# SYSTEM EFFECTIVENESS MODEL FORMULATION

Cameron W. Coates
Oak Ridge National Laboratory
P.O. Box 2008, MS 6281, Oak Ridge, TN 37831-6281

Denise F. Jackson, Ph.D.
University of Tennessee
312 East Stadium Hall, Knoxville, TN 37996-0700

## Abstract

Evaluation of system effectiveness has numerous pitfalls. System objectives may be poorly defined, may shift during the system life, or may be hard to quantify. Further, individual perceptions of the quantifications may differ. Whatever the cause, system effectiveness has been an elusive term to quantitatively define. The proposed model presents a quantitative system effectiveness model and establishes a utilitarian approach for its use with the illustrative application to a nuclear safeguards system. The model uses the Type I and Type II statistical error rates as input to the component or subsystem effectiveness calculation which, when combined using a utilitarian methodology, quantifies the overall system effectiveness. The methodology will use a survey of expert judgment to determine the relative importance of the individual subsystems through a statistically designed Web survey. The Web-based survey will be available to nuclear material protection, control, and accounting experts attending the 2008 INMM conference. This model and methodology will provide a repeatable quantifiable measure for any system, but in this case a simple safeguards system is used as an example.

## Introduction to System Effectiveness Model

This research develops a generic systems effectiveness model and applies it to the domestic (state) safeguards case. This integrated heuristic approach is designed to utilize performance data in the form of Type I and II error rates. This methodology uses estimates of the effectiveness of the basic elements (subsystems) of a safeguards system to quantify the overall system effectiveness. The International Council on Systems Engineering defines a system as "a combination of interacting elements organized to achieve one or more stated purposes"[1]. Clearly, any system exists to achieve a defined purpose, and the lifecycle begins with a requirements review and identifying stakeholders' needs. Evaluation of any system is a natural part of the system's lifecycle. During the various stages, one cannot build and operate a system to satisfy stakeholder needs without an ongoing evaluation (verification and validation) scheme. System effectiveness is a natural element in any system evaluation scheme. Villemeur describes failure modes and effects analysis (FMEA) as an inductive analysis used to systematically study causes and effects likely to affect the performance of a system. There are four main steps in performing an FMEA: [2]

1. Definition of the system, its function and components;
2. Identification of the component failure modes and their cause;
3. Study of the failure mode effects;
4. Conclusions and recommendations.

An FMEA is focused on finding significant failure modes and making changes in the system that correct the failures. Although many of the activities in an FMEA are useful in determining

effectiveness, the focus is not on determining the performance (effectiveness) of the system. In a number of cases, Type I and Type II errors may not be "failures" of the system.

Soban and Mavris recognize the need for an integrated and efficient framework that can rapidly assess system effectiveness for today's complex systems. They recognize that the definitions of system effectiveness vary widely and are often application dependent. They quote some of the more common definitions [2]:

*"The overall capability of a system to accomplish its intended mission"* [3]

*"The probability that the system can successfully meet an operational demand within a given time when operated under specified conditions"* [4]

*"A measure of the degree to which an item can be expected to achieve a set of specific mission requirements, and which may be expressed as a function of availability, dependability and capability"* [5]

Soban and Mavris posit a new definition for system effectiveness, as the term "effectiveness" implies an element of quantification: "System effectiveness is a quantification, represented by system level metrics, of the intended or expected effect of a system achieved through functional analysis." There are two fundamental approaches to evaluating system effectiveness: a systems resource approach and a goal-centered approach. [6] Under a **resource approach,** system effectiveness is determined in terms of resource availability instead of specific task objectives. The term "cost-effective" captures the essence of the resource approach. The term is usually modified by either "more" or "less," indicating a relative evaluation. Under a **goal-centered approach**, system effectiveness is determined by comparing the system performance against specific objectives. Often, under a goal-centered approach, effectiveness is defined in terms of percentage of effective and usually indicates a more absolute measure of obtaining the objective. Under either grading approach, there will always be interest in improving system effectiveness.

The algorithm and methodology presented herein are based on the goal-centered approach to system effectiveness evaluations. The concept is simple: know the system goal and know, with a measure of precision, how often the system goal is achieved. A good starting definition of system effectiveness is made by Blanchard and Fabrycky (1998): "the probability that a system can successfully meet an overall operational demand, within a given time, when operated under specific conditions." This definition captures the nature of systems effectiveness but fails to account for types of errors. Type I and Type II errors are defined in statistics as errors based on testing the null hypothesis ($H_0$) and the alternative hypothesis ($H_1$) as seen in Table 1.

Table 1. Type I and II errors

| Statistical decision | True state of the null hypothesis ($H_0$) | |
|---|---|---|
| | $H_0$ True | $H_0$ False ($H_1$ True) |
| Accept $H_0$ | Correct ($1-\alpha$) | Type II error ($\beta$) |
| Reject $H_0$ | Type I error ($\alpha$) | Correct ($1-\beta$) |

Conceptually, a Type I error in relation to a system could be likened to the times the system acted when it should not have acted, and the Type II error to those times the system did not act when it should have acted. The terms $\alpha$ and $\beta$ represent the probability of Type I (false positive or false

alarms) and Type II (false negative or missed true alarms) errors, respectively. Other conceptual statements relating to these quantities are 1-$\alpha$, the probability the system "did it right," often referred to as the ***confidence level*** of a test; and 1-$\beta$, the probability the system "did not do it wrong," often referred to as the ***power*** of a test

## Algorithm

Using the quantities 1-$\alpha$ and 1-$\beta$, a generic mathematical model for system effectiveness can be developed. The posited relationship of system effectiveness ($e_s$) for a generic system can be constructed as follows:

$$e_s = f(1-\alpha) \cdot f(1-\beta)$$

Stated in words, this formula is *the effectiveness of a system is a function of the confidence level times a function of the power of a system*. In developing the functions of this relationship, another conceptual construct will be useful. The quantities $\alpha$ and $\beta$ can be thought of in safeguard systems as representing the probability of either false alarms ($\alpha$) or missed true alarms ($\beta$). Recognizing that the quantities $\alpha$, 1-$\alpha$, $\beta$, and 1-$\beta$ are always valued from 0 to 1, a relationship for system effectiveness needs to appropriately emphasize the false-alarm term or true-alarm term when needed; therefore, an appropriate penalty on effectiveness needs to be developed. Defining the error ratio **r** = $\alpha_0/\beta_0$ as the system manager's tolerance for false alarms in proportion to tolerance for missed true alarms where $\alpha_0$ is the acceptable rate of Type I errors (false alarms) and $\beta_0$ is the acceptable rate of Type II errors (missed true alarms), each term can be adjusted based on this ratio. This leads to a revised function for effectiveness that increases the effect of $\alpha$ or $\beta$ appropriately to the overall effectiveness, as seen in Equation 1:

$$e_s = (1-\alpha^{K_a}) \cdot (1-\beta^{K_b}) \qquad (1)$$

where

$K_a = (r)^{1/c}$ for $\boldsymbol{r} > 1$ ; otherwise $K_a = 1$
$K_b = (r)^{-1/c}$ for $\boldsymbol{r} < 1$ ; otherwise $K_b = 1$

Parameter "*r*" is the relative tolerance of false alarms to missed alarms ($\alpha_0/\beta_0$) in a non-stressed environment. The stress could be threat level, increased consequence of failure, or other local conditions leading to a need for more effectiveness. Parameter "*c*" is the stress level to the system. Again this can be threat level, increased consequence of failure, or other local stresses. When $c = 1$, stress is neutral; increasing *c* means increasing stress levels. A graph of the $K_a$ term versus the Type I error with an ratio r = 20 in this equation can be seen in Figure 1.

Figure 1 shows that when the baseline tolerance for false alarms versus missed alarms equals 20, the curve for c=1 extends a great distance, allowing a large tolerance for false alarms before the effectiveness based on false alarms is changed. As *c* increases above 1, the tolerance for false alarms is reduced. This equates to increased stress on the system and changes the effectiveness based on the stressed conditions. With a high enough stress, the tolerance for false alarms could be all but negated. A reasonable range for *c* has not been established; however, the range could be from 1 to 20, 1 to 10, 1 to 5, or 1 to 2, depending on the application and the system owners' requirements.

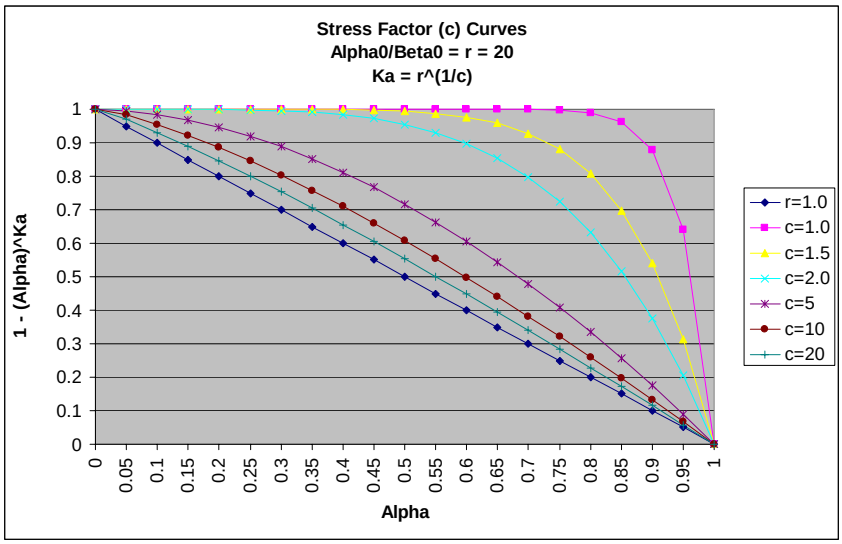


**Figure 1. System stress factor curves.**

The input values and primary variables for the determination of any given system's effectiveness will be the error rates for the different subsystem components (rates of Type I ($\alpha_i$) and Type II ($\beta_i$) error). Every system deployed should have an established testing procedure and be keeping records on "false alarms" (Type I errors) and "missed alarms" (Type II errors). There are such things as nuisance alarms (such as a small animal tripping a motion sensor), which, depending on context and focus, can be treated as either false alarms (Type I error) or true alarms (no error). These variables have the distinct advantage of being directly measurable and will facilitate the determination of system effectiveness for specific systems that can be tracked over time.

Turban and Metersky developed a utility theory approach to multivariable system effectiveness for the Naval Air Development Center [8]. They attempted to reduce subjective evaluation of the system's performance by developing a procedure, based on decision and utility theories, so that the evaluation can be calculated objectively. They posit that the system effectiveness is the sum of the values of the measures of effectiveness (MOEs). The value of the MOE ($v_{ij}$) for each course of action is determined by the product of the relative importance (utility) of the MOE $u(M_j)$ times the utility of the performance level $u(x_{ij})$ of the MOE [7]:

$$v_{ij} = u(M_j)\, u(x_{ij})$$

The example of airport passenger screening is used to illustrate the use of the parameters. In this example, a walk-through metal detector (WTMD) will be the system boundaries. In the WTMD case, a false alarm ($\alpha$) will be defined as the detector alarming when a small amount of metal in a nonhazardous form is detected (some analysts might call this a nuisance alarm since metal is detected but is not a threat). A missed alarm ($\beta$) would be a threatening form of metal making it through the WTMD. In this example, under non-stressed conditions, airport security may be able to accept 100 false alarms to 1 missed alarm ($\alpha_0/\beta_0 = r = 100$). The solution space for this situation would appear as in Figure 2. If there is a stressed condition, such as an specific threat to a given airport, then the effectiveness solution space changes in relation to the threat. In this case the example of the stress factor of $c$=5 is shown in Figure 3, which shows an area of acceptable effectiveness (whatever the level of acceptable effectiveness) that has decreased significantly. If the system owner wanted to make a change to the solution space to gain back system effectiveness, a

logical change would be to greatly increase the tolerance for false alarms so that $r_0 = 5000$. This modification can be seen in Figure 4. It shows that the compensatory measure—increasing the sensitivity of the WTMD by allowing 5000 false alarms to one missed alarm—has indeed increased the solution space for system effectiveness, but it may not be considered enough. In the event that the baseline requirements cannot be met if the tolerance is changed, either some compensatory

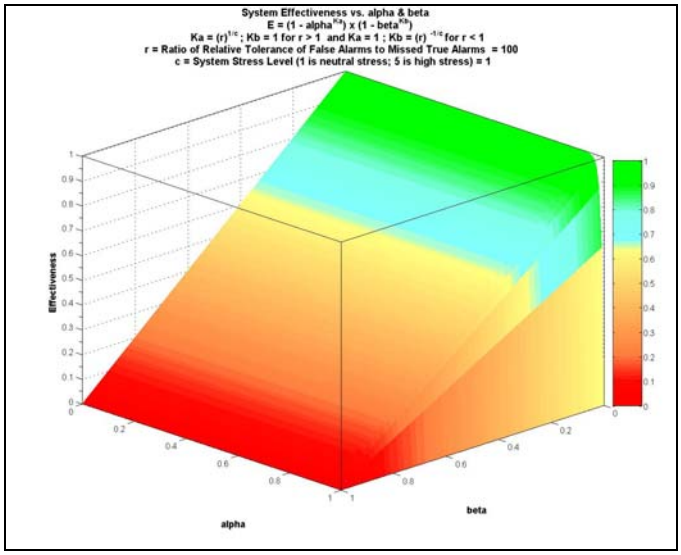


**Figure 2. Example baseline airport solution space.**

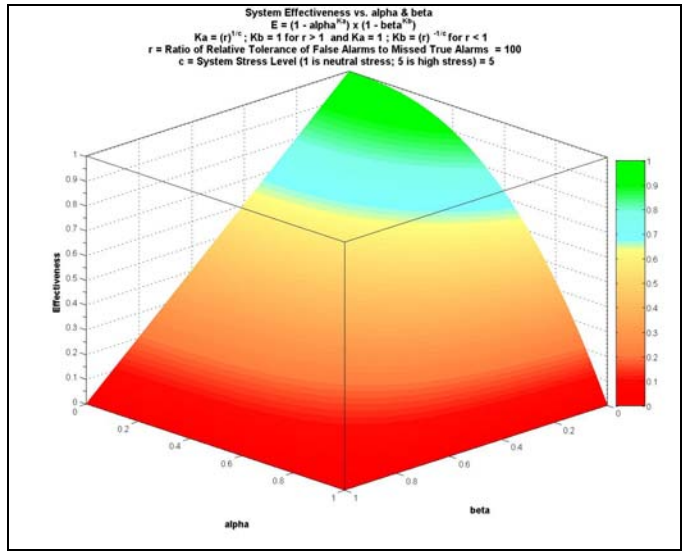


**Figure 3. Example airport security under stress.**

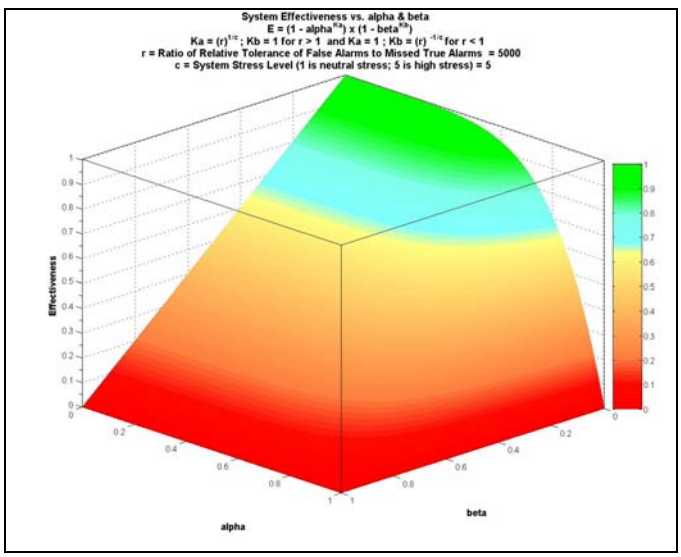


**Figure 4. Example under stress with compensation.**

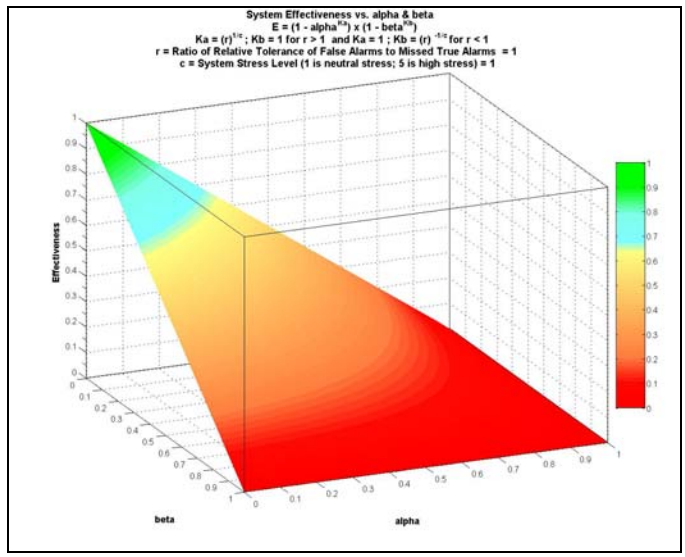


**Figure 5. Baseline system effectiveness.**

measure would be required to regain baseline effectiveness requirements or the system owner would accept additional risk. The generic baseline system effectiveness relationship can be seen in Figure 5. This would be the case when the tolerance for false alarms and missed alarms is the same.

## Algorithm Use

This work uses the systems approach of decomposing the system into units with measurable Type I and Type II errors. The next stage of the research is to determine how to apply Eq. (2) in a system

of systems. The utilitarian approach to the system effectiveness ($e_s$) for a system of systems was the choice for this work. Assume

$$e_s = u_p e_p e_m + u_c e_c e_m + u_a e_a e_m \tag{2}$$

subject to

$$0 \le e_i \le 1 \qquad 0 \le e_m \le 1 \qquad \sum u_i = 1 \ ,$$

where

$\boldsymbol{u_p}$ = the relative importance of the physical protection subsystem,
$\boldsymbol{u_c}$ = the relative importance of the material control subsystem,
$\boldsymbol{u_a}$ = the relative importance of the material accounting subsystem.

And for specific sub-systems:

$$e_p = (1-\alpha_p^{K_{ap}}) \bullet (1-\beta_p^{K_{bp}}) \qquad e_a = (1-\alpha_a^{K_{aa}}) \bullet (1-\beta_a^{K_{ba}})$$
$$e_c = (1-\alpha_a^{K_{ac}}) \bullet (1-\beta_a^{K_{bc}}) \qquad e_m = (1-\alpha_a^{K_{am}}) \bullet (1-\beta_a^{K_{bm}}) \ ,$$

with $K_{ap}$ and $K_{bp}$ related to $r_p$, the tolerated ratio and stress level for the physical protection subsystem;
with $K_{aa}$ and $K_{ba}$ related to $r_a$, the tolerated ratio and stress level for the material accounting subsystem;
with $K_{ac}$ and $K_{bc}$ related to $r_c$, the tolerated ratio and stress level for the material control subsystem;
with $K_{am}$ and $K_{bm}$ related to $r_m$, the tolerated ratio and stress level for the management subsystem.

What remains is to determine the relative importance of the separate subsystems to define a solution space for calculating a given safeguards system's effectiveness and simulate an example environment to illustrate the utility of the methodology.

**Survey**

The surveyed population in this case will be defined as members of the Institute of Nuclear Material Management (INMM) and those that attend the INMM annual meetings. The INMM organization currently has more than 1000 members worldwide and holds annual technical meetings with approximately 700 attendees. Both members and interested and experienced non-members attend. The basic instrument will be a Web-based survey that gathers response data in an SPSS data file. Figure 6 shows an example Web survey under construction using the University of Tennessee's Statistical Consulting Center's SSPS interview builder (mrInterview) with example questions to determine the modalities of conducting a Web-based survey. The interview builder allows for building and testing the survey prior to distribution of the web link.

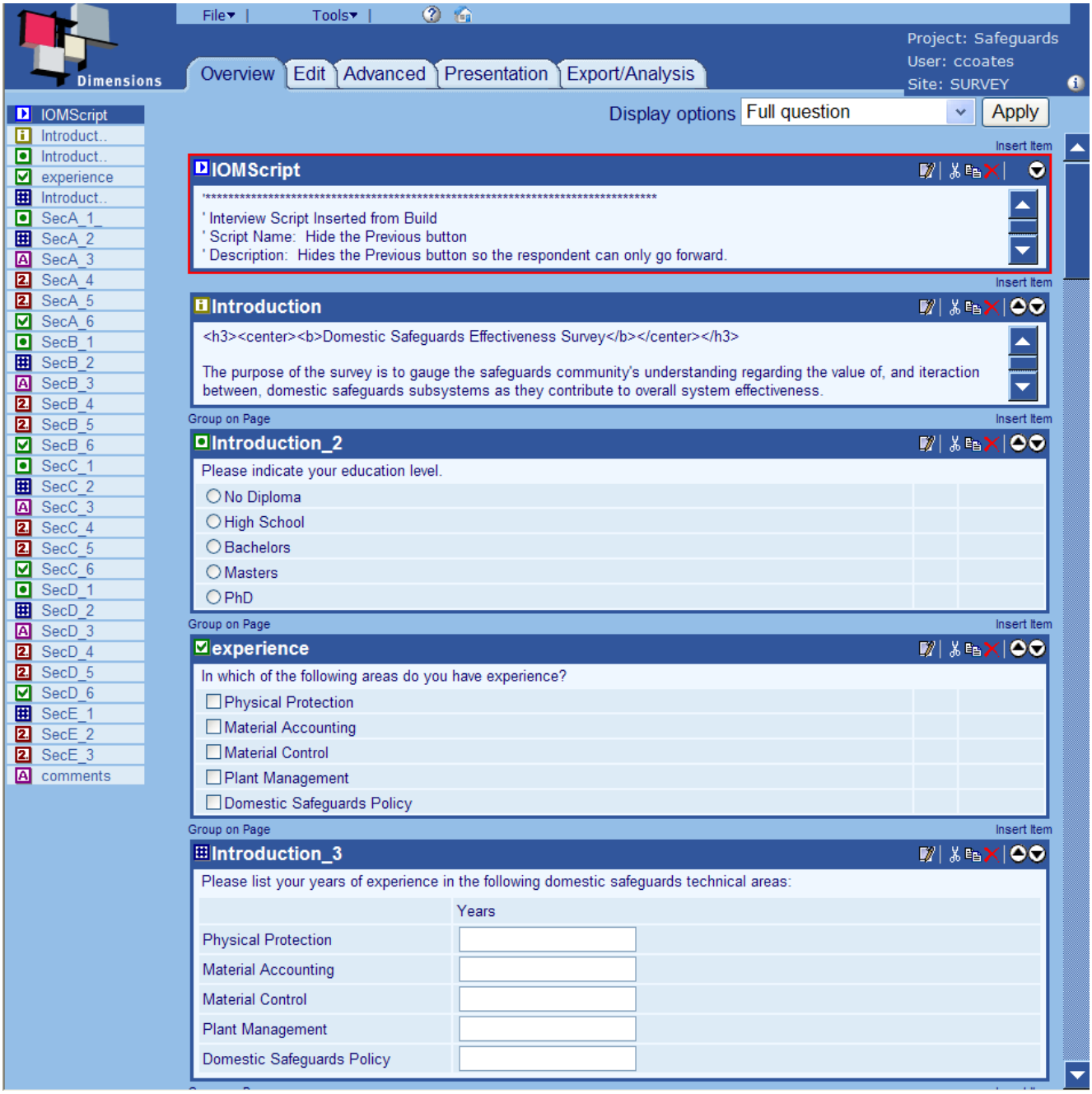


**Figure 6. Sample safeguards survey.**

## References


1. International Council on Systems Engineering (INCOSE). *Systems Engineering Handbook v3.1*. 2007 [cited; Version 3.1:[Available from: http://www.incose.org/ProductsPubs/products/sehandbook.aspx.
2. Soban, D.S. and D.N. Mavris. *Formulation of a Methodology for the Probabilistic Assessment of System Effectiveness*. [Presented at the AIAA 2000 Missile Sciences Conference, Monterey CA, November 7-9, 2000.] 2000 [cited; Available from: http://www.asdl.gatech.edu/publications/2000/AIAA-MSC-2000-DS.pdf.
3. Tillman, F.A., C.L. Hwang, and K. Way, *System Effectiveness Models: An Annotated Bibliography*. IEEE Transactions of Reliability, 1980. **Vol. R-29**(No. 4): p. 295-304.
4. ARINC Res. Corp, *Reliability Engineering*. 1964, Englewood Cliffs, NJ: Prentice Hall
5. DoD, *Definitions of Effectiveness Terms for Reliability, Maintainability, Human Factors, and Safety*, US Department of Defense, Editor. 1966.
6. Hamilton, S. and N. Chervany, *Evaluating Information Systems Effectiveness - Part 1 Comparing Evaluation Approaches*. MIS Quarterly, 1981. **5**(3): p. 55-69.
7. Turban, E. and M.L. Metersky, *Utility Theory Applied to Multivariable System Effectiveness Evaluation*. Management Science, 1971. **17**(12): p. B817-B828.