A Framework for Human Factors in Information Security

JOSE J GONZALEZ, AGATA SAWICKA
Dept. of Information and Communication Technology
Agder University College
N-4876 Grimstad
NORWAY
Email: Jose.J.Gonzalez@hia.no URL: http://ikt.hia.no/josejg/

Abstract: – Any security system, no matter how well designed and implemented, will have to rely on people. The fact that human factors play a crucial part in the majority of accidents is a troubling feature of modern "security know-how": We can implement appropriate technical solutions, but we still fail to handle the human factor. Our research project aims at understanding better the role of human factors in information security systems. We develop a system dynamical simulation model to explore the complex security problem. We use a simple, fictitious case to illustrate how system dynamics may deliver insights into the "people security problem" and help in designing robust security policies. For further progress, collaboration with companies or organizations to the effect of collecting case studies is necessary.

Key-Words: – Security, instrumental conditioning, risk perception, system dynamics, policy design

1 Introduction

Information security involves both technology and people. Technological advances make the armory more and more impressive but it is becoming increasingly evident that the human factor is the Achilles heel of information security. In his 1994 book on applied cryptography [1], Schneier argued strongly that a high degree of security was in our hands. But only six years later, in his recent book on digital security in a networked world [2], Schneier revokes such claim: "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[1] Schneier dots the i's: "…I tell prospective clients that the mathematics are impeccable, the computers are vincible, the networks are lousy, and the people are abysmal. I've learned a lot about the problems of securing computers and networks, but none that really helps solve the people problem."[2]

2 Problem Formulation

In this paper we address the "people problem". We subscribe to Reason's contention: the fact that human factors are implicated in 80-90% of organizational accidents adds little to our understanding of how and why such accidents happen [3]. (Of course, one could substitute "organizational accidents" with "security problems".) Human performance must be seen as embedded in a work environment shaped in subtle ways by technology and human behavior. Improvements in security (and safety) require improved understanding of feedback: The dynamics of the problem, i.e. propagation of effects linked by causative mechanisms, is essential. Improving our understanding of such dynamics means analyzing empirical studies, distilling behav–ior patterns from them, developing models that relate putative causal structures to dynamical behavior though dynamic simulation and validating such simulation models by comparison of *model-based* with *empirical* behavior patterns.

2.1 Empirical Studies

There are two sources of data reflecting the interplay of technology, work environment and human behavior in information security systems: (1) field studies and (2) experiments in (simulated) 'microworlds.'

A very interesting type of field studies would be partially collecting, partially inferring data "post festum" (i.e. from case studies after some more or less grave malfunctioning of the security system). Another path would be collaborating with companies that have implemented a successful security policy – including intrusion detection systems – to distill reference data (temporal patterns describing policies and intrusion attempts, e.g.). So far we have not been able to find publicly available studies belonging to any of those two categories.

Nor have we been able to find appropriate studies of human performance in simulated information security systems ('microworlds').

[1] Ref. [2] p. xii.
[2] Ref. [2] p. 255.

2.2 Methodology

The interplay of technology, work environment and human behavior in security settings is necessarily a system characterized by feedback, temporal change (nonlinear dynamics), time delays, soft factors, and interdisciplinary aspects. Clearly, the ultimate practical reason for studying such systems is to achieve desired goals and to prevent undesired performance. In other words, security systems need to be managed. A discipline explicitly designed to manage systems characterized by the above factors (feedback, dynamics, time delays, soft factors, interdisciplinary aspects) is system dynamics [4].[3]

A basic tenet of system dynamics is that one should not model a "system" – but rather a problem: The problem specification – clearly delimited in terms of time and structure, and characterized by the problem's behavior patterns as well as by the desired behavior, the so-called "reference behavior modes" – serves as Occam's razor to sever irrelevant aspects of the system, keeping just what is essential for the problem in question. Believing that system dynamical studies of security systems will provide valuable supplementary insights to information security, we go on to present a system dynamical model of a crucial aspect of the "people problem" – viz. factors shaping compliance with security measures. Our goal is to discuss the model itself and policy suggestions suggested by the model. Thus, our – admittedly preliminary – system dynamical model dealing with compliance and risk perception can serve as illustration of what the methodology can do with modest (generic) empirical information and as appetizer for organizations that could be tempted to collaborate on the identification of reference behavior modes for comprehensive system dynamic modeling.

3 Dynamics of Compliance

3.1 Factors Shaping Compliance

Many factors can affect compliance with security measures, e.g. throughput pressure, by imposing higher priority on production and less on security (see e.g. [3]); cost-benefit factors, incl. perception of personal gains and losses [6]; conflicts between personal and organizational goals [7] – both acting to the detriment of security goals; … and finally risk, or rather perceived risk.

The role of risk perception is particularly interesting: (1) While other potential influences (e.g. throughput pressure) may or may not be present, there is always some impact of (changing) risk perception. (2) Further, risk perception is highly volatile and dependent on direct and indirect circumstances (i.e. own and reported experiences), making its influence on compliance presumably equally volatile and conspicuous. (3) A powerful psychological mechanism – viz. instrumental conditioning – would imply that alertness to risk has a positive impact on compliance. (4) A lamentable aspect of instrumental conditioning – viz. extinction of conditioned behav–ior – is likely to be a key reason for why compliance tends to decay over time.

3.2 The behavioral regulation theory

3.2.1 Introduction

The behavior regulation theory of instrumental conditioning leads quite straightforward to dynamic models of compliance [8, 9]. All in all, it seems that modeling the dependence of compliance on risk perception should be a good starting point for studying the dynamics of information security systems.

Instrumental conditioning is learning through consequences: Subject's behavior that produces positive results (high "instrumental response") is reinforced, and that which produces negative effects (low "instrumental response") is weakened. Two aspects are central: (1) Introduction of a contingency between a highly desirable event ("reinforcer") and one perceived by the subject as less desirable ("instrumental response"). (2) Contiguity between instrumental response and reinforcer [10].

The behavioral regulation theory is a relatively recent development that answers two key questions about instrumental conditioning, viz. what makes something effective as a reinforcer and how does the reinforcer produce its effect [11-13]. The behavioral bliss point (BBP) – defined as the subject's preferred distribution of activities in the absence of procedural restrictions – is a key concept here. E.g. for Kim, a teenager fond of music listening and less fond of school work the BBP would be employing the available after-school time in 6:1 proportion.[4] To increase Kim's school work her parents impose an instrumental conditioning procedure: They demand that she spends a given amount of time on school work before her being allowed to spend an equal amount of time listening to music. The 1:1 "instrumental contingency" is a constraint on Kim's preferences for the available response alternatives, and it does ensure temporal contiguity between instru-

[3] Originally, the discipline was called "industrial dynamics" and such is the title of ref. [4]. For a comprehensive exposition of modern system dynamics – "business dynamics" – see ref. [5].

[4] See "Kim's example" in Ch. 8, p. 130ff of ref. [10].

mental response (school work) and reinforcer (music listening). In the absence of other response options Kim will opt for doing a total of X hours of school work, "earning" her X hours of music listening. The behavioral regulation approach predicts that Kim's choice will be on the "schedule line" (here a 1:1 distribution of the two activities) but the precise conditioning result (i.e. the actual value of X) will be dependent on the cost:benefit function for Kim. If Kim's parents revoke the instrumental contingency the conditioned behavior decays gradually ("extinct–ion of conditioned behavior"). The model of "Kim's example" is found in [14].

3.2.2 A Case of Risk-dependent Compliance: Kim's Security Problem

Assume that Kim, now an adult, works as computer scientist in a small university. In the past her institution's computer network has not suffered particularly from attackers. Kim has become accustomed to a low level of risk and her preferred distribution of activities at work, her BBP in this connection, is to dedicate a time slot every fortnight to security-related issues (virus scanning, updates and patches, etc.) – we call this a (security-related) *task*. By some reason, since July 1, 2002, Kim's university has become a popular target for hackers. Following a major accident, more stringent security procedures are introduced and Kim complies with the recommended security measure of executing one security-related task per day. Such security measures are (more than) sufficient to prevent accidents. In fact, accidents will normally not happen if security measures stay above a certain threshold, implying keeping the risk below the "accident zone".

3.2.3 Identification of Reference Behavior for Kim's Security Problem

We proceed to formulate the time frame and the reference behavior modes for Kim's security problem, doing so in stages that become clearer as the logic unfolds: (1) We look at a time scale long enough to accommodate changing risk perceptions, but not so long that the expected long-term (quasi-) regularities in the recurrences of accidents lead to fundamental behavior changes. (2) A typical life cycle of risk perception would be that the perceived risk gradually declines because accidents do not happen (as a consequence of improved security). As perceived risk declines, so does compliance with security measures until Kim's computer network becomes vulnerable again. After a serious accident, risk perception soars, so does compliance and a new cycle starts. (3) Depending on Kim's personality (and other circumstances, e.g., university policies), this cycle would reoccur a few times until the fundamental lesson is learned. (4) We operate on a time scale excluding fundamental learning, i.e. a couple of "risk perception cycles."

3.3 Modeling Kim's Security Problem

3.3.1 Structure of the Dynamic Model

In the context of instrumental conditioning, compliant behavior can be interpreted as instrumental response and the satisfaction (such as reduction of anxiety, absence of accidents) derived from feeling protected as reinforcer. Here, accurate risk perception is the instrument (the contingency): Only if risk is correctly perceived will the reduction of anxiety fully come into play. Assuming that the perceived level of risk guides the individual's choice of compliance level, risk perception may be understood as a natural instrumental contingency modulating compliance.

Our model is found at http://ikt.hia.no/josejg/. Here, we describe the main aspects of the model in terms of its causal structure (Fig. 1).

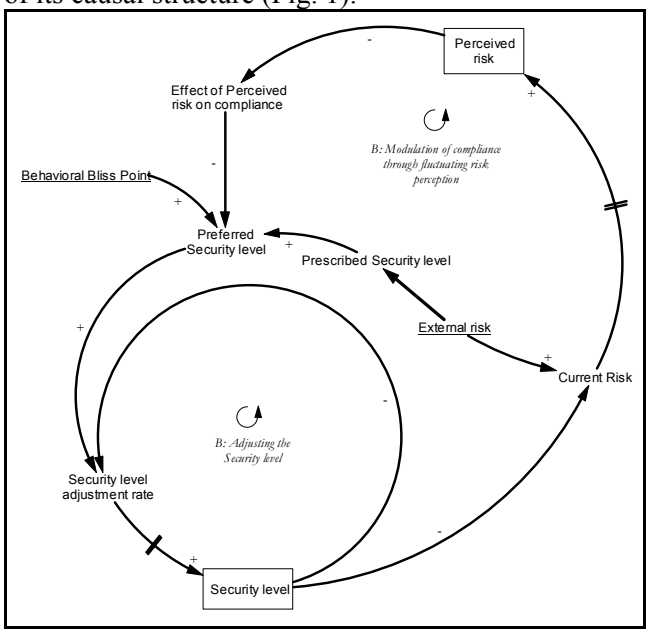

Fig. 1 Causal loop diagram of security dynamics under the influence of risk perception.

'External risk' is an external parameter describing a pattern of low risk before the key date July 1, 2002, and high risk afterward. *'Prescribed Security level'* is affected by *'External risk'*: before the key date we assume that *'Prescribed Security level'* corresponds to Kim's BBP, i.e. that it equals 1 security-related task per 14 days; after the key date, *'Prescribed Security level'* becomes 1 task/day. *'External risk'* and *'Security level'* jointly determine the actual risk (*'Current risk'*). For a given external risk, the lower the security level (defined as the actual number of

security-related tasks executed per day), the higher the probability that an accident happens. (In this connection, an accident means a major security breakdown as result of an attack.) *'Perceived risk'* is a stock (a state variable in the parlance of system dynamics, i.e. a persistent variable only changed gradually over time by flows) describing Kim's perception of risk. Risk perception is basically changed by two flows, a positive one increasing risk perception when accidents happen and a negative flow decreasing risk perception during the periods when accidents do not happen. Both processes take time and the corresponding time constants are different. However, the causal loop diagram simplifies the relationship to one influence acting with a time delay (indicated by the double slash on the influence line). *'Perceived risk'* impacts Kim's *'Preferred Security level'*: We have defined this influence in terms of a value table (*'Effect of Perceived risk on compliance'*), the shape of this relationship complying with a number of reasonable constraints, viz. that very low risk perception should imply *'Preferred Security level'='Behavioral Bliss Point'*, that high risk perception should yield *'Preferred Security level'='Prescribed security level'*, and that the resulting graph *'Effect of Perceived risk on compliance'* vs. *'Perceived risk'* increases monotonically, as an S-shaped curve.
'Security level' is again a stock – a persistent quantity only changed gradually over time by flows. Provided that *'Preferred Security level'* is above the current value of *'Security level'*, the value of the stock is increased by an inflow describing basically the instrumental conditioning effect from sufficiently high risk perception. As risk perception declines, so does the instrumental contingency. When *'Preferred Security level'* drops below the current value of *'Security level',* the value of the stock is decreased by an outflow describing the extinction of conditioned behavior (i.e. return to the BBP). We assume that extinction (forgetting) takes much longer time, viz. an average of one year, than learning (instrumental conditioning), viz. one week.

3.3.2 Model Behavior vs Reference Behavior

Figs. 2-4 illustrate the result of a simulation run during a period of time corresponding to roughly three "risk perception cycles."
Fig. 2 shows the behavior of actual (current) risk and perceived risk and the occurrence of accidents once the current risk enters the accident zone. Since there is a stochastic element (regulated by the probability that an attack succeeds) the duration of "risk perception cycles" is (slightly) variable.

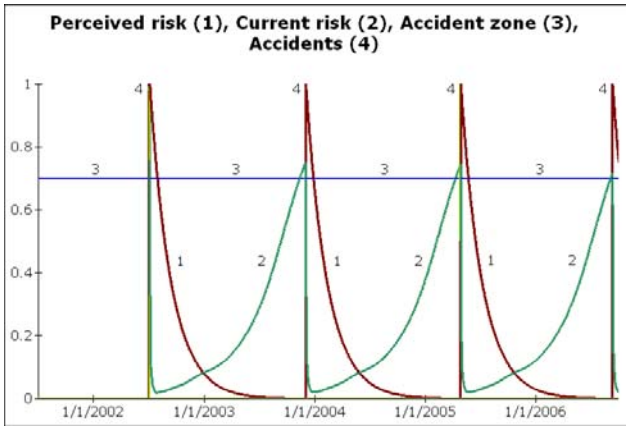

Fig. 2 Perceived risk is out of phase with actual (current) risk due to a perception delay. Accidents happen with increasing probability when current risk enters the accident zone.

During each cycle there is a significant time interval where risk is misperceived as too low. It is well-known that most people have great problems with correctly estimating risk [15].
Fig. 3 illustrates the behavior of actual and preferred security level.

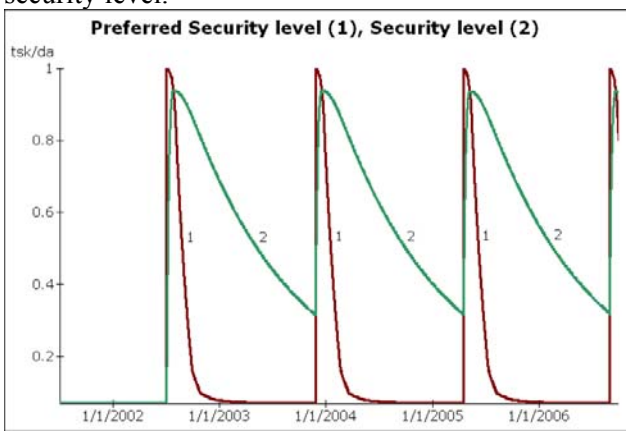

Fig. 3 Preferred security level is strongly influenced by the occurrence of accidents. Due to an assumed long time constant for the extinction of conditioned behav–ior and the low probability of accidents the actual security level decays slowly (lags behind).

Fig. 4 can be interpreted as depicting the effect of risk perception (cf. Fig. 2) on compliance. Note, however, that compliance has been defined as a parameter shaping Kim's preferences – the decay of the actual security level is ultimately determined by how long the conditioned behavior lingers (i.e. how fast the extinction of conditioned behavior occurs).
The model behavior seems to correspond to the reference behavior modes – the caveat being that so far model parameters are based on common sense rather than on empirical data.

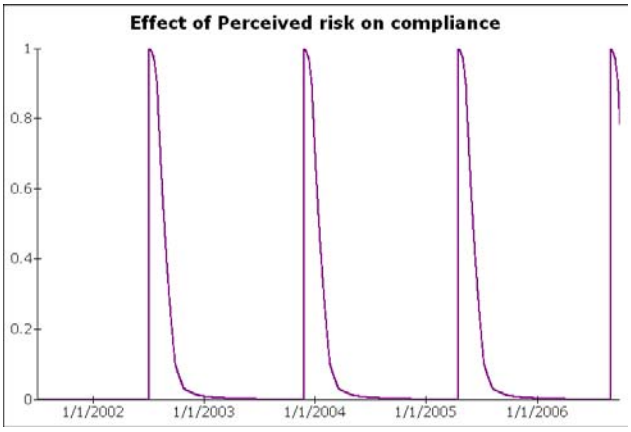

Fig. 4 In intervals without accidents risk perception decays, and so does compliance as a consequence.

3.3.3 Analysis of Model Behavior

During any of the "risk perception cycles" one can distinguish two zones, depending on whether *'Preferred Security level'>'Security level'* or *'Preferred Security level'<'Security level'*. The first case is the "conditioning zone" – the subject's risk perception correctly leads to reinforcement of compliance; the second one is the "extinction (of conditioned behavior) zone" – and this has quite troublesome and counterintuitive aspects (cf. Fig. 5).

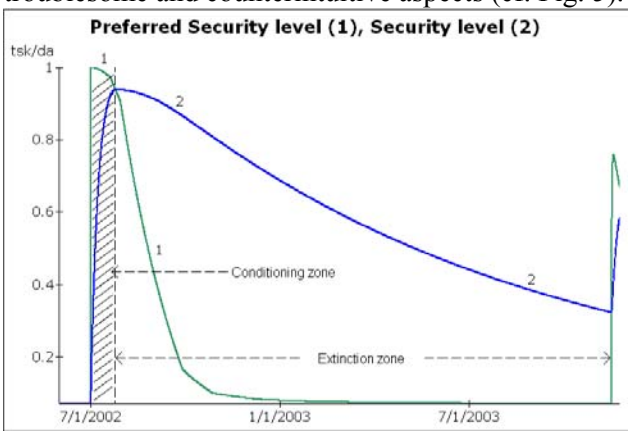

Fig. 5 Conditioning of higher compliance only occurs during a short interval in a "risk perception cycle." Misperception of risk and the absence of accidents – due to secure technology – act during a longer interval to decondition desired behavior (extinction zone).

Why is the conditioning zone comparatively short and the extinction zone correspondingly long? And why is this a problem? The answer to the second question should be straightforward: In the extinction zone one has contiguity between noncompliant behavior and lack of accidents – due to the very success of modern security technology that wards off most attacks. This implies that the extinction zone is a favorable setting for "superstitious learning" [16, 17]. The answer to the first question is compounded: First, instrumental conditioned behavior is much more persistent if the reinforcement schedule is "partial", i.e. reinforcement is not given every time [10; p. 113ff] – and this is likely to be the case in a normal working environment where various demands and time pressures might interfere with delivery of reinforcement (here in the sense of being aware of averted risk). Second, the low probability of successful attack in modern information security settings means that noncompliance can occur for long time without apparent negative consequences. In other words, information security systems become victims of the success of modern security technology in that a comparatively long "extinction of conditioned behavior zone" is induced and "superstitious learning" – wrong inferences about risk, consequences of risk and the impact of noncompliance – is facilitated in the extinction zone.

3.4 Policy Analysis and Design

How one can escape the vicious circle of accidents suggested by our dynamic model? Remember that Kim is most compliant when she perceives the risk as sufficiently high. Kim's perception of risk is "updated" by accidents: Their occurrence increases her perceived risk sharply; their absence decreases her perceived risk and, as a consequence, her compliance. From the point of view of policy design, the positive effect accidents have on compliance is interesting. For obvious reasons, accidents themselves are not a viable policy tool for improvement of information security. We need other ways to sustain an appropriate level of risk perception. Also, it appears desirable that compliance with security measures is "brought back" to a safe level long before the system enters the accident zone, preferably before it enters the extinction of conditioned behavior zone. Both aims can be served by "risk perception renewals" that lift the declining risk perception to a higher, more accurate level. Various trainings, publications, seminars and other kind of interventions focusing on IT-risks may be suggested as potentially effective tools for increasing and refreshing the security knowledge among the IT-system users (and here we talk about both the systems' end-users as well as their managers). Indeed, organizations are introducing such training-like interventions as part of their security policies. But note that interventions must be appropriately scheduled to be most effective: As suggested by our model, interventions to emulate the accidents' positive impact should occur at the start of periods of decaying risk perception to ensure a correction of course before the system becomes too vulnerable and to avert superstitious learning.

4 Wanted: Reference Modes for Real-life Security Systems

Information security systems need a sound management policy in accord with human nature. Alas, too often one relies solely on technical issues. Either are human factors in security systems treated as "obvious" marginalities or considered unmanageable, hoping that technological solutions should automate security. Such approach is futile: The literature on human error emphasizes the "ironies of automation": Trivial tasks can be technologically addressed, leaving more demanding tasks to people (see e.g. [18]). Concerning the interaction between people and technology Schneier [2] states "…this interaction is the biggest security risk of them all."

To improve the robustness of modern information security systems an increased understanding of the role of human factors – especially, of their dynamics – is essential. Gaining insight into the intrinsic interactions between people, technology and working environment in security systems is a main goal of our research. The problem requires an interdisciplinary approach involving relevant knowledge from technology, information science, psychology and management. Understanding its dynamics means understanding the causal structure of the problems and opening paths for more successful policies (i.e. employing system dynamics).

Thus far in our research we have concentrated on exploring theoretical aspects of the problem. Having gained initial theoretical understanding of the problem, we are now ready to expand our approach, including looking for applications. We are interested in collaborating with organizations to the effect of obtaining data on the performance of information security systems (technology, environment and people). Such "reference behavior modes" would guide development and validation of comprehensive system dynamics models, and their application in terms of specific recommendations to improve security policies. We hope that this paper instigates a collaboration between organizations and us.

References:

[1] Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. New York: John Wiley & Sons, Inc., 1994.

[2] Schneier, B., *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, Inc., 2000.

[3] Reason, J., *Managing the Risks of Organizational Accidents*. Hants, UK: Ashgate Publishing Ltd, 1997.

[4] Forrester, J.W., *Industrial Dynamics*. Cambridge, MA: MIT Press, 1961.

[5] Sterman, J.D., *Business dynamics : systems thinking and modeling for a complex world*. Boston: Irwin McGraw Hill, 2000.

[6] Battmann, W. and P. Klumb, Behavioural economics and compliance with safety regulations. *Safety Science*, Vol. **16**, 1993, p. 35-46.

[7] Reason, J., D. Parker, and R. Lawton, Organizational controls and safety: The varieties of rule-related behaviour. *Journal of Occupational & Organizational Psychology*, Vol. **71**, (4), 1998, p. 289-304.

[8] Gonzalez, J.J., Modeling Erosion of Security and Safety Awareness. *Proceedings of the Twentieth International Conference of the System Dynamics Society July 28 - August 1, 2002 Palermo, Italy*, 2002.

[9] Gonzalez, J.J. and A. Sawicka. *Origins of compliance – An instrumental conditioning perspective*. Submitted to *Fifth International Conference on Cognitive Modeling (ICCM 2003). 2003. Bamberg, Germany*.

[10] Domjan, M., *The Essentials of Conditioning and Learning*. 2 ed. Belmont, CA: Wadsworth/ Thomson Learning, 2000.

[11] Allison, J., *The nature of reinforcement*. In *Contemporary learning theories: Instrumental conditioning theory and the impact of biological constraints on learning*, S.B. Klein and R.R. Mower, Editors. 1989, Erlbaum: Hillsdale, NJ. p. 13-39.

[12] Timberlake, W., *A molar equilibrium theory of learned performance.* In *The psychology of learning and motivation*, G.H. Bower, Editor. 1980, Academic Press: Orlando, FL. p. 1-58.

[13] Timberlake, W., Behavioral regulation and learned performance: Some misapprehensions and disagreements. *Journal of the Experimental Analysis of Behavior*, Vol. **41**, 1984, p. 355-75.

[14] Gonzalez, J.J. and A. Sawicka. *Modeling Instrumental Conditioning – The Behavioral regulation approach*. In *36th Hawaii International Conference on System Sciences (HICSS 36)*. 2003. Big Island, Hawaii.

[15] Kahneman, D. and A. Tversky, *Choices, Values, and Frames*: Cambridge University Press, 2000.

[16] Hogarth, R.M., *Judgement and Choice: The Psychology of Decision*. 2nd ed. Chicester: John Wiley & Sons, 1987.

[17] Sterman, J.D., Superstitious Learning. *The Systems Thinker*, Vol., 1997, p. 1-5.

[18] Reason, J., *Human Error*. New York: Cambridge University Press, 1990.