System Archetypes and Dynamic Stories on Information Security Risks in the transition to Integrated Operations in the Oil and Gas Industry

By

Tor Ivar J. Nordmo

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

System Archetypes and Dynamic Stories on Information Security Risks in the transition to Integrated Operations in the Oil and Gas Industry

Abstract

From a situation where the drilling and production platforms were solely run on site (offshore), the industry is now working on establishing land based control systems to decrease production costs, and consequently increase income. The ongoing project Integrated Operations (IO) (http://www.olf.no/io/) expects to yield up to 30% cost reduction and a 10% increase in production. One of the key factors to achieve these goals is reliable and secure information technology between offshore and onshore installations. Information security incidents can cause serious damage on personnel, production and installations.

To address this, a project named AMBASEC (A Model Based Approach to Security Culture) has been launched from Agder University College (AUC) in collaboration with SINTEF, www.sintef.no, The Norwegian Oil Industry Foundation (www.olf.no/english/about/) and the State University of New York University at Albany. A System Dynamic simulation model has been created by the AMBASEC design team to address information security risks emerging from the IO project.

System Dynamics (SD) thinking and modeling may be excellent tools for this, the complexity of the models often makes the communication of the results and policies difficult to understand for persons untrained in SD, in this case managers and strategic decision makers.

E. Wolstenholme (2002) has with his award winning paper *"Towards the definition and use of a core set of archetypal structures in system dynamics"(Wolstenholme 2002)* proposed a core set of four System Dynamic Archetypes, which can be thought of as collapsed system dynamic models.

The System Dynamic Archetypes, with their simpler structure, may be more suited to communicate results and effects of various policies. In this thesis I will try to identify System Archetypes hidden in the model (IO version 1.95) developed by the design team, create System Dynamic Stories to accompany and explain the System Archetypes, and in the end suggest policies to counteract the unintended consequences.

After testing the model provided the conclusion is to put focus on maturing processes, knowledge and technology by using extra resources on maturing.

When putting more resources on maturing knowledge than on the others the vulnerability index stayed the lowest and new initiatives burden decreased. The work processes completed ahead of schedule.

1 Table of Content

1 Introduction

1.1 Integrated Operations

Integrated operations (IO) were initiated by the Norwegian Oil Industry Association (OLF)[1] autumn 2004 as a program to improve the value creation on the Norwegian continental shelf. The program has been divided into two generations where generation 1 will integrate both processes and people offshore and onshore by the use of information and communication technology (ICT). The objective is to implement collaboration arenas where onshore and offshore personnel have access to the same information in real-time, through reliable communication infrastructure. The implementation of onshore control centers opens up for continuous support and surveillance of production.(work-group-Integrated-Operations 2005) Generation 2 will integrate operators and vendors in such a way that services can be delivered through ICT. Vendors will take over some of the processes like monitoring, analyzing and optimization of tasks.(work-group-Integrated-Operations 2005) The IO program expects to yield up to 30% cost reduction and a 10% increase in productions. The implementation plans for the two generations are shown in Figure 1 below.

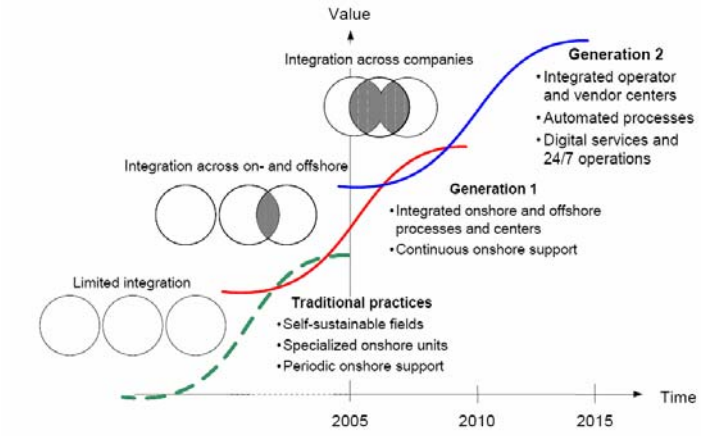


Figure 1 Implementation plan (work-group-Integrated-Operations 2005)

Reliable and secure information technology and infrastructure is a necessity to achieve these goals. Information security incidents can cause serious damage on personnel, production and installations. If a process should be started by mistake, or by malicious attackers during onsite maintenance, lives can get lost. In a “denial of service” attack, down time can cost the owners millions of dollars in lost production. These are just two examples of possible consequences if information security is neglected, or given low priority

[1] www.olf.no

1.2 System Dynamics

System dynamics society[2] defines it as:

"System dynamics is a methodology for studying and managing complex feedback systems, such as one finds in business and other social systems. Feedback refers to the situation where X is affecting Y and Y in turn affects X."

System Dynamics (SD) thinking and modeling may help the IO project to reveal unintended consequences that may appear as a feedback from the system, triggered by intended actions.

1.3 AMBASEC

To address the new information security challenges the transition may cause, a project named AMBASEC (A Model Based Approach to Security Culture) has been launched from Agder University College (AUC)[3] in collaboration with SINTEF, OLF and the State University of New York University at Albany. A System Dynamic simulation model has been created by the AMBASEC design team to address the information security risks that may emerge from the IO project.

1.4 Problem Description

System Dynamics modeling, and thinking, may be excellent tools for analyzing the behavior of complex dynamic systems over time. But the complexity of the computer simulation models can create problems when communicating policies and results to persons untrained in system dynamics. It's hard to persuade decision makers to make investments based upon a SD model they don't understand the behavior of. The use of system dynamic archetypes may be an adequate tool to try to overcome these barriers. E. Wolstenholme (2002) has in his award winning paper *"Towards the definition and use of a core set of archetypal structures in system dynamics"* (Wolstenholme 2002) proposed a core set of four generic System Archetypes which with their simpler more intuitive nature can be easier to understand.
I will in this thesis try to identify System Archetypes corresponding to Wolstenholme's definitions hidden in the system dynamic model (IO version 1.95). Thereafter I will try to

[2] http://www.albany.edu/cpr/sds/
[3] http://www.hia.no/english/

create System Dynamic Stories to accompany and explain the System Archetypes, and in the end suggest policies to counteract the unintended consequences.

1.4.1 Communication

To be able to communicate these findings in an appropriate way, some thoughts on good communication can be useful. In the article "just what is "good" communication?" (2000) the author Merrie Spaeth highlights the importance of not only being aware what you want to say, but to keep in mind the following, quote: (Spaeth 2000)

"Good communication is based on what your audience at the moment, frequently your customer, *hears, believes, and remembers.*"

1.5 Research questions

-Which System Archetypes does the model contain?

-Which impact on the systems output have these System Archetypes?

-Which scenarios will give the System Archetypes a dominant role in the model?

-What is needed to minimize, or neutralize the unwanted effect of the System Archetypes?

-What is needed to enhance, or maximize the wanted effect of the System Archetypes?

-Which policies will give the IO project the highest probability to make the transition with the lowest information security risks?

2 Literature Review

2.1 System Dynamics

Sterman, J.D., “Business Dynamics. Systems Thinking and Modeling for a Complex World”. Boston, Irwin McGraw-Hill, 2000

The book gives an introduction to the many challenges in the growing dynamic complexity in our society today. This is affecting many aspects in our society like: business, science, politics etc. Given that each of these elements is a system, the book tries to explain the actions, the consequences, and the causes that combined form the world as we see it today. To achieve these understandings the book introduces system dynamics modeling for the analysis of policies and strategies.

One important tool to capture the feedback structure of a system is Causal loop Diagrams (CLD). Sterman states that CLD 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 CLD consists of variables and arrows (links) denoting their causal influences and polarities either by + or -, or by S (same effect) or O (opposite effect).

A positive link (+ or S) tells us that if the **cause** increases the **effect** will also increase *above* what it otherwise would have done. If the **cause** decreases, the **effect** decreases *below* what it otherwise would have done. (Sterman 2000)

If the fractional “Birth rate” in the example (Figure 2) increases, the “population” increases *above* what it otherwise would have done, and “Birth Rate” will again increase. If “Birth Rate” decreases, the “Population” would decrease *below* what it otherwise would have done, and “Birth rate” will again decrease. The positive links (+) are sometimes denoted (S) for “Same (effect)”. This feedback loop is called a positive loop, or reinforcing loop, notated with an R inside a circular arrow showing which direction the loop are to be read.

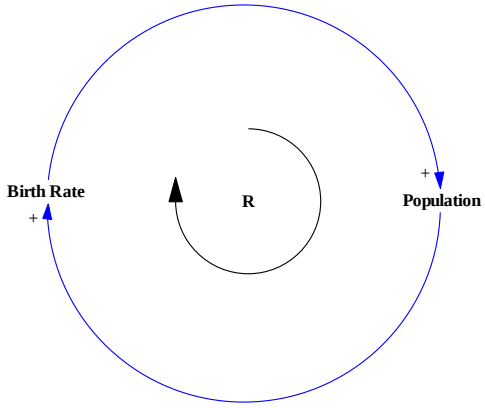


Figure 2 Positive feedback loop (Sterman 2000)

A negative link (- or O) means that if the **cause** increases, the **effect** decreases *below* what it otherwise would have, and if the **cause** decreases, the **effect** increases *above* what it otherwise would have done.

An example of this is shown in Figure 3. If "Death Rate" increases, "Population" decreases *below* what it otherwise would have done. If "Death Rate" decreases, "Population" will increase *above* what it otherwise would have done. The negative links (-) can also be denoted (O) for "Opposite (effect)". This is called a negative feedback loop and notated with a B, for balancing loop, inside a circular arrow showing which direction the feedback loop are to be read.

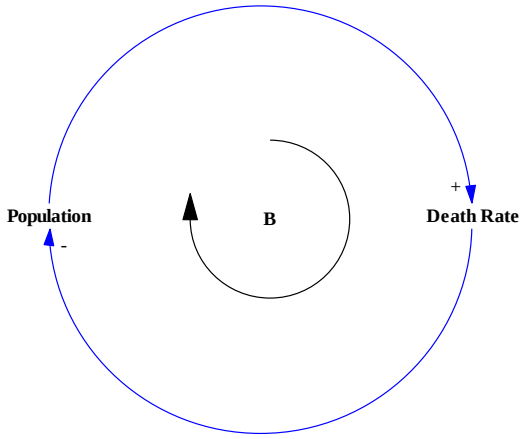


Figure 3 Negative feedback Loop (Sterman 2000)

It's important to emphasize that the diagrams only describe the structure, and not the behaviour of the variables. They describe what happens *if* a change in one of the variables should occur, and not what actually happens.

Delay is an important term in system dynamics which gives inertia to the system, and can create oscillations.

Delay is a process where output lags behind its input, creating an accumulation between input and output. (Sterman 2000) This is denoted as two parallel lines on the links, as shown in figure 3. When a delay is present, there's at least one stock with corresponding inflow and outflow. In Figure 4 "Birth rate" and "Death rate" are flows and "Population" is a stock.

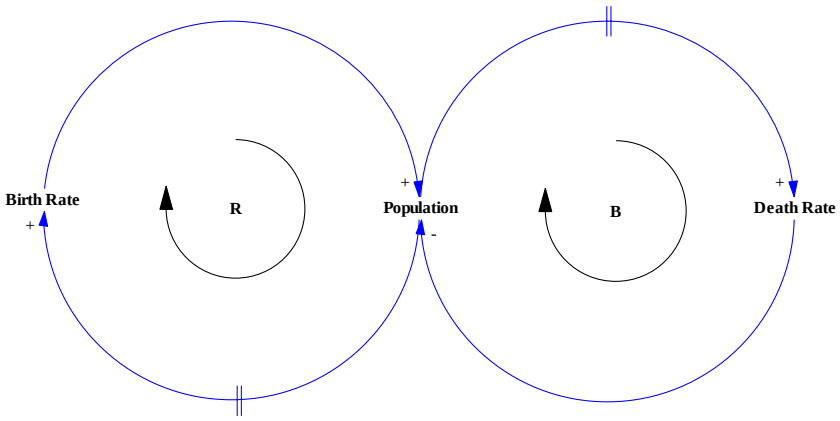


Figure 4 Two loop system with Delays(Sterman 2000)

Stocks and flows

One drawback with CLD is that they don't distinguish between stocks and flows.

Sterman defines stocks as follows:

"Stocks are accumulations. They characterize the state of the system and generate 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 inflow and outflow in a process. By decoupling rates of flow, stocks are the source of disequilibrium in dynamic systems."

The notations for stocks and flows according to Sterman (Sterman 2000) are:

• Stocks are denoted by rectangular boxes, representing a container.

• Inflows are represented by a pipe pointing into, and adding to the stock.

Outflows are represented by pipes pointing out of the stock, subtracting from the stock.

• Valves control the flows.

• Clouds represent the source and sinks for the flows.

A cloud is representing a stock outside the boundary of the model. Sources and sinks are assumed to have infinite capacity, and can never constrain the flows they support.

The mathematical expression of stocks and flows is:

Stock = INTEGRAL (Inflow – Outflow, Stock t0)

Figure 5 Stock and flow model(Sterman 2000)

An everyday example of a stock and flow system can be a bathtub with the water tap as inflow, the bathtub itself as the stock and the outlet as the outflow.

The level of the stock is the accumulated difference between the inflow and the outflow, over time.(Sterman 2000)

All together, these tools allow the creation of “micro-worlds” where space and time can be compressed and slowed down for analytic purpose. The result is the experience of the long- and short-term side effects of decisions that are made. With this knowledge one can develop the understanding of complex systems, design structures and strategies for greater success in strategic decision making.

2.2 System Archetypes

Wolstenholme, E.F., "Towards the definition and use of a core set of archetypal structures in system dynamics" System Dynamics Review, 19 (7), pages 7 – 26, 2003

This article focuses on generic causal loop structures known as System Archetypes.
The author defines three postulates he debates later in the article.

- System Archetypes can be usefully condensed down to a more understandable core set of four totally generic archetypes consisting of pairs with reinforcing and / or balancing feedback loops.

- For every "problem" archetype there exists a closed loop "solution" archetype.

- Each archetype has important characteristics, which are vital to understand the role of archetypes in assisting System dynamics thinking.

Wolstenholme presents a set of four generic system archetypes where the problem archetypes are presented before the closed solution loop is added. The article introduces organizational boundaries to define a notation to show the hidden reactions of the system. Organizational boundaries imply that reactions are often ''hidden'' from the ''view'' of the source responsible for the actions.(Wolstenholme 2002)
Each generic archetype presented consists of a two loop system where the loops are either reinforcing (R) or balancing (B). The solution archetype is presented with the same two loops and in addition a solution loop that's either B or R.
The four condensed archetypes are named underachievement, relative achievement, out of control and relative control.
His experience in using and teaching System Archetypes, to a wide range of audiences, gives indications that system archetypes have a role in both ends of the modeling process. In the beginning by using their isomorphic properties to get the conceptualizing activities started, and at the end to collapse the model for easier presentation of insights derived from the more complex simulation models.

He states that System Archetypes are first and foremost a communication tool to share dynamic insights. System Archetypes are basically generic causal loop structures, which are much easier to comprehend than e.g. models of Stock-and-flow character.
System Archetypes can be viewed upon as short-hand versions of more complex systems and are excellent for communicating dynamic insights and knowledge from the dynamic systems. The Archetypes describe the problem using a CLD with two loops, Intended consequence feedback loop (IC) and unintended consequence feedback loop (UC). The loops are either reinforcing (R) or balancing (B).
The four combinations of system archetypes:
"Underachievement" (Intended loop R, unintended loop B)
"Out of Control" (Intended loop B, unintended loop R)
"Relative Achievement" (Intended loop R, unintended loop R)
"Relative Control" (Intended loop B, unintended loop B)

To get the IC, an action is initiated and after a time delay, due to the systems nature, UC will counteract the wanted outcome. These UC are often masked behind system boundaries that exist in all organisations and may be of both physical and/or mental nature. An IC started in one part of a company may trigger UC in another part of the same company. The notation is shown in Figure 6 where the tilted line shows what's behind the system boundary. The solution Archetype suggests a solution feedback loop to have a close awareness towards the systems reaction, and make corrections underway to minimize the effect from these unwanted reactions.

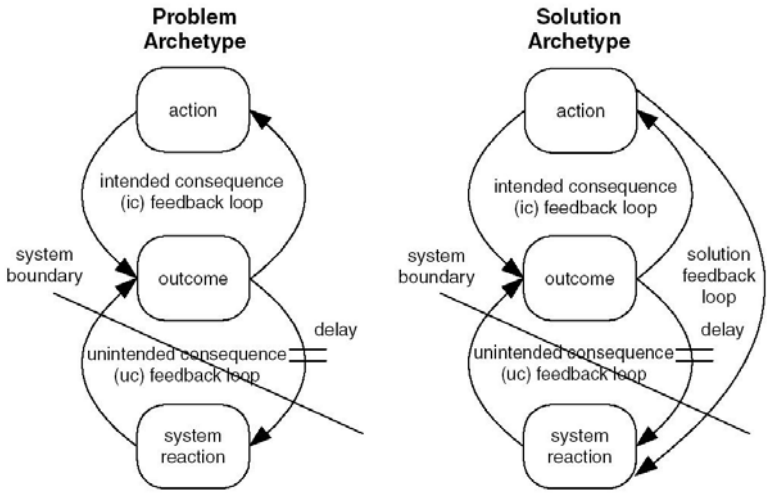


Figure 6 Generic System Archetype(Wolstenholme 2002)

2.3 System Dynamic Stories

Diana M. Fischer gives a brief description of what she believes dynamic stories are in her book “Modelling Dynamic Systems: Lessons for a first course”.(Fischer 2005) . In her introduction to system dynamic stories in chapter 9 she writes:

> “The system stories are a collection of scenarios that describe a situation that is to be modelled. The story provides the data necessary for the model, although not always in consistent units.”

Her angle to dynamic stories is more as a starting point to give students the necessary data and descriptions to start developing a model. The description has strong elements of communication in it, but in this thesis the use of System Dynamic Stories will be used to explain and clarify the System Archetypes and their dynamic behaviour over time, or in other words, Dynamic Stories to be used as supplementary tools to assist the communication of results and policies to support the system archetypes.
The dynamic stories should be of an industry related nature, describing a story that could have happened in the industry in question. The dynamic stories can be pure fiction, or if available, linked to actual happenings in the related industry.
The main purpose is to clarify, and make it easier for the audience or reader to understand the dynamic behaviour of the identified system archetypes.

3 Description of the System Dynamic model, IO version 1.95

The AMBASEC model has been created with Vensim DSS (www.vensim.com) which is one of the leading tools for system dynamics modelling.
The model has eight sub models presented on 9 pages and is named IO (Integrated Operations) version 1.95.
The eight sub-models are named according to what part of the Integrated Operations they describe/model.
The eight parts are Work Processes, Knowledge, Vulnerability, Incidents, Learning from incidents, Technology, Security culture and Risk 1 and 2.

3.1 Work processes

There are defined a total of twenty work processes which are to be changed in the transition from traditional operations to integrated operations. Areas were these work processes apply are, among others, daily production, maintenance and optimization. The model distinguishes between three stages for each work process, traditional, immature new and mature new work processes. The flow “developing new work processes” shifts the work processes from a traditional to an immature new stage and the flow “maturing new processes” shifts it further to a mature new stage. The rate in which this happens is influenced by the resources (man hours) dedicated to each task, and the effectiveness of these. The effectiveness of the resources dedicated to developing and maturing the new processes are depending on the state of “new initiatives burden” ,extra work load from new initiatives, (if high decreases the effectiveness) and the feedback from immature new work processes (if high increases the effectiveness).

The effectiveness on maturing will in addition depend on knowledge of incidents and technology. The state of new initiatives burden will mainly depend on the fractions of immature knowledge and work processes. A “snap shot” of the sub-model is presented in Figure 7.

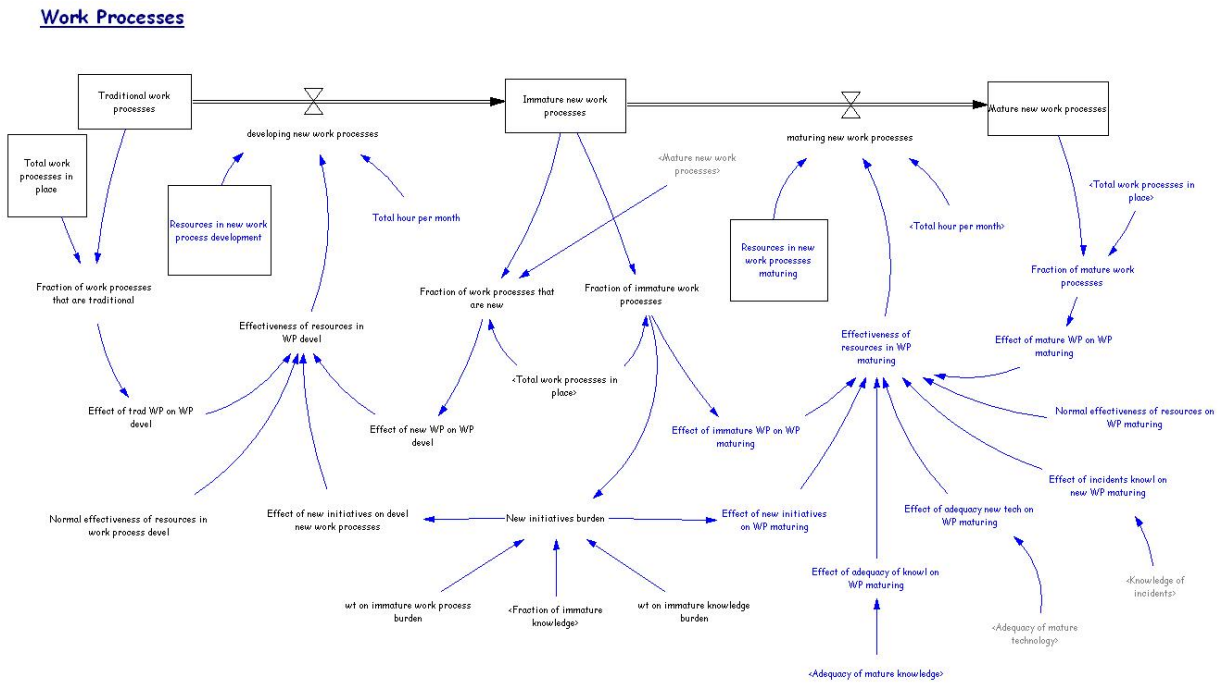


Figure 7 Work processes

3.2 Knowledge

Knowledge (Figure 8) gathers the total knowledge in the organization with inputs from the sub-models technology, learning from incidents, incidents, vulnerability and work processes. This sub-model is almost identical to “work processes” in structure.

It has three stages, traditional knowledge, immature new and mature new knowledge, with developing and maturing new knowledge as the flows in between. The main differences are that work processes now gives inputs where knowledge gave input in the sub-model work processes.

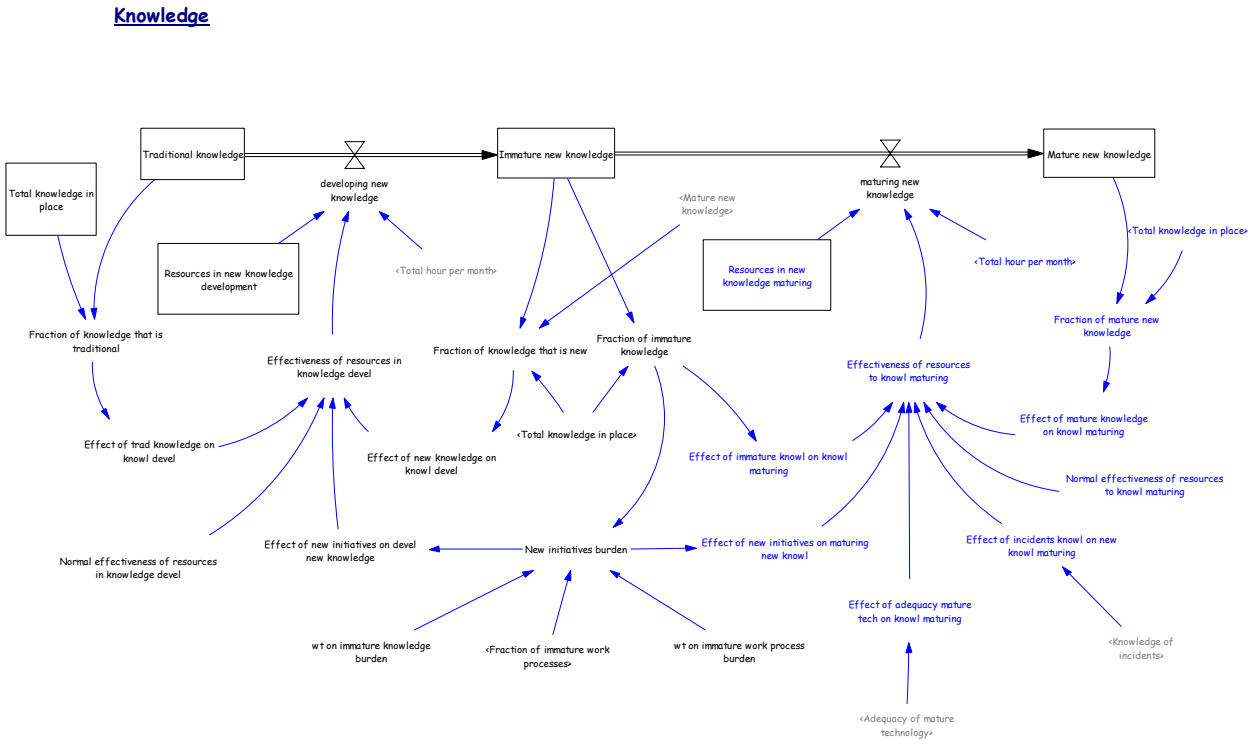


Figure 8 Knowledge sub-model

3.3 Vulnerability

The main function of the sub-model Vulnerability (Figure 9) is to generate the vulnerability index. The vulnerability index is an aggregated measurement on the overall security status of the system and can move between 0 and 1 (1 being vulnerable, and 0 being hardened). The main inputs to the vulnerability index are the fraction of immature knowledge and work processes (increasing the vulnerability index if higher than total knowledge and work processes in place, at any given time).

If adequacy of mature knowledge and technology increases the effects of this will decrease the vulnerability index. A high value from security culture and knowledge of incidents will decrease the vulnerability index. This will be further explained in the corresponding sub-models security culture and learning from incidents.

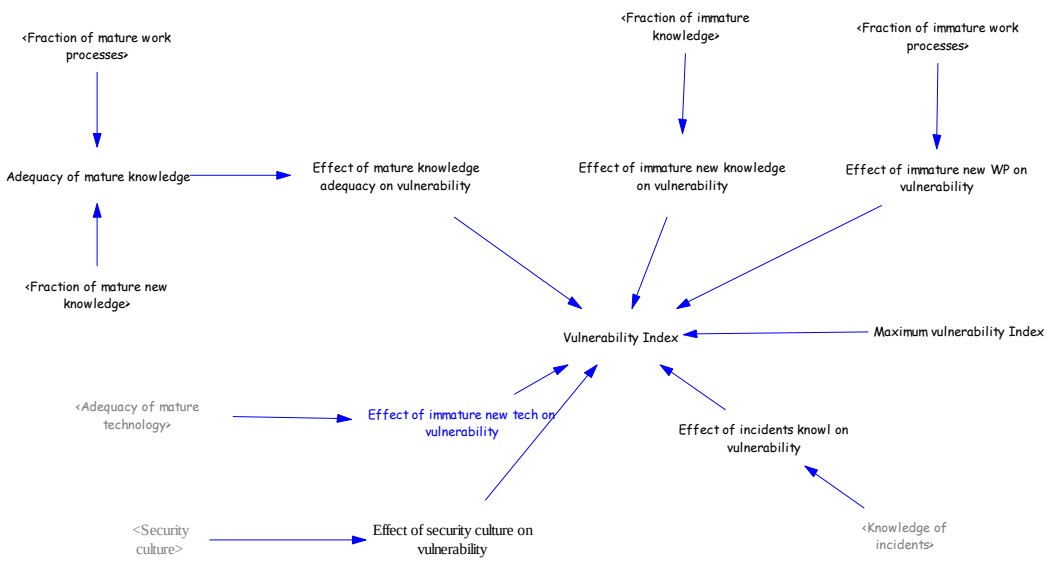


Figure 9 Vulnerability sub-model

3.4 Incidents

The main objective of the Incidents (Figure 10) sub-model is to obtain a value for frequency and severity of incidents and add this to the average incidents cost to be able to calculate a cumulative incidents cost in NOK (Norwegian kroner).

Frequency of (security) incidents (incidents meaning events "successful" in causing damaging) is a product of the vulnerability index and the frequency of events. High vulnerability index allows more events to become incidents. The "frequency of events" variable is the product of the effects from immature new work processes, knowledge, technology and the normal frequency of events. As for the severity of incidents, the effects from resilience and knowledge of incidents handling, together with normal severity of incidents gives input to the average cost of incidents. The "frequency of detected incidents" gives output to learning knowledge of incidents and incidents handling. The higher the frequency, the more knowledge is gathered.

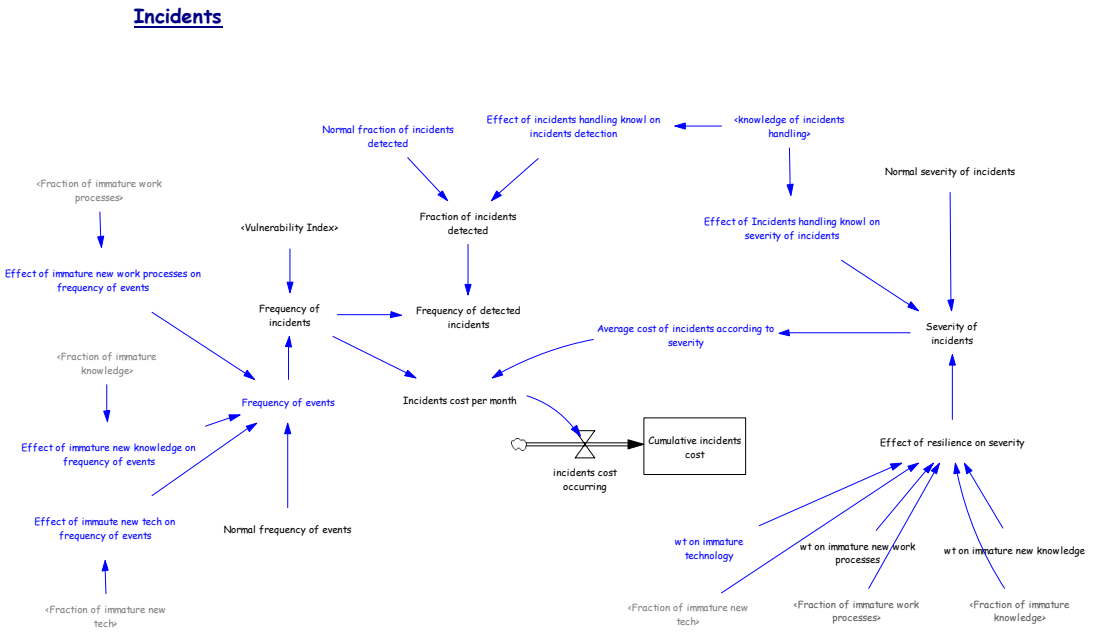


Figure 10 Incidents sub-model

3.5 Learning from incidents

The sub-model (Figure 11) presents the learning and forgetting knowledge aspect of the model.

There are two separate stocks, knowledge of incidents and knowledge of incidents handling. Each of the stocks has a “learning” inflow and a “forgetting” outflow, originating and vanishing outside the boundary of the system (model).

The flow rate of “learning knowledge of incidents” is determined by the frequency of detected incidents and the learning gained per incident. Learning per incident is derived from the accumulated “knowledge of incidents” (and its effect) and the adequacy of mature knowledge (derived from the vulnerability sub-model) in addition to the effect of the severity of incidents. The outflow, forgetting knowledge, is determined by the “time to forget” (set to 6 months).

The “knowledge of incidents handling” flow has the same structure with incidents handling as the focus instead of incidents. Adequacy of mature technology is the changed input variable (originated from the technology sub-model).

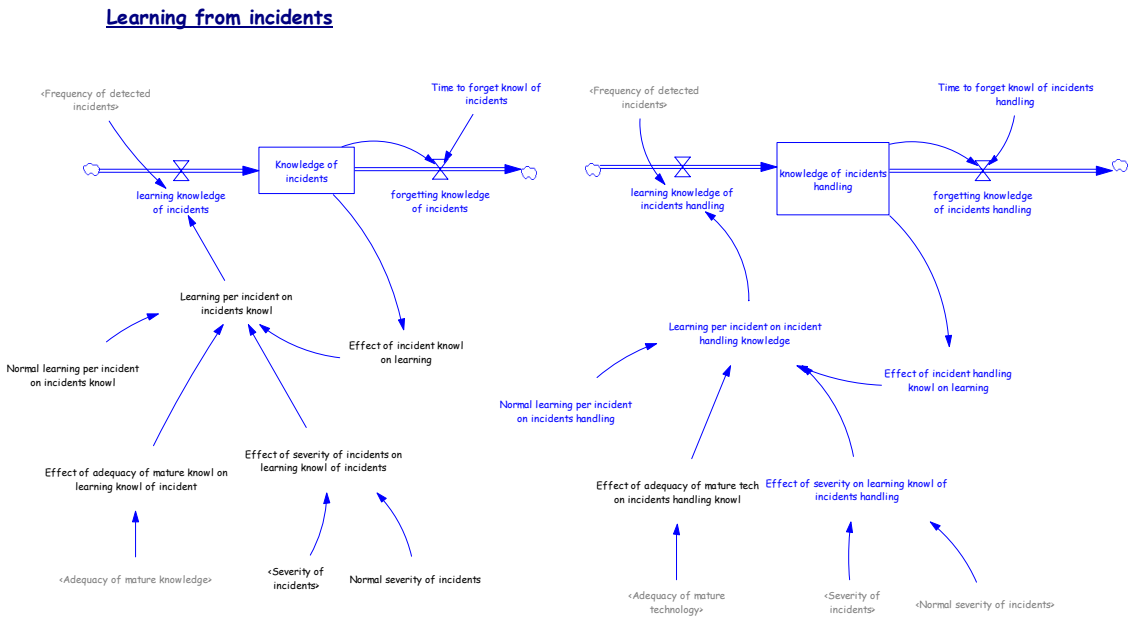


Figure 11 Learning from incidents sub-model

3.6 Technology

There are two stages in this sub-model (Figure 12), immature and mature new technology know-how. The inflow (to immature) “developing new technology know-how” is originating outside the systems boundary, denoted with a cloud. The rate of the inflow is determined by how many new technologies, used in each new work process, and the rate of the development of new work processes (if developing work processes increase, developing technology know-how also increases). The resources in maturing new technology know-how (in man hours), together with the effectiveness in technology maturing, determines the flow rate of the maturing. Knowledge of incidents, adequacy of mature knowledge and technology together with the effects of immature and mature technology determines the effectiveness in technology maturing.

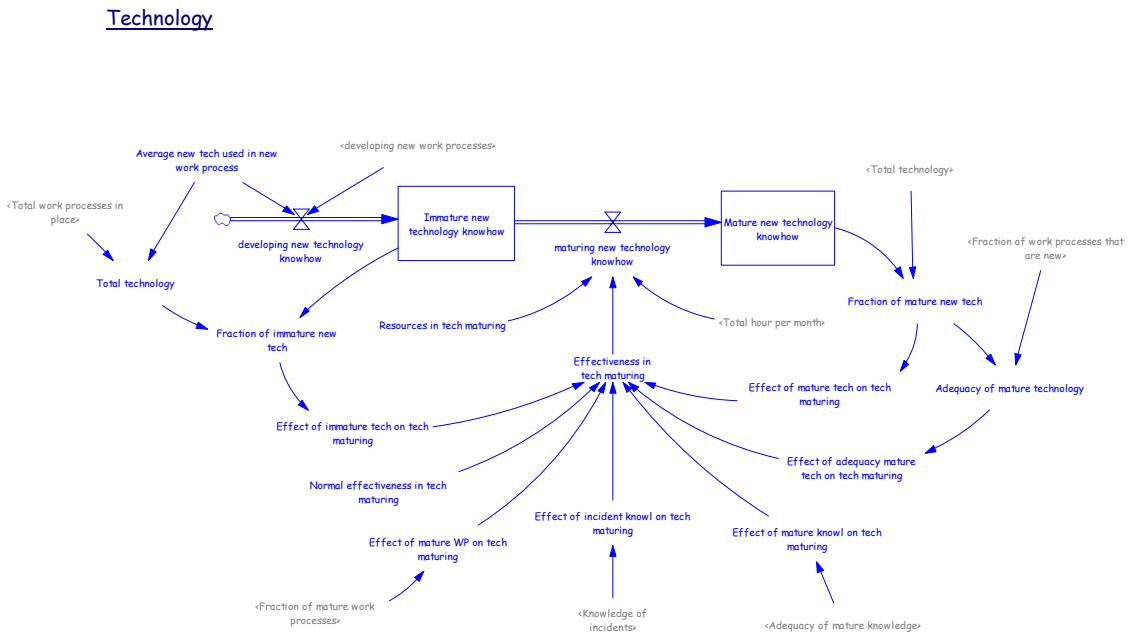


Figure 12 Technology sub-model

3.7 Security culture

The terms pathological, calculative and generative security culture follows the same definitions as in the SINTEF report "The Track to Safety Culture"(Stig Ole Johnsen 2004)

1. Denial culture – Pathological culture: The organisation is ruled by a desire to preserve status quo: denial of signals, punish whistle blowers, attack reputation of HSE scientists, avoid reporting recording, and "out of sight – out of mind" attitude. There are no feedback systems in the organisation.

3. Calculative culture – a bureaucratic, purely rule based culture: The organisation is using rules, they stay within normal wisdom, downplay the implications, implements limited scope of repair and remedial actions.

5. Generative culture – the learning culture: The organisation is concerned both with fundamental rules but also with goals, values and continuously learning. It welcomes and encourages danger signals, disseminates, sees wider implications, and is positive to system changes. There is a higher order feedback system – hence a learning organisation.

The sub-model (Figure 13) has two objectives, first to determine which security culture that's dominant. Then compare it to desired security culture, and make adjustments to obtain the wanted culture through security gap and the flow change of perceived security gap. Learning knowledge of incidents, if increased, increase the transition rate of moving to calculative culture and generative culture. New initiatives burden counteract calculative security culture and increase the flow back to pathological culture.

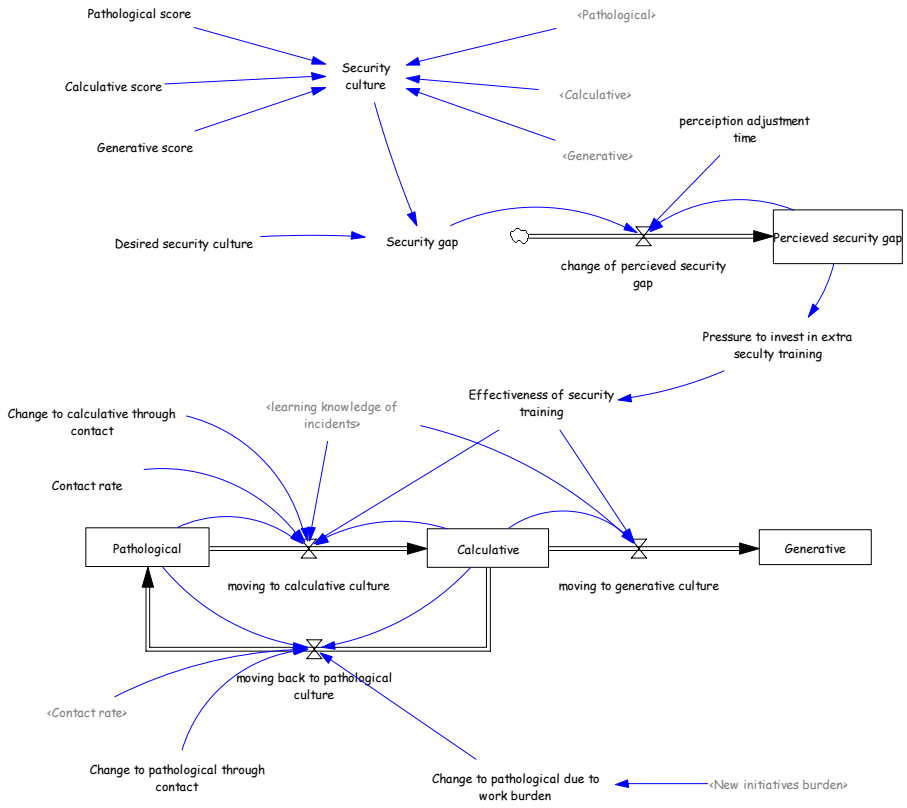


Figure 13 Security Culture sub-model

3.8 Risk 1 and 2

The sub-models, Figure 14 and Figure 15, maps all, so far, identified information security threats to the integrated operations project and give it a value for the cost of each incident in M (million) NOK/month.

The result is the total cost of all incidents. This is calculated by adding up the "sub–costs" from terror attacks, component failure, human errors, virus and worms, illegal insider activities and the incidents due to loss of situation awareness. Vulnerability index, security culture give inputs to the sub-costs insider activities, and virus and worms. The product of fractions of immature work processes, knowledge, new technology and adequacy of mature knowledge, together with initial frequency of human errors, leads to the cost of human errors.

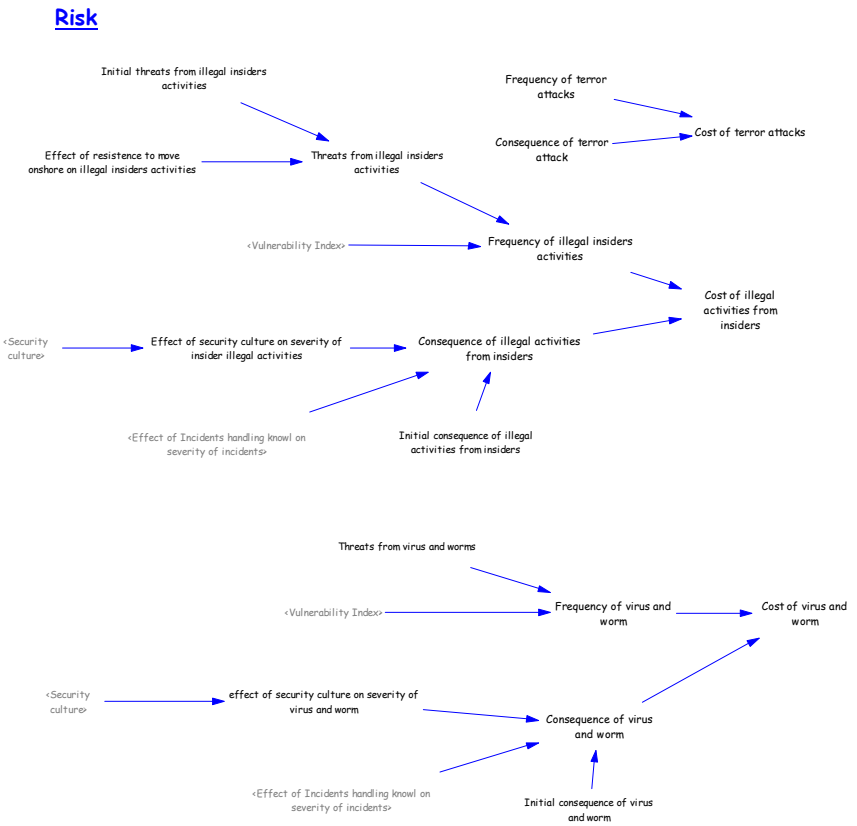


Figure 14 Risk 1 sub-model

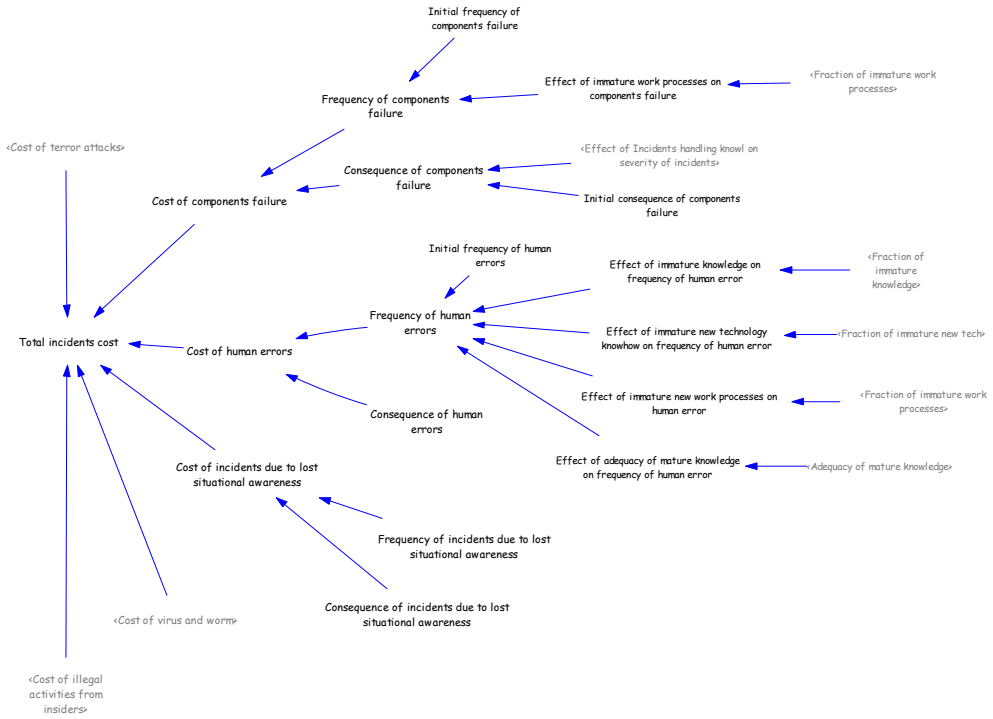


Figure 15 Risk 2 sub-model

3.9 CLD of model

To present the most important loops in the model, a CLD (causal loop diagram) is presented in Figure 16. The CLD is presented with labelled boxes as a reference to the above described sub-models. The sub-models Risk 1 and 2 are not presented in the CLD since they don't give any feedback to the dynamic behaviour of the model. The main objective of risk 1 and 2 is to present a value for total incidents costs, in M NOK.

The stocks are framed with rectangular boxes to differentiate them from the other variables and flows (rates). The links, between the variables, have been labelled S (same effect) and O (opposite effect) to show the polarity. The reason for choosing S and O for polarity is of communicative reasons. Managers and decision makers in the industry are often trained in economics and may interpret + and – as "to add" and "to subtract" instead of causal dependencies where increase in one variable gives an increase (S) in the dependant variable.

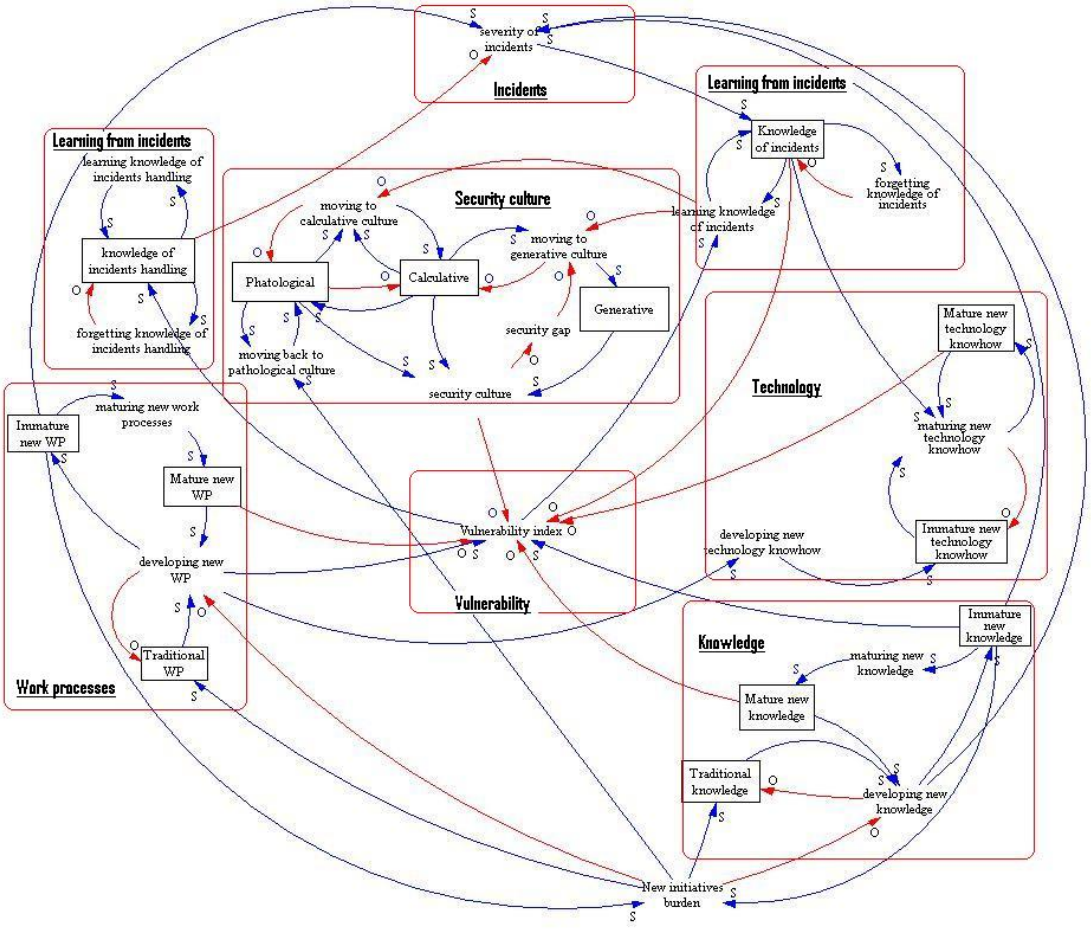


Figure 16 CLD with boxed sub-model

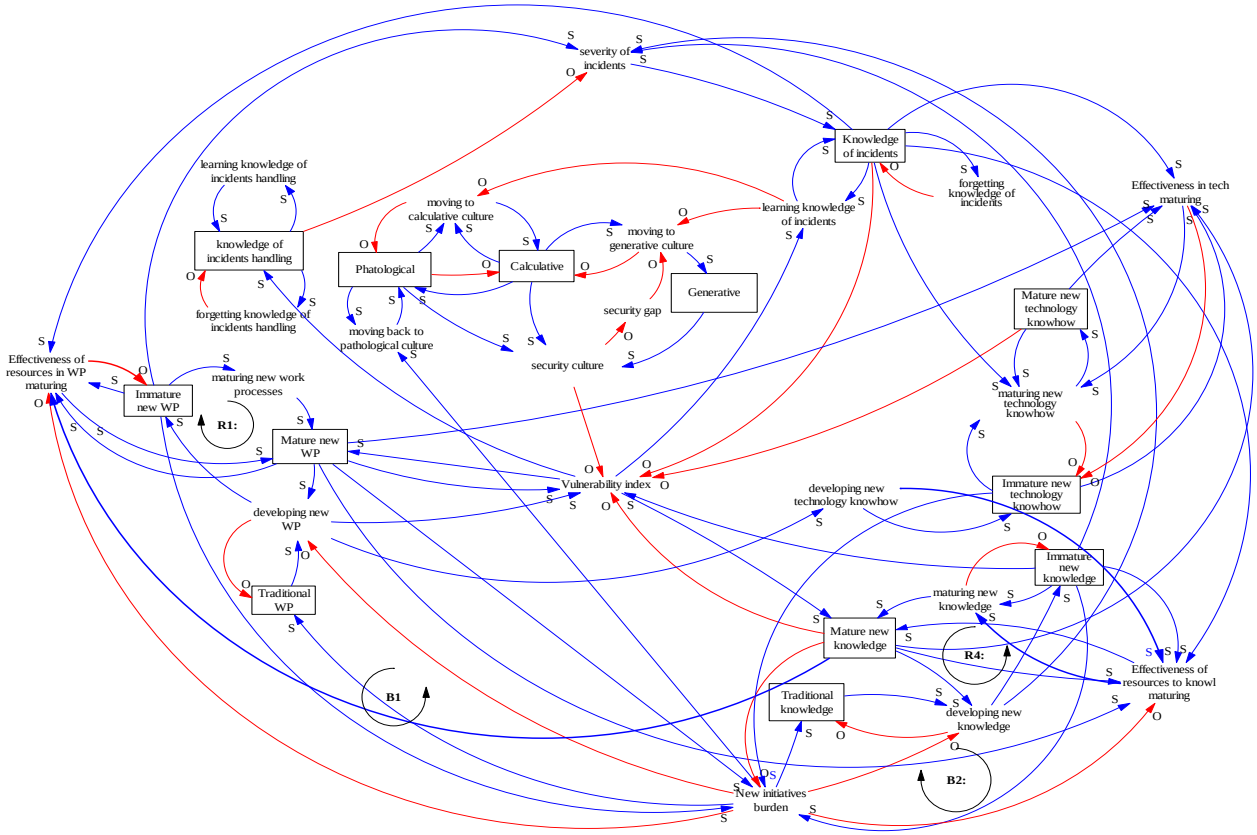


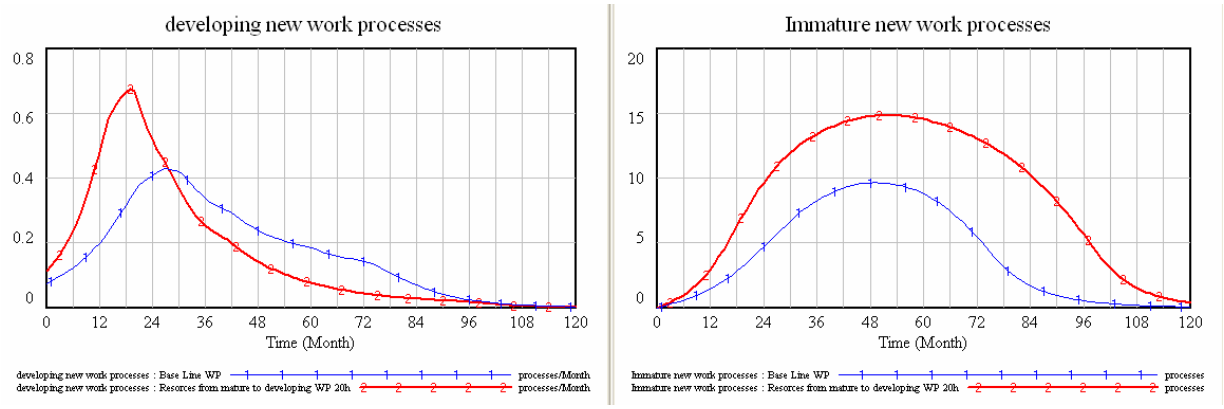
Figure 17 CLD presentation of the model IO version 1.95

4 Model Analysis with proposed System Archetypes and Dynamic Stories

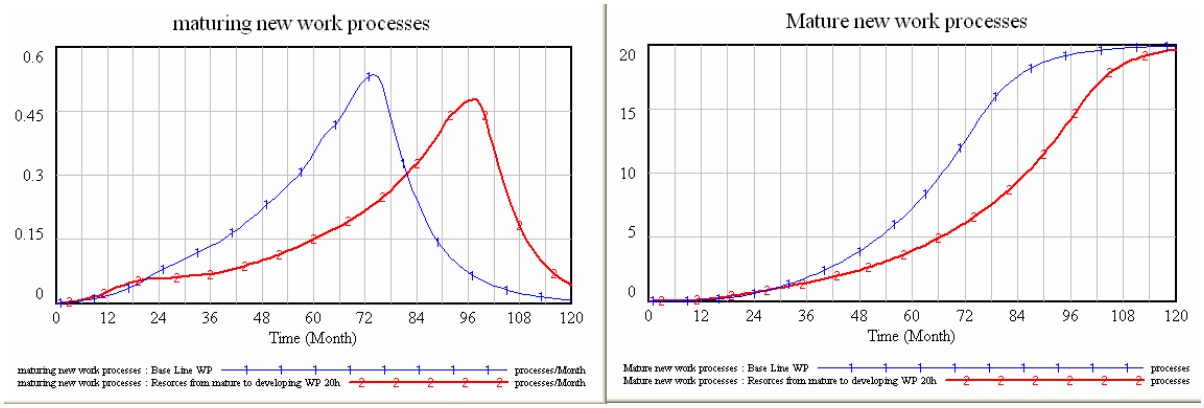
The values of constants and variables in the developed model (IO version 1.95), are provided by the IO project and is defined as Base runs, for comparison, throughout the testing. In the first part of the testing I assume that the total amount of resources in the model is constant and is transferable. They can not be increased in one part without being decreasing in other parts of the model. For the rest of the testing random values will be chosen, altering one value/variable for each run, to monitor the behaviour of the model (IO version 1.95).
Since the main objective of the IO project is to make the transition from traditional to integrated processes, the focus of the testing will be trying to reveal unintended consequences (slowing down the transition) from intended actions taken. At the end of the testing the proposed solutions will be evaluated regarding information security risks

4.1 First scenario: Work Processes

What happens if resources on "developing new WP (work processes)" were increased as an attempt to speed up the transition from traditional WP to New WP's? To test this scenario "resources in developing new WP" were increased by 20 man hours per month. Resources on "maturing new WP" were decreased by 20. The results are presented below in graphs.

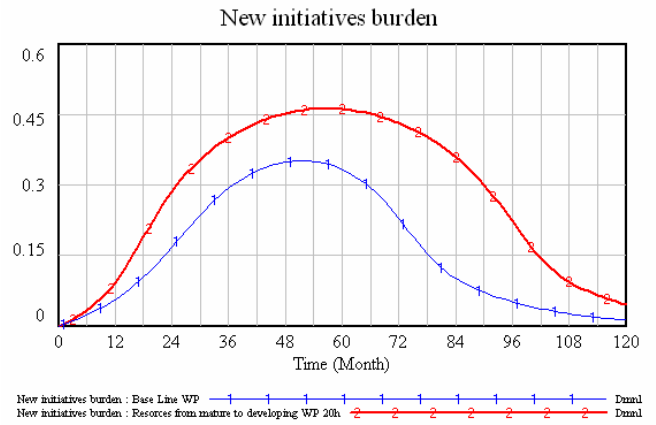


The development of new WP now peaks after only ca.15 months at a much higher level than the Base run did, and goes toward zero after ca. 84 months, about one year prior to the Base run. As for Immature new WP, meaning implemented not mature new WP, the level increases rapidly and stays above Base run through the whole simulation period.



The maturing of new WP now lags behind the Base run and mature new WP (Mature WP meaning that personnel have enough knowledge about the WP, and know well the embedded technology and how to operate it) are severely delayed in time compared to the Base run. To find out what may cause this unintended outcome (UC) we look at the inputs to the flow "maturing new WP".

From the equation in the flow “maturing new WP”, << Resources in new work processes maturing/Total hour per month*Effectiveness of resources in WP maturing>>, we see that if “Effectiveness of resources in WP maturing” increases the contribution to “maturing new WP” will decrease (below what it otherwise would have) due to the increase “New initiatives burden” gets from “Immature new WP”



This can be presented as a System Archetype where the increased new initiatives burden triggers the unintended consequence in reduced mature new WP.

4.1.1 Underachievement Archetype: “Developing new WP”.

To place the system archetype in context with the rest of the model, Figure 18 shows the system archetype with thicker links and the loop indicators R1 and B1

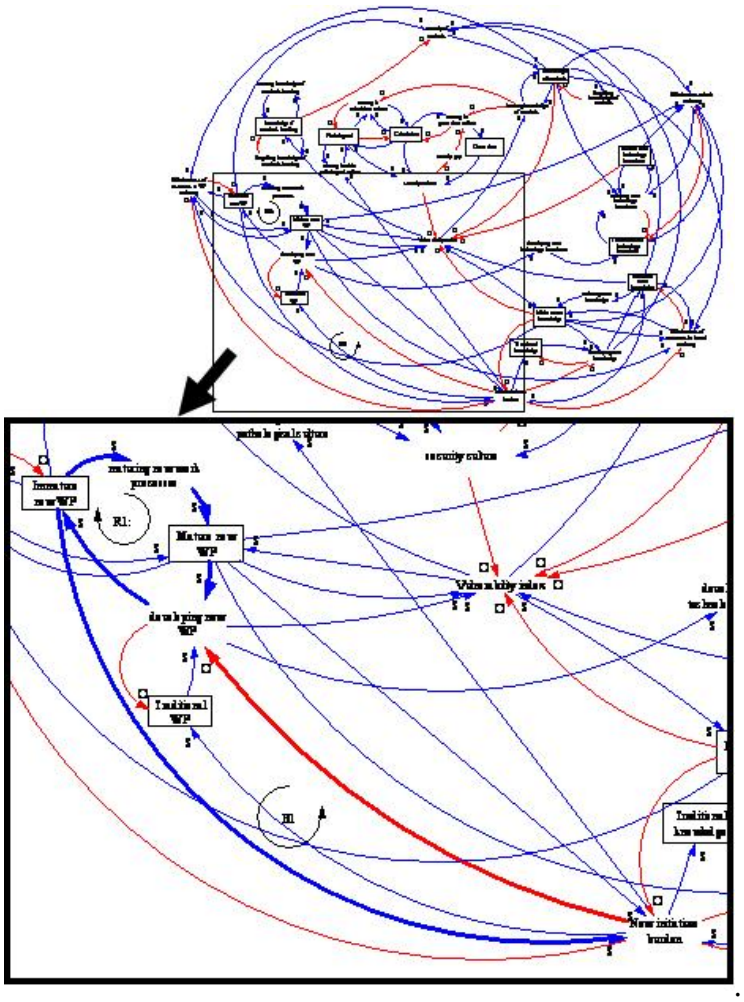


Figure 18 1st System archetype in context

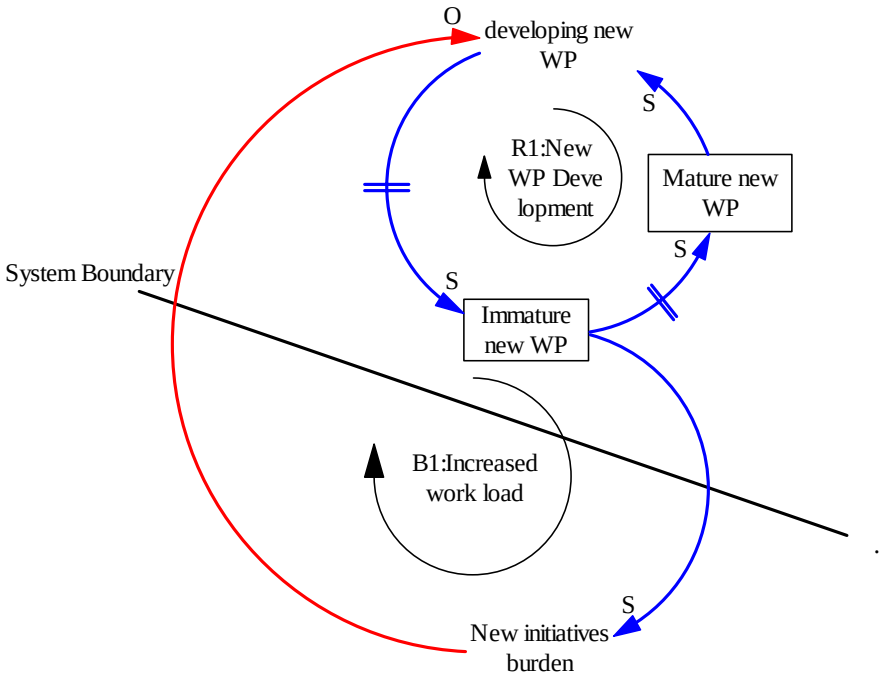
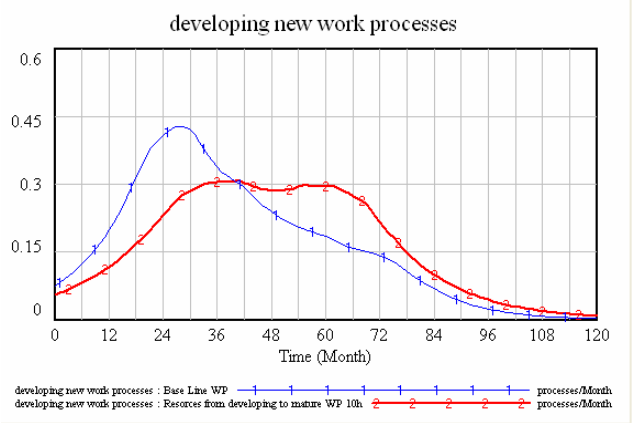
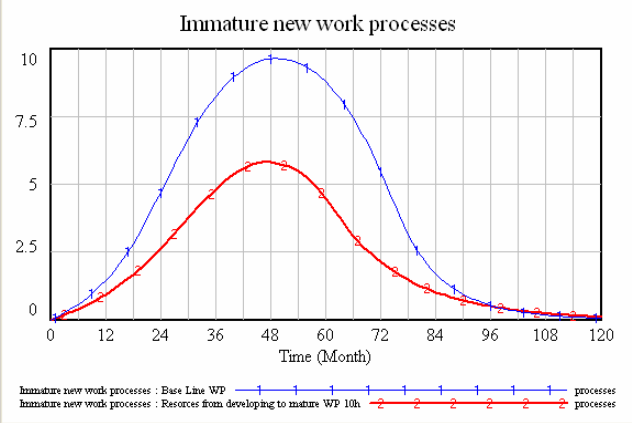


Figure 19 Underachievement: New WP

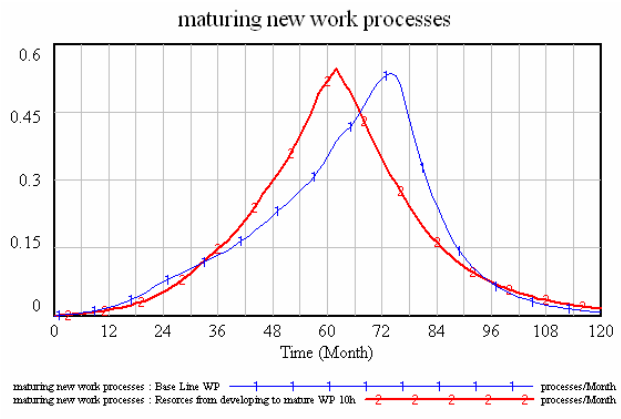
If management (Figure 19) adds resources to “developing new WP”, “immature new WP” will increase (above what it otherwise would have), and will after a delay increase “Mature new WP”, which again will increase “developing new WP”.
We now have the reinforcing loop, R1: New WP development. After a delay due to the systems inertia, “New initiatives burden” increase and as a result, decrease new WP, giving the balancing loop B1: Increased work load.

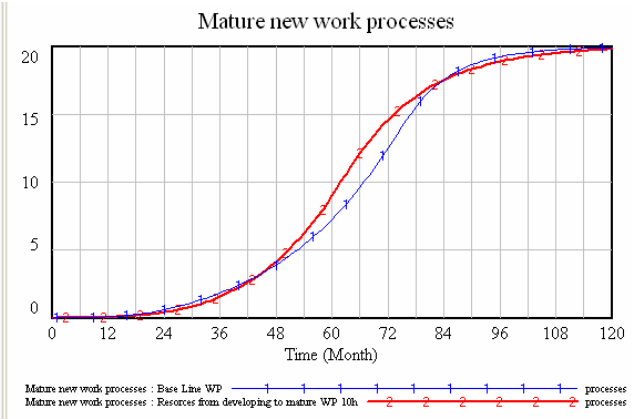
The proposed solution is to shift resources from developing new WP to maturing new WP. If we increase resources in maturing new WP by 10 man hours per month, and decrease resources in developing new WP an equal amount, this happens.



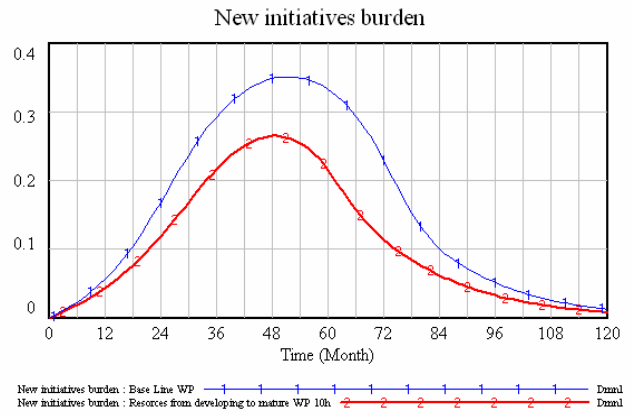


Developing new WP now has a decrease at first, but then increases above Base line. Immature new WP decrease below base line. (Base line is marked 1)





Maturing and mature new WP gets a better result, and the new initiatives burden decreases.



4.1.2 1st proposed solution archetype: Focus on maturing WP

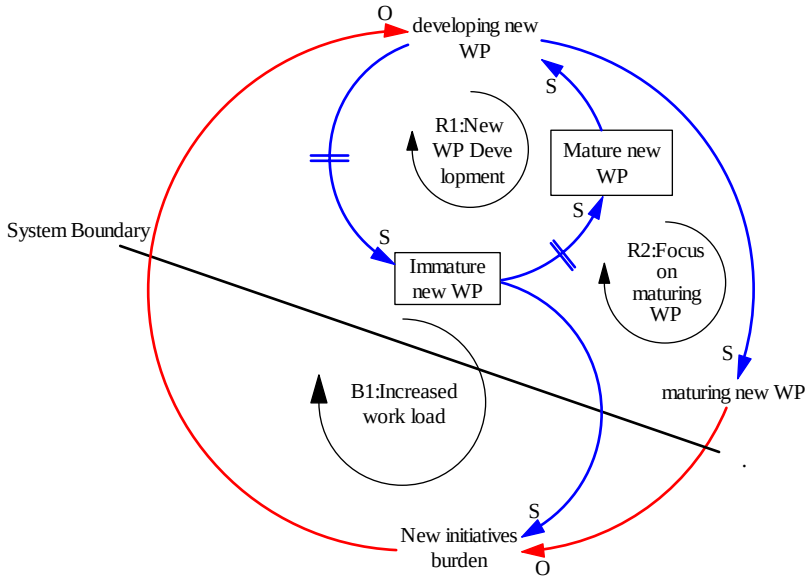
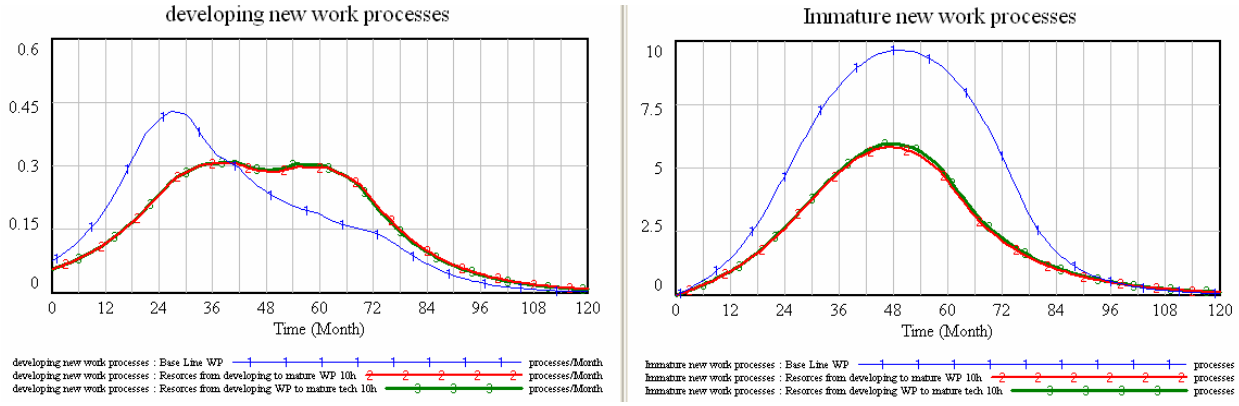


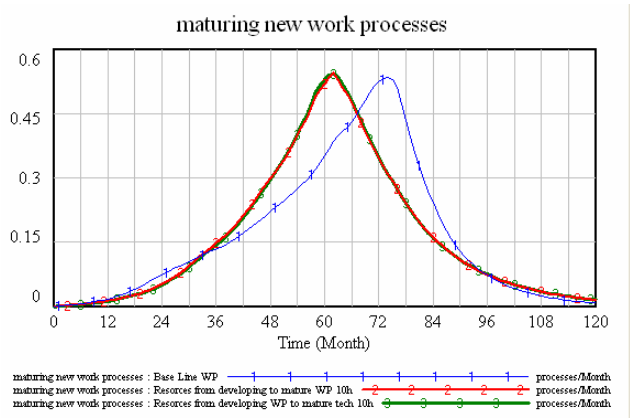
Figure 20 solution: Focus on maturing WP

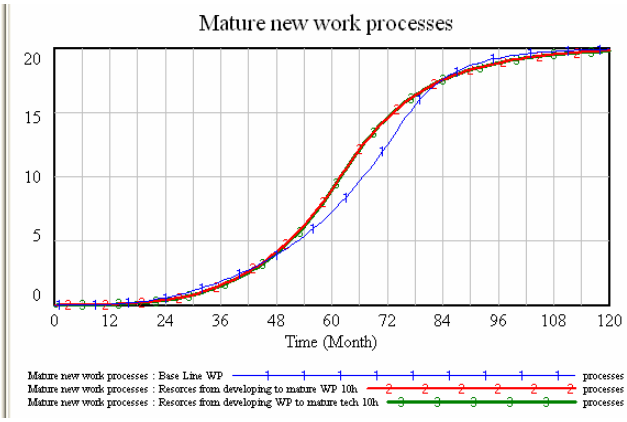
Resources are shifted from developing new WP to maturing new WP, giving a decrease in new initiatives burden which again increases developing new WP. The increase in developing new WP increases maturing new WP resulting in the reinforcing loop R2: Focus on maturing WP.

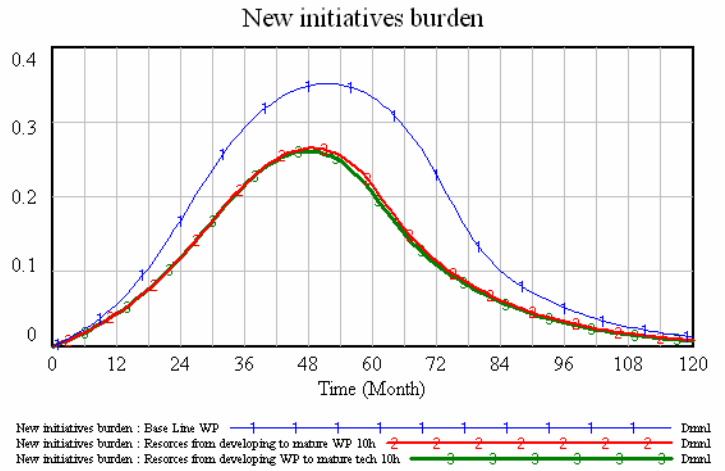
4.1.2 Same problem archetype with new proposed solution

If resources from developing new WP are added to maturing new knowledge instead, we get this result.









This presents a similar result compared to shifting resources to maturing new WP.

4.1.4 2nd Proposed Solution Archetype: Focus on maturing knowledge.

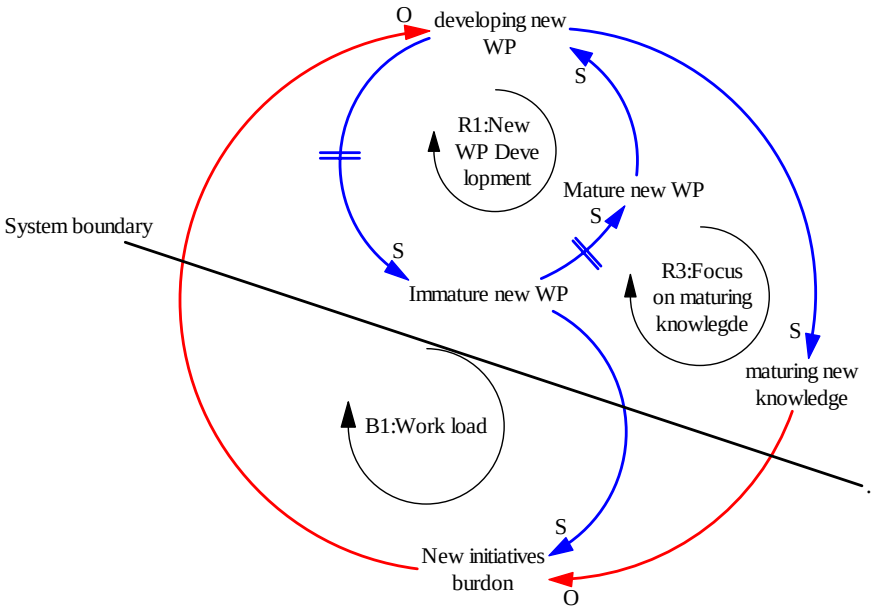


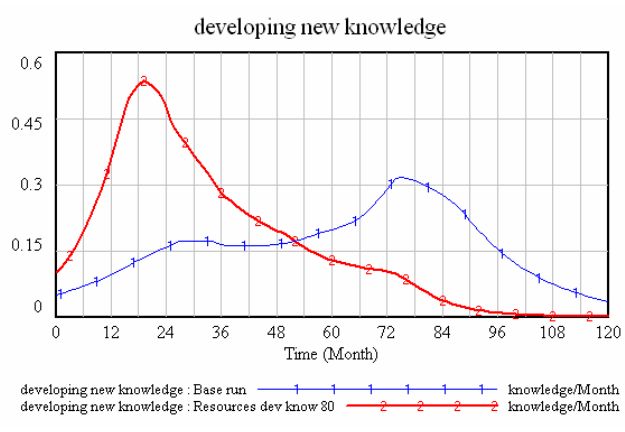
Figure 21 Solution2: Focus on maturing Knowledge

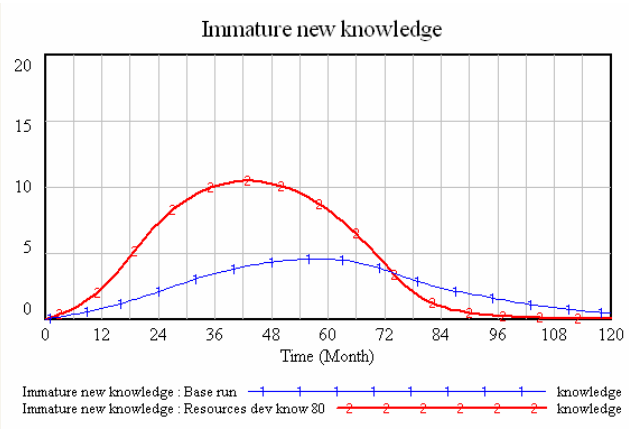
Resources are shifted from developing new WP to maturing new knowledge, giving a decrease in new initiatives burden, which again increases developing new WP. This again increases maturing new knowledge resulting in the reinforcing loop R3: Focus on maturing knowledge.

4.2 Second scenario: Knowledge

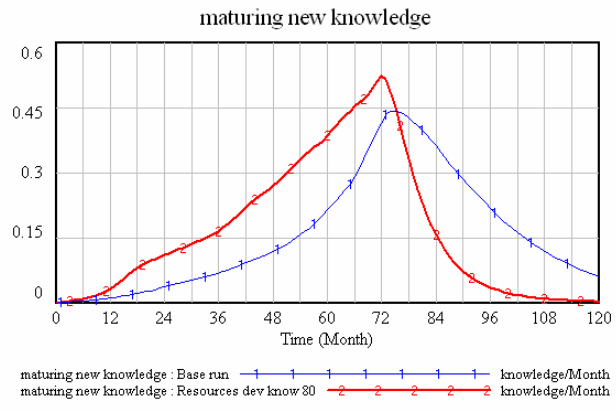
I will here make the assumption that extra resources are available to be able to test the dynamic behaviour with only one input value changed for each test.

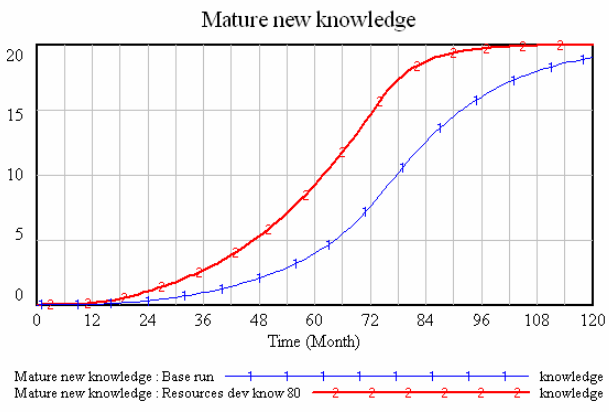
If resources in new knowledge development were increased from 40 to 80 man hours per month, as an attempt to speed up the maturing of knowledge, this would happen.



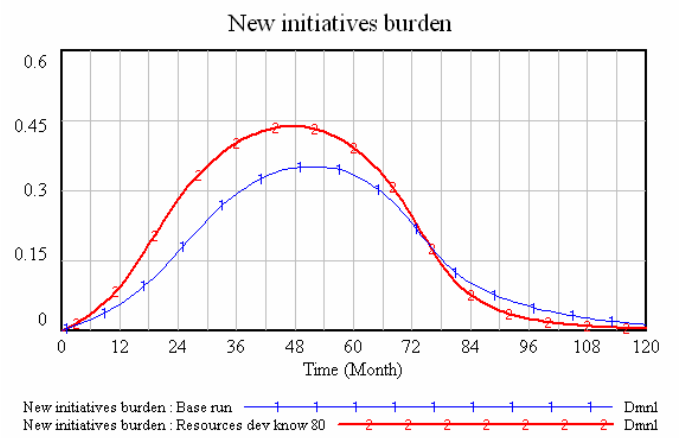


Developing NK (NK = new knowledge) has now a step increase from start to approx. 20 months into the project. It then decreases to converge against zero around month 96. Immature NK will also increase since the increase in development of NK builds a stock in immature NK. It converges at approx. the same time as developing NK does.





Maturing NK reaches its peak at approx. the same time as Base run, but at a higher level. Mature NK reaches its peak more than 2 years ahead of the Base run.



The increased new initiatives burden will after a delay behave as a brake to developing NK and slow down maturing NK, this resulting in a decrease in mature NK.
This can be presented as an underachievement System Archetype.

4.2.1 Underachievement System Archetype: Slowing down knowledge development.

The system archetype can be seen in context with the rest of the model in Figure 22, below. The reinforcing loop R4 is the knowledge development loop, and B2 is the counteracting loop increased work load.

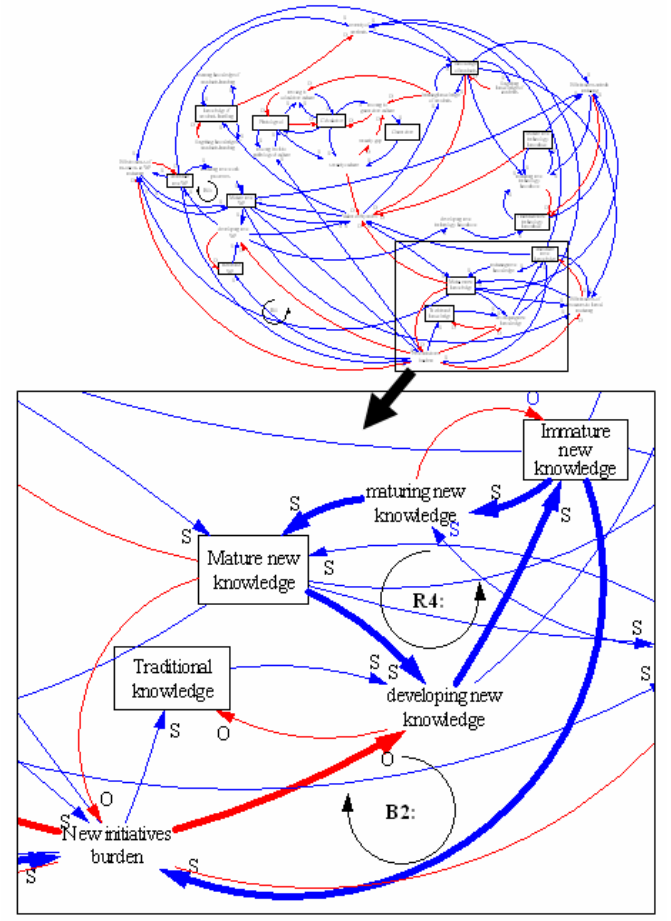


Figure 22 2nd System Archetype in context

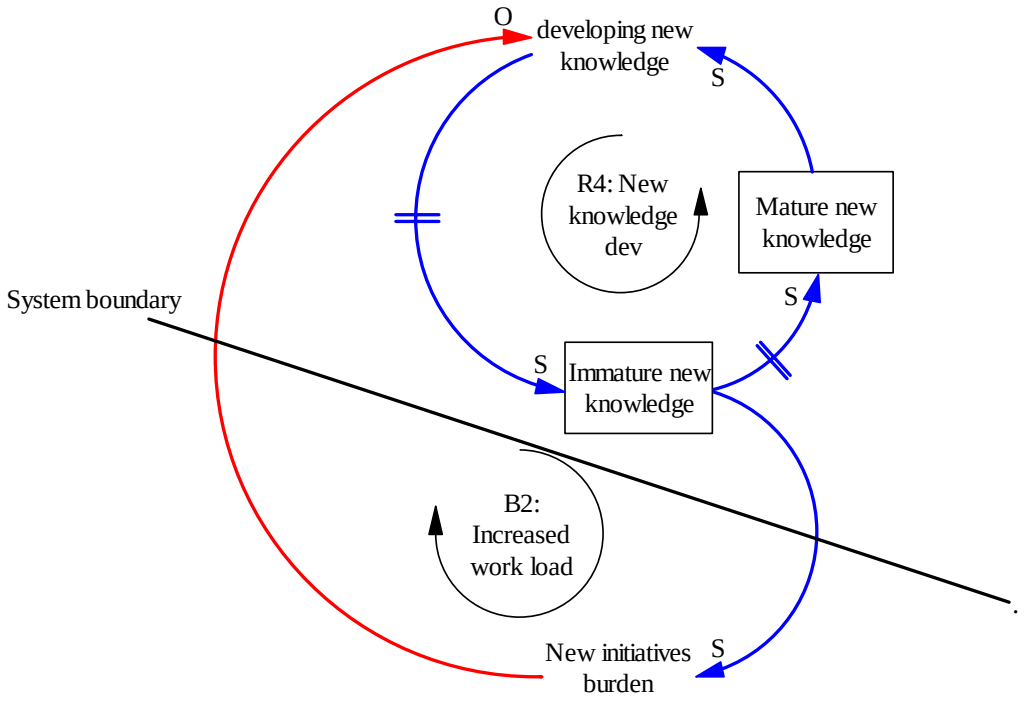


Figure 23 UA System Archetype: New Knowledge development

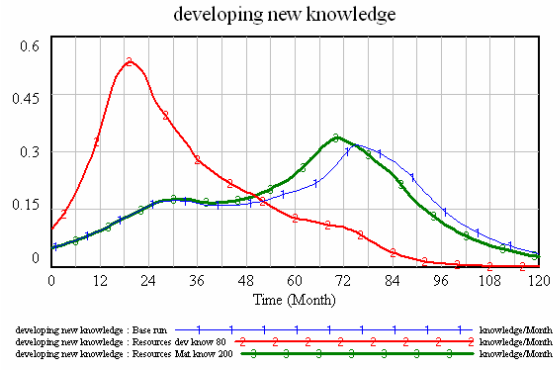
Dynamic behaviour of the UA problem Archetype, Figure 23

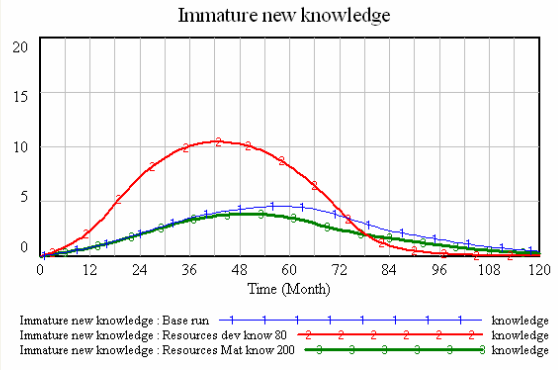
If management adds resources to “developing NK”, “immature NK” will increase (above what it otherwise would have), and will after a delay increase “Mature NK” which again will increase “developing NK”.

We now have the reinforcing loop, R4: New knowledge development. After a delay due to the systems inertia, “New initiatives burden” increase and as a result, decrease developing NK, giving the balancing loop B2: Increased work load.

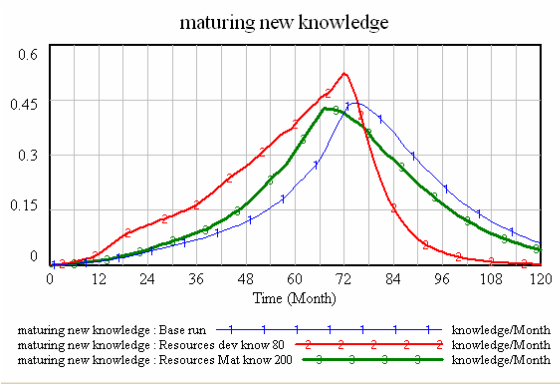
4.2.2 1st Proposed Solution: Focus on maturing knowledge.

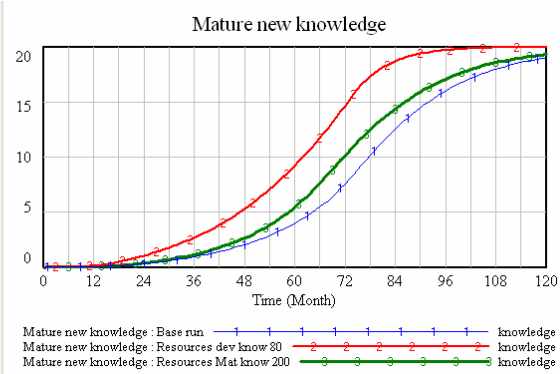
To try to counteract the unwanted feedback from new initiatives burden, resources in maturing NK were increased to 200 man-hours per. Month.
The results from the test are presented in graphs below.



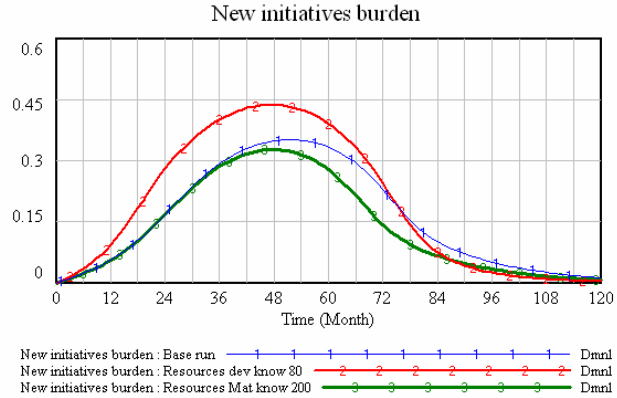


Developing NK now gets of to a slower start, but is still better than the base run. Immature NK is even lower than the base run from month 48 until end of project.





Maturing NK has a similar curve as the base run, but now peaks 6 months earlier. Mature NK has a slightly better performance than the base run.
To see if the actions taken is giving a decrease in work load, lets look at the results for new initiatives burden.



The new initiatives burden now has a similar increase as the base run up until the 36th month, and then decreases at a higher rate than the base run did.

4.2.3. 1st solution archetype: Focus on maturing knowledge.

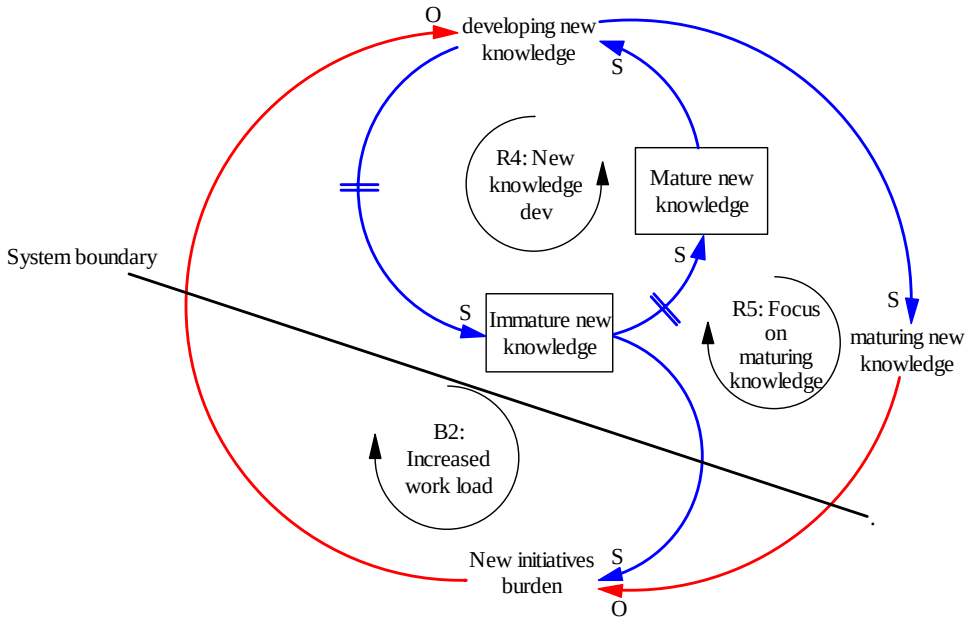
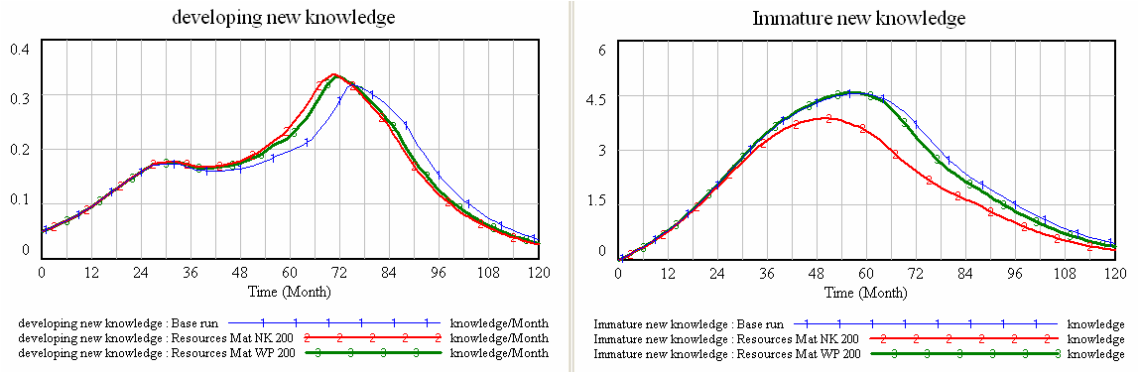


Figure 24 Solution 1: Focus on maturing Knowledge

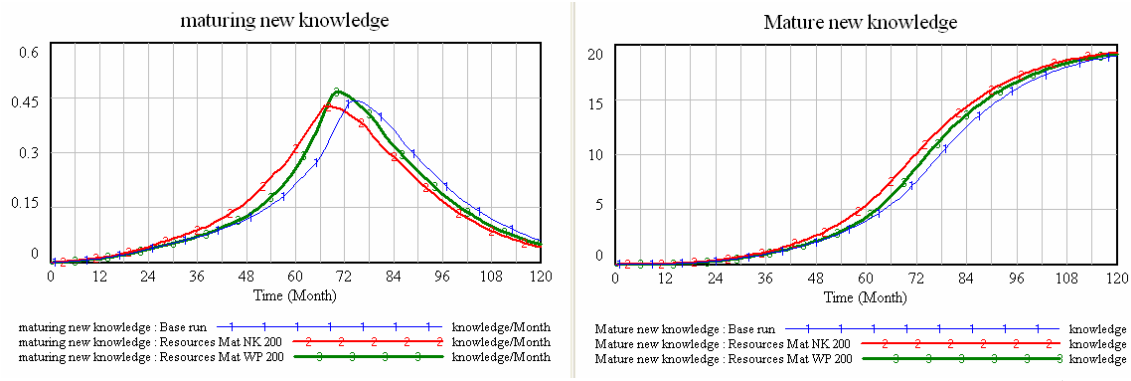
Resources are increased in maturing NK, giving a decrease in new initiatives burden, which again increases developing NK. This again increases maturing NK resulting in the reinforcing loop R5: Focus on maturing knowledge.

4.2.4 2nd Proposed Solution: Focus on maturing work processes.

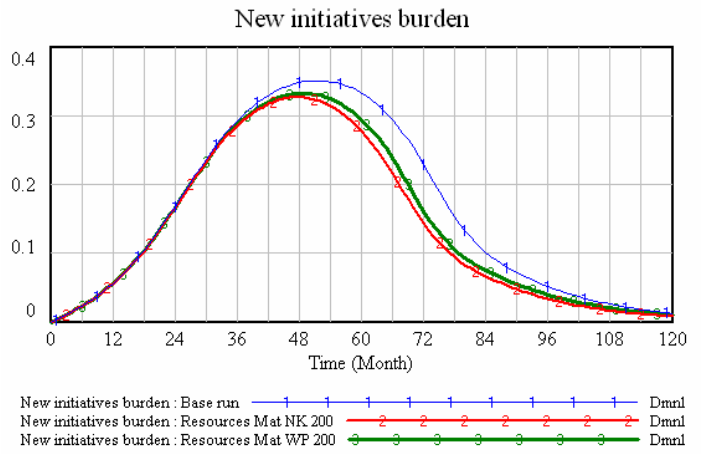
Another possible solution might be to increase resources in maturing new work processes. Maturing new work processes were increased to 200 man-hours per. month, giving the results below.



The 2nd solution gives a slightly poorer result on developing NK, but still better than Base run. Immature NK increases compared to the first proposed solution but stays slightly below base run.



Maturing NK has a slower increase, but reaches a higher level than both base run and 1st solution (marked 2 on graph). Mature NK places itself in the middle between base run and 1st solution run, giving a slightly poorer result than 1st solution.



Same behaviour as the 1st solution up until the peak point, but decreases at a slower rate than the 1st proposed solution did.

4.2.5 2nd solution archetype: Focus on maturing work processes.

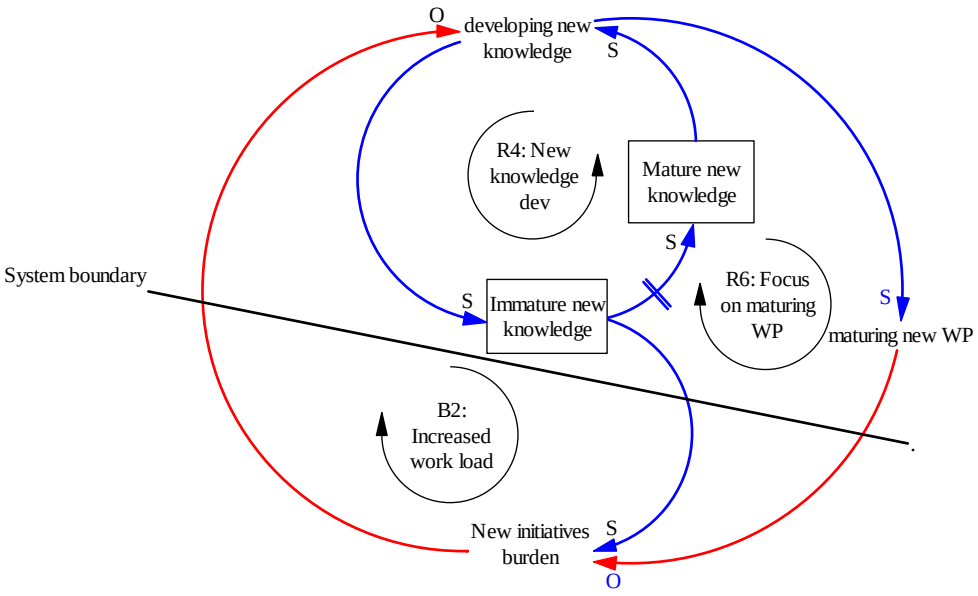
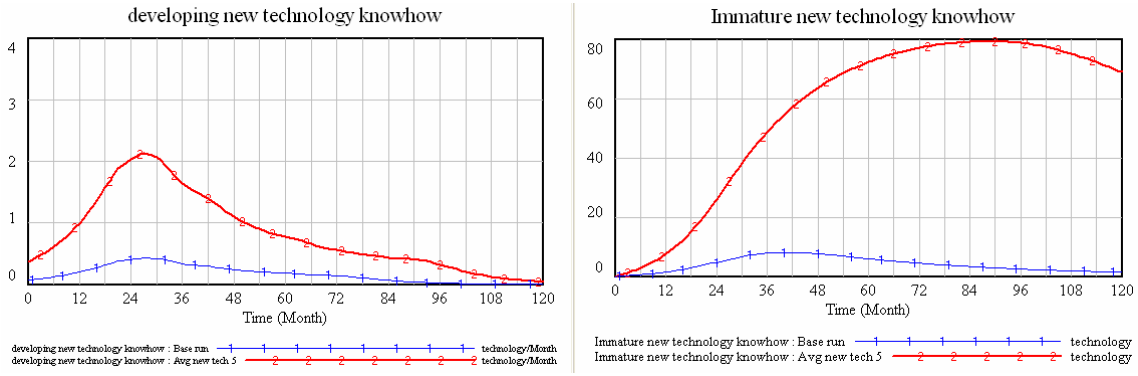


Figure 25 Solution 2: Focus on maturing work processes

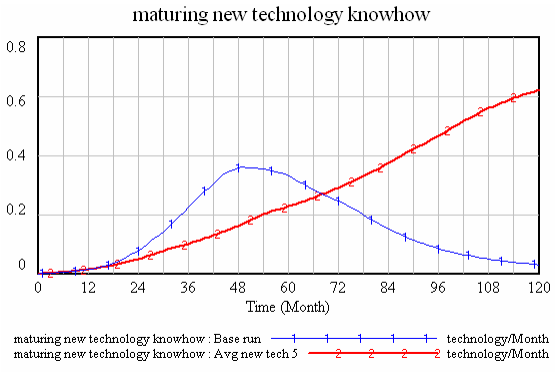
Resources are increased in maturing new WP, giving a decrease in new initiatives burden, which again increases developing NK. This again increases maturing new WP resulting in the reinforcing loop R6: Focus on maturing WP.

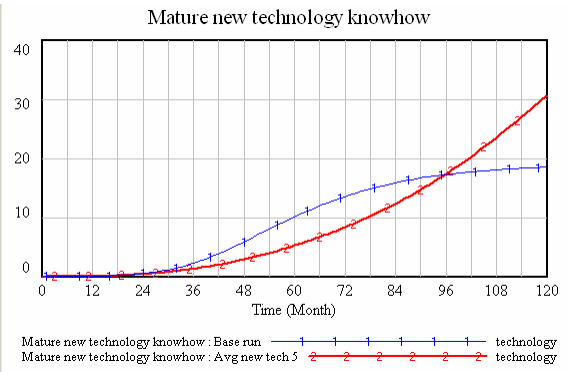
4.3 Third scenario: Technology

If it was decided to increase the use of new technology in new WP, from 1 to 5 technologies, this would happen.

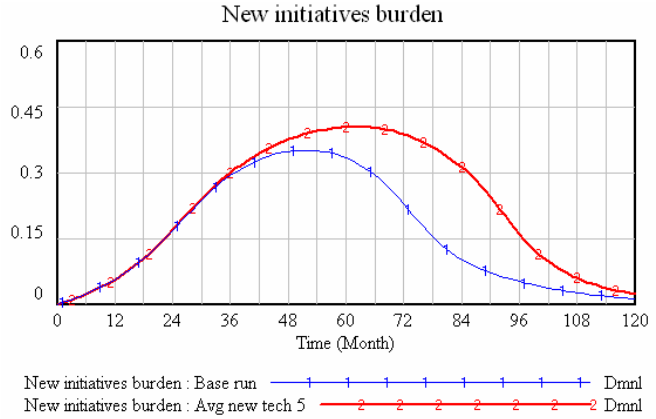


Developing new technology know-how would increase rapidly since the number of developed new WP would be multiplied with 5. This again increases immature new tech know-how.





Maturing new tech know-how increases at a linear growth compared to the base run. Mature new tech know-how stays below the base run at first, then increases rapidly after month 96.



New initiatives burden increases above base run after month 36, and stays way above. This can be presented as an underachievement archetype where the intended action mature new technology know-how is counteracted by the unintended consequence increased new initiatives burden.

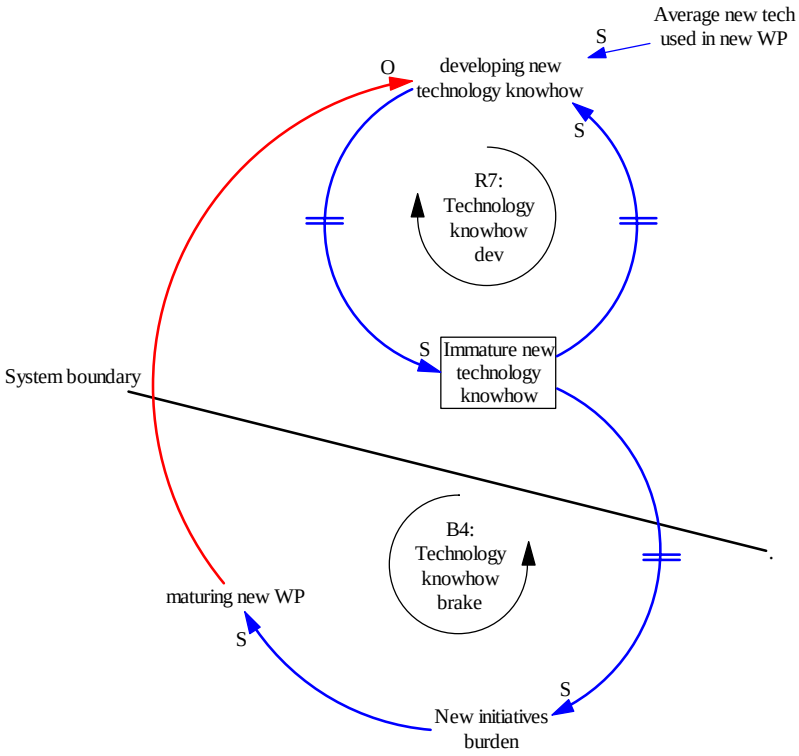
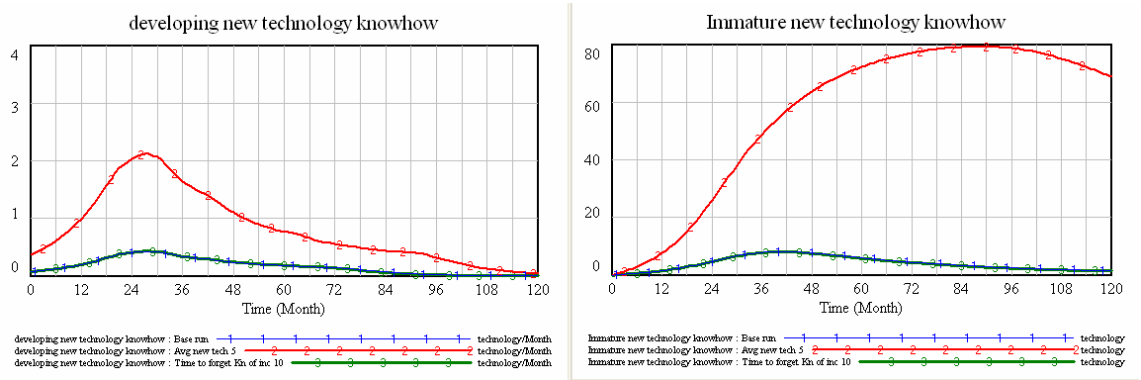


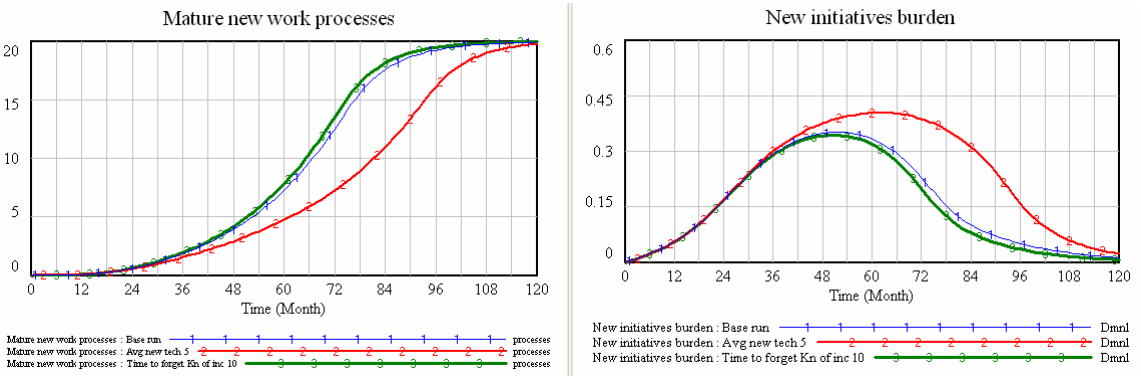
Figure 26 UA System Archetype: Technology know-how development

When increasing number of new technologies used in new WP, dev NTKh (New Technology Know-how) increases which again increase immature NTKh. This again increases dev NTKh, and the reinforcing loop R7: Technology know-how development is shown in Figure 26.
The balancing loop B4: Technology know-how brake is counteracting the intended outcome of immature technology know-how.
When Immature NTKh increases, the new initiatives burden increases due to the extra resources needed to mature NTKh.
New initiatives burden increases maturing new WP through the decrease in “effect of new initiatives on WP maturing” variable, and developing NTKh decreases as a result.

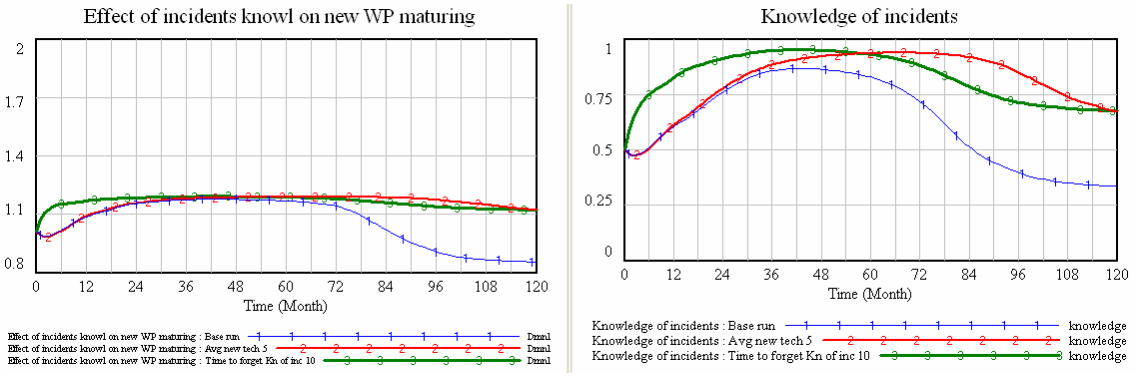
4.3.1 1st proposed solution: Security training to increase time to forget knowledge of incidents.



All graphs follow the Base run graph except for maturing new WP and new initiatives burden which got slightly better results.



The fraction of immature knowledge decreases and has a decreasing effect on new initiatives burden. “Effect of incidents knowledge on new WP maturing” gives a higher value due to the increased Knowledge of incidents.



4.3.2 Proposed solution archetype: Security training to raise knowledge of incidents.

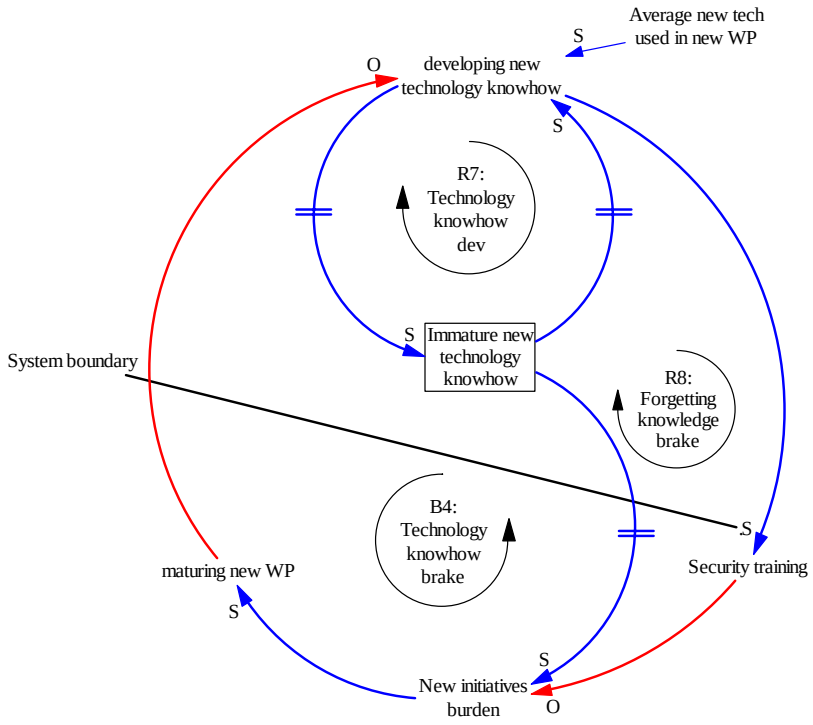
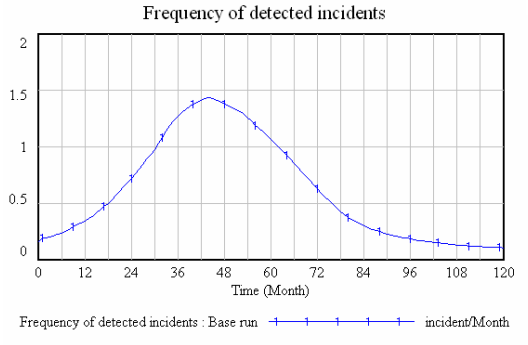


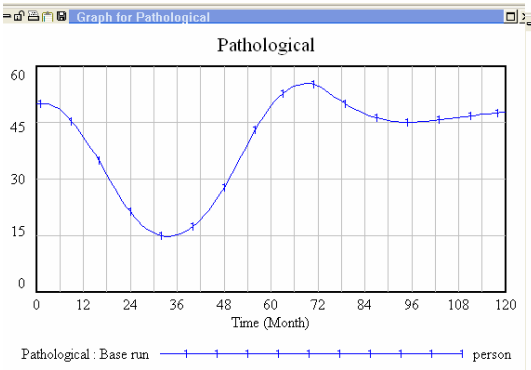
Figure 27 proposed solution Archetype: Forgetting knowledge brake

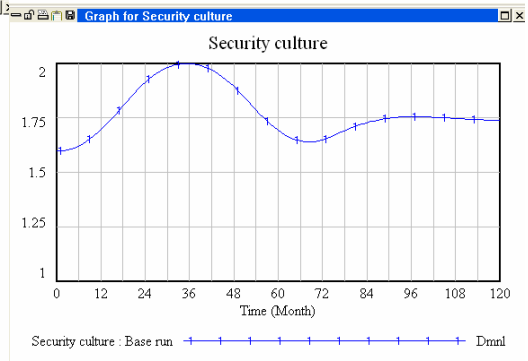
Security training to slow down the frequency of “time to forget knowledge of incidents” gives a decrease in new initiative burden, which again decreases maturing new WP. This again increases developing new technology know-how “through developing new WP”. We now have the solution loop R8: Forgetting knowledge brake

4.4 4th scenario: The Relative Control Archetype.

If we look on the graphs for frequency of detected incidents and pathological we see that when frequency of detected incidents increase, pathological decrease. When vice versa.







The same apply for vulnerability index where the security culture gives input to the vulnerability index, but the decrease is triggered by the increase around month 70 in Pathological.

These findings indicate strongly that a relative control archetype exists.

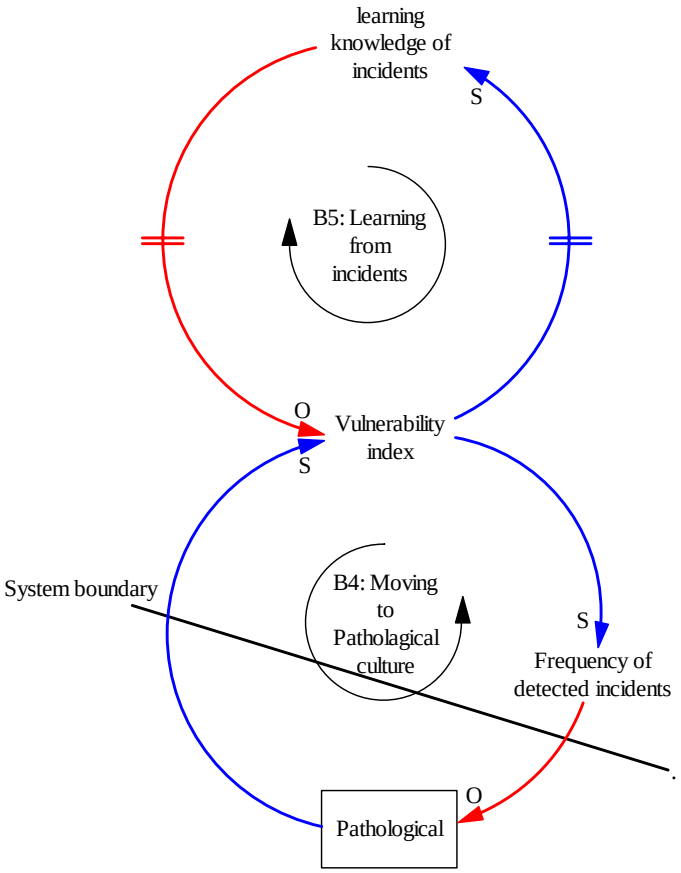


Figure 28 Relative control problem archetype: Security culture

If Vulnerability index increases, learning knowledge of incidents will increase since more incidents will lead to more knowledge about the incidents. This is wanted. High knowledge of incidents leads to a decrease in the Vulnerability index since the more we know, the lesser it's likely we'll be attacked. The loop B5: Learning from incidents shows this.
On the other hand, a decrease in the vulnerability index will decrease the frequency of detected incidents which again will increase Pathological. When Pathological increase the vulnerability index will increase and we have the balancing loop B4.
These two loops will alternate in dominating since both are trying to balance the same system.

A possible solution for this archetype may be to set an absolute target for how many incidents are acceptable and adjust the security culture and policies according to the target.
If there are few incidents people get sloppy and don't keep focus on security, meaning some incidents are "good" since it keeps the focus on security high.

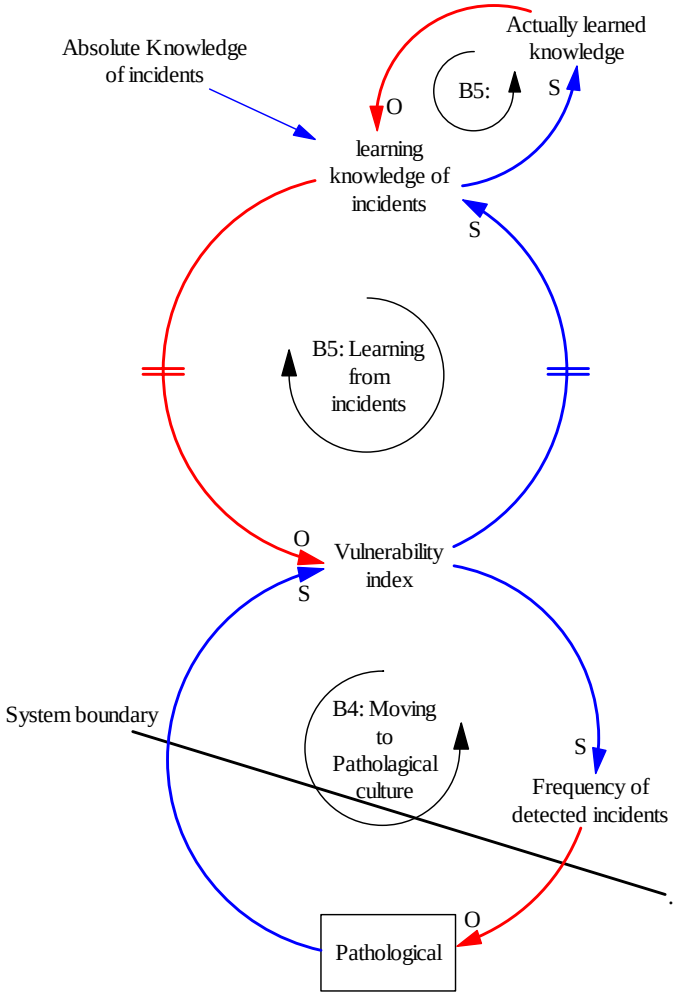
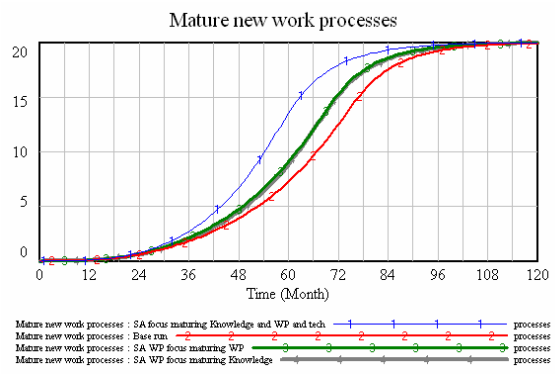
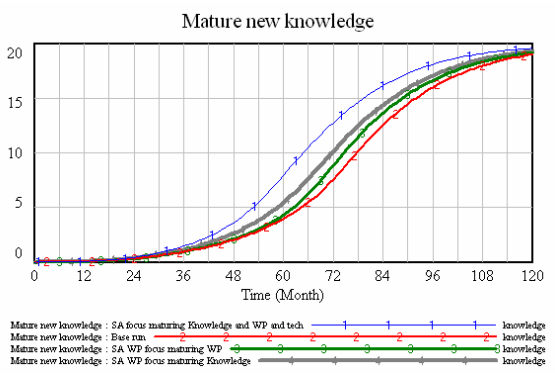


Figure 29 Targeting Knowledge

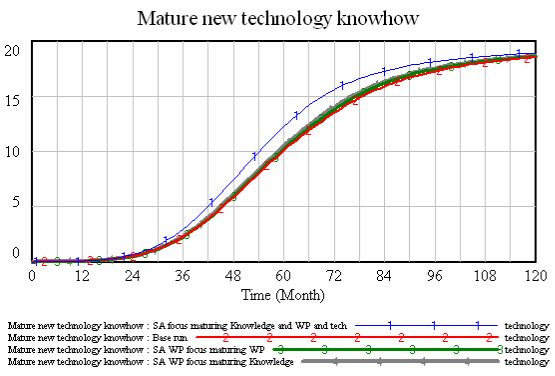
5 Policy recommendations

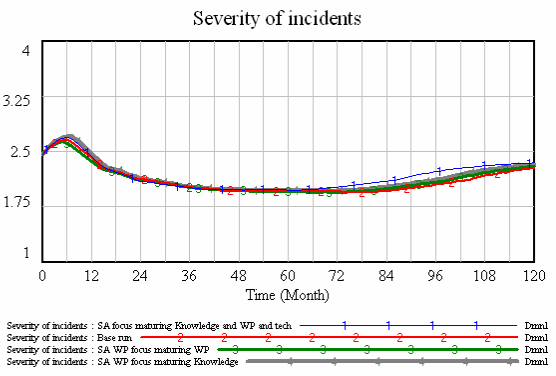
After testing the different scenarios, a combination of solutions were tried.
The solutions indicated that an increase in maturing resources gave the best results on completing the integrated operations transition from traditional WP to mature new WP.
When increasing resources in WP maturing (200 man hours), Knowledge maturing (230) and tech maturing (200) the results looked like this:



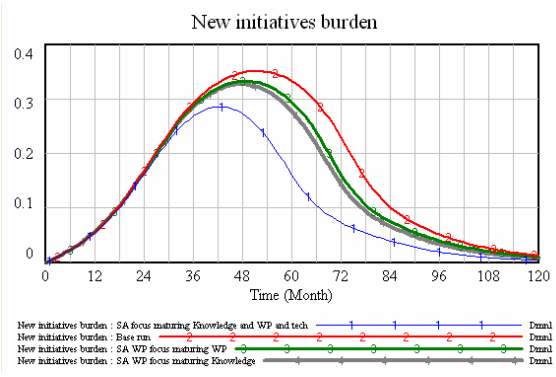


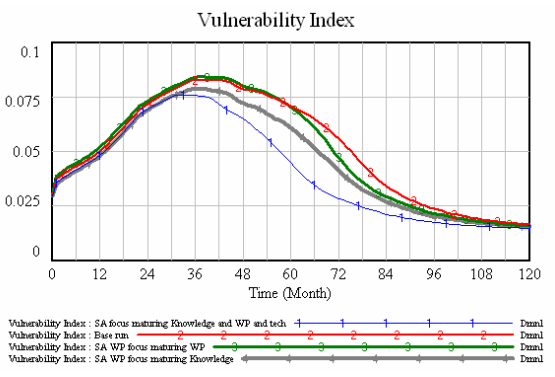
Mature new WP has a much steeper increase and is through maturing WP before end of IO. Mature new knowledge also has a better result combined than each proposed solution on its own.





Mature new technology also shows a better result. Severity of incidents stay at a low level, but increases slightly at the end.





New initiatives burden decreases compared to the other proposed solutions, and vulnerability index is decreasing at a much higher rate from month 32.

The equation in “Adequacy of mature knowledge”= (Fraction of mature new knowledge + 1e-011) / (Fraction of mature work processes+1e-011). The fraction of mature knowledge should always be kept higher than the fraction of mature WP. A decrease in the value of “Adequacy of mature knowledge” will increase vulnerability index.

6 Additional findings.

One qualitative system archetype will be presented here to show one lesson learned from my experience in the telecom industry.

Underachievement Archetype: Change resistance.

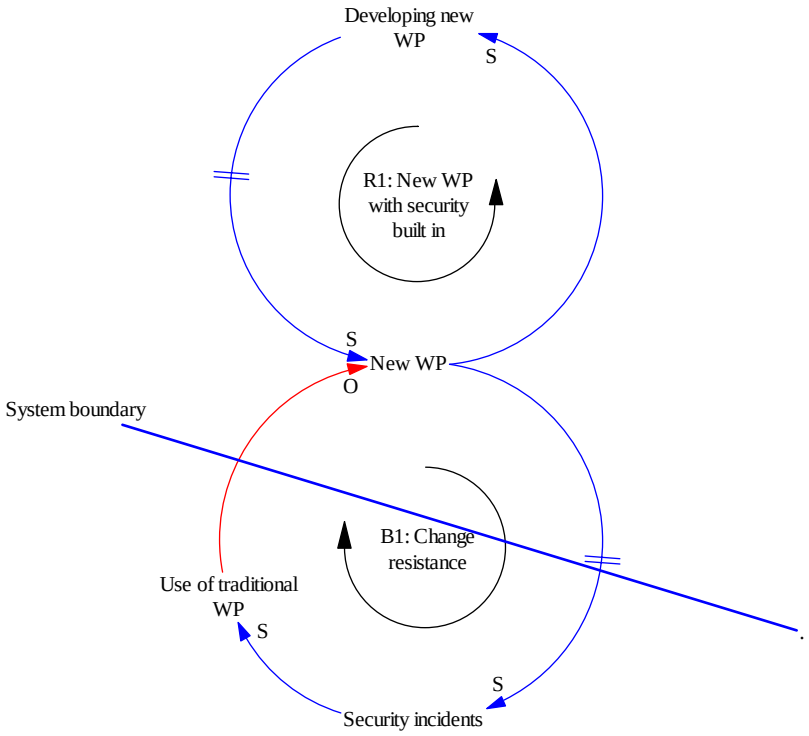


Figure 30 Change resistance

New Work Processes are wanted and the development of new WP is initiated. After a delay new WP are implemented and as a result new ones are being developed, R1: New WP with security built in.

Due to the new WPs that are not yet mature, security incidents may occur and the employees fall back to the use of traditional WP where they feel no problems occurred.

This again put a brake on the implementations of new WP.

If management loose focus on security issues and processes this may very well happen.

The employees should always be kept in the loop regarding the importance of using the policy defined processes.

Proposed solution

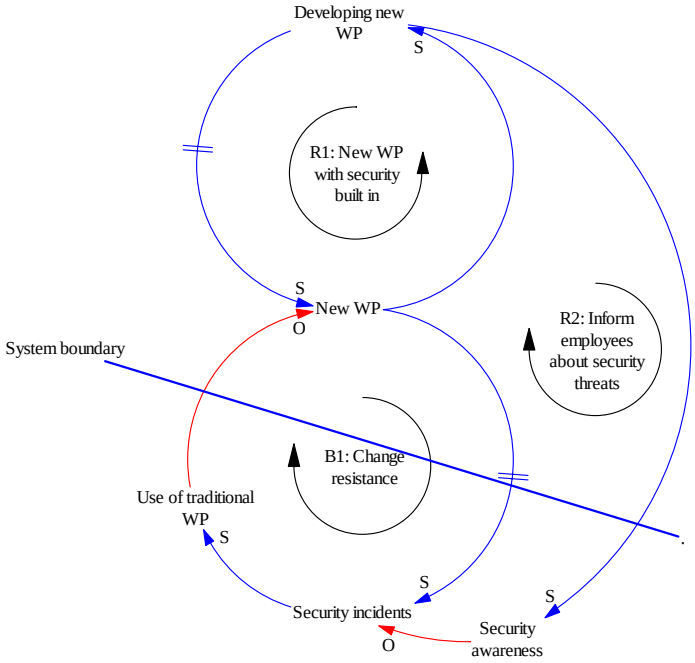


Figure 31 Information of employees

7 Conclusions and discussion on results.

To summarize the results I'll look on the research questions asked in the start of this thesis.

Research questions

-Which System Archetypes does the model contain?

I've identified four different System Archetypes with multiple solutions.

- Underachievement System Archetype (R and B)
  - Developing new Work processes
    - Solutions: Resources on maturing new work processes.
    - Solutions: Resources on maturing new Knowledge

- Developing new Knowledge
  - Solutions: Resources on maturing new work processes.
  - Solutions: Resources on maturing new Knowledge
- Developing new Technology Know-how
  - Solutions: Security training to increase the time to forget technology know-how.

- Relative Control System Archetype (B and B)
  - Vulnerability increases resulting in increased knowledge of incidents and again decreases Vulnerability index. The downside is that this triggers a fallback to pathological security culture from a low vulnerability index. Which in the end increases the vulnerability index again.
    - Possible solution To set an absolute target for allowed frequency of incidents, and adjust according to it.
  -

-Which impact on the systems output have these System Archetypes?

They slow down the wanted outcome, and in some cases counteract the intended outcome.

-Which scenarios will give the System Archetypes a dominant role in the model?

If resources are used on development alone the new initiatives burden will increase and act as a brake on the development.

-What is needed to minimize, or neutralize the unwanted effect of the System Archetypes?

The solution archetypes suggests the use of resources on maturing work processes, technology and knowledge and keep resources on knowledge higher than on work process maturation.

-Which policies will give the IO project the highest probability to make the transition with the lowest information security risks?

When combining extra resources on maturing new WP, Knowledge and technology, with more resources on maturing knowledge than work processes and technology.

8 References

1. Fischer, Diana M. 2005. Modeling Dynamic Systems: Lessons for a first course

2. Spaeth, Merrie. 2000. just what is “good” communication? :6.

3. Sterman, J.D. 2000. Business Dynamics, Systems Thinking and Modeling for a Complex World: Boston, Irwin McGraw-Hill.

4. Stig Ole Johnsen, Ivonne A. Herrera, Erik Jersin, Dr.Ragnar Rosness, Dr.Jørn Vatn, Mads Veiseth, Malene Tungland, Camilla Elén B. Bergersen. 2004. The Track to Safety Culture (SafeCulture).
A Toolkit for operability analysis of cross border rail traffic, focusing on safety culture: SINTEF Industrial Management.

5. Wolstenholme, Eric F. 2002. Towards the definition and use of a core set of archetypal structures in system dynamics. System Dynamics Review:pages 7 – 26.

6. work-group-Integrated-Operations. 2005. Integrated Work Processes
Future work processes on the Norwegian Continental Shelf.