# How a System Backfires: From a Redundancy Solution to Redundancy Problems in Security

Navid Ghaffarzadegan
navidg@gmail.com
Rockefeller College, the State University of New York at Albany, USA

**Abstract**
Increasing attention is being paid to reliability, safety, and security issues in social systems. Scott Sagan (2004) examined why more security forces (a redundancy solution) may produce less security (redundancy problems). In that paper, he discussed how the system could cause backfire in three major ways (i.e. "common mode error", "social shirking", and "overcompensation"). Using Sagan's hypotheses, I simulate and analyze a simplified and generic security system as more guards are added. Simulation results support two of the hypotheses, showing "common mode error" makes the system backfire, and "social shirking" creates inefficiency in the system as well as exacerbating the common mode error's effect. Simulation results show "overcompensation" has no effect on backfiring, but leads the system to a critical situation, in which it could easily be affected by "common mode error." The structure of the model and simulation results give some insights into developing appropriate security policies.

**Keyword**
Redundancy Solution, Redundancy Problem, Security, System Dynamics

## 1. Introduction

Increasing attention is being paid to reliability, safety, and security issues in social systems. Emergence of societal and global risk issues, public attention about these issues, and the importance of implementing appropriate policies in order to increase safety are some of the key sources of increased attention. An important point is the existence of an inter-related chain among risky situations, risk perception, and policies, in which, we expect to implement appropriate policies after we perceive risks in order to improve the situation. In fact, in the real world, this is not so easy or straightforward.

Social risk perception could have serious impacts on global security as well as organizational safety. High impacts of a realistic public risk perception in the United States on decreasing risks of global warming is discussed by Leiserowitz (2005); however, his reasons could be applied to most global risk issues as well. Kivimaki and Kalimo (1993) do a survey in an organizational environment and show that those workers who estimated the likelihood of an accident higher were less committed to the organization.

Relation between productivity and risk is also discussed in literature. In these works, more focus is on a common sense causal effect that more pressure on productivity and production could decrease our attention from risks and increase system failure. Cooke (2003) discusses the

main reasons of the 1992 Westraymine disaster in Nova Scotia using a system dynamics approach, showing how more concentration on production could increase the rate of incidents. In another work, Cooke and Rohleder (2006) show that disaster can result from productivity pressures and that disaster can be averted by learning from the precursor incidents.

Importance of risk perception has led a wide range of research on explaining how people perceive risks. There are various researches showing the importance of cultural factors (Bontempo et. al., 1997; Viklund, 2003; Kivimaki and Kalimo, 1993; Leiserowitz, 2005) on risk perception. Slimak and Dietz (2005) discuss that, also, risk type is an important factor in shaping risk perception, and discuss that public is more concerned about low probability but high consequence risks. Sjöberg and Drottz-Sjöberg (1991) do an empirical reach on risk perception between employees of a nuclear plant and conclude that those who knew less experienced larger risks. In most of these works, authors agree the intuitive idea that it takes time for people to perceive a risk (for example see Lima et. al, 2005).

As risk perception increases, the social pressure on executives to solve the problem also increases. Weaver and Richardson (2006) discuss effects of competing pressures on security decision makers in a simple signal detection system, and explain why there is a cyclic behavior in setting critical threshold in the system, causing system to oscillate.

The other point is that complexity of situations and lack of time may lead executives to implement inappropriate policies. Some of these problems should be globally concerned (Bunn and Bunn; 2002) and some needs time consuming policies to be fixed. Todinov (2006) argues that increasing reliability of a system does not necessarily decreases the probability of having huge failures. As public is more concerned about low probability but high consequence risks (Slimak and Dietz; 2005), a weak response to those situations even may exacerbate them to high probability and high consequence ones. Wrong responses could also decrease public trust on administrators (Viklund, 2003) leading the system to more forces and more arguments. All of these show the importance of making precise and smart policies in risky conditions.

There is also a wide range of discussions on the human resource mistakes, which makes system fail. Exploring the Chernobyl accident in 1990, Salge and Milling (2006) argue that the accident was caused by the combination of human failures in two stages: the design of the reactor and on-line operations. According to this article people could be blamed as designers of risk generating structures and as who react to failures in ways, which exacerbate the problem. Comparing with Cooke and Rohleder (2006), the important point in Slage and Milling's paper is that people are aware of risky situation and want to decrease it, but behave in a way that would worsen the situation.

These various and complicated causal relations of risk, perception of risk and policy appear in most of social systems. One of the most over-emphasized problems in this area is security issues in risky facilities, which is widely studied by researchers in a variety of fields. In general, those problems are concerned with the question: how can we improve security in systems which potentially could be a target for terrorists (for example see Sagan 2000, Thomas 2000, Rosand 2003, Charney 2001, Davis and Silver 2004.)

Expanding the number of guard personnel is an easy solution for administrators, and is a common and tempting policy (Sagan, 2004). In short, for each previously known as one task, we will have more guards, and this solution is expected to improve the situation. In contrast with public administrators and politicians who try, as an intuitive solution, to increase their ministries' and departments' budgets and to deploy more and more security forces, a system thinker may doubt that such a straightforward solution solves the whole problem in long term.

Deploying more security forces, in some ways, is similar to a solution in reliability problems, called redundancy. The redundancy solution is usually employed and widely discussed in engineering systems (for example see Pate-Cornell et. al.; 2004, Pate-Cornell; 1993, Sklaroff; 1976, Kapur and Lamberson; 1977). Redundancy is the duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe. Using more parallel components in critical areas is expected to increase the whole reliability to some degree. There are some advantages and disadvantages of redundancy in engineering systems. A safer approach to design, an increase in reliability and the simplification of maintenance as the system will still work with one component removed, are some of the primary advantages. However, the cost of parallel components and difficulty of detecting a problem in a parallel component as the whole system works are some of the disadvantages.

In social and political problems, redundancy could be used as a solution (for example see, Ting; 2003). The problem of security in risky facilities is one of them. As noted previously, deploying more security forces to improve the security level, a redundancy solution, is a very common idea.

Scott Sagan (2004) developed an impressive article on the redundancy problem to answer the question: why more security forces (a redundancy solution) may produce less security. In his article, he analyzed how one should think about security and warned about the most tempting solution: to add more security forces to protect risky facilities. However, Sagan's discussion on security could be considered as a general discussion on reliability and team performance in social systems (Apostolakis; 2004). Actually, Sagan's article represented the dark side of redundancy by focusing on how efforts to improve security can backfire and increase the risks they are designed to reduce. Bunn (2004) added some other effects of deploying more guards and discussed positive and negative aspects of this policy. He focused more on per-unit guard effectiveness and discussed the factors which could increase or decrease this variable when increasing the number of guards. Although Sagan accept that the redundancy solution could increase the security and he discussed the possible events in which the system *may* backfire, but Yellman (2006) believes that he has overemphasized the pitfalls of incorporating redundancy into designs. Apostolakis (2004) doubt if we can consider adding more guards to a system as a redundancy solution as each guard can not perform necessarily the required function. But it is obvious that, considering all situations constant, with no insider threat and assuming complete effectiveness for each guard, one can find an acceptable number of guards for each risky facility. Carroll (2004) argues that the most important effect of redundancy is that it makes us feel safe, and suggests considering design logic and operating logic in order to make real safety. Considering these different ideas, an examination of Sagan's hypotheses could be useful. As doing the empirical research and using the actual data in the security related issues is difficult, building the virtual model of the system and simulating it could help us to test it. Also a white box model could help us to have a shared understanding of different aspects of Sagan's ideas.

In this article, a simplified and generic model of security will be developed and tested based mostly on Sagan's hypotheses. System Dynamics, as a way of analyzing complexity and non-linearity, especially in complex social systems, could shed some lights on this problem to show why and how the employed policy may or may not backfire and what the potential results of such a policy are.

Simulation methods and specially System Dynamics is previously used to analyze reliability and security in different systems (for example see Cooke; 2003, Ahmad and Billmak; 2005, Kaminskiy and Ayyub; 2006, Weaver and Richardson; 2006, Cooke and Rohleder; 2006.) Lack

of empirical data on security issues and complexity of such systems give simulation methods the benefit of being on of the only ways to test high risk policies. In this paper, I simulate and analyze a simplified and generic security system as more guards are added mostly based on Sagan's hypotheses.

In each step and for each hypothesis, the model will be simulated, and finally the whole model will be tested. Additionally, this model could be used to test other possible policies.

## 2. Dynamic Hypothesis

As we discussed, a redundancy solution for the security problem could be "to deploy more security guards". It means that in the war between guards and terrorists, we try to increase guards' power in order to increase the level of security.

The important point here is the difference between two concepts: "guard force size" and "guard force power". The variable, which makes these two concepts different, is "guard's per unit effectiveness". It simply means that it is the "guard force size" and "guard's per unit effectiveness" that, together, produce "guard force power". Mathematically, it means that:

$$p(t) = g(t) \times e(t) \qquad \text{(Equation I)}$$

in which *p(t)* is guard force power, *g(t)* is guard force size and *e(t)* is guard's per unit effectiveness.

Differentiating these two concepts helps us to know that there is also a difference between "guard force power adequacy" and "guard size adequacy". There could be an adequate number of guards, but because of their effectiveness, we still lack the power adequacy. In fact, according to the goal of security systems which is to increase the level of security, the "guard force power adequacy" is the important factor for administrators, rather than "guard size adequacy". So when in the redundancy solution, we perceive that the "guard force power" is not adequate, although we may have enough guard force members, we try to increase "guard force size" to get the adequacy in "guard force power". Even our perception about "guard size adequacy" comes form its effect on security.

### 2-1- the base model for redundancy solution

Using these ideas, we can go on building a causal diagram of redundancy solution. In the redundancy solution, when people perceive a gap between the desired level of security and the current level, they go on hiring and deploying more guards and this leads the guard force power to increase. By increasing the guard force power, without considering any other effects, security rises and adjusts itself to the desired level. In a dynamic explanation of the solution, we can say that we continue to deploy guards until we feel that security is in its desired level. Fig. 1 shows an aggregate model of this solution as a balancing loop.

As the model shows, security guard size is a stock variable which is changed to fill security gap. In the model, security gap is considered as percentage of gap between perception of security and desired level, and assumed that security guard size is desired to be increased by this percentage. In a simple word, for example, in a 10 percent fall in security, we want to increase our guard force by 10 percent in an acceptable time period.

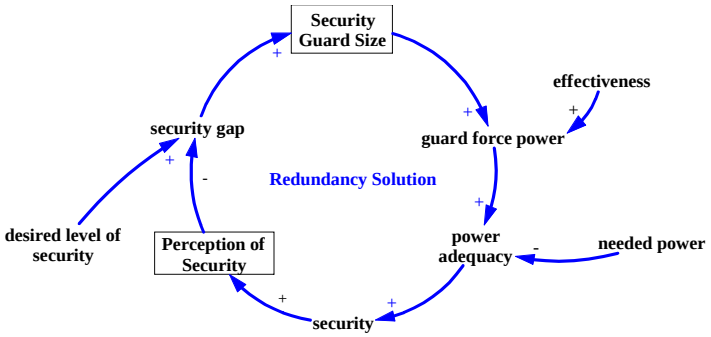


**Fig. 1. redundancy solution as a simple balancing loop increases the "guard force size" in order to fill the "security gap"**

Formulating security perception could be a challenging part in the model, as it is very difficult to be modeled accurately. Perceiving risk, as discussed before, differs across different cultures, is depended on risk type, and takes time for people to perceive a risk. Considering a national bounded high risk problem, we model security perception as a lagged variable of security, and consider security as a reliability factor which is exactly equal to guard force adequacy, meaning that the reliability falls as we lack force adequacy.

Another point that we should consider in our base model is the effect of financial resources (budget) on hiring and deploying security guards. It comes from the idea that there should be a limitation for a country to spend the resources. It doesn't mean that we could not allocate more resources for security, but means that there is a limitation for a country at the macro level. This limit, although may seem very conservative, but helps the SD model to work in its extreme conditions. So, we add a balancing loop that explains we could hire up to the level that the country's financial budget allows us. This model is shown in Fig. 2.

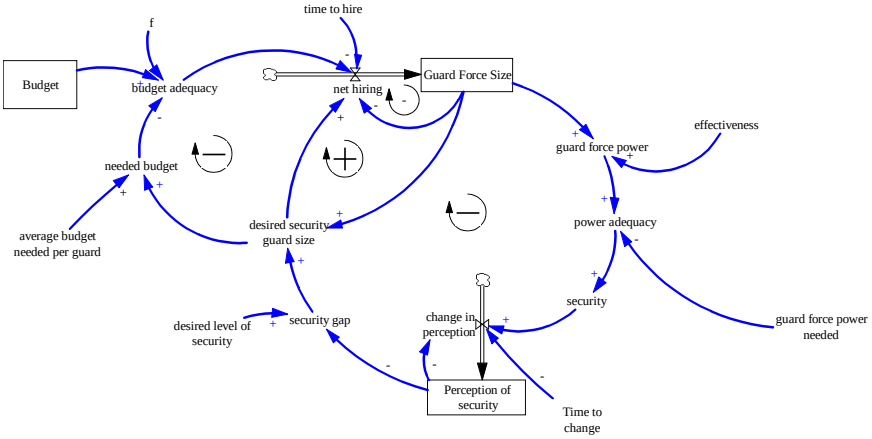


**Fig. 2. Base model**

This model is mathematically formulated, and all equations are illustrated in Technical Appendix 1. The outcome of this model is predictable. Let's suppose that there is a gap between perception of security and the desired security level. This condition could be caused as a result of a change in terrorists' power and so in security. The effect of this change could be perceived and then controlled by increasing the guard forces. Let's suppose that administrators start the redundancy solution in t=0. Fig. 3 shows that with the assumption that there is no other effect on the system, this solution works as it could adjust security level to the desired level (=1).

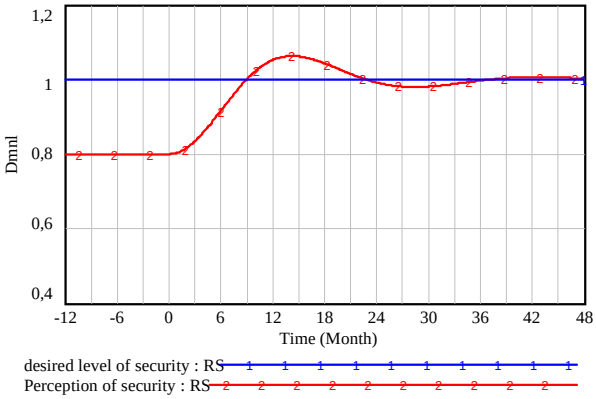


**Fig. 3. The effect of redundancy solution on security**

So in a first glance, it seems that the redundancy solution could be a logical strategy to increase reliability. Now, we go through the three main ways that Sagan introduced.

### 2-2- Common Mode errors

Sagan (2004, p. 937) says that the first problem of the redundancy solution relates to backfires through Common-Mode errors or what is usually called insider threat:

> "The first problem with redundancy is that adding extra components can inadvertently create a catastrophic common-mode error (a fault that causes all the components to fail)."

His example of reliability in aircraft clarifies this error completely. Think about using two engines in an aircraft, so if one has any problem the other could work. But, why don't we use four engines to increase the total reliability? Beside the problem of aircraft weight, we could face some catastrophic errors and that could cause serious problems for the reliability of the whole system. In this example, catastrophic errors are ones which are enough to crash the whole system down, like a fire in one engine, no matter the others work or not, makes the whole system collapsed! In spite of having redundant components, these errors can stop the whole system. So, when you are increasing the number of engines, you are decreasing the chance of having no working engine, and in the same time, you are increasing the chance of having fire in at least one engine. That's a time to think about the trade off.

In our problem, this backfire is the insider threat which could be caused by the guards! It simply means that when we increase the guard forces, the probability of terrorists' infiltration rises. The redundancy solution even makes the situation worse when it recommends recruiting more guards!

But the problem emerges much more when we accept that more security guards need more controlling capabilities and the lack of controlling capabilities affects infiltration possibilities. It simply means that we could not control the newly raised force as we did before. Our controlling capacity was for a lower number of guards.

Mathematically, we formulate infiltrators as the product of "Guard Force Size" and "the possibility of infiltration":

$$i(t) = s(t) \times p(t) \qquad \text{(Eq. 2)}$$

in which *i* is the number of infiltrators, and *p* is a normal distribution function of "possibility of infiltration". So, when we increase the guards not only we increase the number of infiltrators, but also the possibility of infiltration which accelerates infiltration.[1]

Fig. 4 shows how the system reacts to increasing security guards through insider threat. As the number of infiltrators raise, system faces lack of power adequacy and a fall in security. People perceive the fall and administrators' resistance on redundancy solution make it, even, worse by recruiting more guards and increasing the possibility of infiltration.

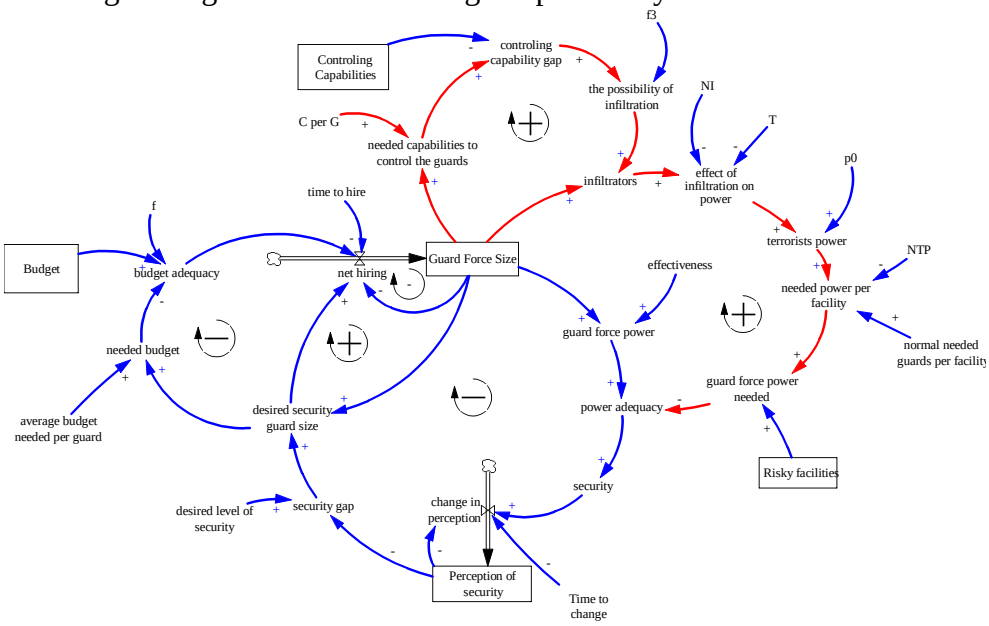


**Fig. 4. Insider threat: Security backfires as the terrorists find more possibility infiltration.**

This model is carefully formulated (see Technical Appendix 2) and result of simulation is illustrated in Fig. 5. This figure shows that first security increases, but before reaching to desired level, it backfires. The model says that the redundancy solution only will increase the guards however an increase in controlling capabilities is needed too. Implicitly, it shows that why an administrator who talks about deploying more and more forces could be in the wrong side and the hiring could not fill the gap.

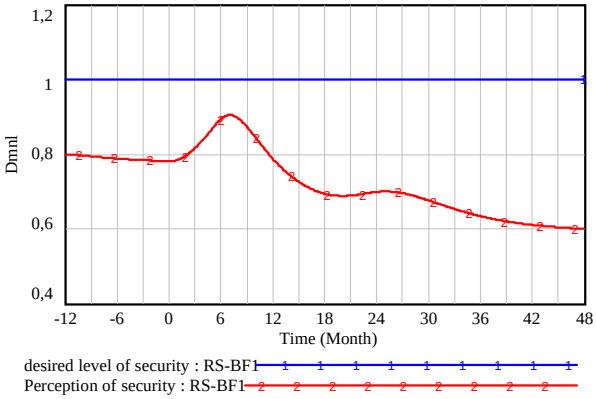


**Fig. 5. redundancy solution could not return security to the desired level.**

[1] It is assumed that it is possible to infiltrate through old guard members as well as new ones.

This simulation shows that, no matter how much you hired, you will need more power; hiring will increase your need to hire, as security declines! In the model “controlling capabilities” is considered as a constant, and it is the budget limit that stops redundancy solution.

### 2-3- Social Shirking

The second way of backfiring, social shirking, is about diffusion of responsibility, and relates to the human systems. Social Shirking is the fact that individuals or groups reduce their reliability in the belief that others will take up the job. This phenomenon is mostly called “Bystander effect” in social psychology literature and the existence of this theory is well documented and tested (for example see Darely and Latan; 1968, Latan and Darely; 1970, Tice and Baumeister; 1985, Levine; 1999). So, in systems which are working with humans, if their components become aware of redundant members, such awareness clearly can influence each unit’s reliability. Another effect that exacerbates bystander effect is “pluralistic ignorance”. Pluralistic ignorance is when bystanders assume nothing is wrong because nobody else looks concerned. Generally, when a person experiences an ambiguous situation, he may look at others’ behaviors before doing any reaction. And if every one behaves this way, pluralistic ignorance happens (Latan and Darely; 1969 and 1970.)

In our problem, this social shirking phenomenon clearly could occur, even in elite military units. Sagan gives two examples of this phenomenon in social systems and concludes that it could be a strong backfire on our redundancy solution in security problem. So, we could expect that in redundancy solution, when guard number rises, social shirking happens. Then the effectiveness of each person decreases. It leads the whole power not to raise that much or even to drop. Fig. 6 shows how this feedback affects the redundancy solution.

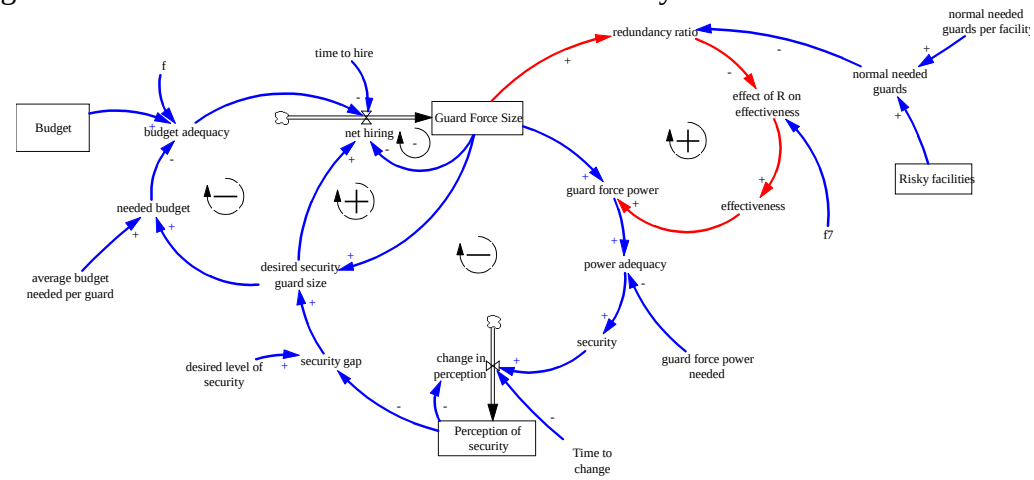


**Fig. 6. Social Shirking:**
**Security backfires as people become aware of redundant members**

So for who is not aware of this social shirking, it could be baffling why increasing the guard members did not raise the security in long term and he may conclude that terrorists have become more strong and he needs to go on recruiting more! In fact, our consistency on recruiting more guards leads us to an overestimating level of guards and maybe overestimating power of terrorists! In comparison with the last phenomenon, in this feedback we have much more guards

than what we really need, but the point is that we loose the effectiveness (reliability) of each member as the result of social shirking.

Formulating the model, it is a challenging question how much social shirking affects effectiveness of each person. Do two persons have less power than one, or just not twice as much as one person? What will happen in extreme, when we have a large ratio of redundancy? In our model we assumed a limit to the effect of social shirking in its extreme condition. It means that as redundancy ratio (*RR*) increases effectiveness of each person (*e*) decreases and in large ratios of redundancy, effectiveness approaches to a small number. In our model it is assumed that *e* is equal to 0.7 for *RR*= 1.2, 0.6 for *RR*=1.5, and 0.55 for any amount of *RR* more than 2. Other formulations for this function do not change the overall behavior of security, i.e. goal seeking pattern, as long as RR tangents to a number other than zero in its extreme. All equations of this model are illustrated in Technical Appendix 3.

I have simulated effects of social shirking, once, with controlling for any other effect (Fig. 7, graph 3), and once with including common mode error effect (Fig. 7, graph 4.) Like the previous runs, the redundancy solution starts from t=0. Simulation results show an interesting result. As graph 3 shows, social shirking could not by itself make the system backfire; however, it exacerbates the effect of common mode error, changing the behavior from graph 2 to graph 4 in Fig. 7.

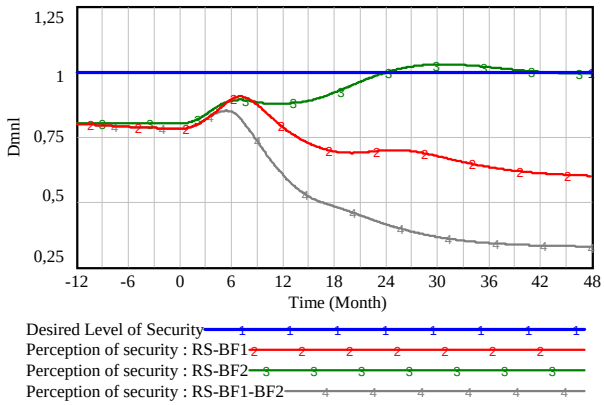


**Fig. 7. The simulation result for social shirking backfire**

Therefore, although simulation results show that social shirking, by itself, makes inefficiency rather than backfire, but combining this phenomenon with the first phenomenon (common mode errors), the problem of backfiring exacerbates. The point is that when we include common mode error to the system, social shirking makes situation worse by decreasing effectiveness of guard force. This makes more need to hire new guards, and, therefore, more possibility of infiltration.

### 2-4- Overcompensation

It is obvious that if we had no risky facilities, we wouldn't have security problems. Or in the other words, when we increase our risky works, we could face more problems of security.

One of the important factors that Sagan mentions in his article is that increasing the security encourages administrators to go more on risky projects. When we perceive an appropriate level of security, we increase our risky works which could be through increasing utilization of risky facilities or through increasing the number and size of risky facilities. Both will increase our

need to guard force and affect power adequacy. So, again, the security could fail, not because terrorists have become more powerful, but because we have increased the projects and need more guards to control them.

Fig. 8 shows these feedbacks. When perception of security increases, it influences starting new projects and increases risky facilities. To examine the effect precisely, we should accept that when we perceive the security gap, it is possible to decrease the utilization of facilities, as well. Related formulas are illustrated in Technical Appendix 4.

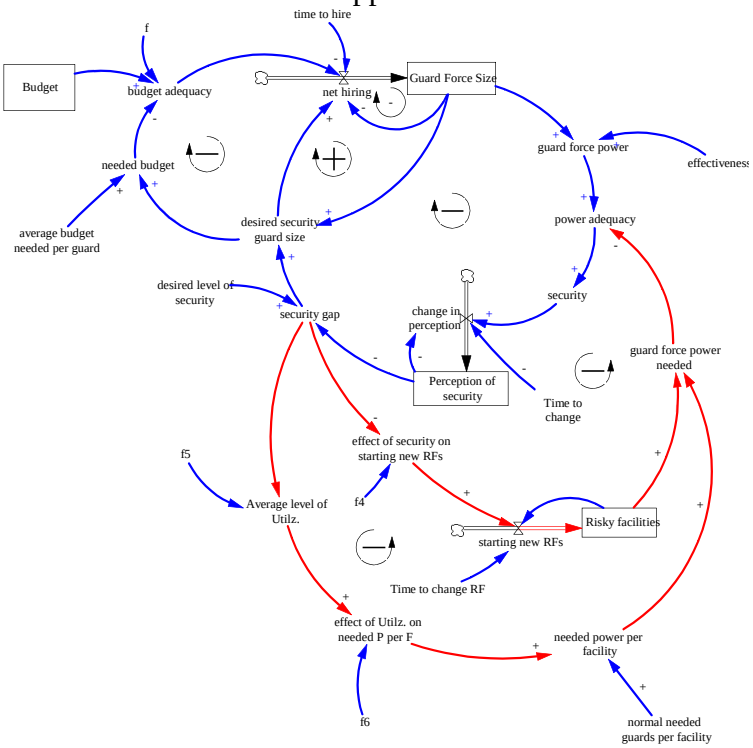


**Fig. 8. Overcompensation eight-shaped reinforcing loop**

In this figure, we can find two eight-shaped reinforcing loops, each one encompassing two balancing loops. This kind of structures could lead the system to increase guards and risky facilities simultaneously, while security gap is oscillating around an acceptable level.

Therefore, it is predictable that, controlling for other effects, this feedback, just, raises number of security guards as well as risky works. Fig. 9, graph 3 shows that overcompensation, as discussed here, did not make system backfire. Including common mode error effect to the system (graph 4 in Fig. 9) we see that it, even, lessens the effect of common mode error. This relates to a fall in capacity utilization after perceiving serious problems in security.

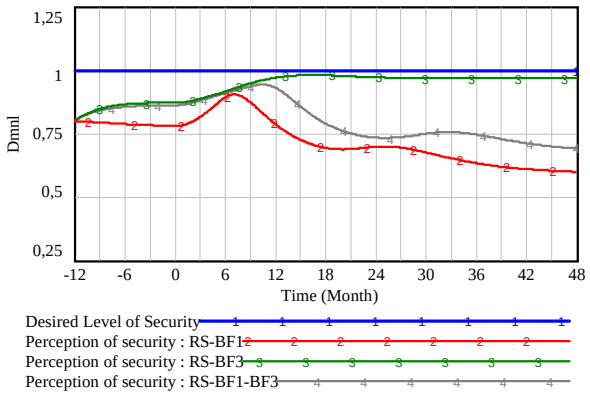


**Fig. 9. The simulation result for overcompensation backfire**

So, what does really overcompensation do? First idea is that security pitfalls are not just caused by guards, but also by other employees in the system. In an appropriate security level, as we increase risky facilities, we increase the number of scientists, engineers, and all other staffs, which is also another possible way for infiltrators. An increase in staffs, also, increases the possibility of information lost. Simulating these phenomena is out of boundary of this paper. There is another important and interesting effect that our model shed some lights on it, and I call it “Birth of Terrorists!” Fig. 10 uses a longer time period, and shows that whatever the terrorist’s power is (P0 is a constant factor representing terrorists’ power), our system will finally backfire, and this phenomenon is the important effect of overcompensation.

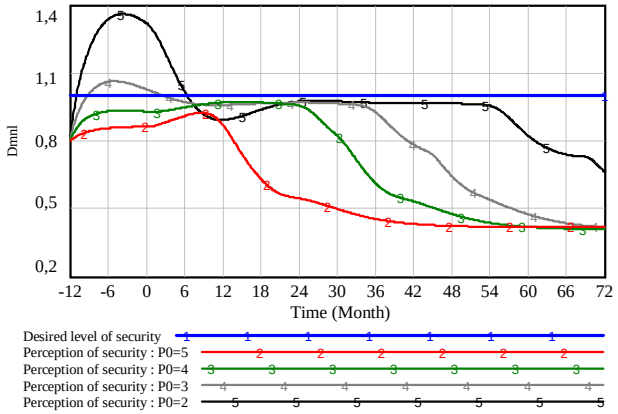


**Fig. 10. System behavior under different quantities for terrorists’ power**

This simulation simply says that overcompensation lead the system to the critical level to backfire. In other words, system always balances its risky facilities to the terrorists’ power. So, even if terrorists’ power was initially negligible, overcompensation gives them more opportunity of attack. Therefore, terrorists’ power just changes the time to backfire. This is also a support for predicted behavior and its independence form common mode error gain.

## 2-5- The whole model and policy insights

Adding the loops together could show how complicated the system is. The whole model is shown in Fig. 11. Redundancy solution, while increasing the guard size, increases security directly, and decreases it through three hypotheses indirectly.

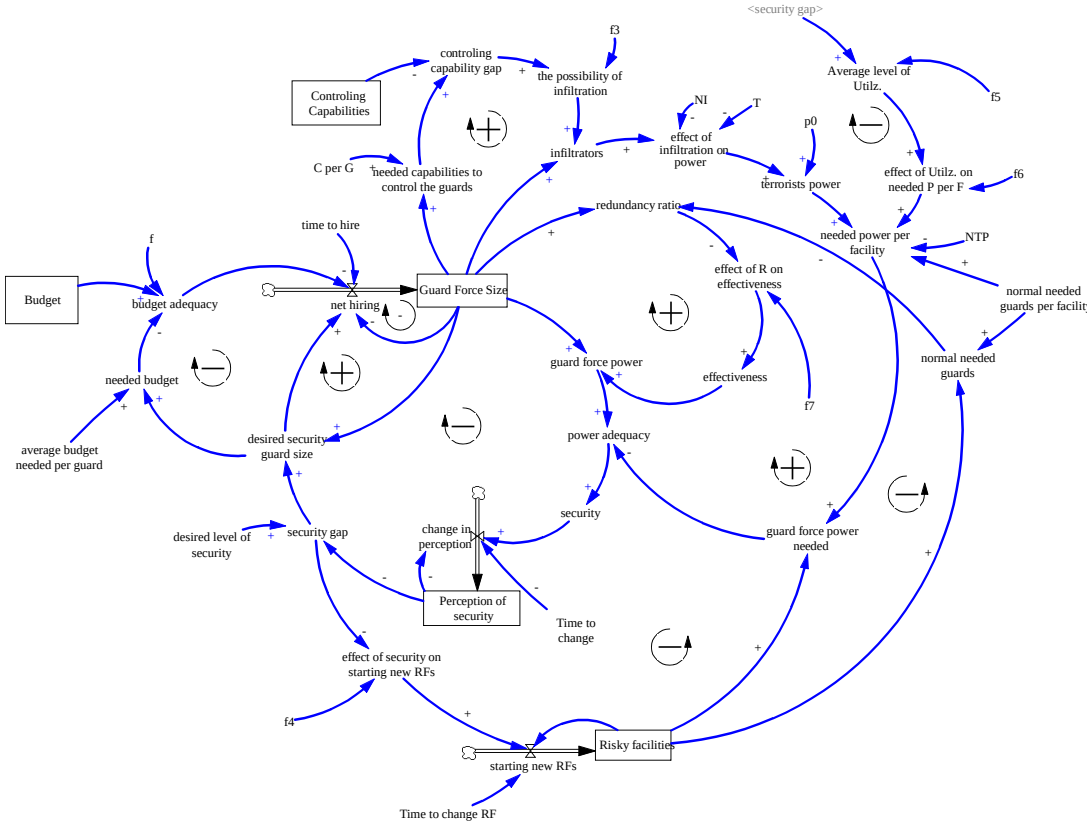


**Fig. 11. Whole model**

To find appropriate policies and develop action plans, we should find the dominant loop(s) which influences the system. Previous discussions show that while in insider threat condition, the system backfires, social shirking and overcompensation are de-emphasized by persisting on the redundancy solution. The main reason that the threat became activated was the limited capability of controlling.

Controlling capabilities are managerial abilities in controlling guards, and could be increased through learning and improving managerial knowledge and abilities. Controlling capabilities, also, could be increased by improving and updating the soft systems to be used in controlling guards. Adequacy of such abilities decreases the possibility of infiltration to guard force.

This insight suggests we look at the redundancy solution in a new way: Improving controlling capabilities as well as increasing guard force size to fill the security gap (Fig. 12) Fig. 13 shows the effect of implementing this policy and compares it with the whole model reaction to redundancy solution.

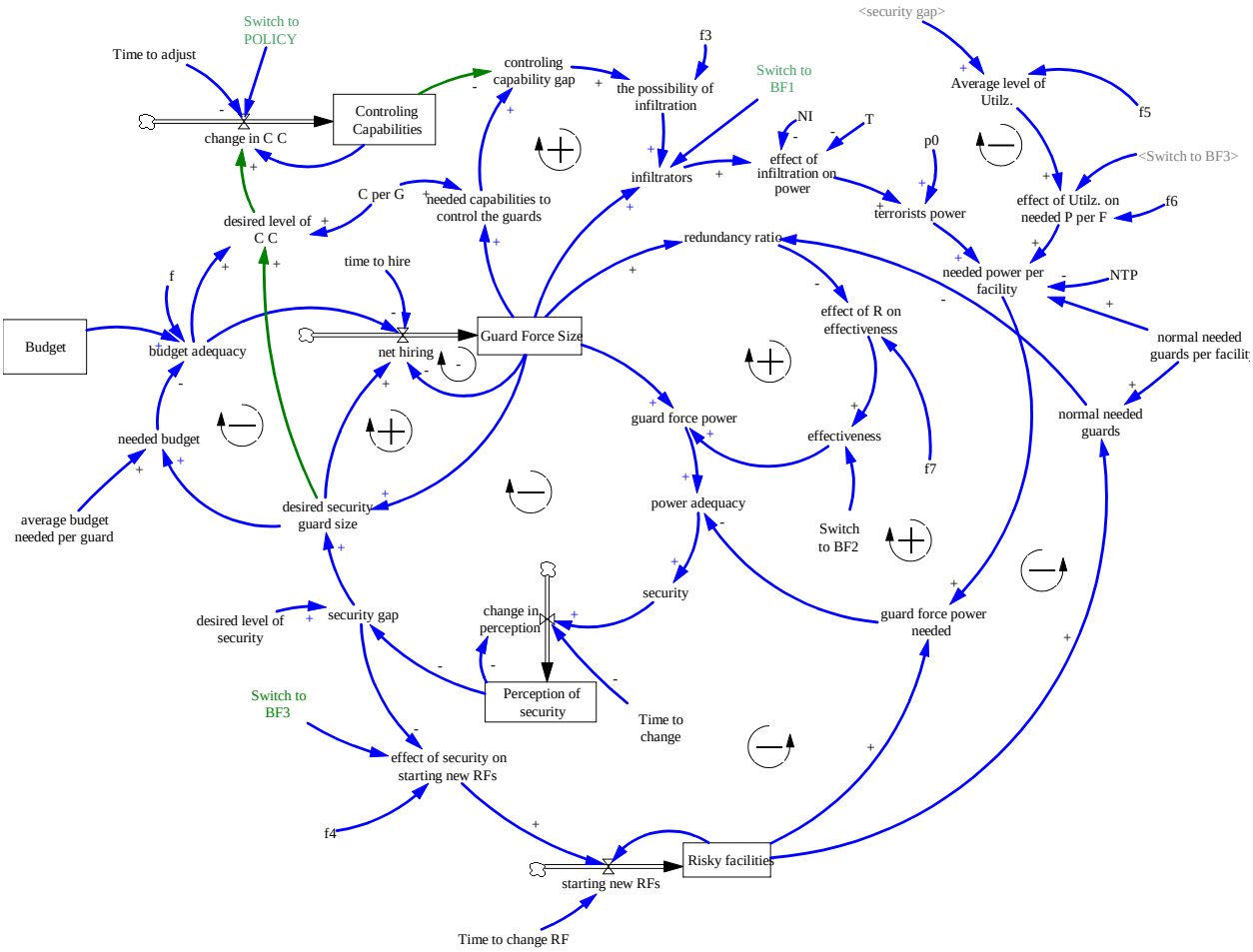


**Fig. 12. Whole model including policy**

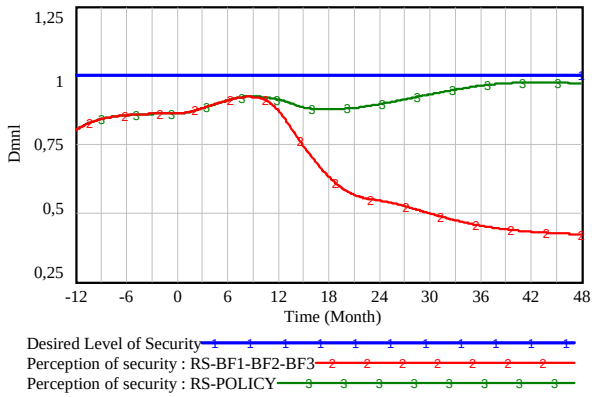


**Fig. 13. Comparison of the whole model result with and with out policy implementation**

## 3. Conclusion

As we saw, persistence in redundancy solution could fall down security in three ways. Increasing the number of guards, terrorists get more opportunity to infiltrate to the system and it

affects security. After a short time, we will get less security level. Social shirking makes a reinforcing loop in which an observer thinks that the number of guard force is not enough, however, the reliability of each guard has been decreased. Simulation results predict that this phenomenon exacerbates the common mode error possibility and decreases efficiency in the system. Overcompensation which is a reaction of the administrators to an appropriate level of security, by itself, does not make the system backfire, however the important effect is that it enters the system to the level that makes terrorist problem an important and critical issue.

This model suggests that “controlling capabilities” is a crucial point to implement an effective policy. Controlling capabilities include the managerial abilities necessary to control guards. Such capabilities could be increased through learning and improving managerial knowledge and abilities. Controlling capabilities could also be increased by improving and updating the soft systems to be used in controlling guards.

Although the model is aggregated, it provides insight into how a security system might receive different feedbacks from the redundancy solution. One could further improve the model by disaggregating social perception of security, adding guard training processes, other employees effect on security, and some other dynamic hypotheses.

## *Technical Appendix 1 – Base Model Equations*

average budget needed per guard= 1, Units: $/Man
Budget=60, Units: $
budget adequacy=f(Budget/needed budget), Units: Dmnl
change in perception=(security-Perception of security)/Time to change, Units: 1/Month
desired level of security=1, Units: Dmnl
desired security guard size=Guard Force Size + Guard Force Size*security gap, Units: Man
effectiveness=1, Units: Dmnl
f([(0,0)-(10,2)],(0,0),(1,0.9),(1.2,1),(10,1)), Units: Dmnl
guard force power=Guard Force Size*effectiveness, Units: Man
guard force power needed=10, Units: Man
Guard Force Size= INTEG (net hiring,8), Units: Man
needed budget=average budget needed per guard*desired security guard size, Units: $
net hiring=(desired security guard size*budget adequacy-Guard Force Size)/time to hire*step(1,0), Units: Man/Month
Perception of security= INTEG (change in perception,0.8), Units: Dmnl
power adequacy=guard force power/guard force power needed, Units: Dmnl
security=power adequacy, Units: Dmnl
security gap=(desired level of security-Perception of security)/desired level of security, Units: Dmnl
Time to change=6, Units: Month
time to hire=3, Units: Month

## *Technical Appendix 2 – Common Mode Error Equations*

average budget needed per guard=1, Units: $/Man
Budget=60, Units: $
budget adequacy=f(Budget/needed budget), Units: Dmnl
C per G=1, Units: capability/Man
change in perception=(security-Perception of security)/Time to change, Units: 1/Month
Controling Capabilities=10, Units: capability
controling capability gap=(needed capabilities to control the guards-Controling Capabilities)/Controling Capabilities, Units: Dmnl
desired level of security=1, Units: Dmnl
desired security guard size=Guard Force Size + Guard Force Size*security gap, Units: Man
effect of infiltration on power=delay1(infiltrators/NI,T)*10, Units: Dmnl
effectiveness=1, Units: Dmnl
f([(0,0)-(10,2)],(0,0),(1,0.9),(1.2,1),(10,1)), Units: Dmnl
f3([(-1,0)-(1,0.02)],(-1,0.0001),(-0.5,0.0002),(0,0.0005),(0.1,0.001),(0.2,0.01),(0.3,0.012),(1,0.015)), Units: Dmnl
guard force power=Guard Force Size*effectiveness, Units: Man
guard force power needed=(Risky facilities*needed power per facility), Units: Man
Guard Force Size= INTEG (net hiring,8), Units: Man
infiltrators=Guard Force Size*RANDOM NORMAL( 0 , 1 , the possibility of infiltration , 0.0001 , 1 ), Units: Man
needed budget=average budget needed per guard*desired security guard size, Units: $
needed capabilities to control the guards=C per G*Guard Force Size, Units: capability
needed power per facility=(terrorists power/NTP)*normal needed guards per facility, Units: Man/Facility
net hiring=(desired security guard size*budget adequacy-Guard Force Size)/time to hire*step(1,0), Units: Man/Month
NI=1, Units: Man
normal needed guards per facility=5, Units: Man/Facility
NTP=5, Units: Man
p0=5, Units: Man
Perception of security= INTEG (change in perception,0.8), Units: Dmnl
power adequacy=guard force power/guard force power needed, Units: Dmnl
Risky facilities=2, Units: Facility

security=power adequacy, Units: Dmnl
security gap=(desired level of security-Perception of security)/desired level of security, Units: Dmnl
T=3, Units: Month
terrorists power=p0*(1+effect of infiltration on power), Units: Man
the possibility of infiltration=f3(controling capability gap), Units: Dmnl
Time to change=6, Units: Month
time to hire=3, Units: Month

## *Technical Appendix 3 – Social Shirking Equations*

average budget needed per guard=1, Units: $/Man
Budget=60, Units: $
budget adequacy=f(Budget/needed budget), Units: Dmnl
change in perception=(security-Perception of security)/Time to change, Units: 1/Month
desired level of security=1, Units: Dmnl
desired security guard size=Guard Force Size + Guard Force Size*security gap, Units: Man
effect of R on effectiveness=f7(redundancy ratio), Units: Dmnl
effectiveness=effect of R on effectiveness Units: Dmnl
f([(0,0)-(10,2)],(0,0),(1,0.9),(1.2,1),(10,1)), Units: Dmnl
f7([(0,0)-(2,1.5)],(0,1),(1,1),(1.2,0.7),(1.5,0.6),(2,0.55)), Units: Dmnl
guard force power=Guard Force Size*effectiveness, Units: Man
guard force power needed=10, Units: Man
Guard Force Size= INTEG (net hiring,8), Units: Man
needed budget=average budget needed per guard*desired security guard size, Units: $
net hiring=(desired security guard size*budget adequacy-Guard Force Size)/time to hire*step(1,0), Units: Man/Month
normal needed guards=normal needed guards per facility*Risky facilities, Units: Man
normal needed guards per facility=5, Units: Man/Facility
Perception of security= INTEG (change in perception,0.8), Units: Dmnl
power adequacy=guard force power/guard force power needed, Units: Dmnl
redundancy ratio=Guard Force Size/normal needed guards, Units: Dmnl
Risky facilities=2, Units: Facility
security=power adequacy, Units: Dmnl
security gap=(desired level of security-Perception of security)/desired level of security, Units: Dmnl
Time to change=6, Units: Month
time to hire=3, Units: Month

## *Technical Appendix 4 – Overcompensation Equations*

average budget needed per guard=1, Units: $/Man
"Average level of Utilz."=f5(security gap), Units: Dmnl
Budget=60, Units: $
budget adequacy=f(Budget/needed budget), Units: Dmnl
change in perception=(security-Perception of security)/Time to change, Units: 1/Month
desired level of security=1, Units: Dmnl
desired security guard size=Guard Force Size + Guard Force Size*security gap, Units: Man
effect of security on starting new RFs=f4(security gap), Units: Dmnl
"effect of Utilz. on needed P per F"=f6("Average level of Utilz."), Units: Dmnl
effectiveness=1, Units: Dmnl
f([(0,0)-(10,2)],(0,0),(1,0.9),(1.2,1),(10,1)), Units: Dmnl
f4([(-0.2,0)-(1,0.4)],(-0.1,0.4),(0,0.15),(0.15,0)), Units: Dmnl
f5([(-0.1,0)-(1,1)],(-0.1,0.95),(0,0.9),(0.1,0.85),(0.2,0.7),(0.5,0.5),(1,0.4)), Units: Dmnl
f6([(0,0)-(1,2)],(0.4,0.7),(0.8,0.9),(1,1.2)), Units: Dmnl
guard force power=Guard Force Size*effectiveness, Units: Man
guard force power needed=(Risky facilities*needed power per facility), Units: Man
Guard Force Size= INTEG (net hiring,8), Units: Man
needed budget=average budget needed per guard*desired security guard size, Units: $

needed power per facility="effect of Utilz. on needed P per F"*normal needed guards per facility, Units: Man/Facility
net hiring=(desired security guard size*budget adequacy-Guard Force Size)/time to hire*step(1,0), Units: Man/Month
normal needed guards per facility=5, Units: Man/Facility
Perception of security= INTEG (change in perception,0.8), Units: Dmnl
power adequacy=guard force power/guard force power needed, Units: Dmnl
Risky facilities= INTEG (starting new RFs, 2), Units: Facility
security=power adequacy, Units: Dmnl
security gap=(desired level of security-Perception of security)/desired level of security, Units: Dmnl
starting new RFs=effect of security on starting new RFs*Risky facilities/Time to change RF, Units: Facility/Month
Time to change=6, Units: Month
Time to change RF=12, Units: Month
time to hire=3, Units: Month

## *Technical Appendix 5 – Whole model Including Policy Equations*

average budget needed per guard=1, Units: $/Man
"Average level of Utilz."=f5(security gap), Units: Dmnl
Budget=60, Units: $
budget adequacy=f(Budget/needed budget), Units: Dmnl
C per G=1, Units: capability/Man
change in C C=(desired level of C C-Controling Capabilities)/Time to adjust*Switch to POLICY, Units: capability/Month
change in perception=(security-Perception of security)/Time to change, Units: 1/Month
Controling Capabilities= INTEG (change in C C,10), Units: capability
controling capability gap=(needed capabilities to control the guards-Controling Capabilities)/Controling Capabilities, Units: Dmnl
desired level of C C= budget adequacy*C per G*desired security guard size, Units: capability
desired level of security=1, Units: Dmnl
desired security guard size=Guard Force Size + Guard Force Size*security gap, Units: Man
effect of infiltration on power= delay1(infiltrators/NI,T)*10, Units: Dmnl
effect of R on effectiveness=f7(redundancy ratio), Units: Dmnl
effect of security on starting new RFs=f4(security gap)*Switch to BF3, Units: Dmnl
"effect of Utilz. on needed P per F"=f6("Average level of Utilz.")*Switch to BF3+1-Switch to BF3, Units: Dmnl
effectiveness=effect of R on effectiveness*Switch to BF2+1-Switch to BF2, Units: Dmnl
f([(0,0)-(10,2)],(0,0),(1,0.9),(1.2,1),(10,1)), Units: Dmnl
f3([(-1,0)-(1,0.02)],(-1,0.0001),(-0.5,0.0002),(0,0.0005),(0.1,0.001),(0.2,0.01),(0.3,0.012),(1,0.015)), Units: Dmnl
f4([(-0.2,0)-(1,0.4)],(-0.1,0.4),(0,0.15),(0.15,0)), Units: Dmnl
f5([(-0.1,0)-(1,1)],(-0.1,0.95),(0,0.9),(0.1,0.85),(0.2,0.7),(0.5,0.5),(1,0.4)), Units: Dmnl
f6([(0,0)-(1,2)],(0.4,0.7),(0.8,0.9),(1,1.2)), Units: Dmnl
f7([(0,0)-(2,1.5)],(0,1),(1,1),(1.2,0.7),(1.5,0.6),(2,0.55)), Units: Dmnl
guard force power=Guard Force Size*effectiveness, Units: Man
guard force power needed=(Risky facilities*needed power per facility), Units: Man
Guard Force Size= INTEG (net hiring,8), Units: Man
infiltrators=Guard Force Size*RANDOM NORMAL( 0 , 1 , the possibility of infiltration ,0.0001 , 1 )*Switch to BF1, Units: Man
needed budget=average budget needed per guard*desired security guard size, Units: $
needed capabilities to control the guards=C per G*Guard Force Size, Units: capability
needed power per facility=((terrorists power/NTP)*"effect of Utilz. on needed P per F")*normal needed guards per facility, Units: Man/Facility
net hiring=(desired security guard size*budget adequacy-Guard Force Size)/time to hire*step(1,0), Units: Man/Month
NI=1, Units: Man

normal needed guards=normal needed guards per facility*Risky facilities, Units: Man
normal needed guards per facility=5, Units: Man/Facility
NTP=5, Units: Man
p0=5, Units: Man
Perception of security= INTEG (change in perception,0.8), Units: Dmnl
power adequacy=guard force power/guard force power needed, Units: Dmnl
redundancy ratio=Guard Force Size/normal needed guards, Units: Dmnl
Risky facilities= INTEG (starting new RFs, 2), Units: Facility
security= power adequacy, Units: Dmnl
security gap=(desired level of security-Perception of security)/desired level of security, Units: Dmnl
starting new RFs=effect of security on starting new RFs*Risky facilities/Time to change RF, Units: Facility/Month
Switch to BF1=1, Units: Dmnl
Switch to BF2=1, Units: Dmnl
Switch to BF3=1, Units: Dmnl
Switch to POLICY=0, Units: Dmnl
T=3, Units: Month
terrorists power=p0*(1+effect of infiltration on power), Units: Man
the possibility of infiltration=f3(controling capability gap), Units: Dmnl
Time to adjust=4, Units: Month
Time to change=6, Units: Month
Time to change RF=12, Units: Month
time to hire=3 Units: Month

**References**


Ahmad, S. & Billimek, J. (2005) Estimating the Health Impacts of Tobacco Harm Reduction Policies: A Simulation Modeling Approach. *Risk Analysis 25* (4), 801–812.

Apostolakis, G. E. (2004). Redundancy and Nuclear Security, *Risk Analysis 24* (4), 947–948.

Bontempo, R. N., Bottom, W. P. & Weber, E. U. (1997). Cross-Cultural Differences in Risk Perception: A Model-Based Approach. *Risk Analysis, 17* (4), 479-488.

Bunn, M. & Bunn, G. (2002). Strengthening Nuclear Security Against Post-September 11 Threats of Theft and Sabotage, *Journal of Nuclear Materials Management, 3*, 48-60.

Bunn M. (2004). Thinking about How Many Guards will do the Job, *Risk Analysis 24* (4), 949-954.

Carroll, J. S. (2004). Redundancy as a Design Principle and an Operating Principle. *Risk Analysis 24* (4), 955–957.

Charney, J. (2001). The Use of Force against Terrorism and International Law. *The American Journal of International Law 95* (4), 835-839.

Cooke, D. L. (2003). A system dynamics analysis of the Westray mine disaster. *System Dynamics Review 19* (2), 139-166.

Cooke, D. L. & Rohleder ,T. R. (2006). Learning from incidents: from normal accidents to high reliability. *System Dynamics Review 22* (3), 213-239.

Darley, J. & Latane, B. (1968). Bystander intervention in emergencies: Diffusion of responsibility. *Journal of Personality and Social Psychology 8*, 377-383.

Davis, D. W. & Silver, B. D. (2004), Civil Liberties vs. Security in the Context of the Terrorist Attacks on America. *American Journal of Political Science 48*(1), 28–46.

Forrester, J. (1961). Industrial Dynamics, New York: Productivity Press.

Kaminskiy, M. P. & Ayyub, B. M. (2006) Terrorist Population Dynamics Model. *Risk Analysis 26* (3), 747–752.

Kapur, K.C. & Lamberson, L.R. (1977). Reliability in Engineering Design. John Wiley & Sons, New York.

Kivimaki, M. & Kalimo, R. (1993). Risk Perception among Nuclear Power Plant Personnel: A Survey. *Risk Analysis 13* (4), 421-424.

Leiserowitz, A. A. (2005). American Risk Perceptions: Is Climate Change Dangerous? *Risk Analysis 25* (6), 1433–1442.

Latané, B. & Darley, J. M. (1969). Bystander "Apathy". *American Scientist 57,* 244-268.

Latané, B. & Darley, J. M. (1970) The unresponsive bystander: Why doesn't he help? Englewood Cliffs, NJ: Prentice Hall.

Levine, M. (1999). Rethinking bystander nonintervention: Social categorization and the evidence of witnesses at the James Bulger murder trial. *Human Relations. 52(9),* 1133-1155.

Lima, M. L., Barnett, J. & Vala, J.(2005) Risk Perception and Technological Development at a Societal Level. *Risk Analysis 25* (5), 1229–1239.

Paté-Cornell, M. E., Dillon, R. L. & Guikema, S. D. (2004). On the Limitations of Redundancies in the Improvement of System Reliability, *Risk Analysis 24* (6), 1423–1436.

Paté-Cornell, E. (1993). Learning from the Piper Alpha Accident: A Postmortem Analysis of Technical and Organizational Factors. *Risk Analysis 13* (2), 215–232.

Richardson G. P. (1996). *System Dynamics.* In S. I. Gass and C. M. Harris (eds.), Encyclopedia of Operation Research and Management Science. Norwell, Mass.: Kluwer

Rosand E. (2003). Security Council Resolution 1373, the Counter-Terrorism Committee, and the Fight against Terrorism. *The American Journal of International Law 97* (2), 333-341.

Sagan, S. D. (2000). The commitment trap: why the United States should not use nuclear threats to deter biological and chemical weapons attacks. *International Security 24*(4), 85-115.

Sagan, S. D. (2004). The problem of redundancy problem, Why More Nuclear Security Forces May Produce Less Nuclear Security. *Risk Analysis 24* (4), 935-946.

Salge, M. & Milling, P. M. (2006). Who is to blame, the operator or the designer? Two stages of human failure in the Chernobyl accident. *System Dynamics Review 22* (2), 89-112

Senge, P., Kleiner, A., Roberts, C., Ross, R. & Smith, B. (1994). The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organization, Doubleday, New York

Sjöberg, L. & Drottz-Sjöberg, B. (1991). Knowledge and Risk Perception Among Nuclear Power Plant Employees. *Risk Analysis 11* (4), 607-618

Sklaroff, J. R. (1976). Redundancy Management Technique for Space Shuttle Computers. *IBM Journal on Research and Development 20* (1), 20-28

Slimak, M. W. & Dietz, T. (2006) Personal Values, Beliefs, and Ecological Risk Perception. *Risk Analysis 26* (6), 1689–1705.

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

Thomas, W. (2000). Norms and Security: The Case of International Assassination. *International Security 25* (1), 105-133

Tice, D., & Baumeister, R. (1985). Masculinity inhibits helping in emergencies: Personality does predict the bystander effect. *Journal of Personality & Social Psychology. 49* (2), 420-428.

Ting, M. M. (2003). A strategic Theory of Bureaucratic Redundancy. *American Journal of Political Science 47* (2), 274-292.

Todinov, M. T. (2006). Reliability Analysis Based on the Losses from Failures. *Risk Analysis 26* (2), 311–335.

Viklund, M. J. (2003). Trust and Risk Perception in Western Europe: A Cross-National Study. *Risk Analysis 23* (4), 727–738.

Weaver, E. A. & Richardson, G. P. (2006) Threshold setting and the cycling of a decision threshold. *System Dynamics Review 22* (1), 1-26

Yellamn, T. (2006). Redundancy in Designs. *Risk Analysis 26* (1), 277-286