Conceptual System Dynamics Model and System Archetypes on Security Improvement in Integrated Operations for the Oil and Gas Industry

by

Lars Slåtsveen Breistrand

Thesis in partial fulfilment of the degree of
Master in Technology in
Information and Communication Technology

Agder University College
Faculty of Engineering and Science

Grimstad
Norway

May 2006

Acknowledgements

First and foremost I would like to thank my supervisor Jose J. Gonzalez for introducing me to system dynamics and allowing me to be a part of the research cell "Security and Quality in Organizations" at Agder University College during my work on this thesis. I am very grateful for his advice, guidance and constructive criticism throughout the course of this work.

I am sincerely indebted to Felicjan Rydzak for his advice and the time he has taken in helping me with my work. I also want to thank Finn Olav Sveen for his valuable comments. A big thank you to Tor Ivar J. Nordmo for the many discussions we have had, both on and off topic.

A big thank you also goes out till the rest of the SQO-group, Agata Sawicka, Stefanie Hillen, Ying Qian, Jaziar Radianti, Bjørn Roalkvam and Tuan Huu Ngo. Working with you all has taught me a lot. I only hope that I have been a valuable "criadera" in the solera system that is the SQO-group.

I would like to thank my friends for being patient with me and sometimes making me take my mind off work. I would also like to thank my girlfriend, Karoline, for her patience, encouragement and support.

Last, and most importantly, I would like to thank my father, Arild, my mother, Sonja, my brother, Petter, and my sister Maren for always supporting me in everything I do.

Abstract

The oil and gas industry are moving into Integrated Operations which will reduce costs, increase production and extend the lifetime of mature fields. They are going to achieve this through better utilization of drilling and production data, and close collaboration between offshore and land based personnel.

Traditional offshore operations (e.g. drilling production, delivery, etc.) are going to be controlled by onshore control centers, using ICT solutions, and in collaboration with sub contractors and other business partners.

This new way of working creates new work processes that have great information security implications. A security incident such as a hacker attack or a virus can for example lead to loss of control of systems or failure of control systems. Some implications can be costly downtime, injuries or loss of life.

A conceptual model of a generic oil and gas company has been created and simulations have been run showing the behavior of the system when incidents happen. These incidents affects the resilience of the system, and if severe or if the company does not have proper management policies in place, the system can move into an undesirable state.

The main conclusion is that it is important for management to keep a focus on and allocate enough resources for pro active work such as information security. This is especially valid when the system has been hit by an incident and its resilience can be weakened. If not done correctly the system can go into an undesirable state of under performance.

These insights are shown in system archetypes.

Table of Contents

Table of Figures

1 Introduction

1.1 Integrated Operations

Integrated Operations, or eOperations, is going to increase production, reduce costs and extend the lifetime of mature fields in the Norwegian offshore sector through better utilization of drilling and production data, and closer collaboration between offshore and land-based personnel.

Integrated Operations entails a new operations practice and with it operators can make better and faster decisions using ICT solutions that include real-time data to integrate work processes across disciplines and between organizations. With the aid of Integrated Operations activities can be managed regardless of geographical distance, e.g. between offshore platforms and land base control centers. The goal is a reduction of operating costs by 30 percent, 10 percent in increased production and up to 4-5 percent increase in recovery rate.

When traditional offshore operations such as drilling, production, delivery etc, which is mostly located at the offshore platforms, are gradually being substituted by onshore operation via computer networks, the success hinges on mastering the information security issues that arise.

1.1.1 Potential Threats

Gonzalez et al.(2005) describes the information security implications spawned by Integrated Operations. From the point of view of information security the transition that spans a long time period (10-12 years) is an “engine” that generates vulnerabilities, vulnerabilities being weaknesses in the Integrated Operations environment that facilitates intended or unintended incidents.

An unintended incident could occur if an onshore operator – believing that the system is in test mode – inadvertently closes valves, thus causing an organizational accident and down-time. A mixture of intended and unintended incident could be caused when a contractor, who under maintenance operations, connects to the Integrated Operations intranet and inadvertently introduces malware from his PC to the intranet. An intended incident could be a

network attack, for example a (D)DoS-attack or intrusion on the intranet. Summing up, the Integrated Operations intranet is vulnerable both to unintended incidents (insider failures) and outsider attacks.

In (Hocking 2005), Paul Hocking, BP PetroTech Advisor – Automation, addresses some dangers affiliated with Integrated Operations. E.g. are general hacker threat, malicious code attack specifically directed against operator, insider threats from within or its business and digital business suppliers, partners and contractors. He points out that a cyber attack can lead to:

- Failure of control systems
- Loss of integrity or control of systems
- Loss of process monitoring and visibility of plant

The effect of such incidents can be:

- Risk of injury or loss of life
- Loss of production
- Environmental damage
- Damage to reputation
- License to operate can be jeopardized

Worms such as Code Red, Nimda, Slammer, Blaster and Sasser have all affected process control systems. In January 2003 the Slammer worm penetrated a private computer network at Ohio's David-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall (Poulsen 2003). Other examples are a disgruntled employee that attacked a sewage control system and released millions of gallons of sewage into a river and hotel ground, and a manufacturing plant that grinded to a halt when a security scan crashed hundreds of PLCs (Programmable Logic Controllers) (Lowe 2006).

1.2 Research questions

1. What are the main characteristics of resilience in a system presented in the form of a conceptual model of Integrated Operations when focusing on information security as a QIP (quality improvement process)?

2. Describe these findings in dynamic stories and system archetypes.

3. Suggest some policies/solution archetypes that increase resilience (against negative change).

4. Resilience can also be towards positive change, can archetypes identifying some important reasons for resilience in Integrated Operations when viewing information security as a QIP be created?

1.3 Thesis structure

Chapter 1 introduces the reader to the problem area of integrated operations and the information security problems that is connected to it. It goes on to state the research questions this thesis attempts to answer.

Chapter 2 describes the methodology used in the thesis. System dynamics, causal loop diagrams, system archetypes and resilience are areas described.

Chapter 3 shortly describes how most organizations view information security today.

Chapter 4 describes the origin of the model, the assumptions it is based on. Goes on to give a thorough description of the stocks in the model and the core structure of it that is made up of four feedback loops.

Chapter 5 contains model verification and validation. Describes the thoughts behind the model and how it works and tests that have been made.

Chapter 6 goes on to describe simulations of different management policies in the model with dynamic stories. The simulations focus on how the system behaves when it is affected by one incident.

Chapter 7 continues describing simulations that have been performed. The dynamic stories describe what happens to the system when it is affected by multiple incidents.

Chapter 8 shows simulations of how the system behaves when it is faced with an increase in the demanded performance.

Chapter 9 contains discussion on the different policies simulated and gives some recommendations. It also describes the dynamic behavior of the model with system archetypes.

Chapter 10 concludes the findings that have been made and makes some suggestions for further research.

2 Methodology

2.1 System Dynamics

System dynamics is a methodology for studying and managing complex feedback systems, such as one finds in for example ecological and economic systems. System dynamics has been used to address practically every sort of feedback system. And what differentiates system dynamics is the use of feedback loops. Feedback refers to the situation of X affecting Y and Y in turn affecting X, possibly through a chain of causes and effect.

2.1.1 Causal Loop Diagrams

In (Sterman 2000) causal loop diagrams are described. As mentioned, feedback is one of the core concepts of system dynamics. Yet our mental models often fail to include critical feedbacks determining the dynamics of our system. In system dynamics several diagramming tools are used to capture the structure of systems, one method being causal loop diagrams.

They are an important tool for representing the feedback structure of systems and are excellent for

- Quickly capturing your hypothesis about the causes of dynamics;
- Eliciting and capturing the mental models of individuals or teams;
- Communicating the important feedbacks you believe are responsible for a problem.

A causal diagram consists of variables connected by arrows denoting the causal influences among the variables. Variables are related by causal links, shown by arrows. Each causal link is assigned a polarity, either positive (+) or negative (-) to indicate how the dependent variable changes when the independent variable changes.

Positive feedback loop

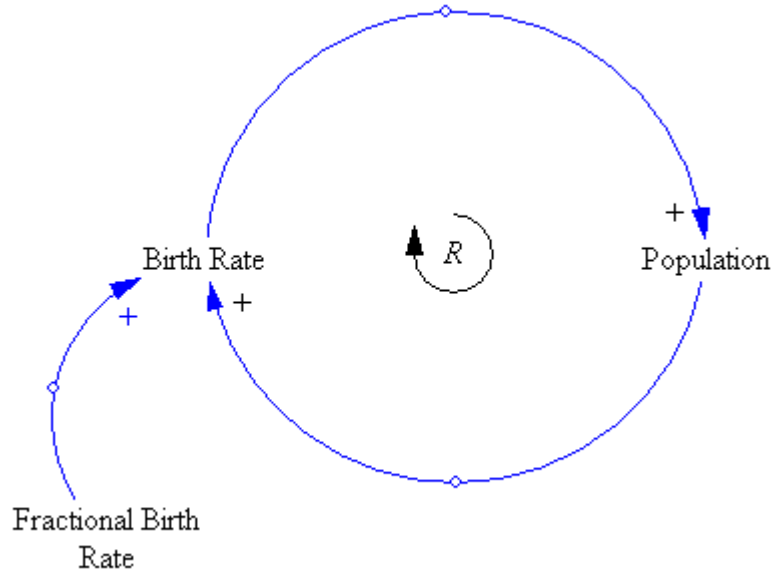


Figure 1 – An example of a positive feedback loop.

Sterman (2000) states:

A positive link means that if the cause **increases**, the effect **increases** *above what it would otherwise have been*, and if the cause **decreases**, the effect **decreases** *below what it otherwise would have been*.

In the example above an increase in fractional birth rate will lead to an increase in birth rate above what it would otherwise have been. A decrease in fractional birth rate will lead to a decrease in birth rate what it would otherwise have been.

Negative feedback loop

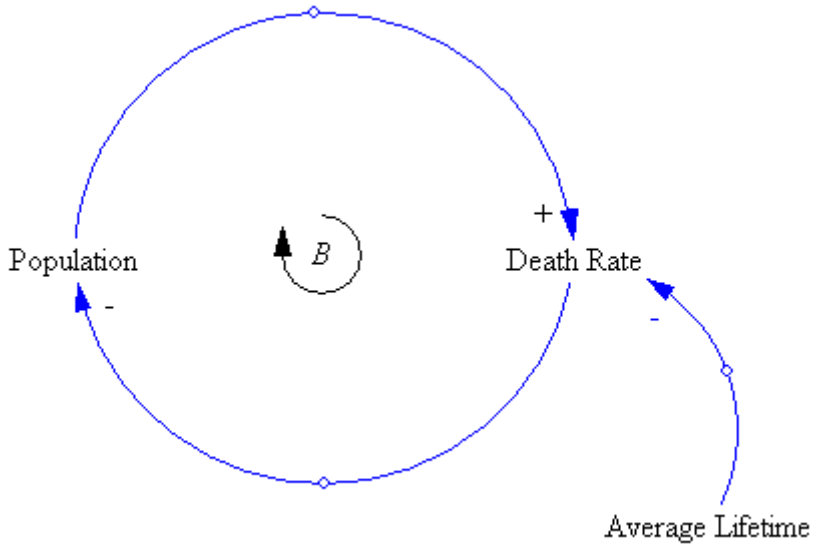


Figure 2 – An example of a negative feedback loop.

Sterman (2000) states:
A negative link means that if the cause **increases**, the effect **decreases** *below what it would otherwise have been*, and if the cause **decreases**, the effect **increases** *above what it would otherwise have been*.

In the example of a negative feedback loop, an increase in average lifetime will lead to a decrease in death rate below what it would otherwise have been. Vice versa, a decrease in average lifetime will lead to an increase in death rate above what it would otherwise have been.

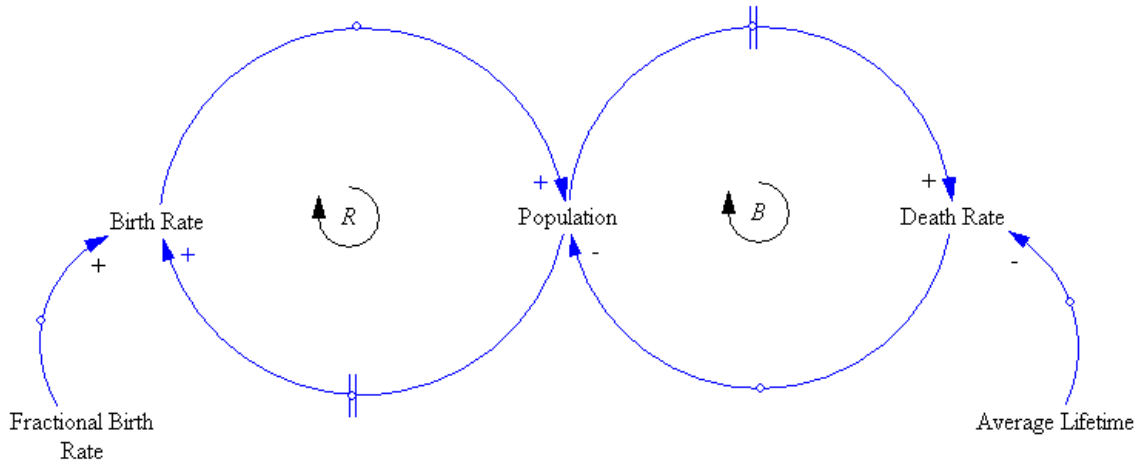


Figure 3 – An example of feedback loops connected.

Link polarities describe the structure of the system. They do not describe the behavior of the variables. That is they describe what would happen **if** there were a change. They do not describe what actually happens. Also, note the phrase above (below) what it otherwise would have been in the definition of link polarity. An increase in a cause variable does not necessarily mean that the effect will increase. First, a variable has more than one input and to determine the actual outcome one needs to know how all the inputs are changing. Second, and more importantly, causal loop diagrams do not distinguish between stocks and flows. For example, an increase in birth rate will increase the population (above what it would otherwise have been), but a decrease in birth rate does not decrease population. You cannot tell whether the population is actually rising or declining. Population will be falling even if the birth rate rises if the death rate exceeds births.

Due to the feedback structure, it is common that loops are formed. A loop can be either positive (reinforcing) or negative (balancing). Positive (reinforcing) loops are denoted by a + or **R**. Negative (balancing) loops are denoted by a – or **B**. In a reinforcing loop a change is strengthened and reinforced, in a balancing loop a change is opposed.

A link in a causal loop diagram can have a delay, denoted by to crossing bars. For example: when population increases there is a delay before the (majority) of the population becomes old and dies.

2.1.2 Stocks and flows

Causal loops are very useful in many situations. At the start of a modeling project capturing mental models, and at the end of a project, communicating the results of a completed model. However it suffers from some shortcomings and limitations. Maybe the most important is their inability to capture stock and flow structures of a system. Stocks and flows are together with feedback the two most central concepts of dynamic systems theory.

Sterman (2000) defines stocks the following way:
"Stocks are accumulations. They characterize the state of the system and generate the information upon which decisions and actions are based. Stocks give systems inertia and provide them with memory. Stocks create delays by accumulating the difference between the inflow to a process and its outflow. By decoupling rates of flow, stocks are the source of disequilibrium dynamics in systems."

Stocks are familiar to us and we experience them every day. Example: the amount of cash in our bank account. What we spend is the outflow, and deposits are the inflow. The workforce in a company is a stock that increases through hiring and decreases via the rate of layoffs, retirements and quits.

Sterman (2000) uses the following notation for stocks and flows:

- Stocks are represented by rectangles (suggesting a container holding the contents of the stock).
- Inflows are represented by a pipe (arrow) pointing to (adding to) the stock. Outflows are represented by pipes pointing out of (subtracting from) the stock.
- Valves control the flows.
- Clouds represent the sources and sinks for the flows. A source represents the stock from which a flow originating outside the boundary of the model arises; sinks represent the stocks into which flows leaving the model boundary drain. Sources and sinks are assumed to have infinite capacity and can never constrain the flows they support.

Stock and flow diagramming notation

Figure 4 – An example of classic stock and flow diagramming notation.

A much used and helpful metaphor for a stock is a bathtub. The amount of water in your bathtub at any time is the accumulation of the water flowing into the tub minus the water flowing out through the drain (the assumption being that there is no evaporation and splashing). The inflow is usually different from the outflow.

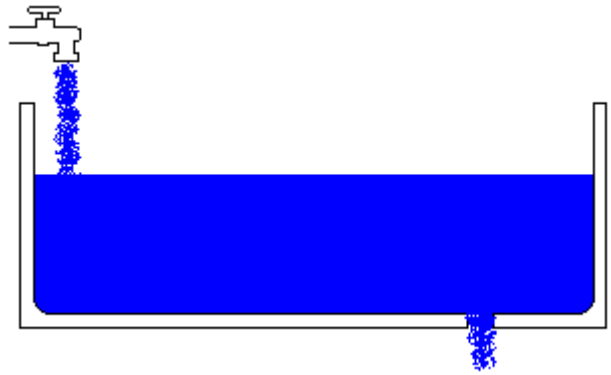


Figure 5 – Thinking of a stock as a bathtub can be a helpful metaphor.

Sterman (2000) uses the following the notation to represent the process of accumulation:

$$Stock = INTEGRAL(Inflow - outflow, Stock_{t0})$$

2.1.3 System archetypes

System archetypes are a relatively new way of thinking in system dynamics. In his book "The Fifth Discipline" from 1990 (Senge 1990), Peter M. Senge describes systems thinking and introduces archetypes as particular types of cycles that describe systems. Senge emphasizes the importance of feedback in systems thinking and seeing relations rather than linear cause-and-effect chains.

The ten archetypes defined in "The Fifth Discipline" are Balancing Process with Delay, Limits to Growth, Shifting the Burden, Shifting the Burden to the Intervener, Eroding Goals, Escalation, Success to the Successful, Tragedy of the Commons, Fixes that Fail and Growth and Underinvestment.

Further work on system archetypes are done by E. F. Wolstenholme in his award winning paper "Towards the definition and use of a core set of archetypal structures in system dynamics." from 2002 (Wolstenholme 2002). In this paper Wolstenholme discusses system archetypes both as a device to aid model conceptualization and as a means of presenting insights derived from a model. Wolstenholme argues that there are four totally generic system archetypes, Underachievement, Out-of-control, Relative Achievement and Relative Control. He describes the archetypes and gives examples of each of them. Also, for each problem archetype there is a solution archetype which is described and shown both generic and with examples. An important aspect which is stressed in this paper is the existence of organizational boundaries. There are several types of boundaries. A boundary may be between an organization and its environment, it could be a physical boundary between different parts of an organization or even a mental barrier between different groups or individuals in an organization.

System archetypes are further discussed in Wolstenholme's paper "Using generic system archetypes to support thinking and modeling." (2004). Here he argues that boundaries should be added to the group of components that make up the system "structure" that the original concept of system dynamics consisted of, and that they are a fundamental facet of system behavior. Boundaries are described, both as to why they are so important, the effects they cause and their behavior. To some extent he describes the use of system archetypes in both the development of advanced models and in the dissemination of the same. Also there are some hints on how to identify feedback loops and archetypes in stock-and-flow diagrams.

From (Wolstenholme 2002) "System archetypes were introduced as a formal and free-standing way of classifying structures responsible for generic patterns of behavior over time, particularly counter-intuitive behavior. Such "structures" consist of intended actions and unintended reactions and recognize delays in reaction times. The system archetypes currently classified can be seen as a synthesis of much qualitative and quantitative modeling effort cumulated over many years by many analysts, which can be used to help to generate

understanding in new application domains. This isomorphic quality makes them a very powerful mechanism for accelerating learning in an increasingly turbulent world."

According to Wolstenholme an archetype has the following characteristics:

- It's composed of an intended consequence feedback loop which results from an action initiated in one sector of an organization with the intended consequence over time as a goal.
- It contains an unintended consequence feedback loop, which is the result of a reaction in another sector of the organization or outside it.
- There is a delay before the unintended consequence manifests itself.

There is an organizational boundary that "hides" the unintended reaction from those who initiated the original action resulting in the intended outcome. For every problem archetype there is a solution archetype.

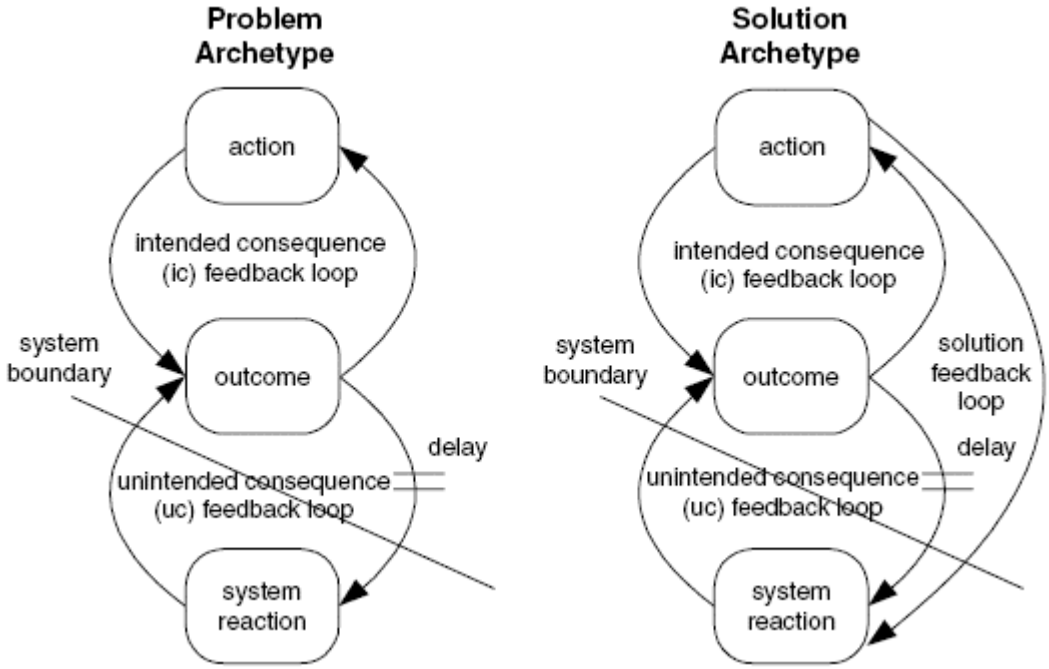


Figure 6 – A generic problem archetype and its solution. Taken from (Wolstenholme 2002).

2.2 Resilience

The term resilience was introduced to the literature by the theoretical ecologist C. S. Holling. The paper "Ecological Resilience – In theory and application" (Gunderson 2000) reviews concepts and multiple meanings of resilience as they have appeared in literature and how

ecological resilience is key to management of complex systems of people and nature. Resilience has been defined in the ecological literature in two different ways, reflecting different aspects of stability. The multiple meanings of resilience are related to the existence of either single or multiple equilibriums in a system.

Many authors define resilience as how long it takes for a system to return to a steady-state or equilibrium after a disturbance, the measure being how far the system has moved from that equilibrium and how quickly it returns. The implicit assumption being that there is only one steady state or equilibrium. If other operating states exist they should be avoided by applying safeguards.

The second type of resilience emphasizes conditions far from steady state condition, where instabilities can flip a system into another regime of behavior. In this case resilience is measured by how much disturbance a system can absorb before moving into another domain of operations.

3 The State of Information Security

The use of information technology seems almost infinite and affects almost every aspect of our lives. Health care, production of goods, logistics, financial institutions and the control of armies are just some examples of areas that are highly affected. And as the use of information technology grows, the potential negative impact of an intended or unintended incident grows with it. Armies can come to a halt, a stock may loose a hundred points, businesses may be bankrupted and individuals can loose their identity. Since its infant days the number of potential vulnerabilities in IT and the sophistication of attacks have grown immensely. In (Rogers 2005) and in Figure 7 from (Woody 2003) it is shown how attacks have gone from the more primitive attempts of password guessing, social engineering attacks and hijacking sessions to DDoS (distributed denial of service) attacks, advanced command and control, and the use of anti-forensic techniques. At the same time, the knowledge needed for an intruder to exploit these vulnerabilities has dropped dramatically. Attack tools, such as well written scripts, that exploit known vulnerabilities are wide spread and require less and less knowledge to use.

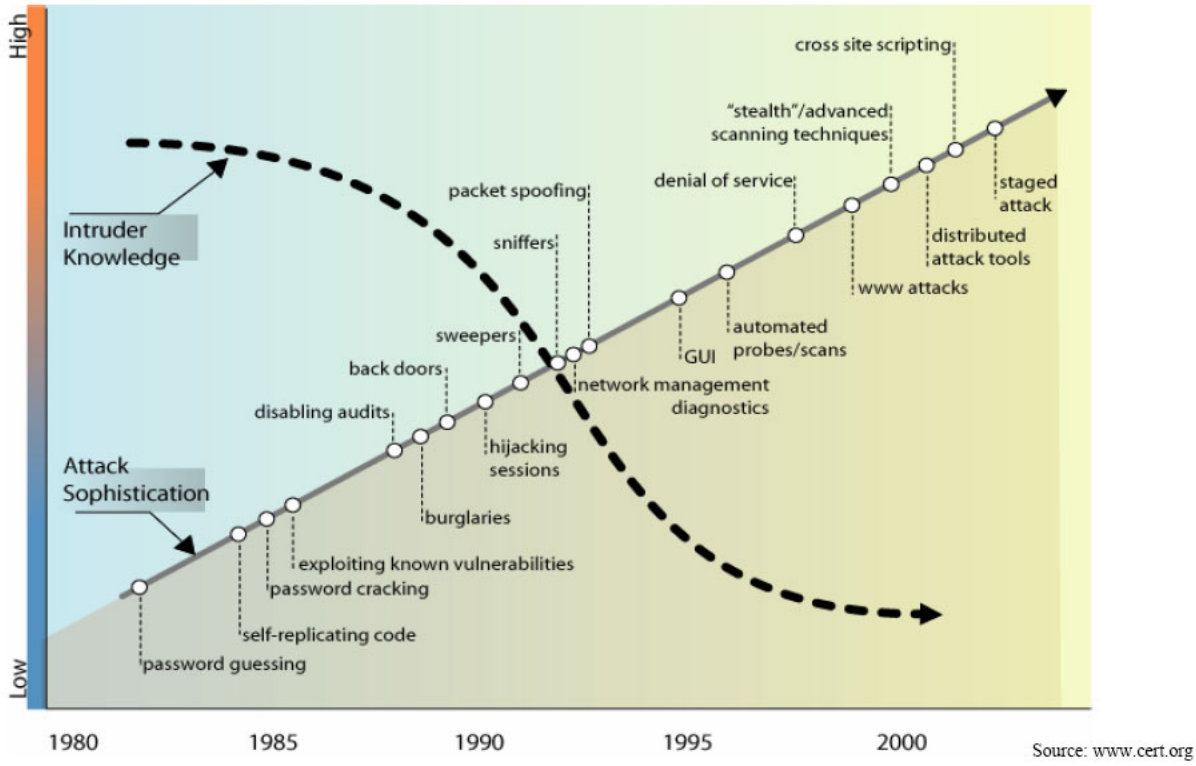


Figure 7 – A graph showing the growing sophistications in attacks being made, and the lesser and lesser amount of knowledge the intruder needs to have to be able carry out such attacks . From (Woody 2003).

“The Global State of Information Security 2005” (PricewaterhouseCoopers) is a world wide survey conducted by CIO magazine and PricewaterhouseCoopers. The results are based on responses from more than 8,200 CEOs, CFOs, CIOs, CSOs, and vice presidents and directors of IT and information security from 63 countries. It covers a broad range of industries such as computer related manufacturing and software, consulting and professional services, banking, government and education. And the results paint a gloomy picture of the state of information security. Millions of personally identifiable records stolen, corporate espionage rings ranging from the UK to the Middle East that uses IT to infiltrate companies. Thousands of phishing scams, and not to forget spam, spyware, zombie networks and DDoS (distributed denial of service) attacks. And last but not least, worms and viruses. Borrowing from forestry parlance, businesses are fire fighters, constantly trying to put out fires, and preventing fire storms and big flare ups.

And even though the numbers show an improvement in the battle to react and fight off security incidents, there is a lack of focus on actions and strategies that could prevent these incidents in the first place. Just 37 percent respond that they have an information security strategy, and only 24 percent of the rest says that creating one is in the plans for the next year. The most common proactive step respondents in the survey have taken is to develop business continuity and disaster recovery plans. That means that even the proactive steps taken are investments in reactive measures. But it is not all bad news. More organizations are employing security executives and focuses on integration between physical and information security. Those companies where the function resides near the top have far better security posture than the average respondent. Only 37 percent of respondents said they have an overall security strategy. At companies with CSOs, the number leaps to 62 percent. Companies with a security executive also report that their spending and policies are more aligned with the business.

The financial services industry is highlighted as a best practices group. The financial sector has long been presumed to practice superior information security, largely because of the preciousness of their assets (which is money) and the fact that its business is carried out almost entirely on IT systems. The stakes are high, the risks are higher, and so the information security protection must be higher too. To en extent, the data supports the notion that companies in the money business are more strategic and more secure than the rest. Financial

services are already using risk models, returns on investment, and other strategic tools in other parts of business, and are now starting to apply these to information security. Also, the financial community knows regulations and has for a long time. One example of organizations in the financial industry being more strategic than others is their planned investment for the next year. Network firewalls is the fifth most strategic priority with all respondents, but it does not even reach the top ten with the financial services companies. The same is valid for data backup which is three overall but not on the financial companies radar. These companies have these important technologies in place, but also seems to have shifted priorities to a more strategic one, perhaps understanding that more technology does not mean more security. Banks was far more likely to have listed compliance testing as an important priority for next year, compared with overall respondents.

4 Modeling the problem

How can one evaluate the effect of information security on oil and gas company's performance, and the impact of information security on the company's resilience against security incidents, both major and minor? This is an important question for the oil and gas industry as it ventures into the era of integrated operations.

For the paper "Exploring Resilience Towards Risks in eOperations in the Oil and Gas Industry" (Rydzak et al. 2006. To appear in Springer's Lecture Notes for Computer Science) for the 2006 SAFECOMP conference, a conceptual model of a generic oil and gas company was created. Using this model I will look at different policies of allocating resources between production and security and hopefully learn some lessons on how they affect the company's performance and resilience.

The problem was suggested and supervised by Professor Jose J. Gonzalez and the modeling was done by Ph.D. student Felicjan Rydzak, research assistant Finn Olav Sveen, and me.

We assume that integrated operations have been fully implemented and are in full deployment. All traditional production processes has been replaced by the Integrated Operations regime and so the model can be kept simple in that it need not consider the transition from traditional work processes to new ones, the introduction of new technology and the maturation of these processes.

By the year 2012 the generic oil and gas company has fully implemented Integrated Operations. Traditional work processes such as drilling, production, delivery and others are now being operated remotely from onshore control centers. Operating costs have been reduced, production is up, and there is an increase in recovery rate. All this due to better utilization of production data, reduced staffing on site, and better collaboration between on- and offshore personnel and operators and their sub-contractors.

The conceptual model represents the generic oil and gas company at a very high aggregation level. There are some aspects that are crucial when modeling the impact of resources on performance:

- The company generates revenue proportional with its uptime.

- To simplify, managers have to consider two aspects; direct resources either to production or to security.
- In today's global market, competition is extremely fierce and every euro counts. So managers have a demand to justify every euro spent on improving and maintaining security, showing return on investment. Hence the assumption is that it is strict management policy to keep investments down. Every euro spent on resources for security means one less euro spent on resources for production, and vice versa.

The model is an extended and adapted version of a casual loop diagram described by Repenning and Sterman in their paper "Nobody ever gets credit for fixing problems that never happened" (2001). Repenning and Sterman have, over the past decade, studied process improvement and learning programs, focusing on the dynamics of implementation and organizational change. The study covers such industries as telecommunications, semiconductors, chemicals, oil, automobile, and recreational products.

Research suggests that the inability of many organizations to reap the full benefits of quality improvement programs is a problem that is rooted in how the introduction of a new improvement program interacts with the physical, economic, social, and psychological structures in which the implementation takes place. Not so much which specific improvement tool is chosen (Repenning and Sterman 2001). The theory in Repenning and Sterman's paper initially originated from a study of two improvement initiatives at a major automotive maker, but they argue that their conceptual model is quite general and can be applied to a range of situations. Similar dynamics have been observed in almost every organization they have studied.

Although it is still early, the trend is towards information security specifically and information technology in general to be viewed more as a traditional business process, and through that undergoing the same quality improvement programs as other processes in a business (Deloitte 2005; Ernst&Young 2005; PricewaterhouseCoopers 2004, 2005).

4.1 Description of Model Stocks and Feedback Loops

Following is a description of the stocks the model contains and the core structure of the model that is made up of four feedback loops.

4.1.1 Security level

Our model consists of three stocks and their connecting flows. First we have the stock *'Security Level'* which has the flows *'Security Level Increase'* and *'Security Level Decrease'*.

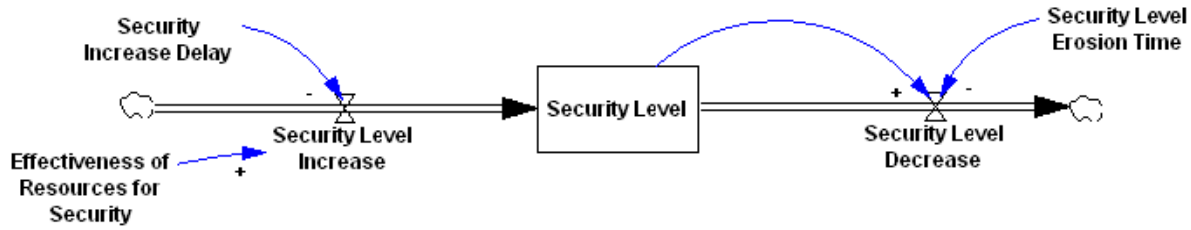


Figure 8 – The Security Level stock in our model.

At any given time the security level in a company is at a given level. The level indicates how well the company is strengthened when facing incidents such as hacker attacks, worms, etc. The security level can be increased through improvement work, but this work can be complicated and take time, and thus there is a delay from work being done on increasing security level and it actually improving. Also, over time, security level will decay with the discovery of new vulnerabilities, more sophisticated attacks, and who employees forget or ignore security policies.

4.1.2 Resources for Increasing Security and Production

To reflect the management issue of considering the two aspects of either allocating resources to increasing security or production we have the two stocks *'Resources to Increase Security'* and *'Resources for Production'*. Managers have limited resources at their disposal and have to allocate them to either security or production. Resources can flow back and forth between the two, though with a delay. This is because moving people between different tasks takes time.

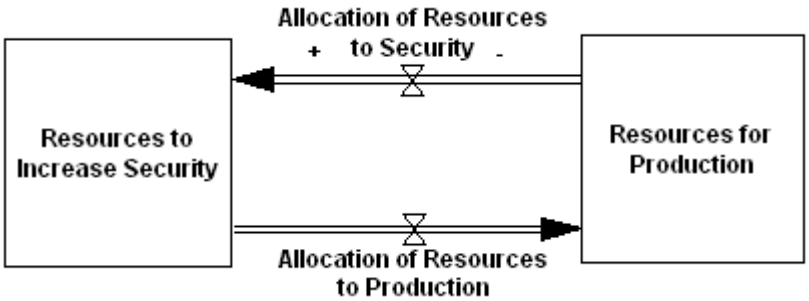


Figure 9 – The stocks for resources for production and to increase security.

4.1.3 Feedback loops

The full model consists of the three stocks and four main feedback loops. These four feedback loops are:

1. B1: PRODUCTION FOCUS – WORKING HARD
2. B2: SECURITY FOCUS – WORKING SMART
3. B3: SHORTCUTS
4. R: REINVESTMENT

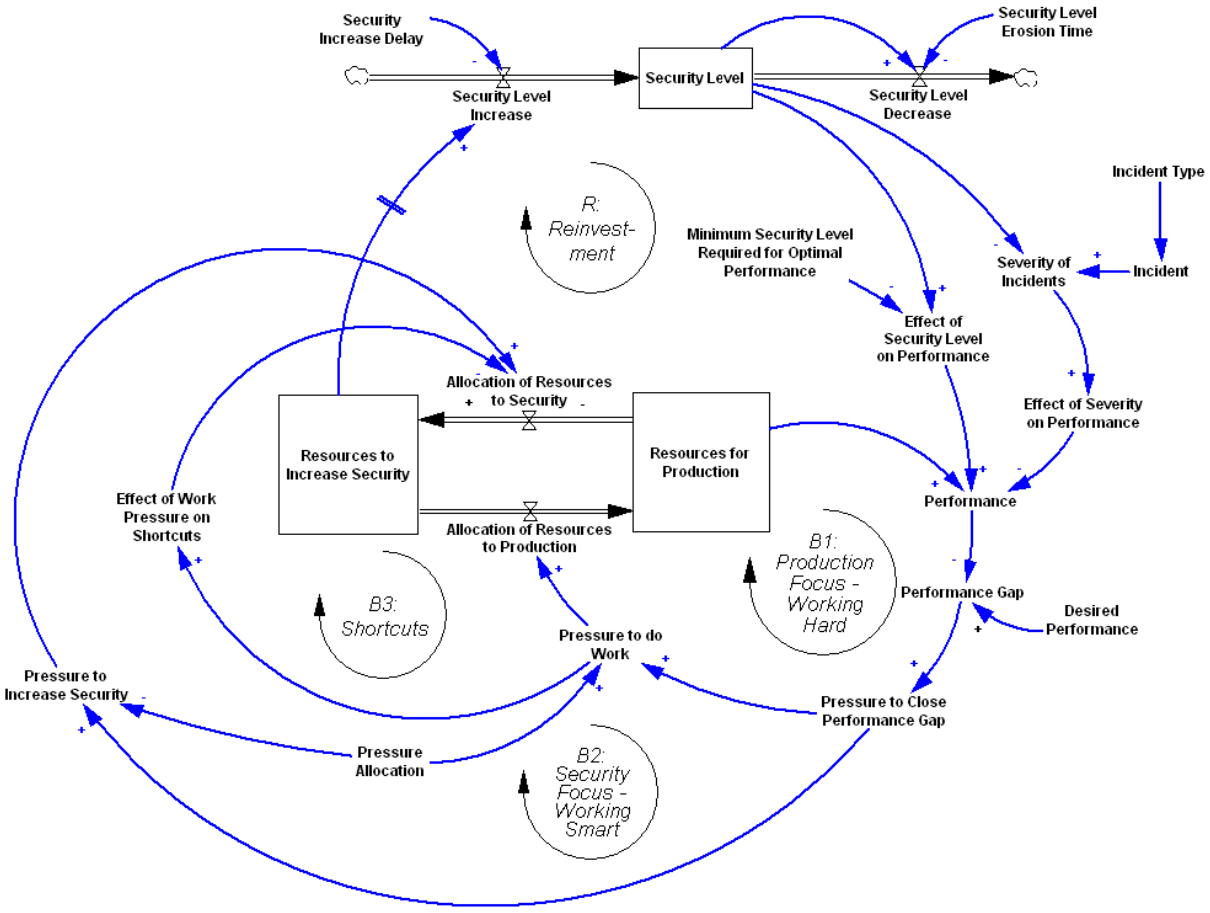


Figure 10 - A ”cleaned up” version of the model. Some lookup parameters are hidden. See appendices for full model view and model print out with all equations.

By analyzing these four loops we can get an understanding of the models dynamic behavior. Following is a description of the four feedback loops.

4.1.4 B1: PRODUCTION FOCUS – WORKING HARD

Our generic oil and gas company has a target for production which is shown in the model as *'Desired Performance'*. Competition is fierce and margins are small, so every little deviation from the targeted production can lead to an economic loss. If an actual performance drops below desired a performance gap occurs. This drop in performance can be due to many reasons: bad weather, equipment trouble, employee failure, etc. The bigger the gap, the greater the pressure is to close it. To close this performance gap management can, and often will, decide to increase production by moving more resources to production. They do this by increasing *'Pressure to do Work'* through *'Pressure Allocation'*. As a result production goes up and the performance gap decreases. But because of our assumption that the company has limited resources, increasing 'Pressure to do Work' through *'Pressure Allocation'* will not only increase *'Resources for Production'* but also reduce *'Resources to Increase Security'* similarly. To understand why this happens we look at the feedback loop B2: SECURITY FOCUS – WORKING SMART

4.1.5 B2: SECURITY FOCUS – WORKING SMART

When management decides to increase the pressure towards production, the consequence is that pressure to increase security diminishes. This is shown in the model with *'Pressure Allocation'*. It has a positive effect on *'Pressure to do Work'* and a negative effect on *'Pressure to Increase Security'*. When *'Pressure to do Work'* increases, more resources are allocated to *'Resources for Production'*. *'Pressure to Increase Security'* decreases and *'Allocation of Resources to Security'* is reduced. With a delay the reduced resources for increasing security will have a negative impact on *'Security Level Increase'* and *'Security Level'* will start to decay. *'Security Level'* has a positive effect on *'Performance'*, as more security means fewer disruptions. Thus, a diminishing *'Security Level'* has a negative effect on the oil and gas company's *'Performance'*, which is production. This has a negative effect on the goal of closing the performance gap through increased production. A different pressure from management towards production versus improving security could cause both feedback loop B1 and B2 to close the performance gap. To see how our oil and gas company can avoid this system reaction we have to simulate the model, which will be done in the next section.

4.1.6 R: REINVESTMENT

The REINVESTMENT loop is a positive feedback loop that tends to strengthen whichever strategy chosen by management. Increasing *'Pressure to do Work'* will lead to an increase in *'Resources for Production'* at the expense of resources devoted to increase security. As there are fewer resources to increase security, *'Security Level'* will diminish having a negative effect on *'Performance'*. As *'Performance'* does not recoup to its desired level, *'Pressure to do Work'* increases even more, creating a vicious circle. The reinvestment loop can also work as a virtuous circle. If '*Resources to Increase Security'* are increased, it will result in an increase in *'Security Level'*. As *'Security Level'* has a positive effect on *'Performance'* it will rise, freeing even more time to working proactively, that is increasing security.

4.1.7 B3: SHORTCUTS

The REINVESTMENT loop means that a temporary emphasis on one management strategy of pressure allocation towards either production or increasing security is likely to be reinforced and driven towards becoming permanent. Organizations that invest in improvement will experience increasing capability and find that they have more time to allocate to working smarter and less need for heroic efforts to solve problems by working harder (Repenning and Sterman 2001). But the reinvestment loop typically works in a downward, vicious direction rather that an upward virtuous direction, in organizations (Repenning and Sterman 2001). The reason for this is the shortcuts loop B3. This loop is also what makes it difficult balancing the allocation of resources between increasing security and production.

When there is a performance gap, increasing pressure to work is a tempting solution. Making people work overtime, redirecting resources from improvement work (i.e. improving security) and cutting corners where possible, gives an immediate result in increased production. The negative effect of such a prioritization has a delay that "hides" them from decision makers. When there is a performance gap at our oil and gas company, employees and managers are tempted by the solution of taking shortcuts and cutting corners where possible to make up for the loss. As a temporary solution more pressure is allocated towards production. *'Pressure to do Work'* increases, *'Resources for Production'* goes up. More resources for production increases *'Performance'*. But abusing the shortcut can be costly in the longer run.
The shortcuts loop and the reinvestment loop works together and creates something that (Repenning and Sterman 2001) calls the Capability trap. Managers often need an immediate

performance lift, and so they take shortcuts and skimp on proactive work, i.e. increasing security. The reinvestment loop, which works reinforcing on whatever regime that the system is in, eventually leads to a drop in capability, i.e. production. This causes the reinvestment loop to work as a vicious cycle, and what was intentionally a temporary shortcut to make up for losses can lead to so many (or severe) security and HSE (Health, Safety and Environment) incidents that the company's performance suffers for a longer period of time.

5 Model Validation and Verification

As Sterman states (2000, p.851): “all models are wrong”. And validation, in the true definition of the word, is impossible. More important questions are if the model is useful and does it shortcomings matter? Following in this section is a description of the model and some tests that have been performed.

As previously mentioned the model consists of three stocks with connecting flows and four feedback loops. The dynamics of these loops have been described and I will not elaborate more on them here.

In the model, the stock *‘Security Level’* simulates the level of security in the organization. *‘Security Level’* can increase affected by *‘Resources to Increase Security’*. This has some delay, as it takes time for workers to complete tasks successfully. Also there is a value indicating the effectiveness of the resources to increase security. This can simulate whether employees are efficient or they are doing a bad job. *‘Security Level’* also has an outflow, as it will deteriorate over time as people tend to forget security policies, new vulnerabilities are discovered, etc.

Our assumption is that performance is dependent on the security level. If security level is poor, people will spend a lot of time on spam, cleaning up after virus attacks, etc., and as a result performance will suffer. There is a *‘Minimal Security Level Required for Optimal Performance’*. This can be perceived as maintaining firewalls and/or other software protecting the operations against casual threats and disruptions. If security level drops below the minimum required level, optimal performance can not be achieved.

The effect *‘Security Level’* has on *‘Performance’* is defined as a lookup graph which input depends on *‘Security Level’* and *‘Minimal Security Level Required for Optimal Performance’*. If *‘Security Level’* is poor *‘Performance’* will be negatively affected. *‘Security Level*’ has an impact on *‘Performance’*, the assumption being that the higher the *‘Security Level’* the less time employees will spend on interruptions caused by threats and disruptions and there will be less downtime. A very high level of security can improve *‘Performance’* above what is produced by resources for production, but only to a certain degree.

To simulate an incident such as a hacker attack, a worm or a virus, or a malicious insider, in the model we have *'Incident'* and *'Incident Type'*. *'Incident Type'* ranges from a type 1 incident to a type 6. Incident type 1 being insignificant and 6 being catastrophic. 0 indicates no incident. This is based on the risk matrix developed from our case studies for the oil and gas field in the Integrated Operations regime. The severity of an incident is affected by the organizations security level. The severity of an incident is more efficiently mitigated the higher the security level is. As an analogy one can think of a bullet proof vest, the better protection, the more of the blow is softened. If security level is high in the organization (security policies are in place and followed and systems are patched and updated) then the severity of an incident will not be as serious.

Next, the effect of an incident on performance is decided by a look up graph. More severe incidents impair performance. In case of a catastrophic incident the performance can drop even to zero if there is not a sufficient level of security. *'Performance'* is decided by the amount of resources dedicated for production, the effect of security level, and the effect of an incident (should one occur). If performance is below the desired performance a performance gap occurs. The performance gap together with the company's goal to close performance gaps creates a pressure to close the gap. The larger the gap is, the higher the pressure to close it.

The pressure to close the gap in the model is linked to 'Pressure to Increase Security' and 'Pressure to do work'. What decides which to be weighted is 'Pressure Allocation' that simulates management's pressure towards focusing on either production or increasing security. It ranges from 0 to 1. 0 being 0% pressure towards production, and 1 indicating 100%. The two types of pressure have an effect on the allocation of resources to production and security. In addition to this, there is an extra loop. This is the shortcuts loop which simulates workers tendency to take shortcuts when faced with an increased demand for production. When faced with pressure to do work, employees tend to take shortcuts and cut corners in their work. This *'Effect of Work Pressure on Shortcuts'* has an effect on the *'Allocation of Resources to Security'*. The higher the pressure to do work, the more the shortcuts loop comes into effect stopping resources being allocated to security. Both *'Resources to Increase Security'* and *'Resources for Production'* has a minimal amount of resources they can not drop below.

The model of the generic oil and gas company is highly aggregated and, thus, "simple". Would making the model more realistic and complex, adding more parameters, change its results significantly? The model should in the future be adapted and extended to give an even better description of an oil and gas company. But we argue that the four feedback loops "B1: PRODUCTION FOCUS – WORKING HARD", "B2: SECURITY FOCUS – WORKING SMART", "R: REINVESTMENT", and "B3: SHORTCUTS" are ubiquitous to many enterprises, both the oil and gas sector and other sectors (Repenning and Sterman 2001, p. 3).

So while the model is simple we argue that it captures the most important feedback structures (and the evolution of these), that shape the dynamic behavior of the system over time.

The model is tested for dimensional consistency. The same is valid for extreme values. If, for example 'Total Resources' is set to zero, resources for production and security is set to zero, and with them performance and security level. If 'Pressure Allocation' is set to its extreme values 1 or 0, either resources for production or to increase security falls to its minimum level. If the minimum amount of resources dedicated to production is set to zero, then resources dedicated to production can fall to zero and if so production also drops to zero. Also, integration tests have been performed.

6 Model Simulations and Policy Testing

In this chapter I will simulate different management policies and look at how different strategies of resource allocation to production and increasing security affect the company's performance. The types of incidents in the model are based on a risk matrix from a genuine oil and gas company. The incidents range from 1 to 6, where 1 is an insignificant incident and 6 is catastrophic. Incident type 1 can occur quite often, while incident type 6 is very rare.

In integrated operations, a security incident can have serious performance and HSE implications. The cost of one day of production downtime in offshore operations is estimated to 1.6 million € for smaller platforms and 25 million € for the larger ones. And although a security incident is serious enough, it can have additional implications to just the short term costs of downtime and HSE implications. As the processes in the company changes, depending on each other, policies chosen by management and other important actors can lead the system into a highly undesirable state.

Following are the simulation of three different management policies and their results. The different policies each have a specific focus. In Policy 1 management has focus on production as a solution to solve performance gaps. In Policy 2 the focus lies heavy on improving security as a way to recoup from drops in performance. In the third policy management makes an effort to balance resource allocation between production and increasing security.

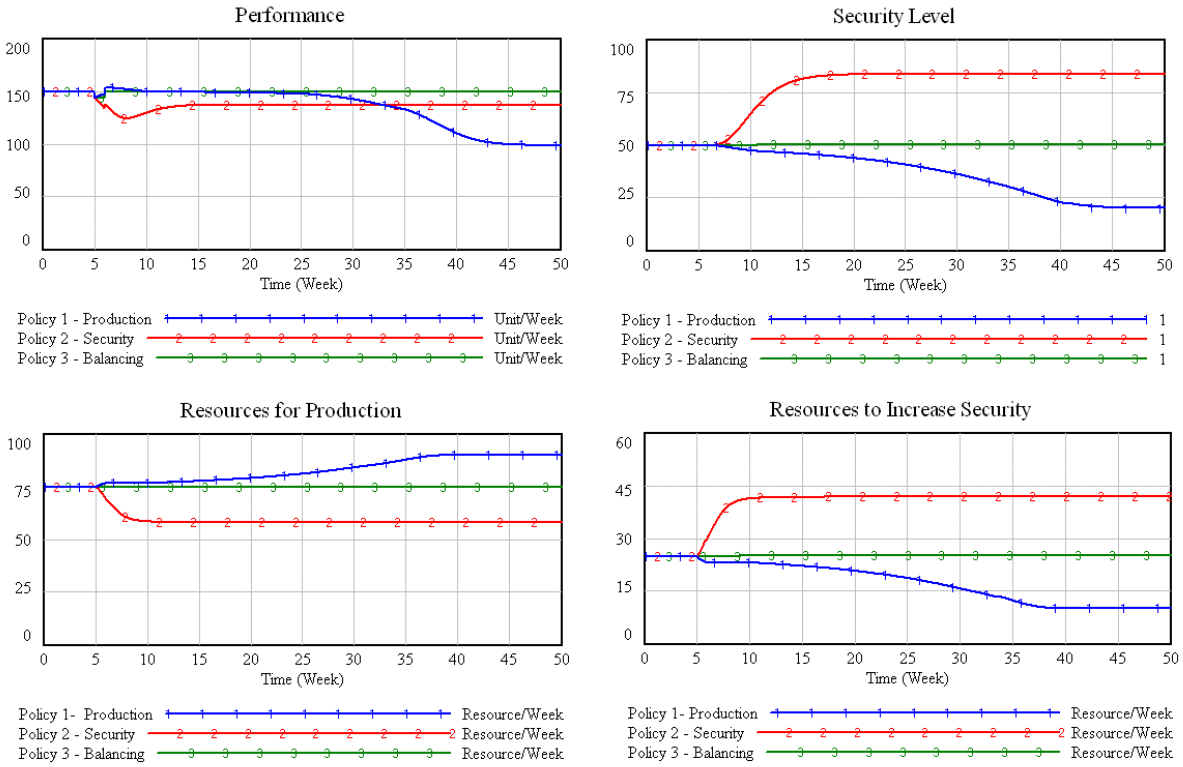


Figure 11 – Results from simulation of policies 1, 2 and 3.

6.1 Policy 1 - Production

In Policy 1 management believes that increased work pressure is the way to get back what is lost when there is a performance drop. *'Pressure Allocation*' in the model is set to 0.9, indicating that there is a 90% pressure towards production when a performance gap occurs. The simulation of this policy is labeled "Policy 1 – Production" in Figure 11 and is the blue line marked with 1's in the four graphs.

Imagine the following scenario: At an offshore platform, production is going good. All systems are functioning well and security level and performance are stable. The system is in equilibrium. But one week (week 5 in the simulation in Figure 11) the platform experiences a security incident, classified as a type 3 security incident. To close the performance gap and get back to desired performance management puts pressure on employees to work overtime and cut corners where this is possible. Employees working on more strategic processes, such as improving security are moved to more pressing matters. The most important thing now is to meet the performance goals that are set by upper management. If these goals are not met there will be repercussions, so proactive work like increasing security will just have to wait.

Besides, putting these tasks on hold does not have any significant negative effect, and moving resources to production gives an immediate return on investment, namely increased production. It is considered a temporary solution, just so the platform can get back to desired performance level and maybe recoup some of the losses.

And initially that is exactly what happens. The company's performance recoups to its original level and actually exceeds it. The management is thrilled, not only have they bounced back from the incident. They are also doing so well that they can make up for some of the losses caused by the incident and its implications. But the company has limited resources, and so moving resources to production means that they have to be taken from another source, in this case increasing security. And the reduced amount of resources used to increase security means that security level will start to deteriorate. Important patches are not installed, or the work of installing them are not done as properly as desired, an analysis of the root cause of the incident can suffer as there are limited resources to perform tasks. And finally the solution to the initial problem may be abysmal.

While production is measured in barrels of oil produced and gives an exact measurement, security is more of an abstract value. It is difficult to measure it in a specific value. Also, the effects of neglecting the task of increasing security are delayed and so they can be difficult for management to see.

As described in the above text, we can see from the performance graph in Figure 11 that performance drops when the company experiences an incident. As there is pressure from management to work extra and cut corners where possible to solve the problem, *'Resources for Production'* increases and *'Resources to Increase Security'* is reduced equivalently. The reduction in resources increasing it causes security level to deteriorate, and in approximately week 45 the security level has dropped so low that even the maximum amount of resources devoted to production does not help. Performance drops down to a more permanent poor level and the system has moved into a highly undesirable state.

6.2 Policy 2 – Security

In policy 2 the management has a much higher focus on improving security, and this is prioritized when there are incidents and disturbances to the system. *'Pressure Allocation'* in

the model is set to 0.2, (20% pressure towards production) indicating that it is management policy to keep focus on security improvement at all times. The simulation of this policy is labeled "Policy 2 – Security" and is the red line marked with the number 2 in the four different graphs in Figure 11.

Imagine the following scenario: In the beginning, as in the first scenario, the system is in equilibrium. But one week (week 5 in the simulation in Figure 11) the offshore platform experiences a security incident. The incident is classified as a type 3 security incident. As opposed to the management policy in the first simulation where the pressure was on production, management now has a different approach. Their focus is on maintaining (and improving) security. When the incident occurs the management keeps their cool, although there is a lot of pressure to recover to the targeted level of production. Resources are moved from production to increasing security and security level rises. The company can thoroughly identify the incident and find the underlying reason for why it occurred. By doing so they can correct it properly and implement a solution that reduces the probability of the incident happening again.

But as in the first policy available resources are limited. As more resources are moved to proactive tasks, i.e. increasing security, the resources dedicated for production are reduced equivalently. And so, even if *'Security Level'* rises, making the company's information security more robust and able to withstand hacker attacks, worms, spam, etc. that lowers performance, since the resources for production are so limited the performance (i.e. production) falls to a level below its original one. However the performance never drops to a lower more permanent level, indicating that the system better can handle incidents when they are putting a lot of attention on increasing their information security. Even so, the company's performance is not as good as original, and one can argue that the process of information security is overdone.

6.3 Policy 3 – Balancing

In the third policy simulated, the company tries to balance the resource allocation between increasing security and production. Information security is considered a risk management area, and investments in security are optimized to minimize their cost-risk product. To simulate this, *'Pressure Allocation'* in the model is set to 0.6, indicating a 60% pressure

towards production. The simulation of this policy is labeled "Policy 3 – Balancing" and is the green line marked with 3 in the graphs in Figure 11.

The scenario is the same as in the previous simulations. The system is originally in equilibrium, but one week the offshore platform experiences an incident (week 5 in the simulation). The incident is classified as a type 3 incident. Management has a balanced view on investing in production versus increasing security. No major changes in the allocation of resources are done and so both *'Resources to Increase Security'* and *'Resources for Production'* remains almost unchanged (slight increase in *'Resources to Increase Security'*). People who are already committed to security work continue working on these processes, correcting the error and preventing it from affecting the system again. At the same time, production is not neglected. The company's performance recovers almost all the way to the target level after just one week, and fully recovers in week 12. The company does not make up for the lost production, but maybe more importantly, it does not fall into an undesirable state and it recovers to its targeted performance level. Resource allocation is not weighted too much to either production or increasing security.

The last policy seems to be the best one. But balancing resource allocation in real life is an extremely difficult task, as parameters change constantly, as do processes. Also, evaluating the value of information security is very difficult. Less than half of business ever evaluate their return on investment on security spend (PricewaterhouseCoopers 2004). Resources spent on information security are seen as overhead rather than an investment. Senior management views information security as a forced expenditure rather than something that can bring business benefits.

Also, in one year the company might experience more than one single incident. This is plausible when considering the risk matrix developed from case studies. Therefore additional simulations are required before any policy recommendations can be given.

7 Multiple Incidents

I have previously simulated what will happen to a company's performance should they experience an incident. But there are no guarantees that only one incident will occur. I will in this section look at what happens when more than one incident occurs, and how this affects the company.

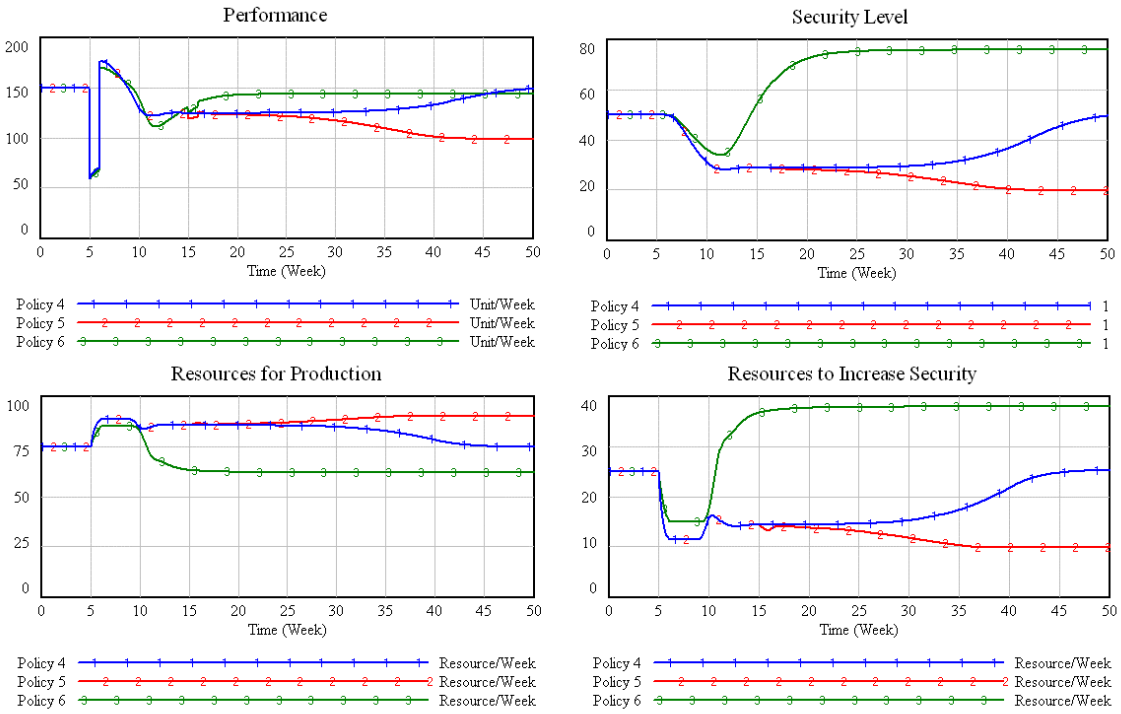


Figure 12 – Results from simulation of policies 4, 5 and 6.

7.1 Policy 4

In this policy simulation the company is only affected by one incident. In the next policy simulated the scenario is similar but the company experiences a second incident some time after the first. I have done this for comparison reasons, showing the different reaction of the system when there are multiple incidents instead of one. In this scenario the company experiences a very severe incident, it is of type 6 and is considered catastrophic, in week 5 of the simulation. This simulation is marked "Policy 4" in graphs in Figure 12 and is the blue line marked with the number1. *'Pressure Allocation'* simulating management policy is set to 0.6 indicating a 60% pressure towards production. Immediately after the incident the

company's performance drops to below half. As a result of the management's policy of focusing on production, *'Resources for Production'* are immediately increased, and *'Resources to Increase Security'* are reduced equivalently. Also, pressure from the *Shortcuts* loop works as an amplifier on this reallocation of resources.

Thanks to the great increase in *'Resources for Production'*, the company's performance recovers quite quickly (in week 6) and actually improves. From week 6 till 9 the performance higher than what it was compared to before the incident. But because of the limited resources now allocated to improving security, the work of analyzing the accident, implementing solutions that fix the fundamental problem is not prioritized. *'Security Level'* diminishes, and as a result it has a negative effect on *'Performance'*. It drops down to a lower level again, on which is stabilizes. Over some weeks, the system mitigates the damages from the incident, and *'Resources to Increase Security'* and *'Resources for Production'* returns to their initial values. This enables the company to recover to its original *'Security Level'* and in approximately week 55 *'Performance'* is back at desired level. This is thanks to the management and their policy to avoid neglecting information security even when there is an incident that affects performance and pressure to recover quickly is high. But is it adequate? In the next policy test I will simulate what happens when there are two incidents.

7.2 Policy 5

The simulation is marked "Policy 5" in the graphs in Figure 12 and is the red line marked with the number 2. In this scenario, the company experiences two incidents. The first one occurs in week 5 and is considered a type 6 incident (catastrophic). And as this is not enough, in week 15 there is a second incident. It is not as serious as the first on, this time a type 3 incident, but it still disrupts the system. According to the risk matrix that is developed from case studies, such a scenario is plausible. *'Pressure Allocation'* simulating management's policy on resource allocation is set to 0.6 indicating that there is 60% pressure towards production.

The dynamics of this scenario is, up until the second incident, identical to that of the previous scenario. But as the second incident occurs it becomes clear that the system is in a fragile state. The second incident, although small, causes a shift in the allocation of resources. Instead of '*Resources to Increase Security'* and *'Resources for Production'* returning to their

original level, the system is not able to mitigate the impact, and shifts into an undesired state with stable underperformance. Not unlike the one seen in "Policy 1 – Production".

7.3 Policy 6

The simulation of this scenario is marked "Policy 6" in the graphs in Figure 12 and is the green line marked with the number 3. This scenario is very similar to the one in Policy 5. The occurrence of incidents and the time at which they happen are identical, but in this scenario the managements focus lie more heavily on proactive work, i.e. increasing security. *'Pressure Allocation'* is set to 0.3 indicating only a 30% management pressure towards production.

Again there is a catastrophic incident in week 5, which severely disrupts performance. And although many resources are moved to production, influenced by (but not only because of) the *Shortcuts* loop, the management policy of keeping much more focus on security *('Pressure Allocation'* = 0.3) keeps the resource allocation more balanced. The performance curve follows much of the same behavior peaking shortly after the incident, but the top is somewhat lower and it actually drops below what was the case in the previous two scenarios. This is because the amount of resources dedicated for production is somewhat lower. At the other hand, this means that *'Resources to Increase Production'* is higher and so *'Security Level'* does not diminish as much, and recovers faster.

The focus on security not only leads to a faster recovery of *'Security Level'*, but when the second incident occurs in week 15, the system can absorb it without going into an undesirable state of under performance. The backside of the medal is that since the focus lie so heavily on increasing security, *'Resources to Increase Security'* stabilizes on a much higher level, which consequently has to lead to fewer resources available for production. The company's performance recovers, but at a level somewhat below what is desired.

7.4 Sensitivity Analysis

Running a sensitivity analysis can give some insights as to how the dynamics of the system behaves. In this sensitivity analysis two incidents are set to occur. A type 6 incident occurs in week 5, and a type 3 incident in week 15. *'Pressure Allocation'* is set to go from 0.3 to 0.8, to

see how the system behaves as management policies change. Since it is *'Pressure Allocation'* that I am interested in, no other values are changed.

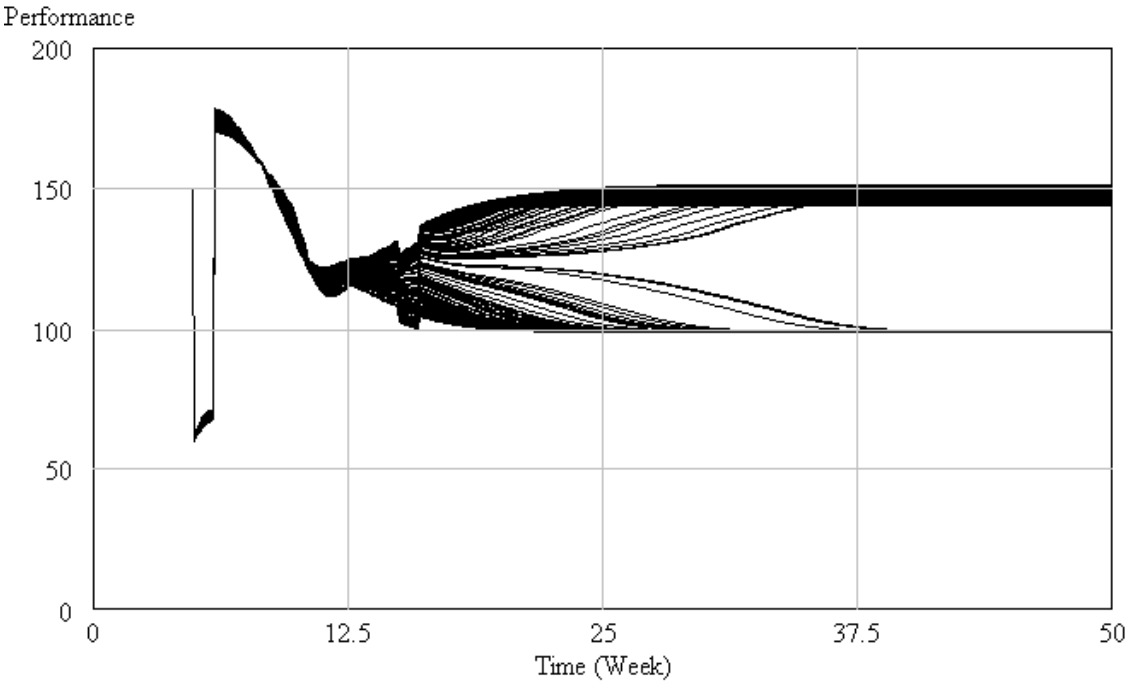


Figure 13 – Sensitivity analysis of 'Pressure Allocation'

From Figure 13 one can see that the system basically has two possible states that it can end up in after having experienced two incidents. Either the performance returns to desired level (with some variations above or below), or the performance drops permanently to a lower level. That is the system enters an undesirable state.

8 Increase in Desired Performance

It is not only incidents that can affect a company's performance. In the following simulations I will look at what happens when there is an increase in the desired performance. Since I am only interested in how the policies from management affects the system when there is an increase in the desired performance, only *'Pressure Allocation'* is changed. All other parameters remain unchanged.

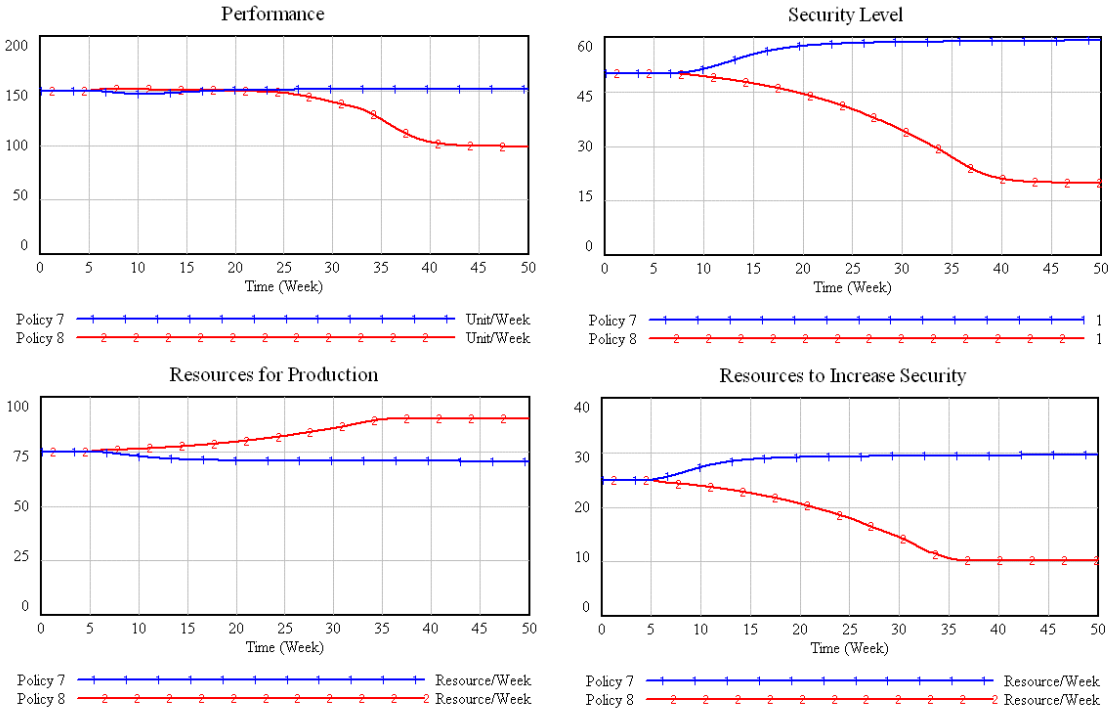


Figure 14 – Results from simulation of policies 7 and 8.

8.1 Policy 7

The scenario is as follows: The production on the offshore platform is going well. Production demands are met and the system is in equilibrium. But one week (week 5 in the simulation) the management on the offshore platform is faced with a demand for increased production. Upper management has decided that the platform has a potential for higher production, and the *'Desired Performance'* is increased by 1% from 150 to 151,5. *'Pressure Allocation'* simulating management pressure is set to 0,5, indicating a 50% pressure towards production.

What happens when policy 7 is simulated is shown in the four graphs in Figure 14 and is the blue line marked with the number 1.

As a result of the increase by 1% in *'Desired Performance'* more resources are moved to increasing security. Consequently *'Resources for Production'* is reduced equivalently. This is because it is management policy to keep focus on increasing information security when facing disruptions. As *'Resources to Increase Security'* rise *'Security Level'* increases. But since it is a delay for it to increase the company will first experience a small drop in performance. When *'Security Level'* starts rising and thus affecting *'Performance'* positively, the company's performance will rise above its initial level, although still falling a bit short of the new desired level of performance.

8.2 Policy 8

The scenario is the same, but in this policy management is much more likely to put pressure on production, asking employees to cut corners and take shortcuts where possible to meet performance demands. To simulate this *'Pressure Allocation'* is set to 0,9 indicating a 90% pressure towards production. The simulation of policy 8 can be seen in the four graphs in Figure 14 and is the red line marked with the number 2.

As a result of the management policy to throw recourses into production when there is a performance gap, *'Resources for Production'* starts to increase when the offshore platform is faced with a new performance demand. As a result of the 1% increase in *'Desired Performance'* in week 5, *'Resources for Production'* starts rising influenced by the *Shortcuts* loop. The company's performance rises, but since the increased focus on production has lead to a decrease in *'Resources to Increase Security'*, with a delay *'Security Level'* starts diminishing, having a negative impact on *'Performance'*. The situation escalates as more and more resources are moved to production as performance starts to drop, and in approximately week 20 is below its original level. Employees spend more and more time on coping with problems caused by the deteriorating security level and eventually the system can not cope, and goes into an undesirable state of stable low performance.

9 Policy Analysis and Recommendations

In this chapter I will analyze the different policies and describe some findings using system archetypes.

9.1 Coping with problems

Wolstenholme (2002) describes the generic problem archetype "Out-of-control" which is shown below in Figure 15. The archetype consists of one balancing loop, which is a result of a control action taken by the organization to handle a problem. The unintended consequence is that there is a reaction from another sector in the organization, and this creates a reinforcing loop. This leads to a worsening of the problem, and it gets more and more out of control. It is usually the control action, rather than the outcome that creates the reaction.

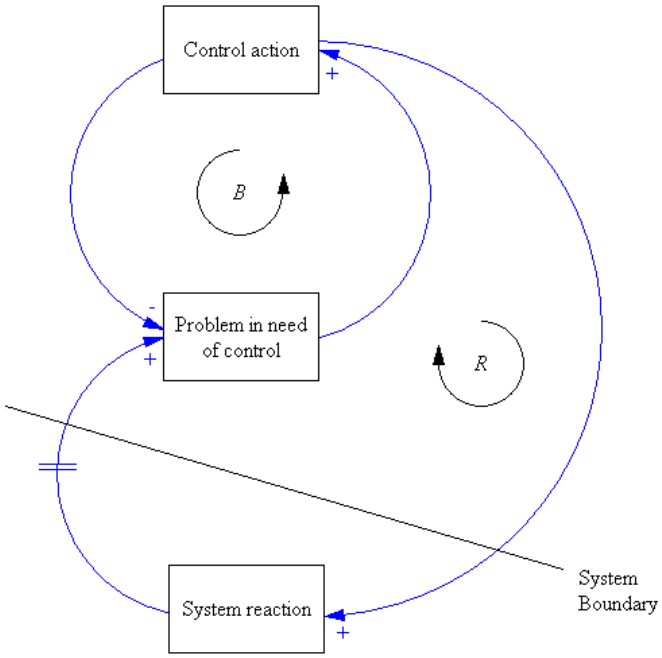


Figure 15 – Out-of-control problem archetype.

For every problem archetype, there is a solution archetype. This is presented in Figure 16. The solution archetype suggests that the solution to an out-of-control archetype lies in emphasizing a direct link between the problem and the unwanted reaction. The purpose of this being is to introduce a balancing loop that counters the reinforcing reaction.

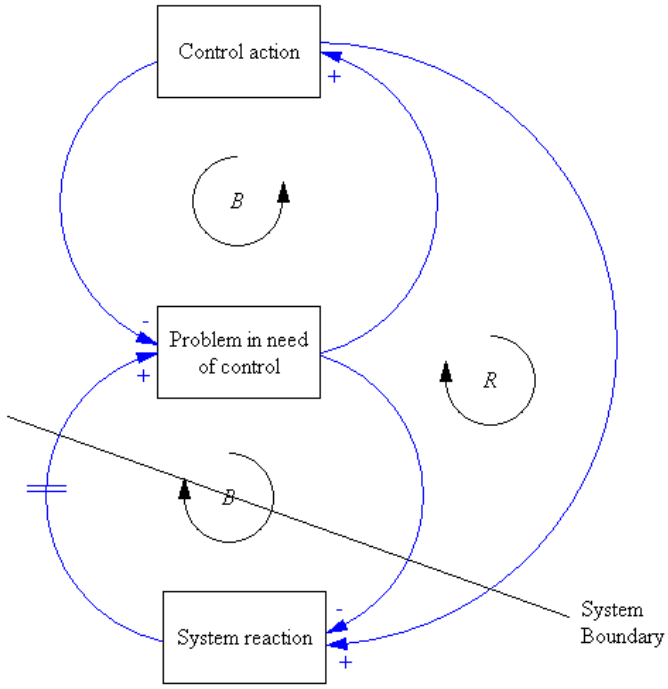


Figure 16 – Out-of-control solution archetype.

I hypothesize that the way companies and management react to information security incidents leading to performance gaps, can move the system state from a desirable one to an undesirable state of weakened resilience. This can possibly cause the system to move into an undesirable state of constant under performance.

The processes working in the company when afflicted by incident(s) can be described by an "Out-of-control" archetype. The problem archetype is seen in Figure 17. In policies 1 and 5 we see typical "better before worse" scenarios, which behavior fits the archetype. The company is afflicted by an incident (in the case of policy 5 there are two incidents) and a performance gap occurs. Management has a production oriented focus, and so employees are more likely to cut corners and take shortcuts where possible, and in addition more resources are moved to production.

Initially this is successful, with a performance that recovers and actually improves. But what can be difficult for management to see is that this kind of focus on production leads to diminishing security level. This can be difficult to recognize for different reasons. There is a division in time between when the incident occurred and the management's policies to focus more in production came into action, to the security level starts deteriorating. The unintended

consequence of a deteriorating security level has a delay that can "hide" it from the view of the decision makers that initiated its cause. Another reason that it can be difficult to recognize that security level will suffer from production focus when facing a performance gap is that security level is very difficult to assess. As previously mentioned, less than half of businesses ever evaluate their return on investment on security spend.

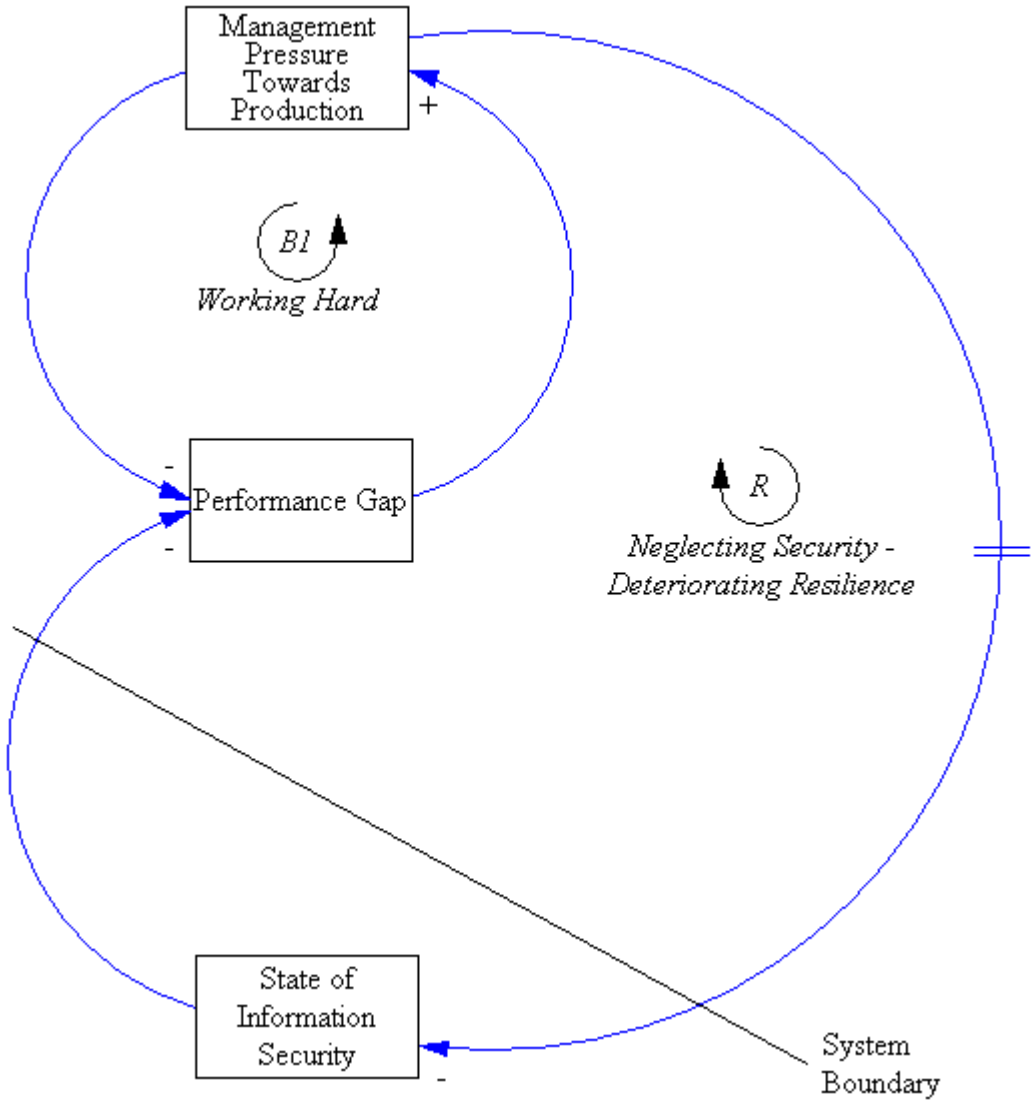


Figure 17 – "Working Hard". An Out-of-control archetype showing some possible dynamics of the system.

As the state of information security worsens, it has a negative impact on performance, causing the performance gap to increase. What was initially a solution has now worsened the problem, as it starts to get out of control. These dynamics are similar to the ones in IT management identified by Moore and Antao (2006), where it is shown that shifting personnel from planned

(pro active) work to problem-repair work to manage downtime can work in the short term, but in long term has costs that can be overwhelming.

Both in policy 1 and 5 (shown in Figure 11 and Figure 12) one can argue the system is not resilient. Resilience, in this case, being the capacity of the system to undergo disturbances and still maintain its functions, structures and controls. As the system experienced an incident it was not able to absorb the impact and it went into an undesirable state of stable under performance.

The solution to the discussed problem would be to have a more balanced allocation of resources, particularly when the system experiences an incident and is fragile. A balanced view on resource allocation would in this case be not moving so many resources to production when there is a performance gap. Alternatively it would be increasing the total number of resources, keeping security from deteriorating.

The solution archetype is shown in Figure 18 and the solution loop *B2: Balanced Resource Allocation* counters the reinforcing loop *R: Neglecting Security - Deteriorating Resilience*. One can see from policy 2, 3, 4 and 6 that when management has a greater focus on maintaining security level (not moving resources to production when faced with a performance gap) that the system does not move into an undesirable state. It is resilient.

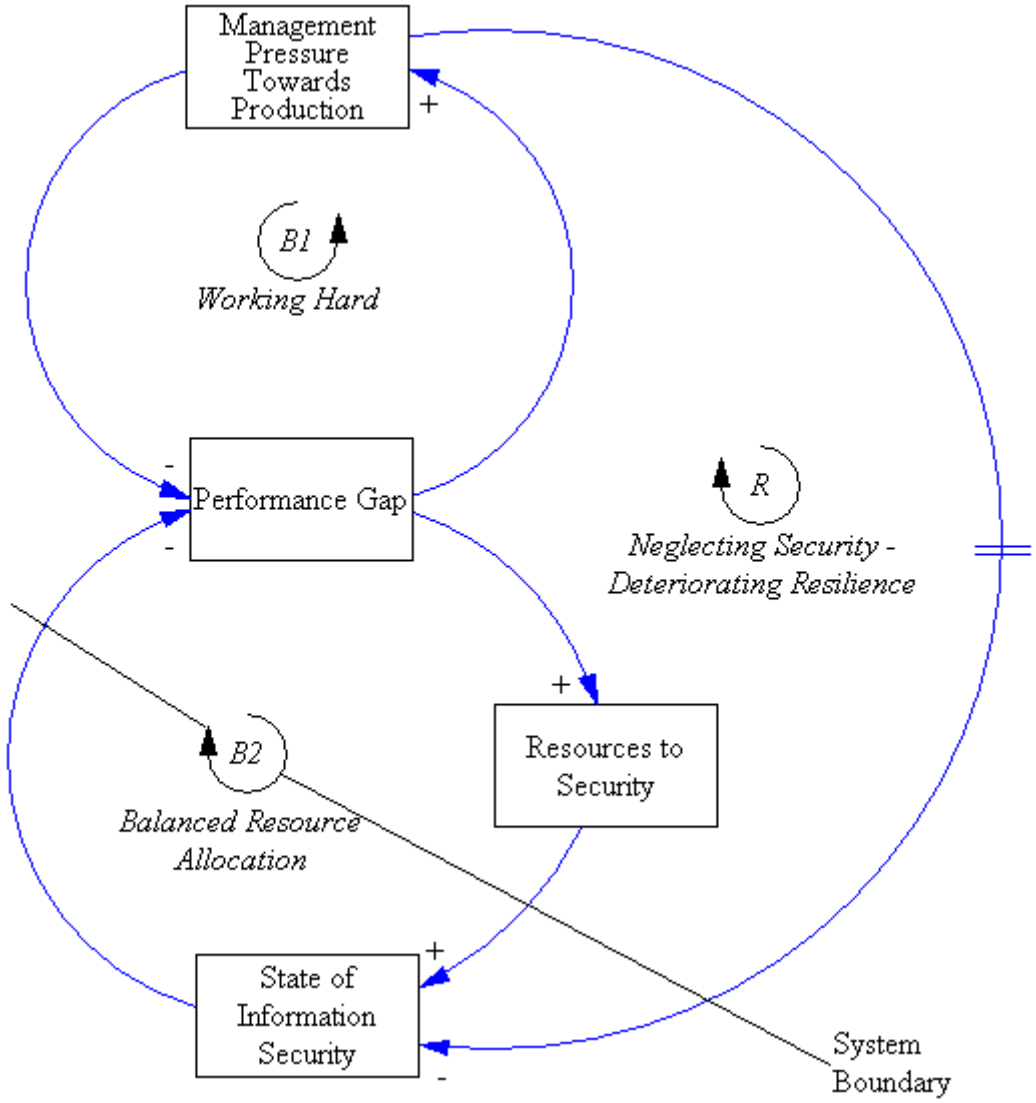


Figure 18 – The solution archetype to the problem archetype in Figure 17.

Cooke (2004) writes:

"While it may be "normal" or "natural" for an organization to respond to production pressures as its first priority, it should be the role of management, especially senior management and the Board of Directors, to make *safety* the organization's first priority. If the company fails to do this, then safety must be enforced by the regulators. Safety commitment is not self-sustaining, and so leverage must be applied to maintain it. Without safety, there can be no assurance of production. Production issues can be dealt with once safety has been addressed. With safety as the first priority, reinforcing feedback loops will operate as virtuous circles instead of vicious circles. As commitment to safety increases, losses from incidents will fall, productive experiences will grow, and production performance will improve."

Even though Cooke (2004) focuses on safety programs and its effect on incidents and production in a coal mine there are some parallels, when viewing safety and security as related areas (Cooke argues that there are conceptual similarities between safety management and quality management). Safety is an important factor influencing production (performance). An incident causes downtime and loss of production. The higher the level of security, the less incidents/impact from incidents. One can argue that with integrated operations, information security will become as mission critical to production as safety is the mining industry.

From the policies we see that the system can work as a vicious circle leading the system into an undesirable state (policies 1 and 5), or a more virtuos circle actually leading to improved performance (policy 4). This is supported by the sensitivity analysis in Figure 13 in which the system, depending on management policy ('Pressure Allocation' in the model) either is resilient or falls into an unwanted state, which in itself is resilient. This is similar to Cooke's (2004) conceptual model where the system can operate in two ways, either as a vicious circle resulting in failure, the other being a virtuos circle resulting in success.

9.2 Increasing Performance

When managers are faced with the challenge of increasing performance, often their focus will lie on production. It can be natural choice, if you produce a certain amount pr man hour, increasing the man hours spent on production will give you the wanted result. And in an organization with unlimited resources that might be true. But in most (dear I say all) organizations that is not the case.

Wolstenholme (2002) describes the generic problem archetype called Underachievement which is shown below in Figure 19. The problem archetype consists of a reinforcing intended loop to achieve a successful outcome in one sector of an organization. The reaction from another sector, usually as a result of hitting against a resource constraint, creates a balancing unintended loop. This causes a delayed underachievement over time.

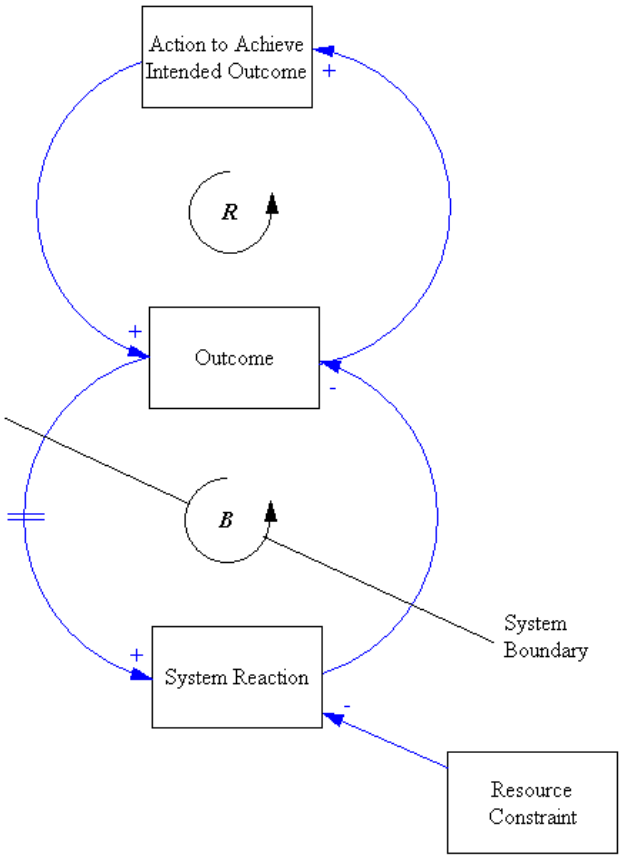


Figure 19 – Underachievement problem archetype.

The solution archetype in Figure 20 suggests that the closed loop solution to an underachievement archetype lies in trying to use some element of the achievement action to minimize the reaction in other parts of the organization. Usually it is unblocking the resource constraint. The way to do this is introducing a reinforcing loop that counters the balancing reaction.

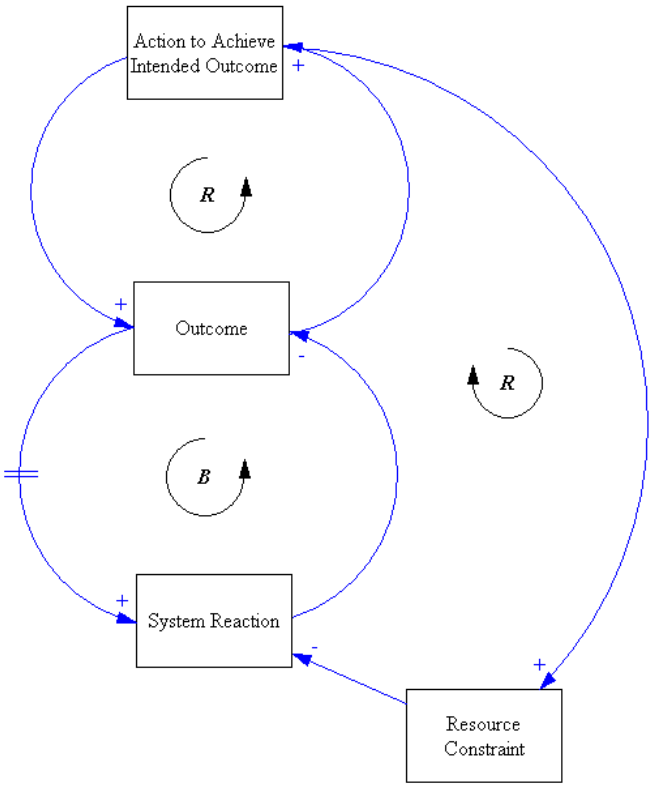


Figure 20 – Underachievement solution archetype.

I hypothesize that manager's actions and policies when faced with a demand of increased performance can constrain the desired performance, or even worse, cause the system to deteriorate into an undesirable state.

The processes working in such a scenario can be described by an "Underachievement" archetype shown in Figure 21. Management's goal is to increase performance, and to achieve this they put pressure on production. Workers are influenced and pushed to cut corners were possible and take shortcuts in their work. Tasks directly related to production are prioritized over more proactive work (i.e. increasing security) and as employee throughput increases so does performance. But the cutting of corners and shortcuts taken by employees has a delayed cost. With a delay their allocation of resources causes security level to drop and it has a negative impact on performance which is balanced and leveled out, or even worse starts to deteriorate. When a performance gap occurs the dynamics of the "out-of-control" archetype in Figure 17 takes over.

In policy 8 shown in Figure 14 we see the result of what happens when there is increase in desired performance. Management's production focus initially gives an increase in

performance as production gains priority over other tasks. But after some delay security level starts to deteriorate. Performance is limited and possibly even starts to decrease, thus causing a performance gap.

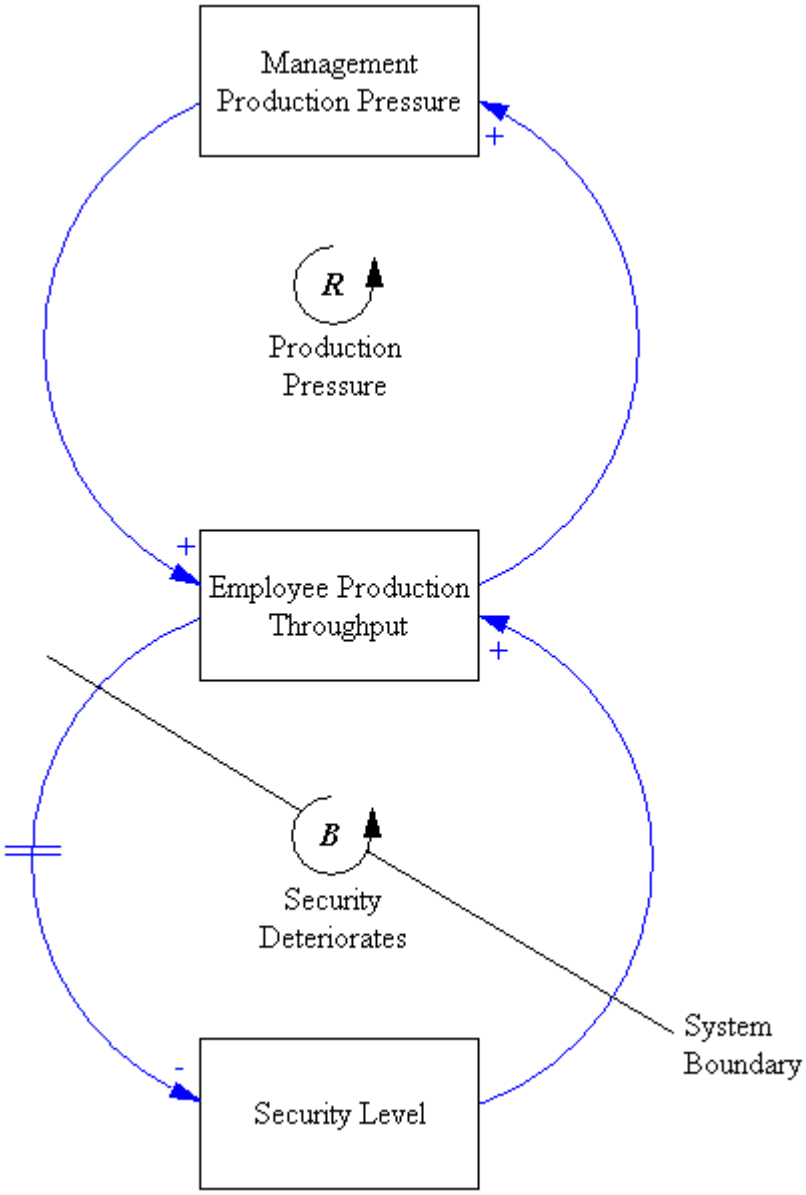


Figure 21 – ”Production Focus”, an Underachievement problem archetype.

The solution to this problem is for management to always have security in focus when trying to increase the company’s performance. The solution archetype is shown in Figure 22. There must be a balance when dividing resources between production and security. If management ensures that enough resources are used on security this will hinder the deterioration of security level, and the company’s performance can increase.

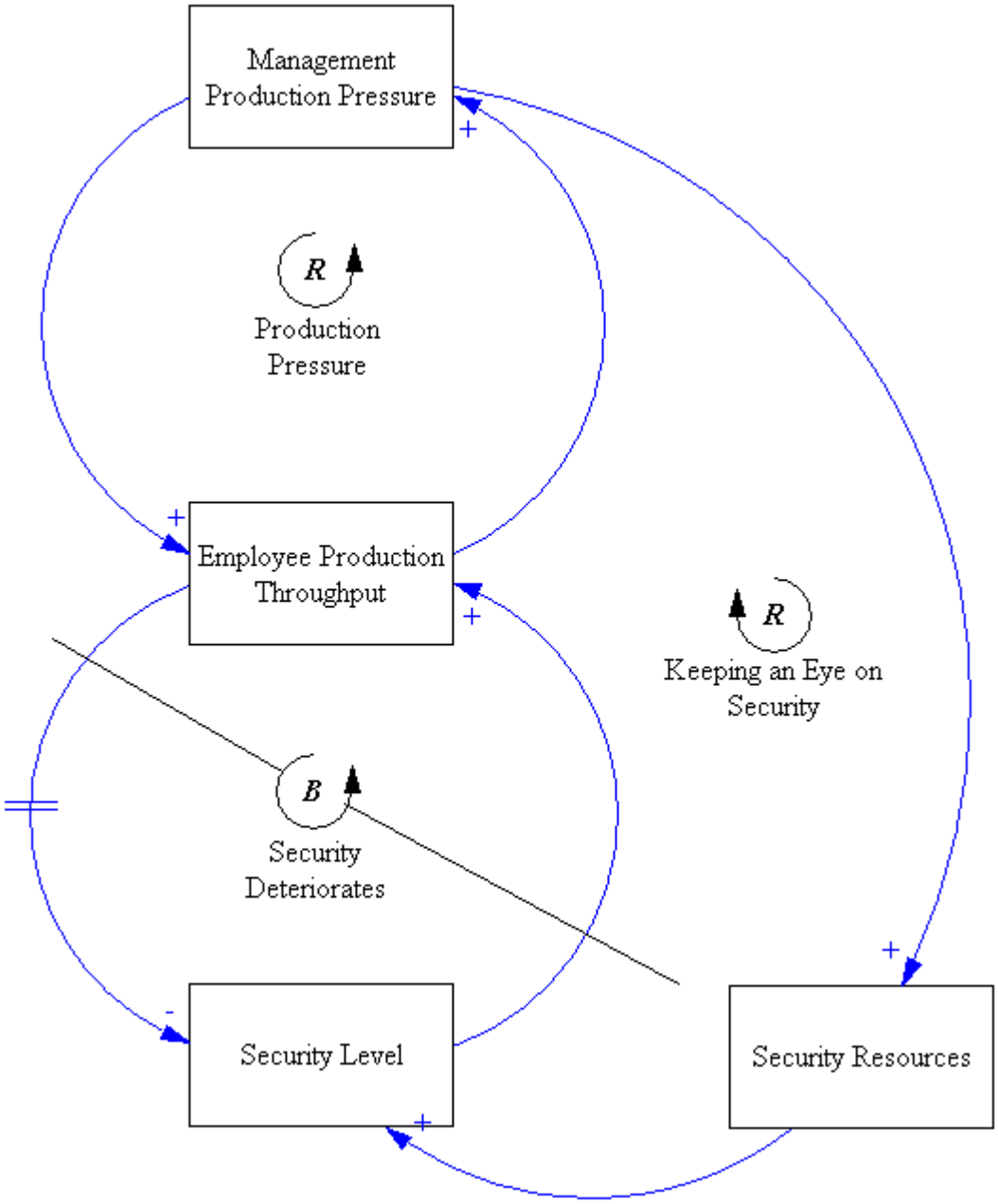


Figure 22 – Solution archetype to the ”Production Focus” archetype in Figure 21.

9.3 Resilience against positive change – Getting out of an undesirable state

IT operational best practices, such as the Information Technology Infrastructure Library (ITIL) provide a framework to start defining repeatable and verifiable IT processes. However organizations face two very difficult questions on their journey towards process improvement: How and where do they start?

In (Behr, Kim, and Spafford 2004) the authors have identified several problems that are common in an IT-department. Say there is a problem with a server that has gone down during patching. For many organizations this is critical and could possibly put them out of business if it is not solved fast. If there are no proper policies in place the problem will be left to the proper person(s) in the IT-department to handle at their own will. Since this in many cases is a very critical problem, the pressure to come up with a solution fast, is very high. An IT-technician's job can be at stake if he does not get the server up and running and so quick fixes are highly probable. The technician works around the problem in his own way, and solves the problem. Chances are the solution is unique (not easily reproduced), and does not fix the underlying problem. Also the solution might not be very stable and it can be difficult, if not to say impossible, for other than the person who implemented it to maintain later on. The quick fix solves the problem but the fix can actually lead to even greater trouble later on. What if the person that is responsible for the server and the fixes no longer is a part of the organization or available to help when there is a problem? Then you have a box which nobody quite knows how works and the organization can be in really serious trouble. Something that is important to think of and that is often overlooked is that if one person single-handedly can save the ship, that person can probably single-handedly sink the ship, too.

From the archetype in Figure 23 you can see that when there is a problem related to the organization's IT system, here called an IT-fire, this will be solved by increased work from IT-personnel. They will most lightly have pressure on them to correct the problem fast, and so it is probable that their solutions not always are in appliance with proper change management policies. They solve the problem, but the number of quick fixes increases, and these can in time cause even more problems, increasing the number of IT fires making the workload so big that the organization will have problems coping, making it an everyday struggle to survive.

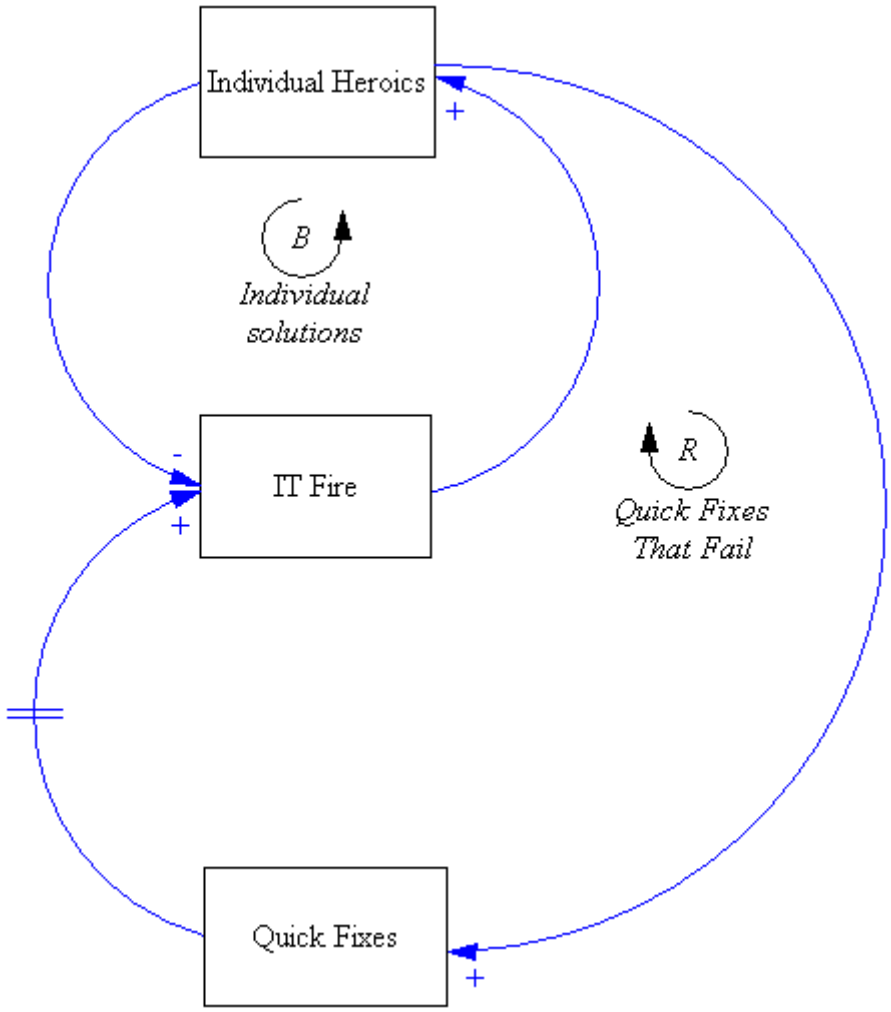


Figure 23 – Out-of-control archetype illustrating the dynamics of quick fixes leading to an increased burden for IT operations.

To counter this problem it is important that management is involved in IT-operations, and specifically as in this example and discussed in (Behr, Kim, and Spafford 2004) that there are strict management policies in place, so that actions taken by IT-personnel adhere to these. Implementing best practice processes like ITIL can help avoiding quick fixes and improve performance continuously.

From the archetype in Figure 24 you can see that the solution is to implement (and follow) management policies that counter and removes the possibility of quick fixes. This will in the longer run help the organization removing IT fires caused by quick fixes. The process has similarities with findings in (Repenning and Sterman 2001). If you allow quick fixes and individual heroics to set the standards you will probably have a better before worse situation, when in the beginning the organization will cope and recoup from errors, but after a while the

results of the quick fixes will start causing increasingly more problems. If one on the other hand follows strict management policies it is possible that one will experience a slight worsening of the situation before it improves, worse before better, but this will in the longer run be the better of the two scenarios.

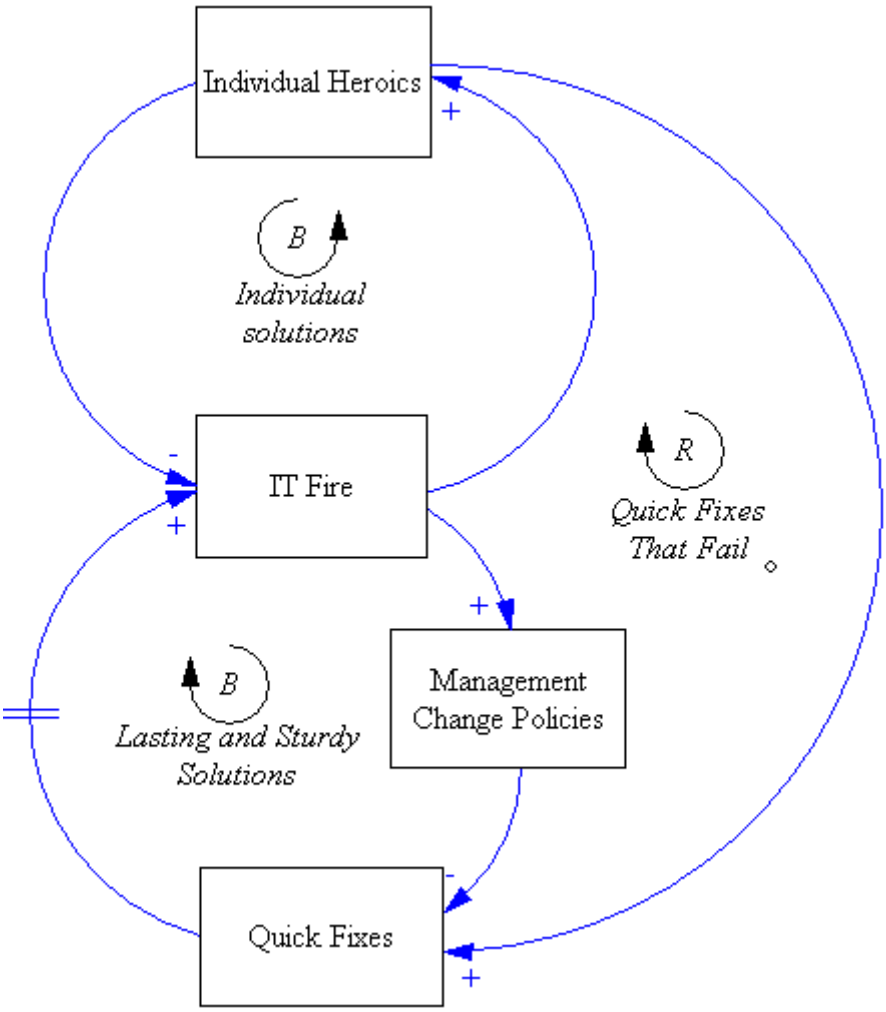


Figure 24 – Solution to the out of control archetype in Figure 23.

9.3.1 Resilience against change

As management tries to implement new practices and apply new policies, employees can learn and self organize to avoid new practices. This resilience against change can seriously undermine the new policies and threaten the organization. One typical reason is that an employee that usually has been responsible for fixing problems has been getting credit for their work when they correct a critical error. Because of their ability to fix critical errors they are seen as important to the organization, an importance that might fade if the system is changed so that quick fixes are avoided and management policies are in place.

From the archetype in Figure 25 one can see the dynamics of what happens when there is an IT fire that is handled by individuals in the organization. In the shorter period of time this reduces the number of IT fires. Another effect is that the employees responsible for fixing problems experiences personal success They get positive feedback for fixing a problem and they are seen as important to the organization. This in turn can increase their resilience against the implementation of effective processes and controls in the organizations, causing the number of IT fires to increase.

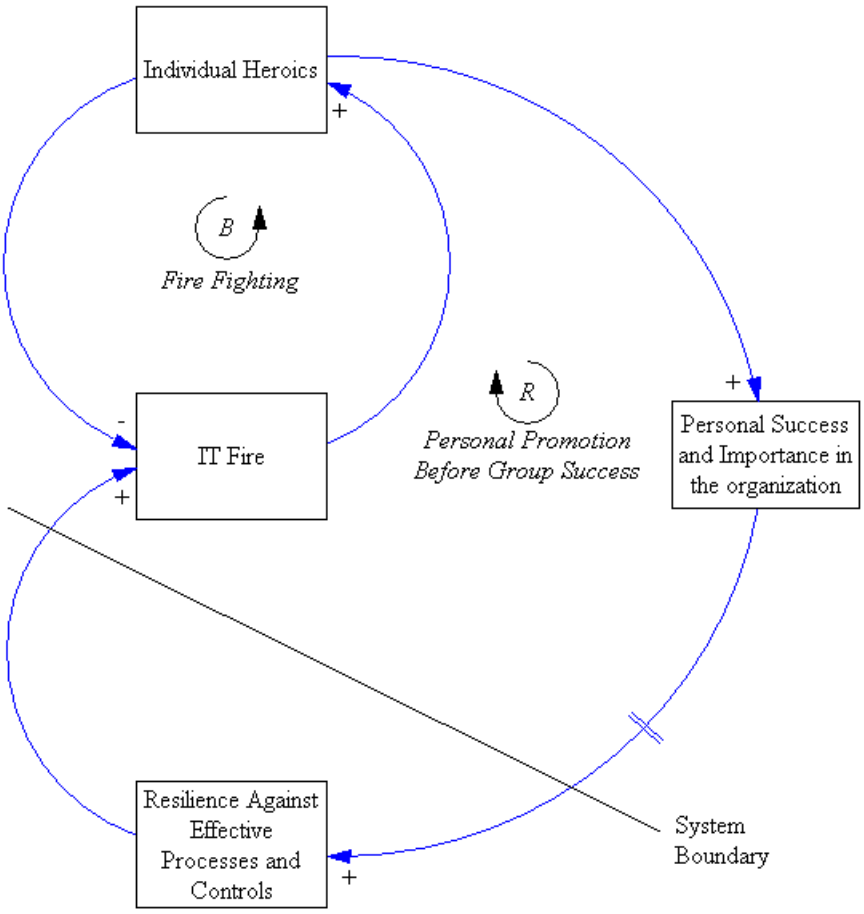


Figure 25 – Out of control problem archetype showing how resilience against effective processes and controls can affect IT operations.

It is important for management to be aware of this possible source of resilience towards positive change. Proper precautions and actions against it must be taken so that IT personnel do not feel that their position in the organization is threatened but, rather they are a valuable part of the new process. If handled correctly by management, they can counteract the

occurrence of resilience in the organization, and subsequently successfully implement proper policies and processes, thus reducing the number of IT fires.

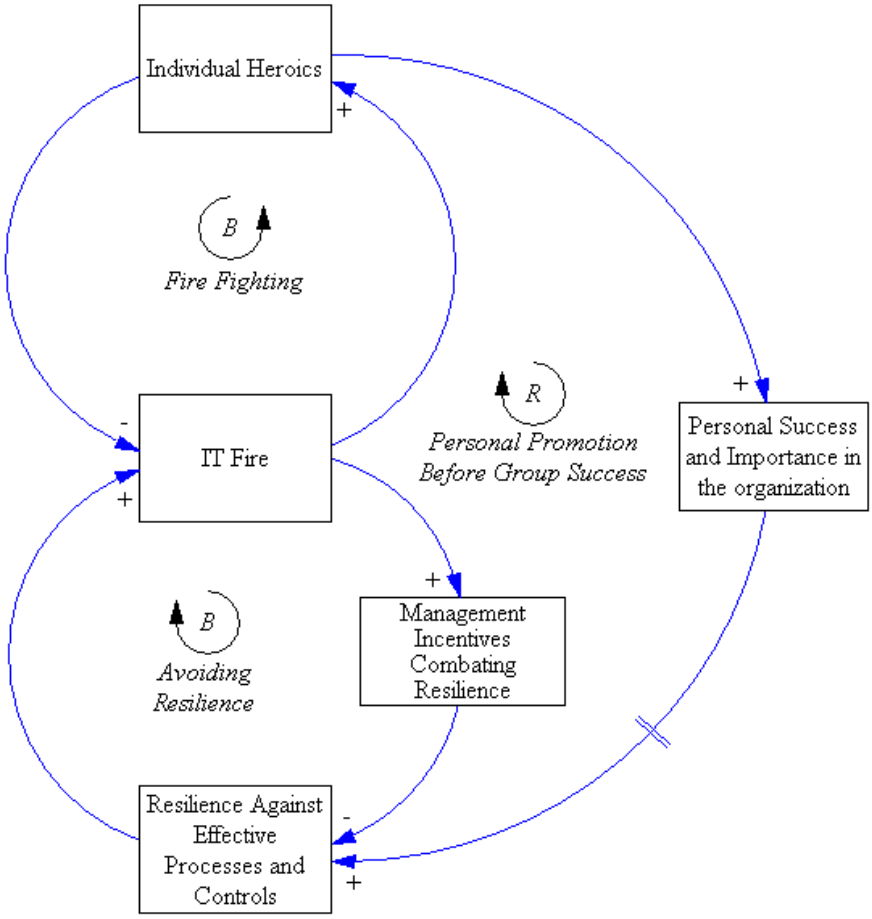


Figure 26 – Solution archetype to the problem shown in Figure 25.

10 Conclusions

In this chapter I will summarize my findings and give a summed up answer to my research questions.

1. What are the main characteristics of resilience in a system presented in the form of a conceptual model of Integrated Operations when focusing on information security as a QIP (quality improvement process)?
In simulations of different policies in chapters 6, 7 and 8 I have identified, described and shown how the oil and gas company's resilience changes as the company experiences disturbances. These findings are further discussed in chapter 9.

One can argue that in policies 1 and 5 the system was not resilient – it was not able to absorb the impacts of incidents and therefore reorganized its configuration. But resilience is not always a positive property. The state the system entered in policies 1 and 5 can also be considered resilient. Adjusting procedures, standards, processes, and maybe even more important, people's behavior and attitude so that security level can be rebuilt and the desired level of performance can be brought back requires a lot of effort and expenditure.

2. Describe these findings in dynamic stories and system archetypes.
The findings are described in dynamic stories in chapters 6, 7 and 8 and system archetypes in chapter 9.

3. Suggest some policies/solution archetypes that increase resilience (against negative change).
Solution archetypes are suggested in chapter 9. Although I do not claim any numerical accuracy, I believe there are some important insights to consider. For an oil and gas company it seems crucial to build up resilience of the desired system state in advance. Building up security level to such a level that optimal performance can be achieved is seemingly the optimal solution. If this is not done, then the company should at least pay more attention to security level when the system has been affected an incident. Examples of this are policies 2 and 6 where the system undergoes various types and amounts of incidents and still preserves its desired state. This is possible due do its focus on maintaining and increasing security rather

than just allocating resources for production to close performance gaps. One may suggest that such policies will lead to less profit. But enterprises that strive for long term effectiveness, profitability and competitive advantage have to consider and secure the long term functionality of their production systems.

One potential insight which is important is the effect strict resource limitations have on the system. Normally having strong budget discipline is sensible, but having strong resource limitations when serious incidents occur can threaten the systems resilience. Having resource redundancy to cope with the occurrence of incidents should be taken into consideration when planning the transfer to and daily operation of integrated operations.

Hopefully these insights of the instability of resource allocation and the need to invest in proactive resilience will prove robust to changes and extensions of the model and analysis in this paper.

4. Resilience can also be towards positive change, can archetypes identifying some important reasons for resilience in Integrated Operations when viewing information security as a QIP be created?

In chapter 9 I show a potential source for resilience against positive change in an organization. These hypotheses are based on the findings in (Behr, Kim, and Spafford 2004) which are a quite generic description of IT organizations and how change and access controls reduce security risk and increase the efficiency and effectiveness of information technology management and operations. As IT undoubtedly will be an important business driver and play a large role in integrated operations, one can argue that the findings in (Behr, Kim, and Spafford 2004) is relevant also for integrated operations.

10.1 Future Research

The model is highly aggregated and thus "simple". It should be extended and adapted to more closely describe real oil and gas companies. Also, assessing security level is a very difficult task. Further research into how the security level in an organization behaves and how it is assessed is needed.

Also there is a need to look more detailed at how performance is affected by information security incidents and how information security can affect performance. How can companies assess their security level so that their production processes can be highly resilient in a high performing state, at the lowest possible cost?

There is a need to communicate the need for a sturdy information security process in companies to management. One suggestion could be the development of a management game, where players experience pressure to produce, information security incidents, and where the players can experience how their allocation of resources affects the system.

11 APPENDIX A - Model Transcript

Minimum Security Level Required for Optimal Performance=

50

~ 1

~ As the name states the minimum security level required for optimal \ performance. Can be perceived as maintaining firewalls or other software / \ devices preventing operations against casual threats and disruptions. If \ the security level drops below the minimum required level, optimal \ performance can not be achieved.

|

Effect of Security Level on Performance=

TEoSLoP(Security Level/Minimum Security Level Required for Optimal Performance)

~ 1

~ If the effect drops below 1, the optimal performance is jeopardized. We \ assume that the performance is dependent on security level. A very high \ security level can improve Performance, but only to a certain degree.

|

TEoSLoP(

[(0,0)-(2,1.5)],(0,0),(0.2,0.3),(0.4,0.55),(0.6,0.75),(0.8,0.9),(1,1),(1.2,1.08),(1.4\ ,1.135),(1.6,1.175),(1.8,1.195),(2,1.2))

~ 1

~ The table function for the effect of security level on performance.

|

Performance=

Resources for Production*Effectiveness of Resources for Production*Effect of Security Level on Performance\

*Effect of Severity on Performance

~ Unit/Week

~ The performance of the organization (can be measured as production of \
barrels per week). It depends on resources for production, the security \
level, the effect from incidents, and the effectiveness of resources for \
production.

|

Effectiveness of Resources for Production=

2

~ Unit/Resource

~ The average number of units a single resource is able to produce.

|

Allocation of Resources to Security=

Pressure to Increase Security*Effect of Work Pressure on Shortcuts*(Resources for Production\

-Min Resources for Production)/Average Resources Allocation Delay

~ Resource/(Week*Week)

~ The rate of resources being allocated to increase security. The value \
depends on the pressure to increase security, the effect of shortcuts, \
minimal amount of resources devoted to production (that can never drop \
below its minimal value), and the allocation delay.

|

Incident=

Incident Type*PULSE(5,1)

~ 1

~ The pulse that imitate an incident occurring.

|

Incident Type=

0

~ 1 [0,6,0.1]

~ The type of incident. Ranges from 1 (insignificant incident) to 6 \
(catastrophic incident). 0 indicates there is not an incident.

|

Desired Performance=

150

~ Unit/Week

~ The desired performance of the organization. It might be a production goal \ appointed by managers or determined by customer orders.

|

Effect of Severity on Performance=

TEoSoP(Severity of Incidents)

~ 1

~ The effect which determines the noticeable impact of the incident severity \ on the performance.

|

Performance Gap=

MAX(Desired Performance-Performance,0)

~ Unit/Week

~ The difference between desired and actual performance. If desired \ performance is greater than actual performance, a performance gap occurs.

|

Security Level Decrease=

Security Level/Security Level Erosion Time

~ 1/Week

~ The rate at which security level deteriorates.

|

TEoSoP(

[(0,0)-(10,1)],(0,1),(1,0.99),(2,0.97),(3,0.95),(4,0.9),(5,0.8),(6,0))

~ 1

~ Table function for the effect of severity on performance. More severe \ incidents impair performance. In case of catastrophic incidents the \

performance can drop even to zero if there is not a sufficient level of \
security.

|

Severity of Incidents=

MAX(Incident-Security Level/100, 0)

~ 1

~ The severity of an incident is affected by the security level in the \
organization. The severity of an incident is more efficiently mitigated \
the higher the security level is.

|

TEoWPoS(

[(0,0)-(1,1)],(0,1),(0.1,0.98),(0.2,0.95),(0.3,0.9),(0.4,0.8),(0.5,0.5),(0.6,0.2),(0.7\
,0.1),(0.8,0.05),(0.9,0.02),(1,0))

~ 1

~ Table function for the effect of work pressure on shortcuts.

|

Effect of Work Pressure on Shortcuts=

TEoWPoS(Pressure to do Work)

~ 1

~ When faced with increasing demand for production, workers tend to take \
shortcuts in their work. The higher the pressure to do work, the more \
likely workers are taking shortcuts - they spare more time for production \
at the cost of security increase.

|

Security Level= INTEG (

+Security Level Increase-Security Level Decrease,

Effectiveness of Resources for Security*Resources to Increase \
Security*Security Level Erosion Time\

)

~ 1

~ The aggregated measure for technical, human and organizational security \
culture. The higher the security level the less damage are caused by \
various incidents. A metaphor of the security level - a shield, armor, \
bullet proof vest. One who wears the bulletproof vest can get hurt but the \
impact of the shot is mitigated.

|

Resources to Increase Security= INTEG (

-Allocation of Resources to Production+Allocation of Resources to Security,

0.25*Total Resources)

~ Resource/Week

~ Resources dedicated to improving security.

|

Min Resources for Security=

0.1*Total Resources

~ Resource/Week

~ The minimal amount of resources dedicated to improving security. Resources \
to improve security can never drop below this value.

|

Min Resources for Production=

0.5*Total Resources

~ Resource/Week

~ The minimal amount of resources dedicated to production. Resources to \
production can never drop below this value.

|

Pressure to do Work=

Pressure to Close Performance Gap*Pressure Allocation

~ 1

~ The pressure in the organization towards production. Is affected by the \
pressure to close the performance gap and a managerial decision regarding \
pressure allocation.

|

Allocation of Resources to Production=

Pressure to do Work*(Resources to Increase Security-Min Resources for Security)/Average Resources Allocation Delay

~ Resource/(Week*Week)

~ The rate of resources being allocated to production. It depends on the \ pressure to do work and the resources for increasing security (which can \ not drop below its minimum value), and the allocation delay.

|

Average Resources Allocation Delay=

1

~ Week

~ It takes some time to move people from one work mode to another. This \ value simulates the average delay which affects the transition of \ resources from increasing security to production or from production to \ security.

|

Pressure to Close Performance Gap=

Performance Gap/Company Goal for Performance Gap Satisfaction

~ 1

~ The pressure which arises in an organization once the performance gap \ (difference between desired and actual performance) exists.

|

Pressure to Increase Security=

Pressure to Close Performance Gap*(1-Pressure Allocation)

~ 1

~ The pressure in the organization to increase security. It depends on \ pressure to close performance gap and a managerial decision regarding \ pressure allocation.

|

Resources for Production= INTEG (

Allocation of Resources to Production-Allocation of Resources to Security,

Total Resources-Resources to Increase Security)

~ Resource/Week

~ Resources dedicated to production.

|

Security Increase Delay=

2

~ Week

~ The time it takes to increase security

|

Security Level Increase=

DELAY3(Effectiveness of Resources for Security*Resources to Increase Security,Security Increase Delay\

)

~ 1/Week

~ The rate at which the security level is built. It is not an instant \ process and requires time, which is modeled as a third order delay.

|

Effectiveness of Resources for Security=

1

~ 1/Resource

~ The effectiveness of resources dedicated to security.

|

Company Goal for Performance Gap Satisfaction=

25

~ Unit/Week

~ The company's goal to close performance gaps.

|

Security Level Erosion Time=

2

~ Week

~ The time it takes for security to erode

|

Pressure Allocation=

0.6

~ 1 [0,1]

~ Pressure allocation indicates the managerial decision regarding allocation \ of resources to improve security or to production. The value ranges from 0 \ to 1. The higher the value, the managers put more pressure towards \ production.

|

Total Resources=

100

~ Resource/Week

~ The total value of available resources in an organization.

|

****

.Control

**********~

Simulation Control Parameters

|

FINAL TIME = 50

~ Week

~ The final time for the simulation.

|

INITIAL TIME = 0

~ Week

~ The initial time for the simulation.

|

SAVEPER =

TIME STEP

~ Week [0,?]

~ The frequency with which output is stored.

|

TIME STEP = 0.1

~ Week [0,?]

~ The time step for the simulation.

|

\\\---/// Sketch information - do not modify anything except names

V300 Do not put anything below this section - it will be ignored

*View 1

$192-192-192,0,Arial CE|10|B|0-0-0|0-0-0|0-0-255|-1--1--1|-1--1--1|96,96,95

10,1,Security Level,601,112,49,26,3,3,0,0,0,0,0,0

12,2,48,311,110,10,8,0,3,0,0,-1,0,0,0

1,3,5,1,4,0,0,22,0,0,0,-1--1--1,,1|(497,111)|

1,4,5,2,100,0,0,22,0,0,0,-1--1--1,,1|(375,111)|

11,5,48,436,111,6,8,34,3,0,0,1,0,0,0

10,6,Security Level Increase,436,135,48,16,40,3,0,0,-1,0,0,0

12,7,48,883,112,10,8,0,3,0,0,-1,0,0,0

1,8,10,7,4,0,0,22,0,0,0,-1--1--1,,1|(835,110)|

1,9,10,1,100,0,0,22,0,0,0,-1--1--1,,1|(718,110)|

11,10,48,792,110,6,8,34,3,0,0,1,0,0,0

10,11,Security Level Decrease,792,134,48,16,40,3,0,0,-1,0,0,0

10,12,Performance,823,447,43,9,8,3,0,0,0,0,0,0

10,13,Performance Gap,816,525,58,9,8,3,0,0,0,0,0,0

10,14,Desired Performance,941,575,44,16,8,3,0,0,0,0,0,0

1,15,1,10,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(688,58)|

10,16,Security Level Erosion Time,903,64,48,16,8,3,0,0,0,0,0,0

1,17,16,10,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(825,68)|

1,18,14,13,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(880,558)|

10,19,Pressure to Increase Security,94,612,58,16,8,3,0,0,0,0,0,0

10,20,Resources to Increase Security,290,416,60,60,3,3,0,0,0,0,0,0

10,21,Effectiveness of Resources for Security,283,159,52,24,8,3,0,0,0,0,0,0

1,22,20,6,1,0,43,0,2,65,0,-1--1--1,|10|B|0-0-0,1|(343,228)|

1,23,21,6,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(357,140)|

10,24,Resources for Production,592,414,59,60,3,3,0,0,0,0,0,0

1,25,24,12,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(687,379)|

1,26,27,24,4,0,0,22,0,0,0,-1--1--1,,1|(492,455)|

11,27,300,445,455,6,8,34,3,0,0,1,0,0,0

10,28,Allocation of Resources to Production,445,478,81,15,40,3,0,0,-1,0,0,0

10,29,Pressure to do Work,515,569,48,16,8,3,0,0,0,0,0,0

10,30,Company Goal for Performance Gap Satisfaction,885,682,61,24,8,3,0,0,0,0,0,0

1,31,30,54,1,0,45,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(805,662)|

1,32,20,28,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(335,490)|

10,33,Total Resources,436,255,53,9,8,3,0,0,0,0,0,0

1,34,27,20,100,0,0,22,0,0,0,-1--1--1,,1|(394,455)|

1,35,29,28,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(475,534)|

1,36,38,20,4,0,43,22,2,128,0,-1--1--1,|10|B|0-0-0,1|(394,377)|

1,37,38,24,100,0,45,22,2,0,0,-1--1--1,|10|B|0-0-0,1|(491,377)|

11,38,732,444,377,6,8,34,3,0,0,3,0,0,0

10,39,Allocation of Resources to Security,444,353,79,16,40,3,0,0,-1,0,0,0

1,40,24,39,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(528,333)|

1,41,19,39,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(86,286)|

10,42,Pressure Allocation,331,656,34,16,8,3,0,0,0,0,0,0

1,43,42,29,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(424,647)|

1,44,42,19,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(209,645)|

10,45,Min Resources for Security,307,530,87,9,8,3,0,0,0,0,0,0

10,46,Min Resources for Production,542,299,60,16,8,3,0,0,0,0,0,0

1,47,45,28,1,0,45,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(407,528)|

1,48,46,39,1,0,45,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(464,320)|

10,49,Security Increase Delay,324,70,50,16,8,3,0,0,0,0,0,0

1,50,49,5,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(401,71)|

10,51,Average Resources Allocation Delay,416,414,65,16,8,3,0,0,0,0,0,0

1,52,51,38,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(426,387)|

1,53,51,27,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(421,434)|

10,54,Pressure to Close Performance Gap,749,626,59,16,8,3,0,0,0,0,0,0

1,55,13,54,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(804,568)|

1,56,54,19,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(427,774)|

1,57,54,29,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(617,607)|

1,58,33,46,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(458,267)|

10,59,Total Resources,376,576,64,13,8,2,0,3,-1,0,0,0,128-128-128,0-0-0,|10|B|128-128-128

1,60,59,45,1,0,43,0,2,192,0,-1--1--1,|10|B|128-128-128,1|(338,565)|

10,61,Effect of Work Pressure on Shortcuts,99,486,47,24,8,3,0,0,0,0,0,0

1,62,29,61,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(335,635)|

10,63,TEoWPoS,101,554,34,9,8,3,0,0,0,0,0,0

1,64,63,61,1,0,0,0,0,64,0,-1--1--1,,1|(97,531)|

10,65,Effectiveness of Resources for Production,965,481,52,24,8,3,0,0,0,0,0,0

1,66,65,12,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(890,473)|

10,67,Severity of Incidents,852,250,36,16,8,3,0,0,0,0,0,0

10,68,Incident,906,167,28,9,8,3,0,0,0,0,0,0

10,69,Effect of Severity on Performance,886,359,57,16,8,3,0,0,0,0,0,0

10,70,TEoSoP,950,302,27,9,8,3,0,0,0,0,0,0

1,71,1,67,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(754,155)|

1,72,67,69,1,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(880,291)|

1,73,70,69,0,0,0,0,0,64,0,-1--1--1,,1|(926,322)|

1,74,68,67,0,0,43,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(885,199)|

10,75,Incident Type,972,245,45,9,8,3,0,0,0,0,0,0

1,76,75,68,0,0,0,0,0,64,0,-1--1--1,,1|(943,211)|

1,77,12,13,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(823,483)|

1,78,61,39,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(97,375)|

1,79,1,82,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(736,245)|

1,80,69,12,1,0,45,0,2,64,0,-1--1--1,|10|B|0-0-0,1|(859,394)|

10,81,Minimum Security Level Required for Optimal
Performance,641,239,62,24,8,3,0,0,0,0,0,0

10,82,Effect of Security Level on Performance,767,319,55,23,8,3,0,0,0,0,0,0

1,83,81,82,1,0,45,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(709,272)|

10,84,TEoSLoP,659,286,31,9,8,3,0,0,0,0,0,0

1,85,84,82,0,0,0,0,0,64,0,-1--1--1,,1|(693,296)|

1,86,82,12,1,0,43,0,2,192,0,-1--1--1,|10|B|0-0-0,1|(800,375)|

12,87,0,696,516,63,63,4,132,0,24,-1,0,0,0,0-0-0,0-0-0,|14|I|0-0-0

B1: Focus on production

12,88,0,513,688,52,52,4,132,0,24,-1,0,0,0,0-0-0,0-0-0,|14|I|0-0-0

B2: Focus on security

12,89,0,530,196,54,54,4,132,0,24,-1,0,0,0,0-0-0,0-0-0,|14|I|0-0-0

R: Reinvest- ment

12,90,0,164,404,55,55,4,132,0,24,-1,0,0,0,0-0-0,0-0-0,|14|I|0-0-0

B3: Shortcuts

1,91,21,1,0,0,0,0,0,0,1,-1--1--1,,1|(436,138)|

1,92,20,1,0,0,0,0,0,0,1,-1--1--1,,1|(456,252)|

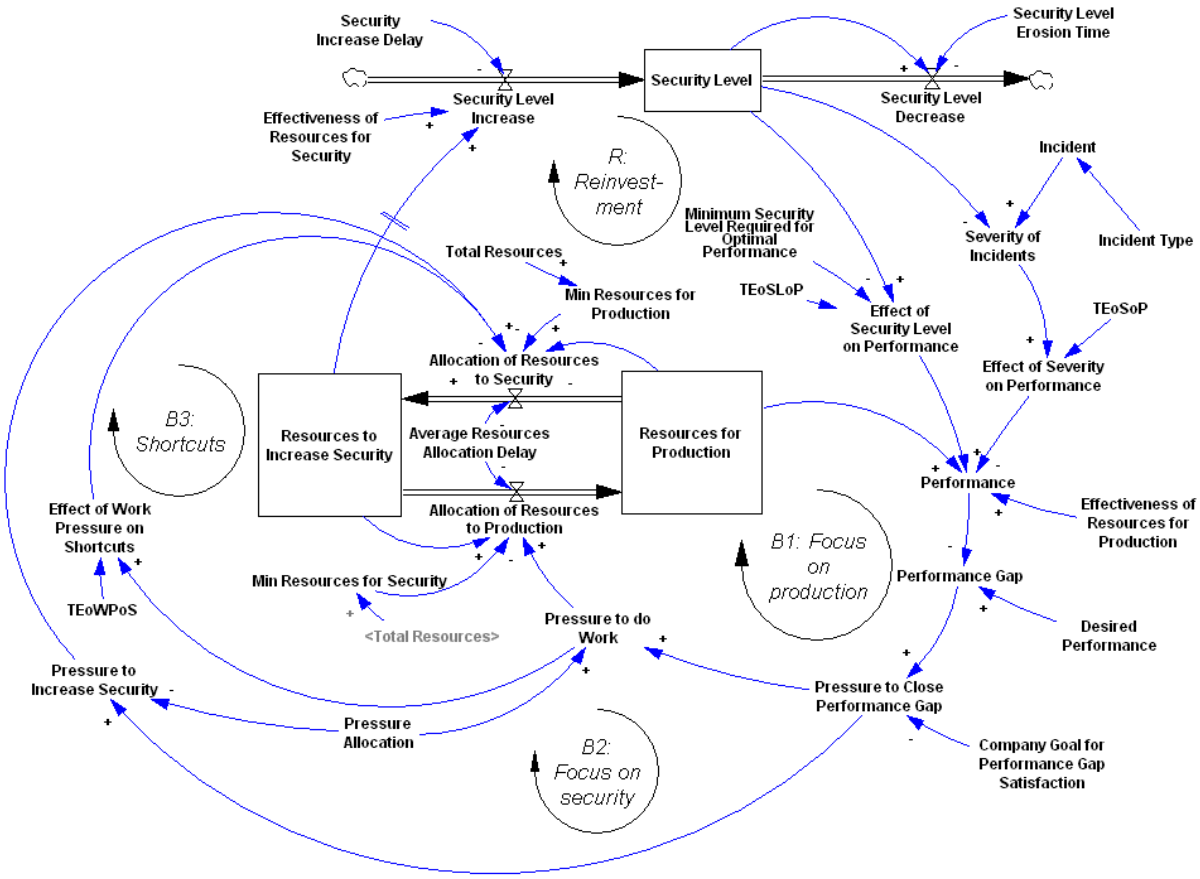
1,93,16,1,0,0,0,0,0,0,1,-1--1--1,,1|(759,87)|

1,94,33,20,0,0,0,0,0,0,1,-1--1--1,,1|(390,304)|

1,95,20,24,0,0,0,0,0,0,1,-1--1--1,,1|(434,415)|

1,96,33,24,0,0,0,0,0,0,1,-1--1--1,,1|(483,304)|

12 APPENDIX B - Full Model View



13 References

Behr, Kevin, Gene Kim, and George Spafford. 2004. *THE VISIBLE OPS HANDBOOK - STARTING ITIL IN 4 PRACTICAL STEPS*.

Cooke, David L. 2004. The Dynamics and Control of Operational Risk. Ph.D.-thesis, Haskayne School of Business, The University of Calgary, Calgary.

Deloitte. 2005. 2005 Global Security Survey. Review of Reviewed Item.

Ernst&Young. 2005. Global Information Security Survey 2005.

Gonzalez, Jose J., Ying Qian, Finn Olav Sveen, and Eliot Rich. 2005. Helping prevent information security risks in the transition to integrated operations. *Telektronikk* 101 (1):29-37.

Gunderson, Lance H. 2000. Ecological Resilience - In Theory and Application. *Annual Review Ecological Systems*.

Hocking, Paul. 2006. *Sikkerhetsutfordringer med Integrerte Operasjoner* 2005 [cited February 2006].

Lowe, Justin. 2006. *Managing industrial control system security risks*. RUSI Conference 2006 [cited 28th may 2006]. Available from http://www.rusi.org/downloads/event_content/9._Lowe.pdf.

Moore, Andrew P., and Rohit S. Antao. 2006. Improving Management of Information Technology: System Dynamics Analysis of IT Controls in Context. In *International Conference of the System Dynamics Society*.

Poulsen, Kevin. 2006. *Slammer worm crashed Ohio nuke plant network* [Internet] 2003 [cited 05.26 2006]. Available from http://www.securityfocus.com/news/6767.

PricewaterhouseCoopers. 2004. Information security breaches surveys 2004.

———. 2005. The Global State of Information Security 2005. *CIO Magazine*:12.

Repenning, Nelson, and John D. Sterman. 2001. Nobody Ever Gets Credit for Fixing Problems that Never Happened: CREATING AND SUSTAINING PROCESS IMPROVEMENT. *California Management Review* 43 (4).

Rogers, Lawrence R. *Home Computer and Internet User Security* 2005 [cited. Available from http://www.cert.org/archive/pdf/HCIU-Security.ppt.

Rydzak, Felicjan, Lars S. Breistrand, Finn Olav Sveen, Ying Qian, and Jose J. Gonzalez. 2006. Exploring Resilience Towards Risks in eOperations in the Oil and Gas Industry. In *Proceedings of Twenty Fifth International Conference on Computer Safety, Security and Reliability - SAFECOMP2006*. Gdansk.

Senge, Peter M. 1990. *The fifth discipline*.

Sterman, John D. 2000. *Business Dynamics - Systems Thinking and Modeling for a Complex World*.

Wolstenholme, Eric F. 2002. Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review* 19 (1).

———. 2004. Using generic system archetypes to support thinking and modelling. *System Dynamics Review* 20 (4).

Woody, Carol. 2003. Managing the Risk of Internet Connectivity. Paper read at K-12 School Networking Conference.