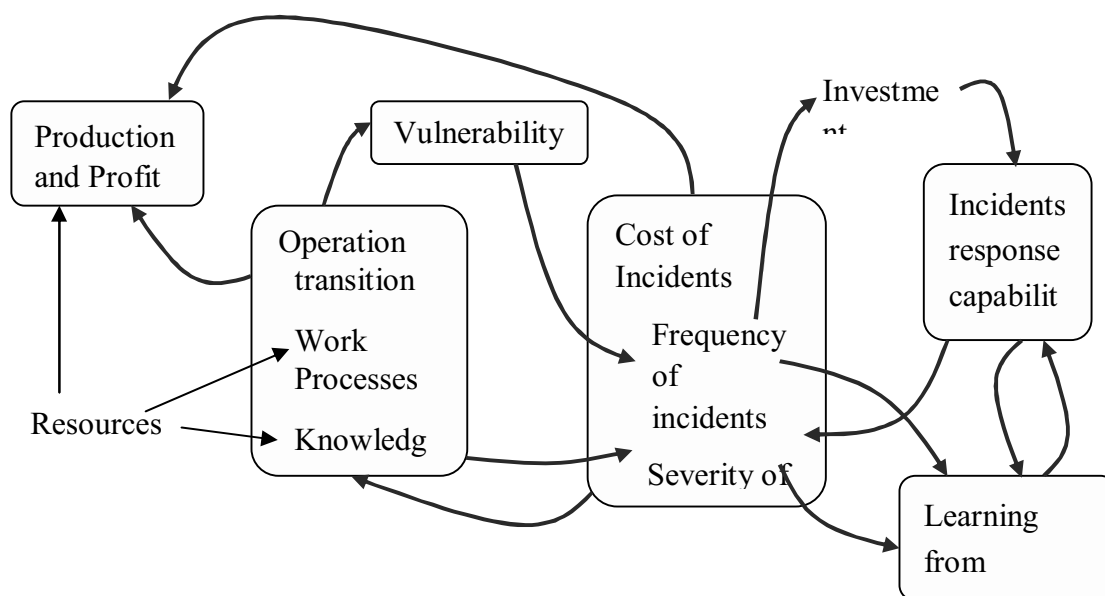
When more incidents happen, people perceive an increasing security risk and the management team will make investment decision to build up incidents response capability to handle incidents. It takes time to build up incidents response capability. The higher incidents response capability, the lower the severity of incidents will be. People learn from incidents. The severer the incident is, the more people learn from it.

Learning from incidents improves incidents response capability. The following figure briefly summarizes the relationship.



3. The whole picture and the system dynamics model

We build a system dynamics model representing the above mentioned structure. The transition to IO has impact on many areas: production, cost, frequency of incidents, severity of incidents and etc. Some of the impacts are desirable while some are not. The desired output, a successful operation transition, is defined as increased profit without major incidents.



In the following sections, I will show you up to six scenarios, depicting results of the transition to IO under different management policies. These scenarios are:

Scenario 1: Base—What will happen under the current policy?

Scenario 2: Focus on production—What will happen if more resources are allocated to production?

Scenario 3: Focus on knowledge—What will happen if more resources are allocated to mature knowledge?

Scenario 4: Quicker to build IR capability—What will happen if less time is needed to build up incidents response capability?

Scenario 5: Higher initial IR capability—What will happen if the perception of risk is low at the beginning of the transition to IO?

Scenario 6: Delay transition—What will happen if the speed of transition to IO is slowed down when the cost of incidents is high?

We will focus on the behavior of following variables. Here are their definition and units:

Mature new work processes: When the operators can smoothly perform their work in the new ways, no further guidance from management team needed, we say these new work processes are matured (work processes)

Mature new knowledge: When the newly developed details of how to perform job tasks for the new work processes has fully integrated into the system and internalized to the operators, we identify them as mature new knowledge (knowledge)

Frequency of incidents: How many incidents happen in a month (incident/month)

Severity of incidents: The total cost of incidents, including the cost of disruption of production and restore the system to normal condition (NRK/incident)

Incidents response capability: How many incidents could be handled in a month (incidents/month)

Monthly profit: It represents the monthly operating income of the platform. In the model, it is calculated as Revenue - cost of production and expenditure - cost of incidents- cost of incidents response capability (NRK/month)

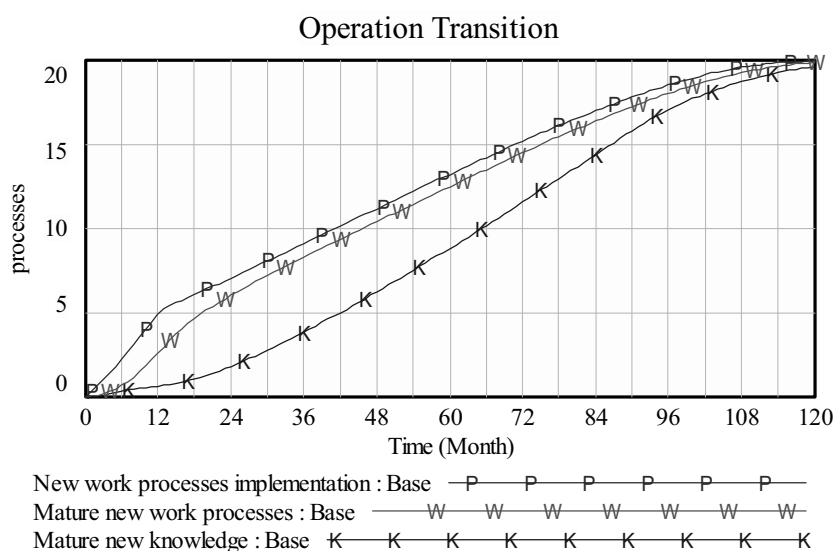
The behaviors of some other related variables are also presented as references for better understanding.

PLEASE STOP READING AT THIS POINT UNTIL THE INTERVIEW.

Scenario 1 Base

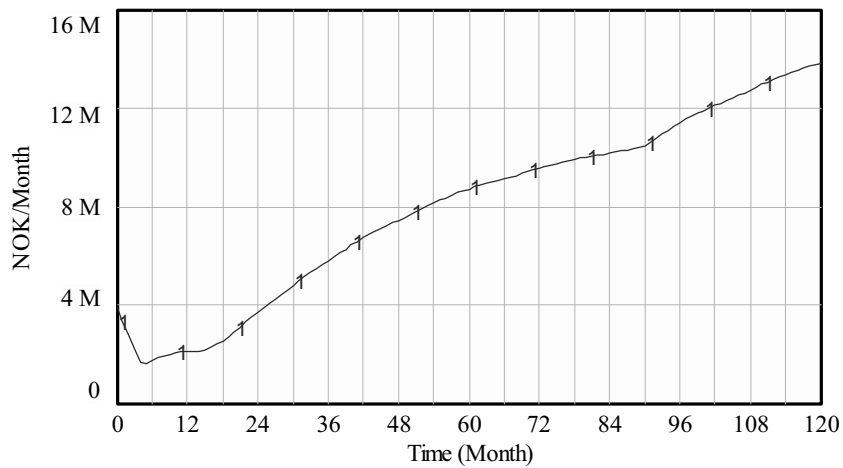
I. What happens?

- As planned, 5 new work processes are implemented in the first year and afterwards, 2 new work processes are implemented each year. It takes sometime for new work processes to mature and it takes even longer time for new knowledge to mature (panel a)
- The 'Monthly profit' decreases at the beginning and then increases. It exceeds its original level around month 30. (panel b)
- The 'Frequency of incidents' increases quickly at the beginning and stays at the high level for several years before it starts to decrease. The 'Severity of incidents' increases quickly in the first year and decreases quickly in the next three years. It is relatively stable from year 4. The 'Incidents response capability' keeps increasing in the first 5 years and then starts to decrease. (panel c, d & e)

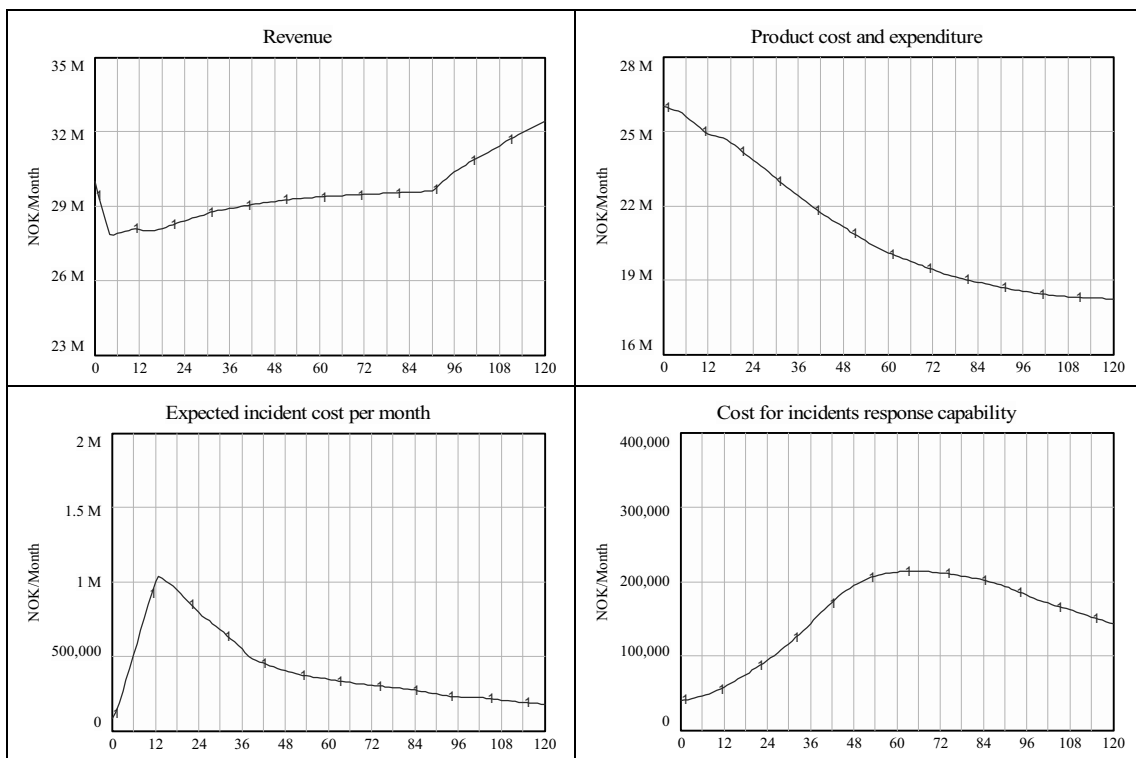


(a)

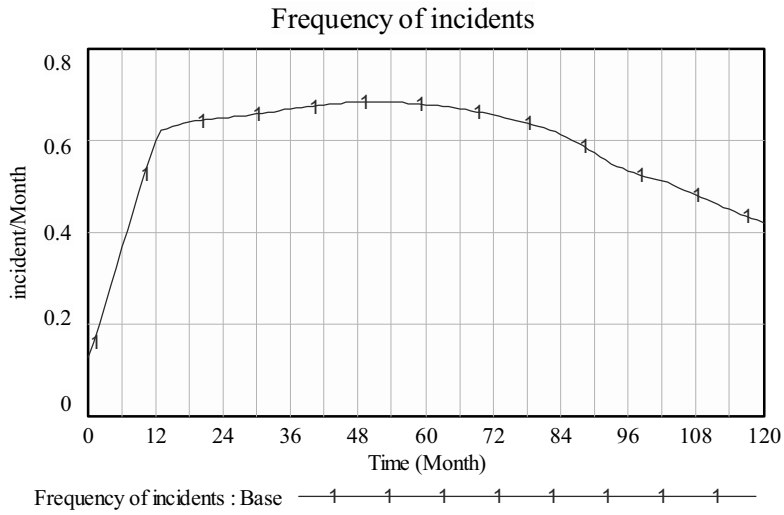
Monthly Profit



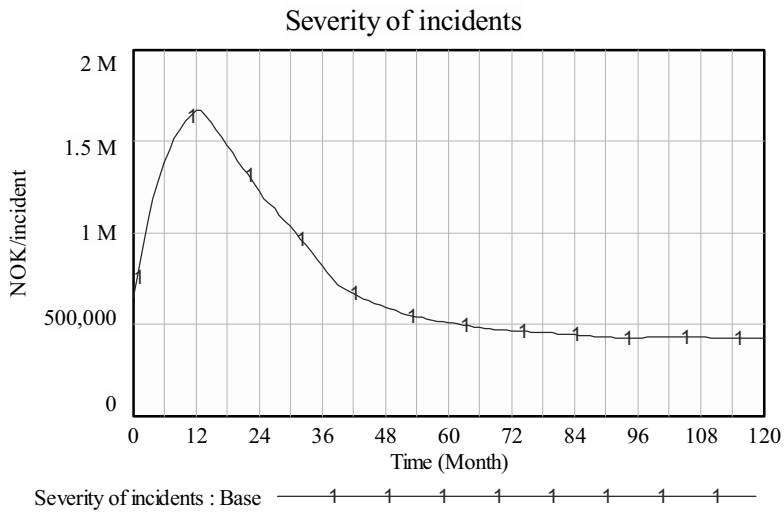
Monthly Profit : Base — 1 1 1 1 1 1 1 1 1



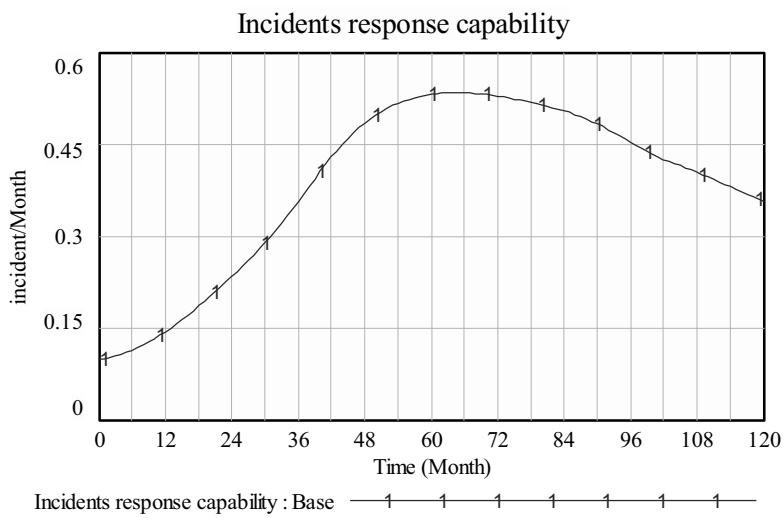
(b)



(c)



(d)



(e)

II. Your thoughts about the scenario 1 “Base”:

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel a) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel a) plausible?

Why or why not?

Q1 c) Is the behavior of *Monthly Profit* (panel b) plausible?

Why or why not?

Q1 d) Is the behavior of *Frequency of incidents* (panel c) plausible?

Why or why not?

Q1 e) Is the behavior of *Severity of incidents* (panel d) plausible?

Why or why not?

Q1 f) Is the behavior of *Incidents response capability* (panel e) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you use a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ The first year saw the most intensive operation transition, with 5 new work processes and knowledge implemented. Not enough resources to mature all of them. As mentioned, in resource conflicts, resources are first allocated to mature new work processes. Therefore, knowledge only matures very little at the beginning. From year 2, only 2 new work processes are implemented each year. The ‘mature new work processes’ steadily follow the new work processes implemented. And the ‘mature new knowledge’ gradually picks up. (panel a)
- ✓ The ‘*Monthly profit*’ drops in the first year mainly due to the drop of revenue and increase of incidents cost. Revenue drops because resources are allocated to mature new work processes and knowledge. And the increase of incidents is caused by the increase of the ‘frequency of incidents’ and the ‘severity of incidents’. The benefit of IO is small at the beginning but it increases as the operation transition continues. ‘*Revenue*’ increases and ‘*product cost and expenditure*’ decreases. And the ‘*expected incidents cost*’ also decreases as more new work processes and knowledge mature. Therefore, the ‘*Monthly profit*’ increases. It exceeds the original level. And after 6 years, the ‘*Monthly profit*’ increases quicker than before since most new work processes and knowledge are matured so that resources are released out to focus on production. (panel b)
- ✓ The traditional operation has been mature for years and the offshore platform does not use ICT technology. Therefore, the frequency of incidents is low. When new work processes using advanced ICT technology is implemented, it introduce new vulnerability to the system. The ‘frequency of incidents’ increases quickly. During the transition period, the ‘frequency of incidents’ stays at a relatively high level as new work processes are continuously

introduced. Until most of the work processes and knowledge are mature, the 'frequency of incidents' starts to decrease. (panel c)

- ✓ The '*severity of incidents*' increases sharply at the beginning since the '*incidents response capability*' is very low in the traditional operation. It takes time to realize the inadequacy of incident response capability and make investment decision and it takes time to build up incidents response capability. As the '*incidents response capability*' builds up, the '*severity of incidents*' starts to drop from year 2. The '*incidents response capability*' starts to decrease around month 60 following the decrease of frequency of incidents. And the '*severity of incidents*' stabilizes. (panel d & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

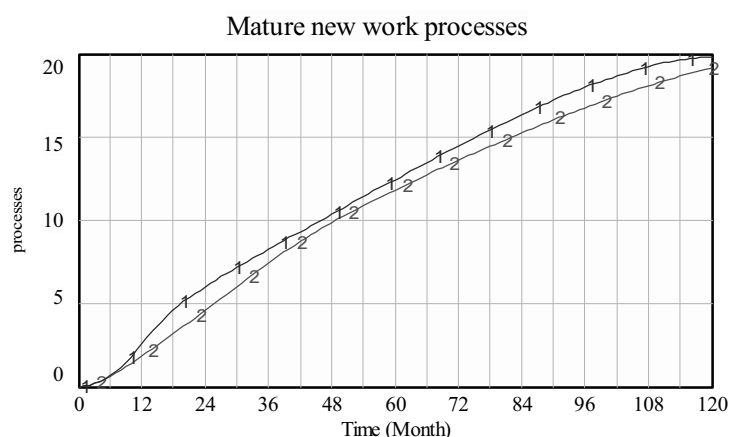
Q4: Has this explanation left out something that might be causing the results?

Scenario 2 Focus on production

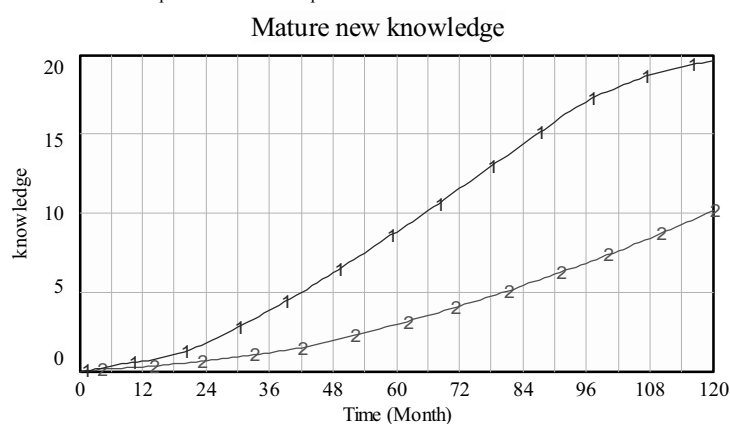
In the base scenario, the minimum resources for production are 90% of the total person hour on the platform. In this scenario, management focus more on production, the minimum resources for production are 95% of the total person hour, which means only 5% of staffs time is available to mature new work processes and knowledge.

I. What happens?

- The '*Mature new work processes*' is a little bit lower than base run. '*Mature new knowledge*' is much lower than base run (panel a)
- The '*Monthly profit*' doesn't drop as low as in the base run at the beginning but doesn't rise as high later. (panel b)
- The '*frequency of incidents*' increases sharply in the first year and keeps increasing in the following several years. The '*severity of incidents*' peaks at month 12 and reduces afterwards. The '*incidents response capability*' increases for the first several years and stays at the high level. (c, d & e)



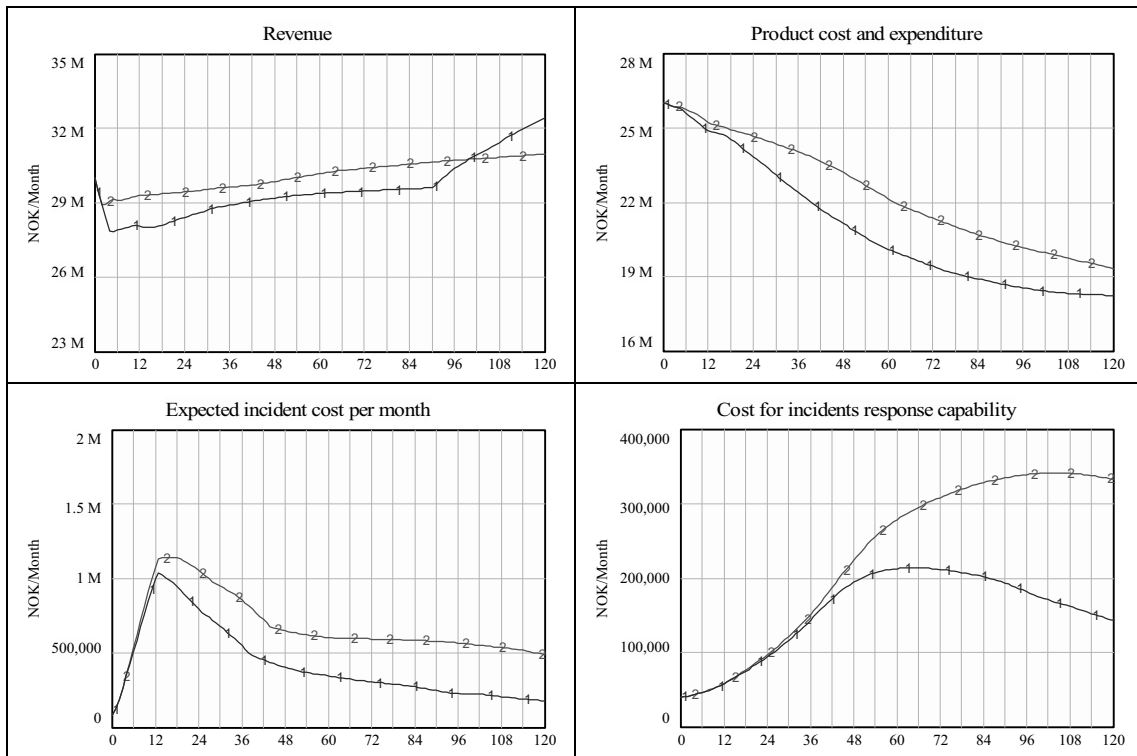
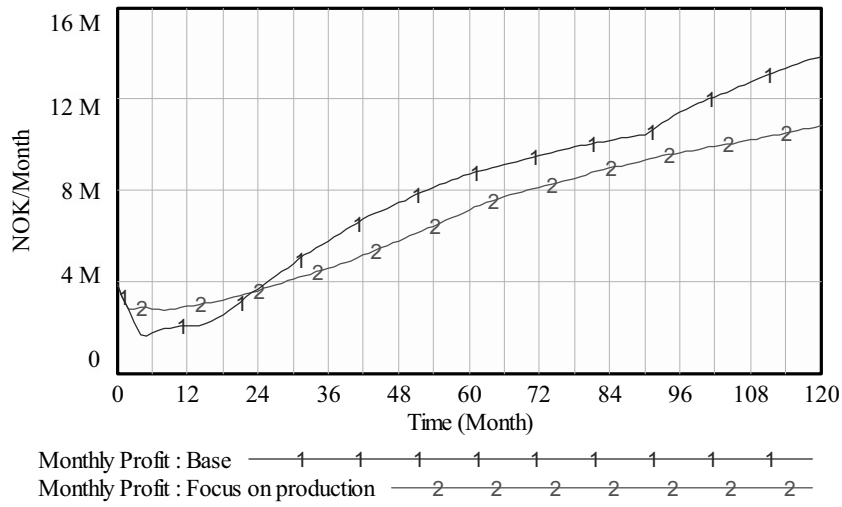
Mature new work processes : Base — 1 1 1 1 1 1 1 1
 Mature new work processes : Focus on production — 2 2 2 2 2 2 2 2



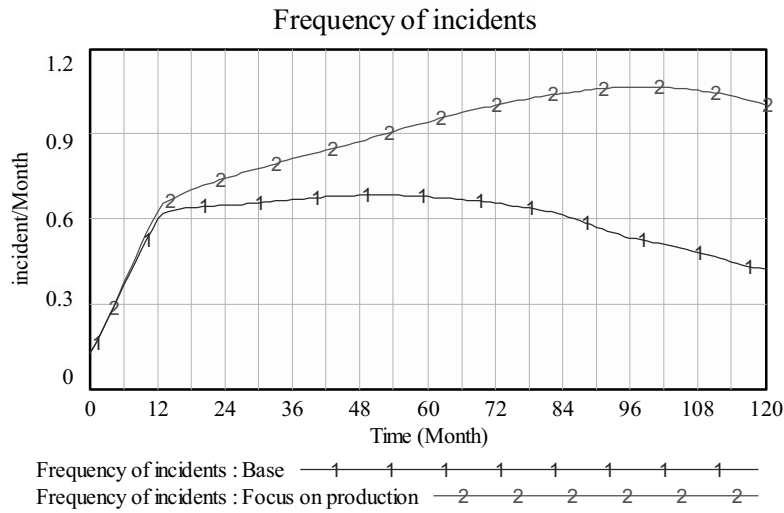
Mature new knowledge : Base — 1 1 1 1 1 1 1 1
 Mature new knowledge : Focus on production — 2 2 2 2 2 2 2 2

(a)

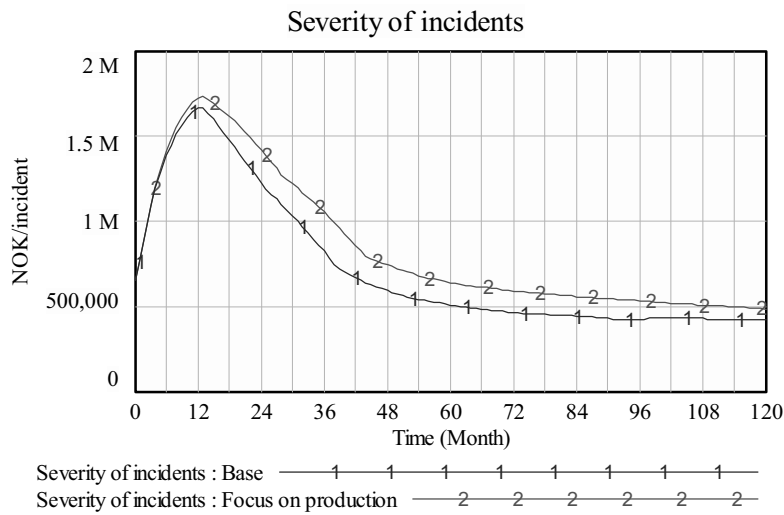
Monthly Profit



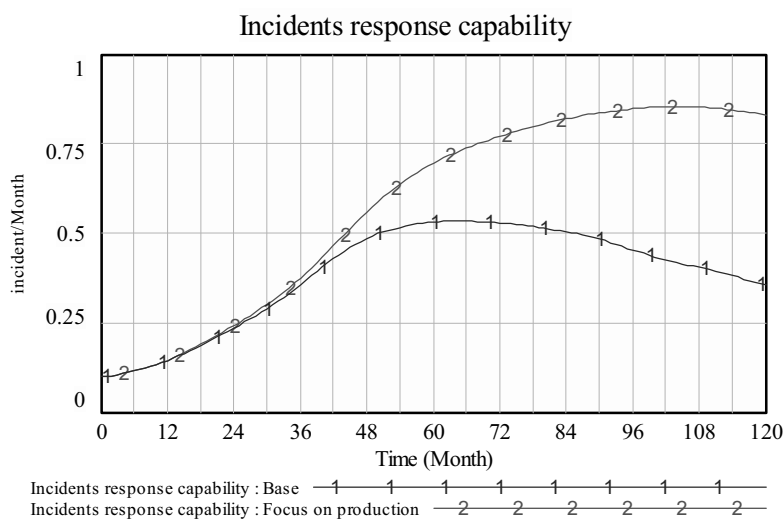
(b)



(c)



(d)



(e)

II. Your thoughts about scenario 2 “Focus on production”.

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel a) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel a) plausible?

Why or why not?

Q1 c) Is the behavior of *Monthly Profit* (panel b) plausible?

Why or why not?

Q1 d) Is the behavior of *Frequency of incidents* (panel c) plausible?

Why or why not?

Q1 e) Is the behavior of *Severity of incidents* (panel d) plausible?

Why or why not?

Q1 f) Is the behavior of *Incidents response capability* (panel e) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you use a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ Since fewer resources are available, the new work processes and knowledge mature slower than in the base run. However, in resource conflicts, resources are first allocated to mature new work processes. Therefore, the ‘mature new work processes’ are not affected much but the ‘mature new knowledge’ is greatly affected by the resource shortage. (panel a)
- ✓ The ‘*Monthly profit*’ drops not that low at the beginning because the revenue does not drop too much with minimum 95% resources reserved for production. However, it increases much slower than in the base run later because a big portion of the new knowledge is not matured, which makes the benefit of IO not able to realize. ‘*Revenue*’ doesn’t increase much and the ‘*product cost and expenditure*’ doesn’t decrease much. Besides, the ‘*expected incidents cost per month*’ is higher. The ‘*cost for incidents response capability*’ is higher due to more incidents response capability needed to handle all the incidents. (panel b)
- ✓ With less ‘*mature new knowledge*’, the system is more vulnerable. The ‘*frequency of incidents*’ keeps increasing for many years since the knowledge gap is increasing. With more incidents happening, more investment is made to improve the ‘*incidents response capability*’. The ‘*incidents response capability*’ reaches higher and thus control the ‘*severity of incidents*’. The ‘*severity of incidents*’ only peaks a little bit higher. (panel c, d, & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

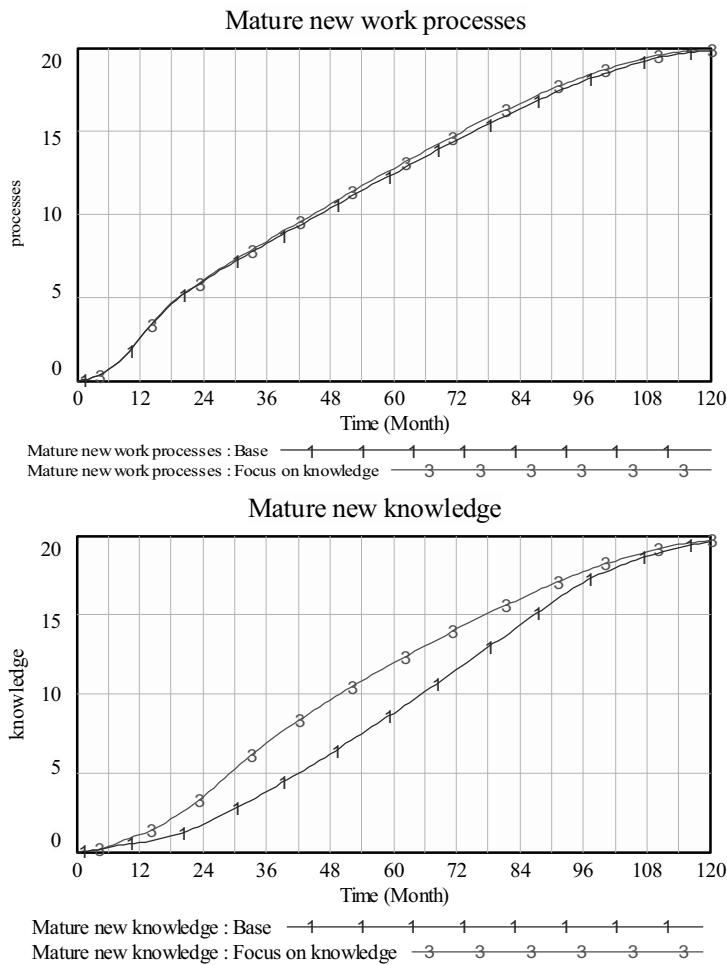
Q4: Has this explanation left out something that might be causing the results?

Scenario 3 Focus on knowledge

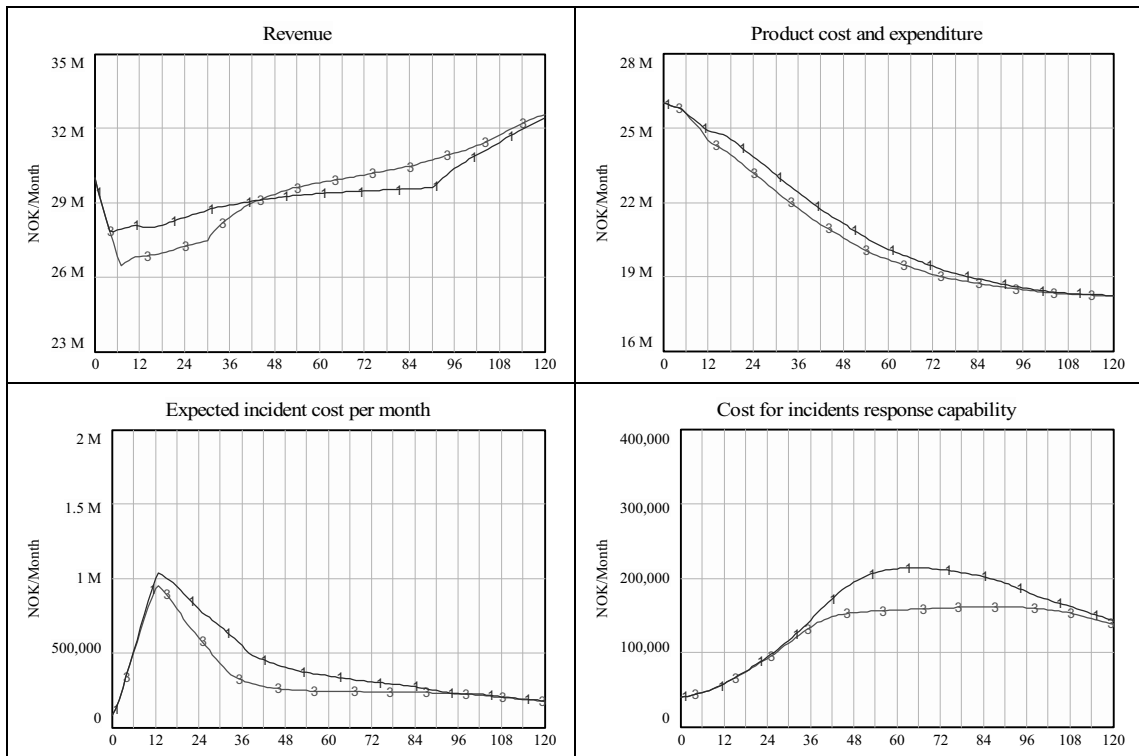
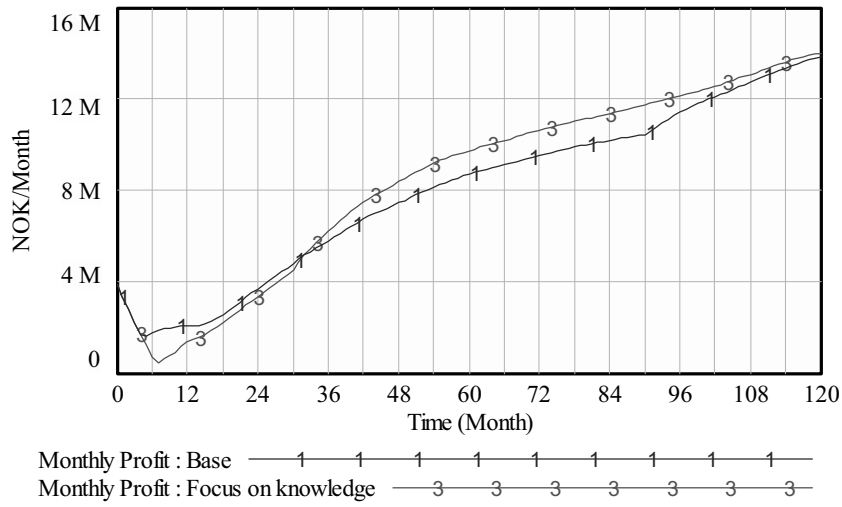
In the base scenario, the minimum resources for production are 90% of the total resources, i.e. 10% of the operators' time is to mature new work processes and knowledge. In this scenario, the minimum resources for production are reduced to 85% of the total resources so that 15% of the operators' time is released out.

I. What happens?

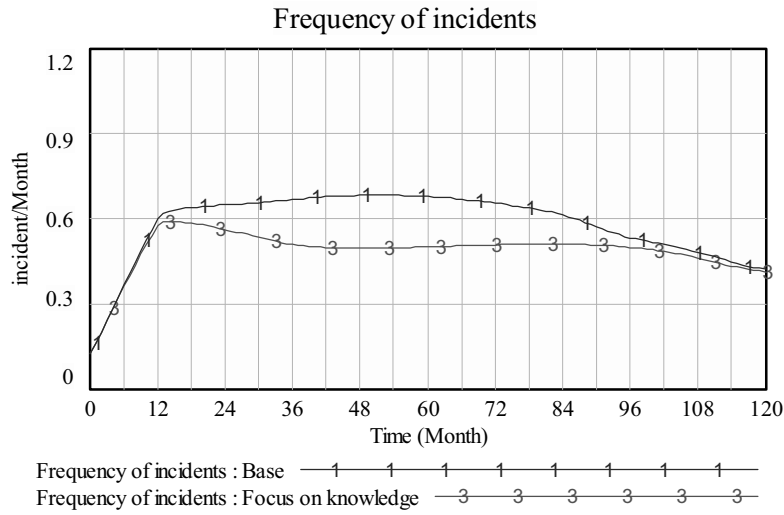
- The 'Mature new work processes' is almost the same as base run. 'Mature new knowledge' is higher than base run (panel a)
- The 'Monthly profit' doesn't drop as low as in the base run at the beginning but doesn't rise as high later. (panel b)
- The 'frequency of incidents' increases sharply in the first year and keeps increasing in the following several years. The 'severity of incidents' peaks at month 12 and reduces afterwards. The 'incidents response capability' increases for the first several years and stays at the high level. (panel c, d & e)



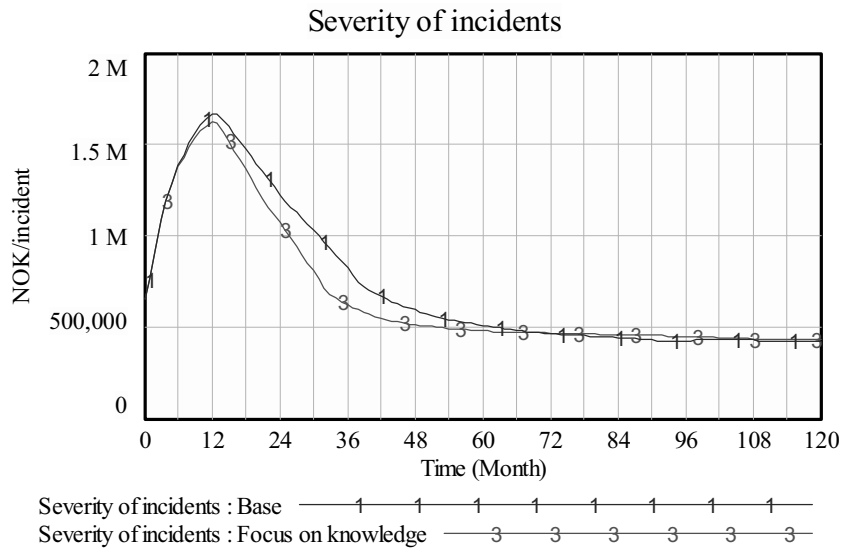
Monthly Profit



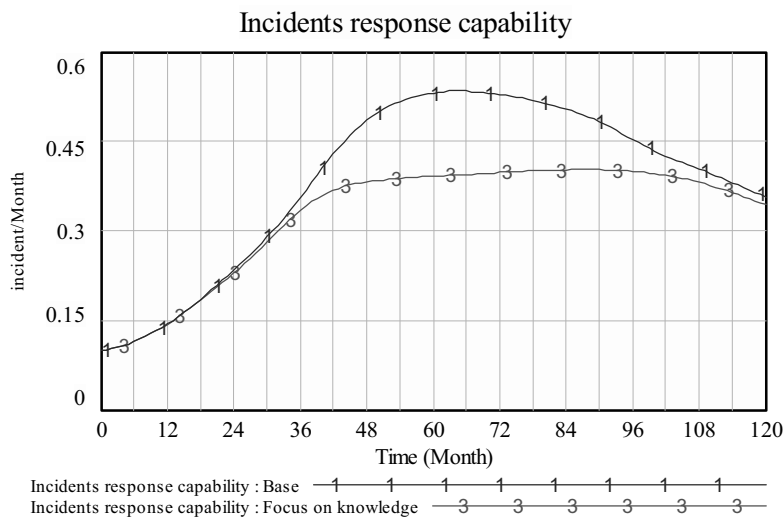
(b)



(c)



(d)



(e)

II. Your thoughts about scenario 3 “Focus on knowledge”.

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel a) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel a) plausible?

Why or why not?

Q1 c) Is the behavior of *Monthly Profit* (panel b) plausible?

Why or why not?

Q1 d) Is the behavior of *Frequency of incidents* (panel c) plausible?

Why or why not?

Q1 e) Is the behavior of *Severity of incidents* (panel d) plausible?

Why or why not?

Q1 f) Is the behavior of *Incidents response capability* (panel e) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you write a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ Since more resources are available, knowledge mature quicker than in the base run. There is no big impact on the '*mature work processes*' because even in the base run, it gets enough resources already. (panel a)
- ✓ The '*Monthly profit*' drops lower in the first year but increases faster later. '*Revenue*' is lower at the beginning because fewer resources are reserved for production. But later, as more mature new knowledge available, '*revenue*' increase to higher than in the base run. At the same time, the '*product cost and expenditure*' is lower due to more mature knowledge available. The '*expected incidents cost*' is lower and the '*cost for incidents response capability*' is also lower. As a result, the '*Monthly profit*' is higher than in the base run later. (panel b)
- ✓ With more '*mature new knowledge*', the system is less vulnerable. The '*frequency of incidents*' peaks lower and decrease quicker to the low level. With less incidents happening, less investment is made to build up the '*incidents response capability*'. The '*incidents response capability*' is lower. The '*severity of incidents*' peaks a little bit lower and drops faster. But it is not largely affected. (panel c, d & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

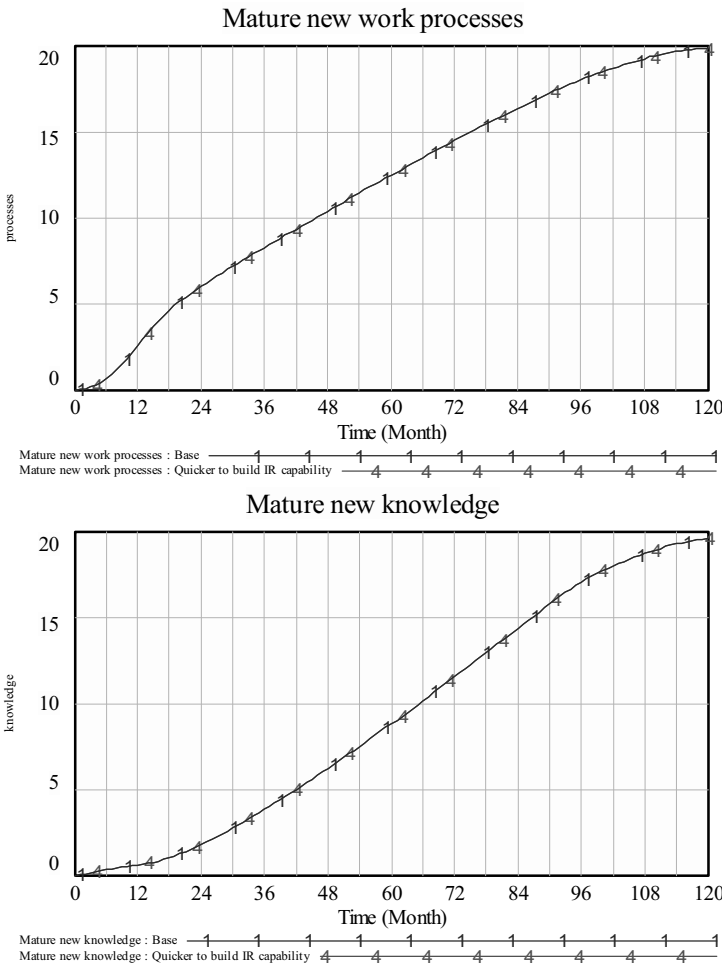
Q4: Has this explanation left out something that might be causing the results?

Scenario 4 Quicker to build IR capability

In the base scenario, it takes 3 months time from management’s investment decision on incidents response capability to incidents response capability ready. In this scenario, we assume that with a focus on security, the time to build up incidents response capability be shortened to 2 months.

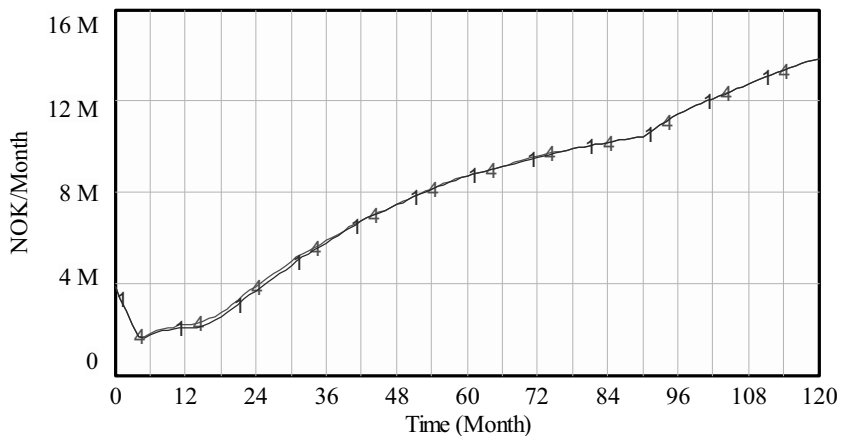
I. What happens?

- The ‘Mature new work processes’ is exactly the same as base run. So is ‘Mature new knowledge’. (panel a)
- The ‘Monthly profit’ is only slightly better for several months. (panel b)
- The ‘frequency of incidents’ is exactly the same as base scenario. The ‘severity of incidents’ peaks much lower and decreases to the lower level much faster. The ‘incidents response capability’ is higher than the base scenario. (panel c, d & e)

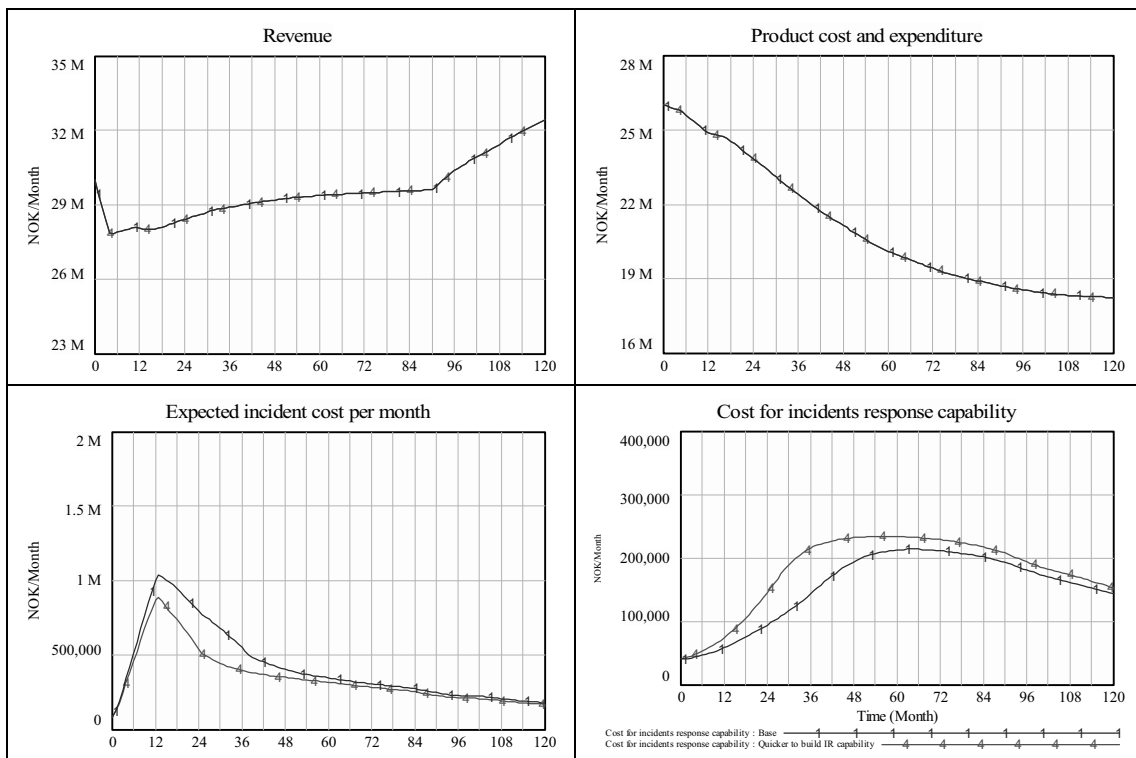


(a)

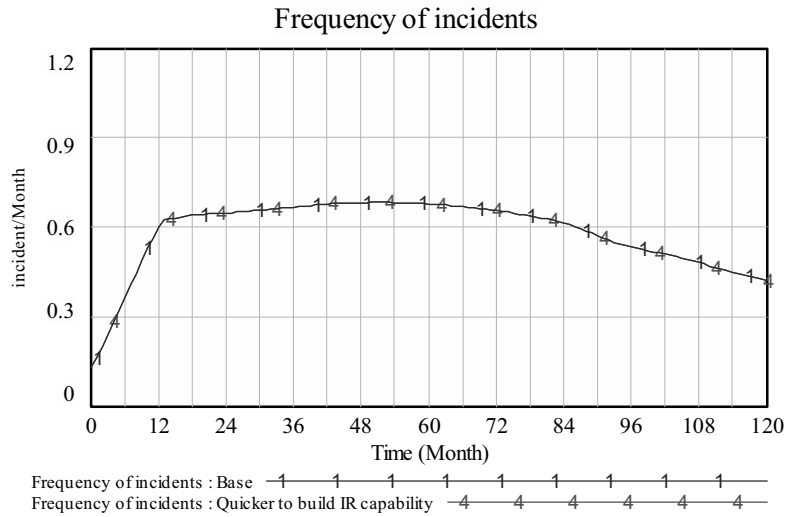
Monthly Profit



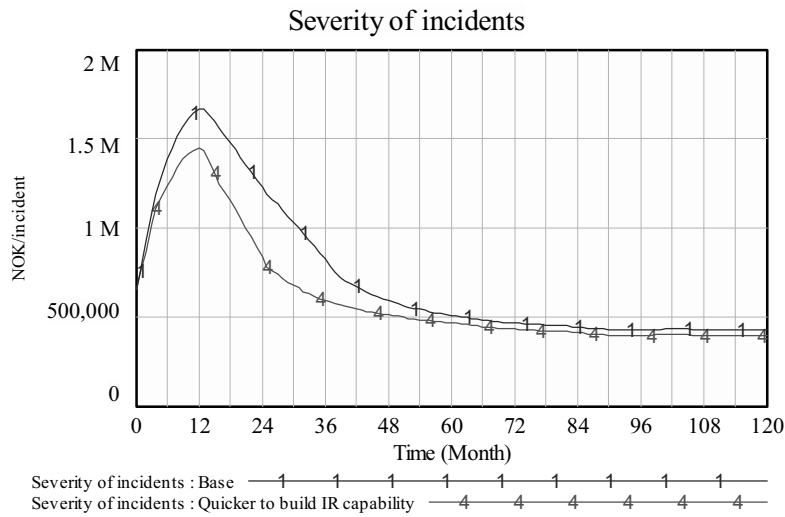
Monthly Profit : Base — 1 1 1 1 1 1 1 1 1 1 —
 Monthly Profit : Quicker to build IR capability — 4 4 4 4 4 4 4 4 4 4 —



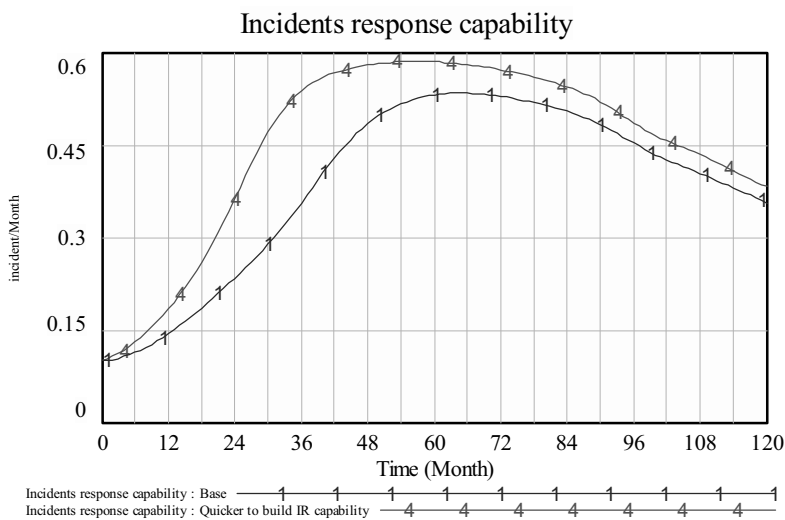
(b)



(c)



(d)



(e)

II. Your thoughts about scenario 4 “Quicker to build IR capability”.

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel a) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel a) plausible?

Why or why not?

Q1 c) Is the behavior of *Monthly Profit* (panel b) plausible?

Why or why not?

Q1 d) Is the behavior of *Frequency of incidents* (panel c) plausible?

Why or why not?

Q1 e) Is the behavior of *Severity of incidents* (panel d) plausible?

Why or why not?

Q1 f) Is the behavior of *Incidents response capability* (panel e) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you use a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ The '*mature new work processes*' and '*mature new knowledge*' behave the same as the base run because this scenario does not affect the transition to IO. (panel a)
- ✓ The '*Monthly profit*' behaves similar because with the same operation transition pace, '*revenue*' and '*product cost and expenditure*' are the same. The '*expected incidents cost*' is lower but the '*cost for incidents response capability*' is higher so that the net effect is small on '*Monthly profit*'. (panel b)
- ✓ With the same pace of operation transition as the base scenario, the vulnerability of the system is the same. So is the '*frequency of incidents*'. However, with shorter time to build up '*incidents response capability*', it increases more quickly. The '*severity of incidents*' is therefore peak lower than base scenario. (panel c, d & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

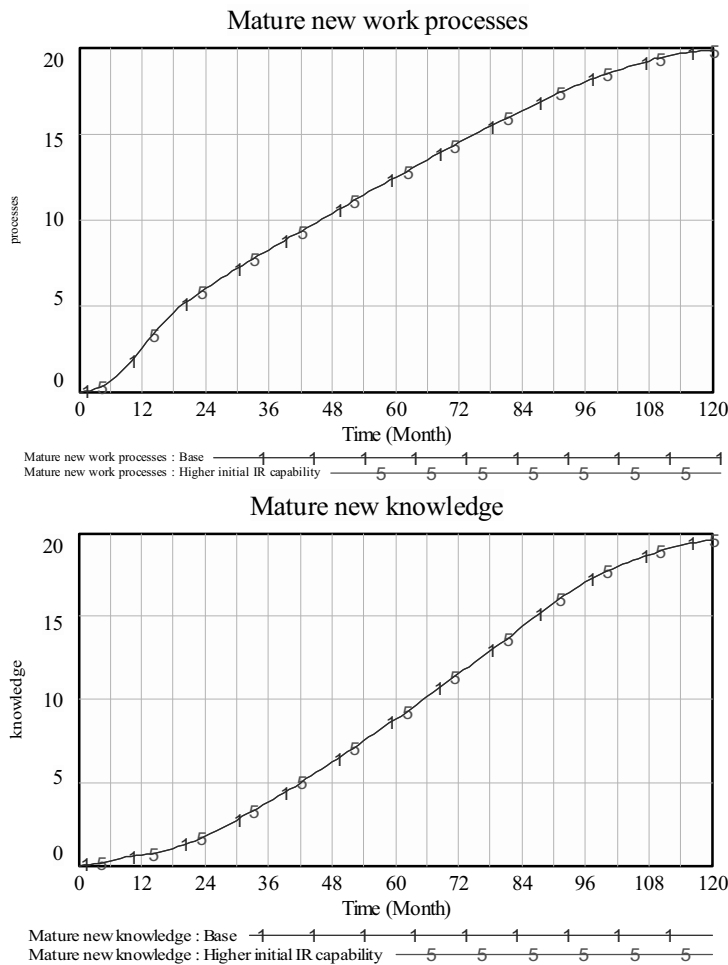
Q4: Has this explanation left out something that might be causing the results?

Scenario 5 Higher initial IR capability

In the base scenario, the initial incidents response capability is low because in traditional operation, the offshore platform is separated from network so that information security risk is low and there is no need to keep high incident response capability. Now we assume that the management team realizes the high risks for IO and raised incidents response capability in advance.

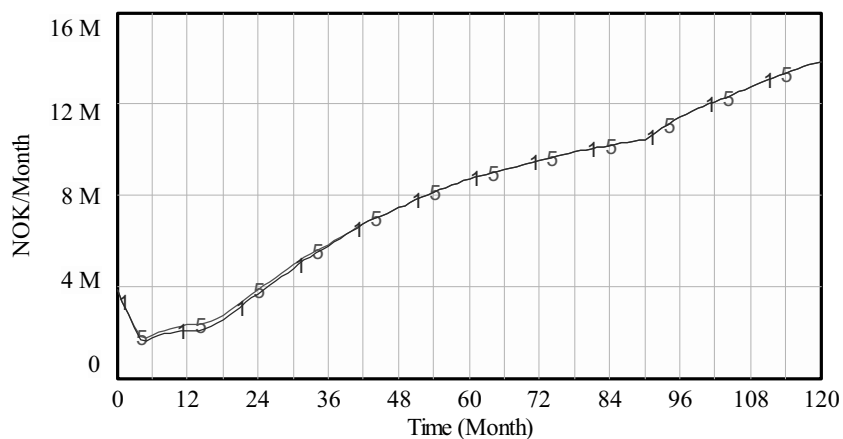
I. What happens?

- The ‘*Mature new work processes*’ is exactly the same as base scenario. So is ‘*Mature new knowledge*’. (panel a)
- The ‘*Monthly profit*’ is only slightly affected for several months. (panel b)
- The ‘*frequency of incidents*’ is the same as base scenario. The ‘*severity of incidents*’ peaks much lower. The ‘*incidents response capability*’ is higher than the base scenario for the first 5 years. (c, d & e)

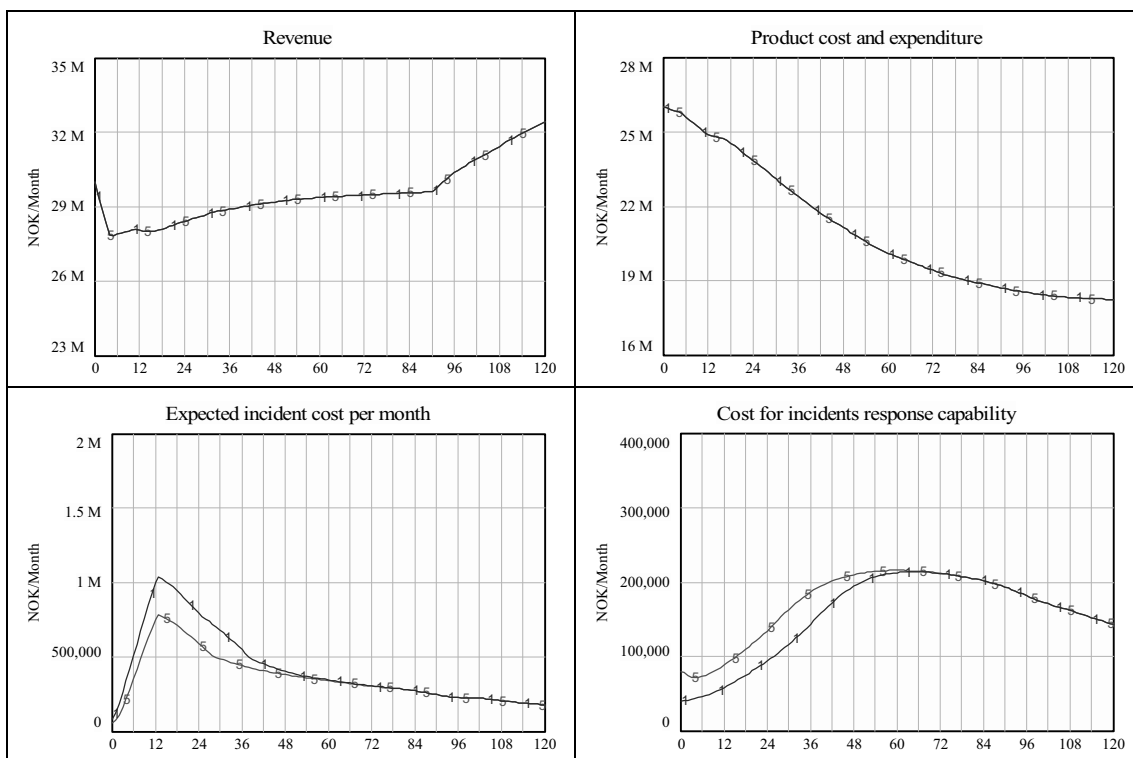


(a)

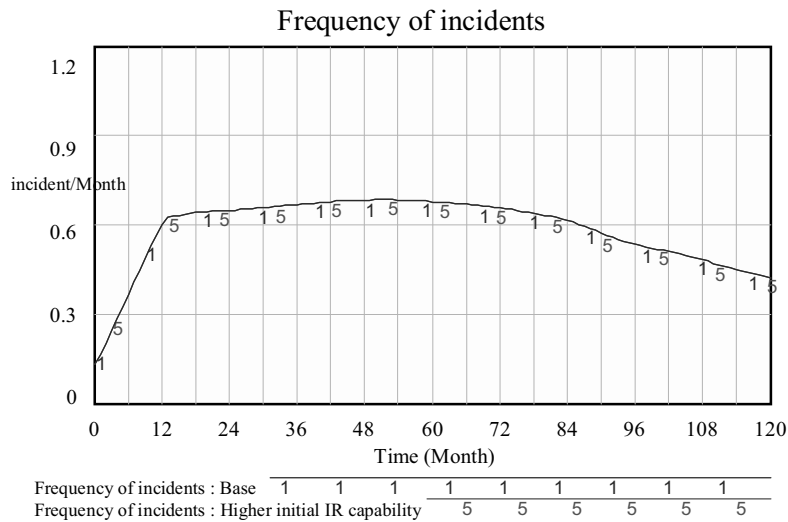
Monthly Profit



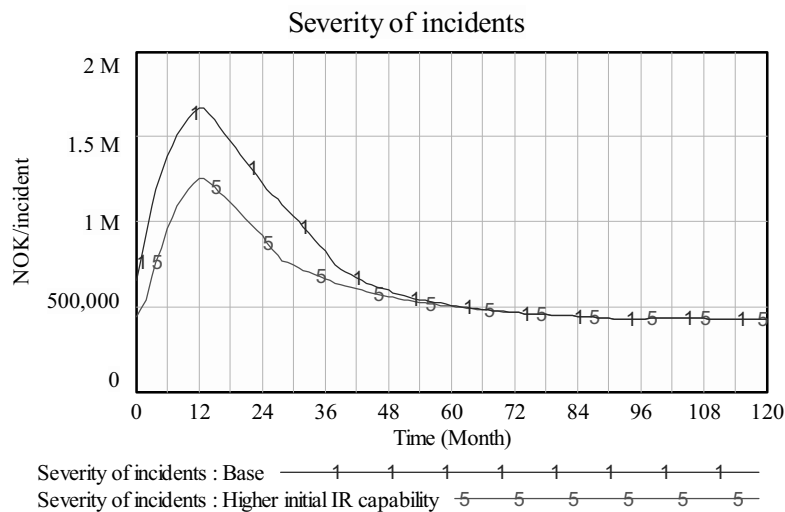
Monthly Profit : Base — 1 1 1 1 1 1 1 1 1
 Monthly Profit : Higher initial IR capability — 5 5 5 5 5 5 5



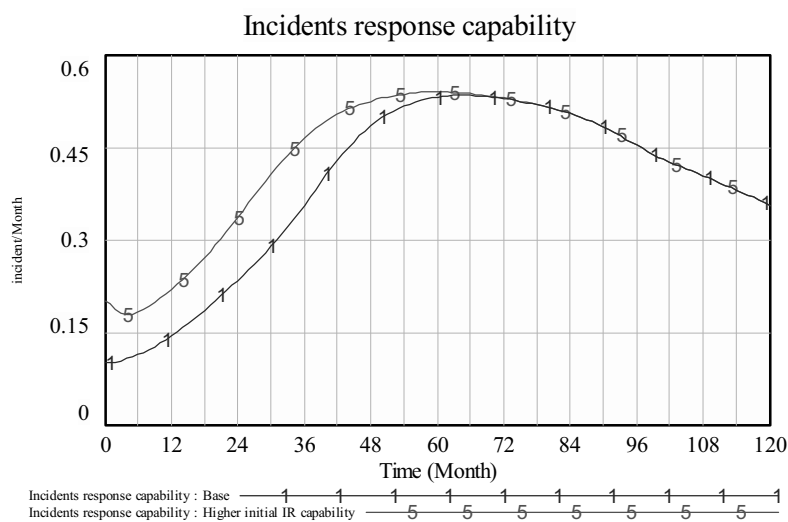
(b)



(c)



(d)



(e)

II. Your thoughts about scenario 5 “Higher initial IR capability”.

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel a) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel a) plausible?

Why or why not?

Q1 c) Is the behavior of *Monthly Profit* (panel b) plausible?

Why or why not?

Q1 d) Is the behavior of *Frequency of incidents* (panel c) plausible?

Why or why not?

Q1 e) Is the behavior of *Severity of incidents* (panel d) plausible?

Why or why not?

Q1 f) Is the behavior of *Incidents response capability* (panel e) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you use a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ The ‘mature new work processes’ and ‘mature new knowledge’ behave the same as in base scenario because this scenario does not affect the transition to IO. (panel a)
- ✓ The ‘*Monthly profit*’ behaves similar to base run because with the same operation transition pace, the ‘*Revenue*’ and ‘*product cost and expenditure*’ are exactly the same. The ‘*expected incidents cost*’ is lower but the ‘*cost for incidents response capability*’ is higher so that the net effect on profit is very small. (panel b)
- ✓ With exactly the same operation transition as in base scenario, the vulnerability of the system is the same. Therefore, the ‘frequency of incidents’ is the same as the base scenario. However, with higher initial incidents response capability, the ‘*severity of incidents*’ is lower than the base scenario for 5 years until it reaches the low stable level. The ‘*incidents response capability*’ is higher than the base scenario for the first 5 years before it starts to decrease. (panel c, d & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

Q4: Has this explanation left out something that might be causing the results?

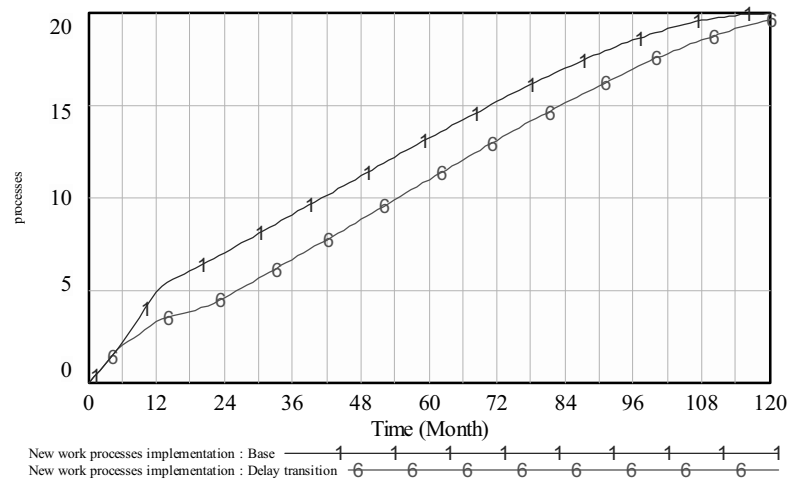
Scenario 6 Delay transition

In the base scenario, the operation transition proceed with its planned pace. The implementation of new work processes is not affected by the incidents happening. However, in reality, when severe incidents happen or high incidents cost occurs, the management might decide to slow down the operation transition. In this scenario, we study how model will behave with such feedback in the model. We assume that when the incidents cost reaches 5 times higher than the initial level, the transition speed will be reduced to half, and when the incidents cost reaches 10 times higher than the initial level, the operation transition will stop. Only when the management feels very secure, the incidents cost is lower than twice the initial level will they make an effort to catch up the delayed implementation schedule.

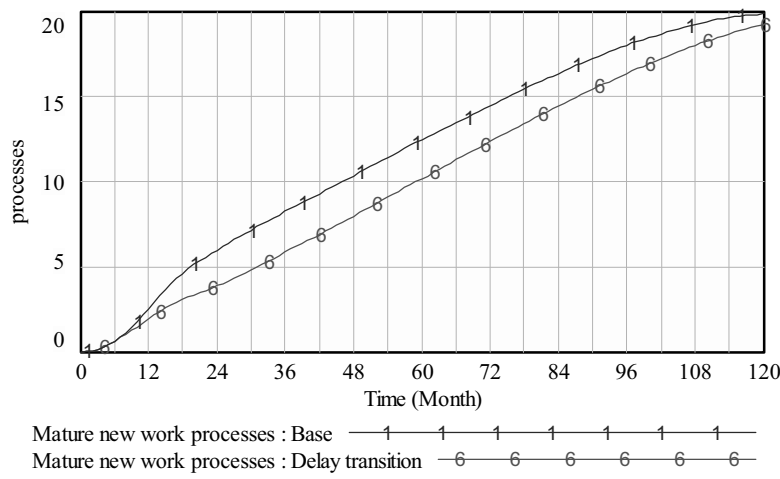
I. What happens?

- The ‘New work process implementation’ is slower than the base scenario, which means it is behind schedule. The ‘*Mature new work processes*’ is lower than base scenario. The ‘*Mature new knowledge*’ is higher than the base scenario at the beginning, but it is lower than the base scenario in the end. (panel a)
- The ‘*Monthly profit*’ underperforms the base scenario. At the beginning, it is similar, but later, the ‘*Monthly profit*’ is lower than the base scenario. (panel b)
- The ‘*frequency of incidents*’ is lower than the base scenario for most of the time but it doesn’t drop as low in the end. The ‘*severity of incidents*’ peaks lower and stabilize at almost the same level later. The ‘*incidents response capability*’ is lower than the base scenario most of the time but a little bit higher in the end. (c, d & e)

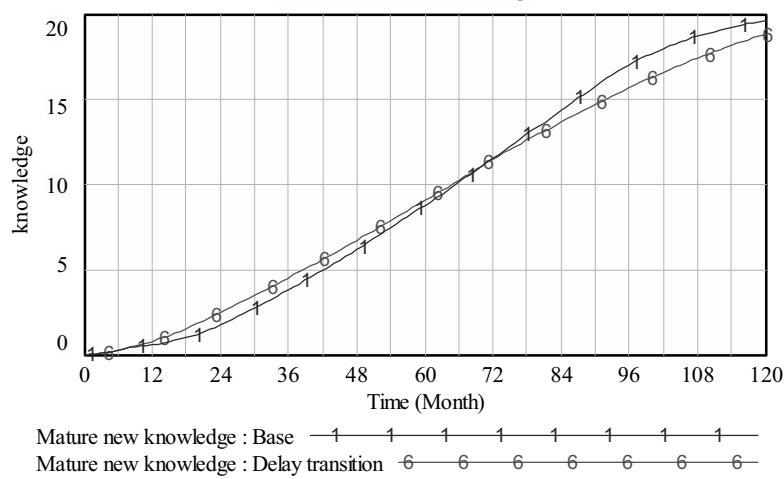
New work processes implementation



Mature new work processes

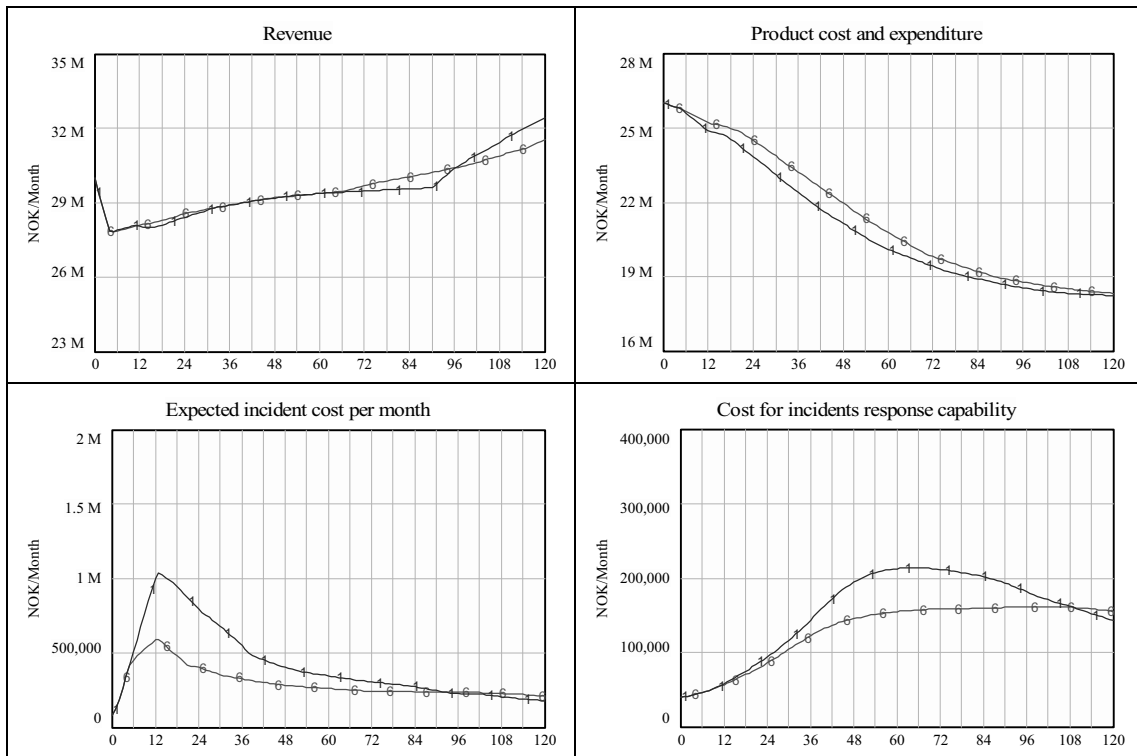
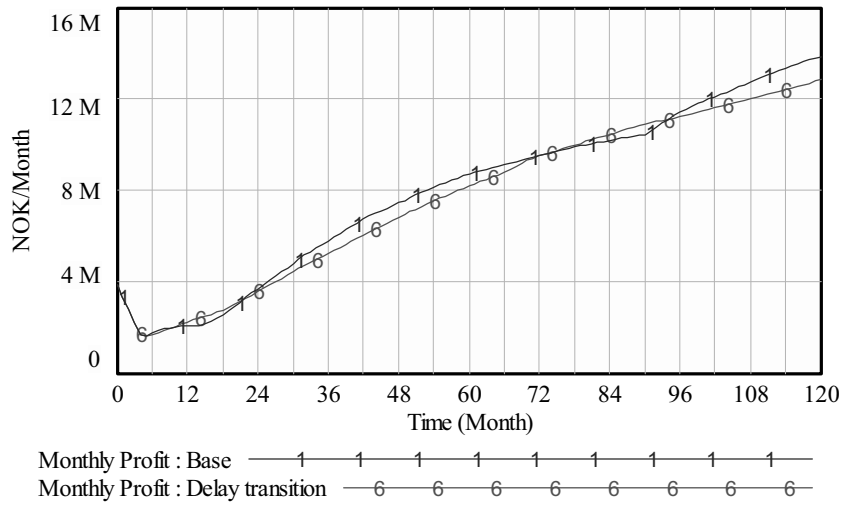


Mature new knowledge

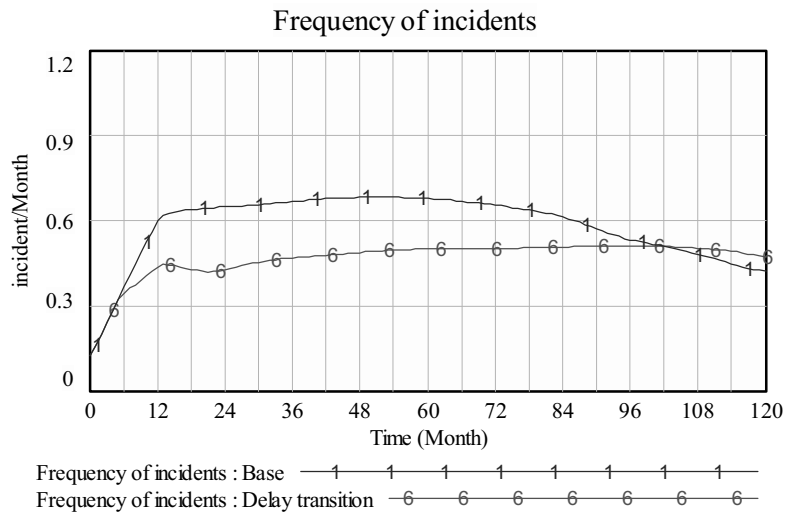


(a)

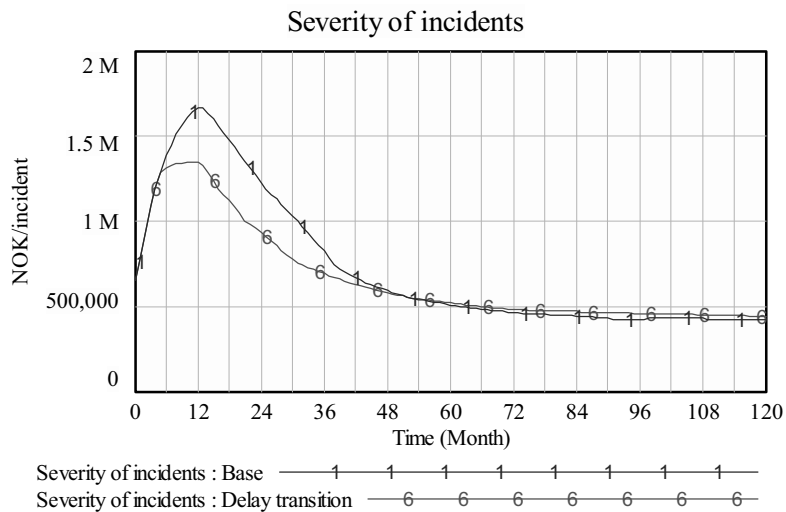
Monthly Profit



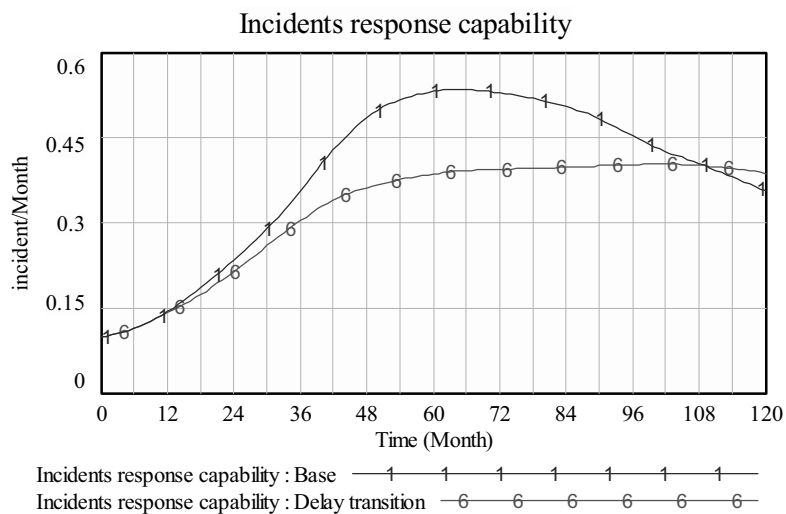
(b)



(c)



(d)



(e)

II. Your thoughts about scenario 6 “delay transition”.

Q1: Is the behavior of the key variables plausible? Do they match your beliefs about the transition to IO and its effects?

Q1 a) Is the behavior of *Mature New Work Processes* (panel b) plausible?

Why or why not?

Q1 b) Is the behavior of *Mature New Knowledge* (panel d) plausible?

Why or why not?

Q1 c) Is the behavior of *Frequency of incidents* (panel e) plausible?

Why or why not?

Q1 d) Is the behavior of *Severity of incidents* (panel f) plausible?

Why or why not?

Q1 e) Is the behavior of *Incidents response capability* (panel g) plausible?

Why or why not?

Q1 f) Is the behavior of *Profit* (panel i) plausible?

Why or why not?

III. Explaining why this occurs:

Q2 The above presented graphs are a summary of the model behavior. Can you use a few lines to tell us what you think the mechanism is for such behavior to happen?

Below, we present one interpretation of the model behavior. Please answer the related questions following it.

- ✓ The speed of operation transition is slowed down when the incidents cost is high. Therefore, the ‘mature new work processes’ and ‘mature new knowledge’ are lower than the base run. (panel a)
- ✓ The ‘*profit*’ behaves similar in the first 2 years. Though we are a little bit behind schedule, but the ‘*expected incident cost per month*’ is much lower. After year 2, it is a little bit worse than the base scenario, because the benefit of IO is delayed as the transition is behind the schedule. The ‘product cost and expenditure’ does not drop as quickly as the first scenario. (panel b)
- ✓ When the transition speed is reduced, less immature new work processes and knowledge are there. Therefore, the system is less vulnerable and the ‘*frequency of incidents*’ is greatly reduced. With fewer incidents, the incident response capability is more adequate so that the ‘*severity of incidents*’ is also lower than in base run. With less incidents happening, the investment on incidents response capability is less so that the ‘*incidents response capability*’ does not go as high as the base scenario. (panel c, d & e)

Q3: Is the explanation of this scenario plausible? Is the outcome surprising?

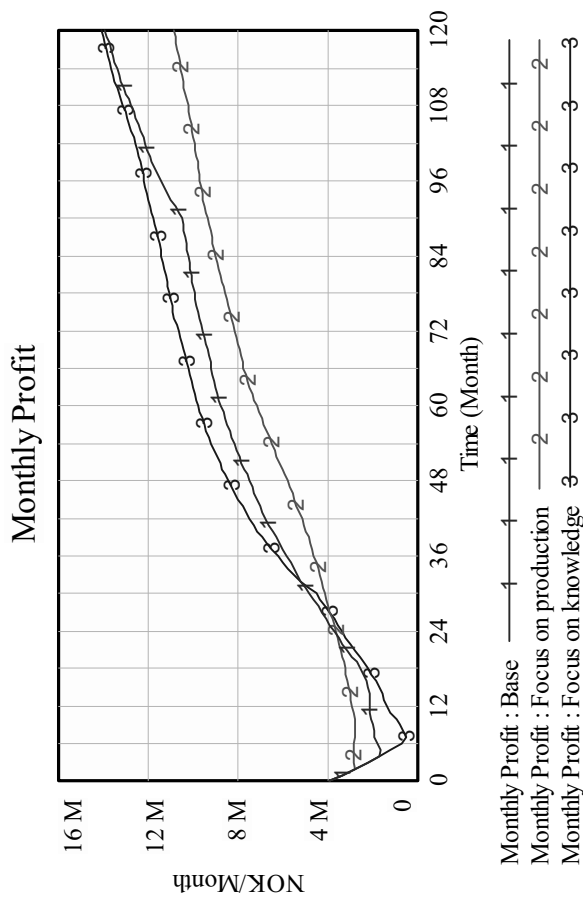
Q4: Has this explanation left out something that might be causing the results?

Closing questions

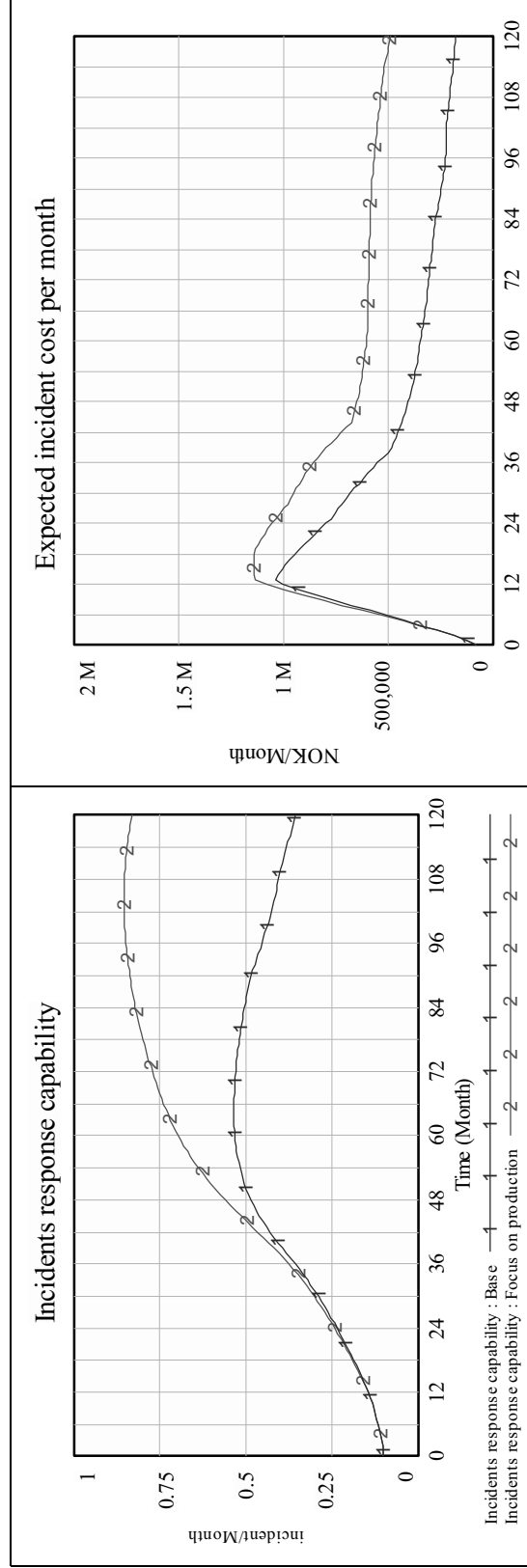
1. With most resources reserved for production, Scenario 2, focus on production, ends with least profit in the long run. With lowest resources reserved for production, Scenario 3, focus on knowledge, ends with most profit in the long run. Are the model behaviors surprising?

Could you please briefly explain the reasons for the above mentioned model behavior?

Do you think such behaviors are sound representation of the reality?



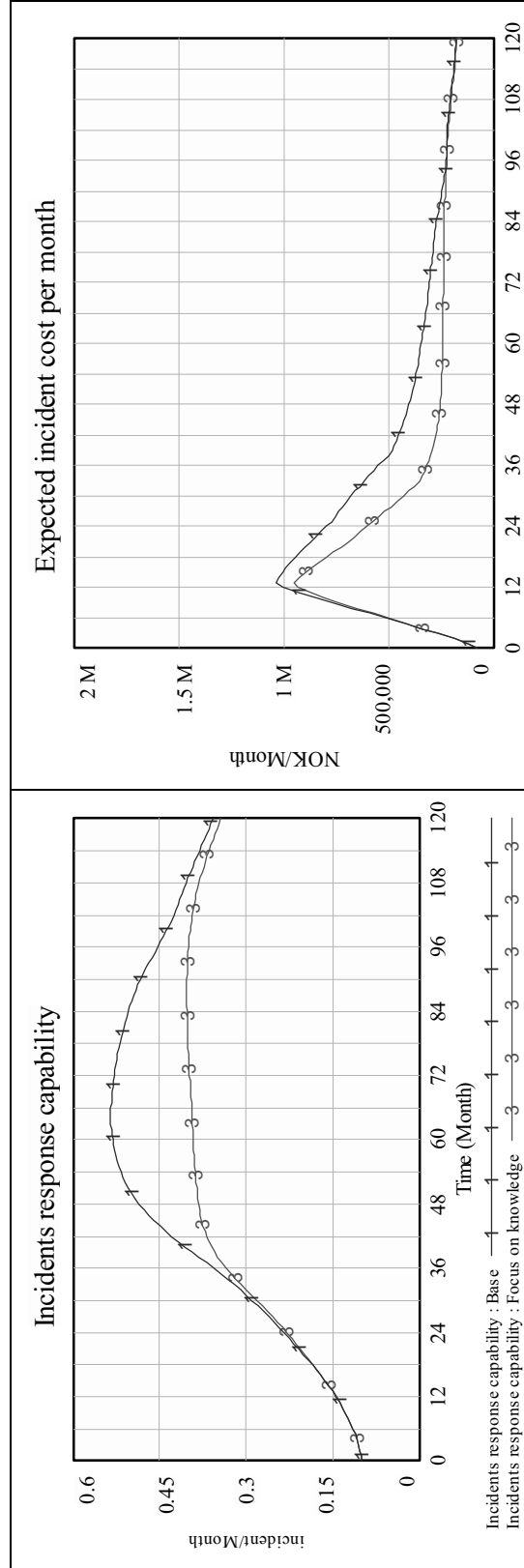
2. In scenario 2, focus on production, the management has invested much on incidents response capability building, but the cost of incidents still remains high. Are the model behaviors surprising to you?



Could you please briefly explain the reasons for the above mentioned model behavior?

Do you think such behaviors are sound representation of the reality?

3. In scenario 3, focus on knowledge, the investment on incidents response capability building is less than the base scenario, but the cost of incidents is lower. Are the model behaviors surprising to you?



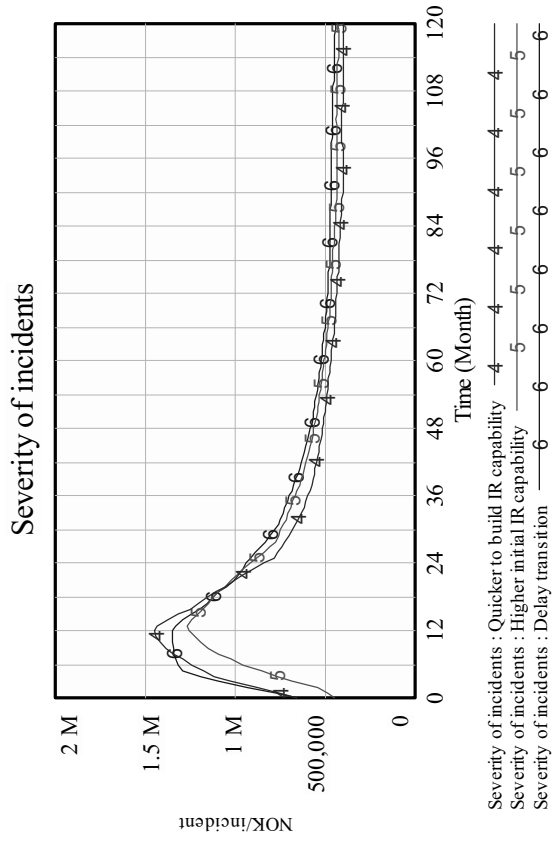
Could you please briefly explain the reasons for the above mentioned model behavior?

Do you think such behaviors are sound representation of the reality?

4. Compare scenario 4 'quicker to build IR capability', scenario 5 'high initial IR capacity' and scenario 6 'delay transition', scenario 5 'high initial IR capability' has the most impact on lower the peak of severity of incidents. Are the model behaviors surprising to you?

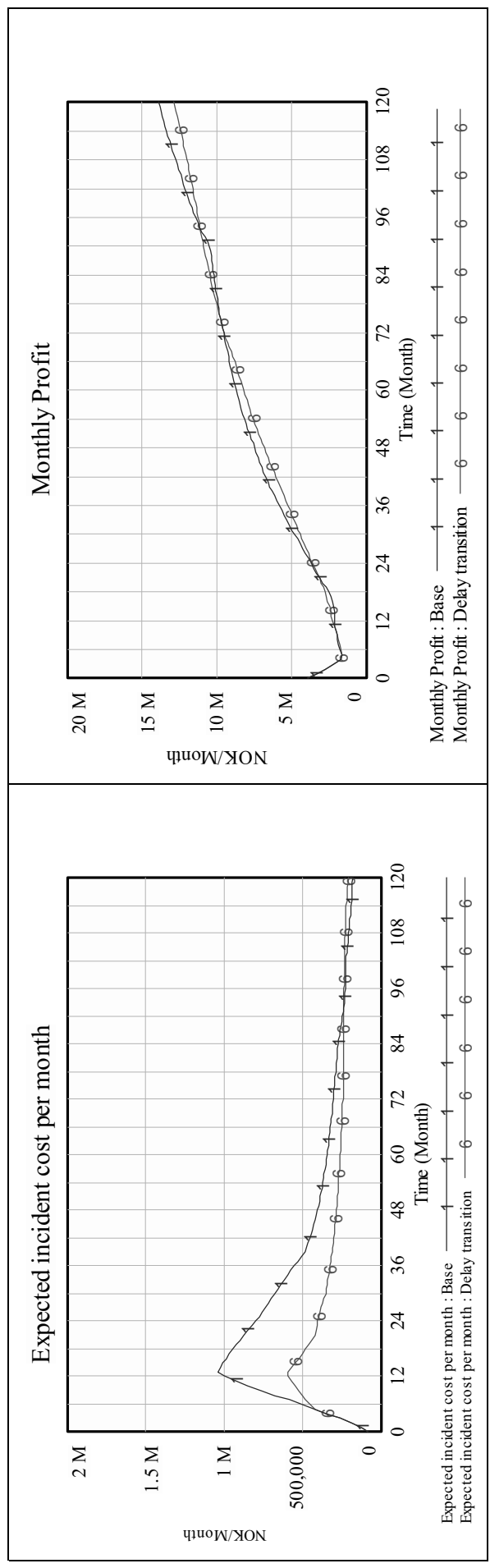
Could you please briefly explain the reasons for the above mentioned model behavior?

Do you think such behaviors are sound representation of the reality?



Severity of incidents : Quicker to build IR capability
Severity of incidents : Higher initial IR capability
Severity of incidents : Delay transition

5. Scenario 6, “delay transition”, we see that the ‘expected incidents cost per month’ is reduced almost 50%. However, the ‘the monthly profit’ in scenario 6 does not perform so well. Is this behavior surprising to you?



Could you please briefly explain the reason for this model behavior?

Do you think such behavior is sound representation of the reality?

6. Are there other variables or structures of transition to IO that should be added to the model? Please list your suggestions below, with the important listed first.

(1) _____

(2) _____

(3) _____

7. Are there other variables or structures of incidents response capability that should be added to the model? Please list your suggestions below, with the important listed first.

(1) _____

(2) _____

(3) _____

8. Are there other scenarios that would provide additional insight? Please describe what they would be.

(1)

(2)

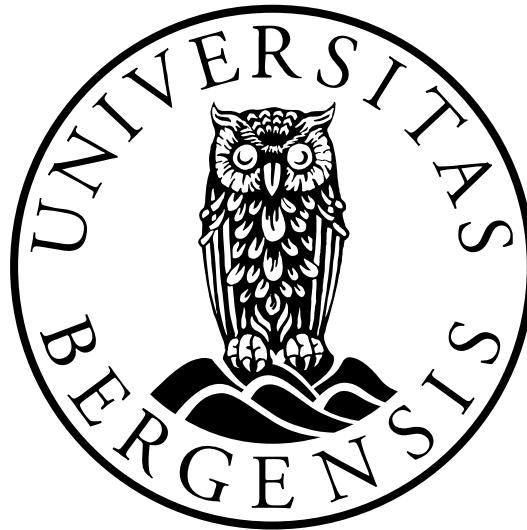
(3)

Thank you again for your assistance. This research project would not be possible without your help.

**Errata for
Mitigate information security risks during the
transition to Integrated Operations:**

Models and data

Ying Qian



Thesis for the degree philosophiae doctor (PhD)
at the University of Bergen

(signature of candidate)

(signature of faculty)

Jun 12 2010

Errata

Page iii “Odd H Longva” –changed to “Odd Helge Longva.” Helge is not a mid name but part of first name. It has to be spelled out

Page iv “has been proved to high” – “has been proved high” grammatically, to is not needed here

Page 2 “see Figure 1-2” has formatting problem. There is an unnecessary “enter”. The “enter” has been deleted.

Page 10 The caption of figure 1-7 is moved to page 10, following the figure.

Page 16 “incident cost incident cost” changed into “incident cost”.

Page 16 “These are studies” changed into “They are investigated” There is grammatical problem with the first expression

Page 31 Figure 2-1 is replaced by a high resolution figure. Except the resolution of the figure is high, there is no other difference.

Page 59 “affect” changed into “effect”. “affect” here is the wrong word, it should be “effect”

Page 67 “This exercises helps” changed into “This exercise helps”. It is not right using plurality

Page 67 “The X axis and Y axis represents” changed in “The X axis and Y axis represent”. Grammatical error corrected

Page 75 “incidents reporting” changed into “incident reporting”. “incident reporting” is used as the term in the document

Page 150 “see Figure 6-1” there is an “enter” there. The “enter” is deleted

Page 155 “Table 6-5 Table 6-5” delete one

Page 173 “Table 7-5” there is a space on this caption. Delete the space.

Page 207 “oto increase” changed into “to increase”. This “o” is a misspell

Page 210 “decision rule In the long” changed into ”decision rule. In the long”. Lack a full stop

Page 234 ”at hand .” changed into ”at hand.” There is an unnecessary space before the full stop. Delete it

Page 243 ” Goerge” changed into ” George”. Misspell the name.

Page 250 ”This variable range from” changed into ”This variable ranges from”. Grammatical error.