Sensing systems efficiency evaluation and comparison for homeland security and homeland defense

Alexander A. Pakhomov[*]
Security&Defense Research, LLC, 576 Valley Ave, Yonkers, NY 10703

ABSTRACT

Designers and consumers of various security, intelligence, surveillance and reconnaissance (ISR) systems as well as various unattended ground sensors pay most attention to their commonly used performance characteristics such as probability of a target detection and probability of a false alarm. These characteristics are used for systems comparison and evaluation. However, it is not enough for end-users of these systems as well as for their total/final effectiveness assessment. This article presents and discusses a system approach to an efficiency estimation of the security and ISR systems. Presented approach aims at final result of the system's function and use. It allows setting up reasonable technical and structural requirements for the security and ISR systems, to make trustworthy comparison and practical application planning of such systems. It also allows finding forward-looking, perspective ways of systems development. Presented results can be guidance to both designers and consumers.

Keywords: Efficiency estimation, security, intelligence, surveillance, reconnaissance.

1. INTRODUCTION

Efficiency evaluation and assessment is the key point for all designers, consumers and end users of various security, intelligence, surveillance and reconnaissance (ISR) systems as well as various unattended ground sensors. Knowledge of the appropriate characteristics allows making reasonable systems comparison, setting up technical and structural requirements for such systems, performing their practical application planning, and finding forward-looking perspective ways of future systems development. As usual, designers and consumers pay the most attention to the commonly used systems performance characteristics such as probability of target detection $\mathbf{P_D}$ and probability of false alarm $\mathbf{P_{FA}}$**.** These basic characteristics are used for systems comparison and evaluation. However, they are not enough for end users as well as for total and final effectiveness assessment. The basic characteristics $\mathbf{P_D}$ and $\mathbf{P_{FA}}$ describe the system's positive reaction in cases of target presence or absence in the system's detection area. In other words, if a target is definitely present or not present in the detection area, the system's positive response may occur with probabilities $\mathbf{P_D}$ and $\mathbf{P_{FA}}$ respectively.

Unfortunately, in the real life, system's end users face a different situation. For example, the system's users know for sure that their system generates a positive response (alarm) and the question is whether the target is present or not in the detection area. What is the probability of those two events? Let us call these two new characteristics as probability of correct detection $\mathbf{P_{CD}}$ and probability of false detection $\mathbf{P_{FD}}$. How do these new characteristics correlate with common probabilities $\mathbf{P_D}$ and $\mathbf{P_{FA}}$? What does the end user have to do if the system generates an alarm? What efficiency, what chance of success does the end user really have in such a situation? How does a real tactical situation affect the probabilities $\mathbf{P_{CD}}$, $\mathbf{P_{FD}}$ and, as a result, the end user's success? Under which scenarios even a "weak" system can be very useful, and when a "reliable" system may not bring much result?

In this paper we will try to give an answer to all these and many other questions. This paper presents and discusses a system approach to efficiency evaluation and comparison of security and ISR systems. Presented approach aims at final result of the system's function and use. We also report on the modeling results that allow transforming knowledge of common $\mathbf{P_D}$ and $\mathbf{P_{FA}}$ in the practically important probability of correct detection $\mathbf{P_{CD}}$ and probability of false detection

[*] alexander.pakhomov@sndresearch.com; phone 1 914 462-2639; sndresearch.com

$\mathbf{P_{FD}}$. We illustrate our results for typical detection ability of the unattended ground sensors in possible tactical situations and in real ones. Presented results can be very useful guidance to both designers and consumers.

2. RESULTS AND DISCUSSIONS

2.1 General principles

2.1.1 Purposes of the systems use and efficiency levels

In this paper we discuss various security, intelligence, surveillance and reconnaissance (ISR) systems as well as unattended ground sensors that allow getting information about targets, and sometimes about environmental conditions, and also about our forces. Let us call all these systems for short the Information Systems (IS). The IS provide us with information about our surroundings. Commonly we have some preliminary (a priori) information about our surroundings. The IS provide us with new (a posteriori) and hopefully more correct and reliable information that better describes our surroundings.

From system analysis point of view, a very important question is: what is the final purpose of such information systems use? In other words, why do we want to design and then use these systems? The answer to this question defines the efficiency characteristics of the information systems and the efficiency evaluation approach in general. An easy answer to this question is: we want to get information about target presence, and we want to detect "bad guys". The more correctly the IS describes surroundings the better the Information System is. Let us call this level of efficiency evaluation and system evaluation as the level of **information efficiency,** because at this level we keep in mind only information factors and results of direct function.

Unfortunately, information itself does not make any direct changes to our world. It does not catch "bad guys". Therefore, an easy answer about the purpose of information systems use mentioned above, does not allow building a full set of the efficiency characteristics of those information systems. We have to consider a higher level of the purposes and we have to be able to answer the question, how the evaluated information system increases our ability to catch "bad guys" and to improve our surrounding conditions by using the signals from that Information System. The more the Information system increases our ability to catch "bad guys" and to improve our surrounding conditions, the better the Information System is. Let us call this level of efficiency evaluation and system evaluation as level of the **operational efficiency**, because at this level we keep in mind the results of our material operation (of our response) using signal/data from the Information System. This level of efficiency can be also called **usefulness level**.

The Information System itself (its design, manufacturing, use, and maintenance) as well as our material operation (response) with use of signal/data from the Information System cost some money. Therefore, we have to consider the next higher level of purposes and we have to be able to answer the question, how the evaluated information system increases our ability to catch "bad guys" and to improve our surrounding conditions by using the signals from that Information System with taking into account corresponding costs. The smaller are the costs with other factors being equal, the better is the Information System. Let us call this level of efficiency evaluation and system evaluation as the level of the **operational-economic efficiency** or just **economic efficiency**, because at this level we keep in mind not only the results of our material operation (of our response) with use of signal/data from the Information System, but also all costs related to this operation.

Consecutive system analysis of the Information Systems and their efficiency evaluation and comparison has to include evaluation and comparison at all mentioned above three levels of efficiency. It is important to note that at the level of information efficiency only the systems that generate/provide information with the same information structure can be compared correctly. At the level of operation efficiency only the systems that provide information to the same operations can be compared correctly. And at the level of the operation-economic efficiency all Information Systems can be compared with each other.

2.1.2 Information efficiency characteristics

In this paper for simplicity we will consider only the Information Systems that provide information in discrete form. (Presented results can be easily generalized for systems that provide information in continuous form.) That means that all possible data that can be provided by system and all surrounding conditions that system can recognize we can enumerate with integer numbers. Let’s use symbol/number **m=0, 1,.., M** for surrounding conditions description. Symbol/number **^m=0, 1,.., M** we will use for description of the responses/data provided by the information system. **M** is the total number of surroundings conditions and the total number of the various systems responses.

Information systems are not ideal because of many independent and objective reasons. Therefore, when we have a real surrounding condition **m,** our information system can generate data **^m≠m.** On the other hand, if an information system generates data **^m,** the real surrounding condition **m** can be different from **^m,** in other words, **m≠^m** in general. The results of the information system function are random, and so we can use two matrices of probabilities to describe the situation mentioned above: **[P (^m/m)]** and [**P (m/^m)]**. Matrix **[P (^m/m)]** describes random results of the information system function **^m** in case when a surrounding condition is **m.** Matrix **[P (m/^m)]** describes possible surrounding conditions when the system generates data **^m. P (^m/m)** is the probability that the system generates results **^m** if in reality the surrounding condition is **m. P (m/^m)** is the probability that the real condition is **m** when the system generates result **^m.**

For better understanding we will consider a simple detector that can discriminate only between two surrounding conditions: **m=1** (target is present in the detection area) and **m=0** (target is not present in the detection area). Therefore, **^m** can be only **1** or **0**. This example perfectly represents the detection ability of the vast majority of existing unattended ground sensors [1-4]. (For more advanced detectors that can recognize many classes of targets [5-10] **M≥2**.)

For a simple detector (**^m=0, 1**), the relation between elements of the matrix **[P (^m/m)]** and commonly used probability of detection **P_D** and probability of false alarm **P_{FA}** is understandable, and according to the definition of **P_D** and **P_{FA}** is represented by the following formula:

$$\left[P({}^\wedge m/m)\right] = \begin{array}{cc} & \xrightarrow{\qquad} m \\ \downarrow {}^\wedge m & \begin{bmatrix} P({}^\wedge 0/0) & P({}^\wedge 0/1) \\ P({}^\wedge 1/0) & P({}^\wedge 1/1) \end{bmatrix} \end{array} = \begin{bmatrix} 1-P_{FA} & 1-P_D \\ P_{FA} & P_D \end{bmatrix} . \tag{1}$$

$$m,\ {}^\wedge m = 0,\ 1$$

But for real life and for practical users of the information system, the elements of the matrix **[P (m/^m)]** are critical because they indicate what is going on in reality when we have (or do not have) an alarm signal from the information system. Suppose, the information system generates an alarm (**^m=1**). With conditional probability **P (1/^1),** the target is present in the detection area, and with probability **P (0/^1)** the target is not present in the detection area. Let’s call these probabilities the probability of correct detection **P_{CD}** and the probability of false detection **P_{FD}** respectfully. Correspondingly, if the information system does not generate an alarm (**^m=0**), the target is present in the detection area with probability **P (1/^0),** and with probability **P (0/^0)** the target is not present in the detection area. Let’s call these probabilities: probability of false undetection **P_{FUD}** and probability of correct undetection **P_{CUD}** respectfully. It is clear that the following equations are correct

$$\begin{aligned} \mathbf{P_{FUD} = 1 - P_{CUD}} \ , \\ \mathbf{P_{FD} = 1 - P_{CD}} \ . \end{aligned} \tag{2}$$

The probabilities presented above can be described by the following equation (3)

$$\left[P(m/\wedge m)\right] = \underset{m}{\downarrow} \overset{\longrightarrow \wedge m}{\begin{bmatrix} P(0/\wedge 0) & P(0/\wedge 1) \\ P(1/\wedge 0) & P(1/\wedge 1) \end{bmatrix}} = \begin{bmatrix} P_{\mathbf{CUD}} & P_{\mathbf{FD}} \\ P_{\mathbf{FUD}} & P_{\mathbf{CD}} \end{bmatrix} = \begin{bmatrix} P_{\mathbf{CUD}} & 1- P_{\mathbf{CD}} \\ 1- P_{\mathbf{CUD}} & P_{\mathbf{CD}} \end{bmatrix} \tag{3}$$

$m, \wedge m = 0, 1$

According to the Bayes' Theorem [11], we can write the general equation

$$P(m/\wedge m) = \frac{P(\wedge m/m)*P(m)}{\sum\limits_{m} P(\wedge m/m)*P(m)}\ , \tag{4}$$

that allows calculating practically interesting characteristics **P(m/^m)** using conditional probabilities **P(^m/m)** and a priori probabilities **P(m).** Even the general expression (4) allows understanding that final relation between information system response and real surroundings depends not only on immanent abilities of information system but also and, drastically, on surroundings themselves and on our a priori knowledge about these surroundings. Therefore, the same information system that can be very useful and trustworthy/reliable in one tactical situation or for one kind of application can be completely useless and not trustworthy/not reliable in another situation. In other words, knowledge of only two basic characteristics $\mathbf{P_D}$ and $\mathbf{P_{FA}}$ does not allow making the final decision about "quality" and usefulness of concrete/specific information system for a particular tactical situation and security and defense application.

2.1.3 Operational efficiency characteristics

It is important to note that information systems themselves can not change surroundings and the situation on the ground. They can not catch "bad guys". They are only supporting systems. We need special response forces or just support forces that can act accordingly after getting an alert from information systems. Only presence of such response forces and ability to act accordingly creates a situation where information systems can be reasonably used.

Response/support forces always have their original acting/operation alternative that typically is updated and optimized to match the existing a priori information. Let us call that original alternative as $\mathbf{n_1}$. An information system provides response forces with new knowledge about surroundings. (In our case the information system generates **^m.**) After corresponding processing of that information and decision making, the response forces instead of the original alternative $\mathbf{n_1}$ get a new acting/operation alternative $\mathbf{n_2}$ that is more optimal for the existing surroundings. If the average efficiency characteristics for alternatives $\mathbf{n_1}$ and $\mathbf{n_2}$ are $\mathbf{\Theta_{n1}}$ and $\mathbf{\Theta_{n2}}$ respectively, the difference

$$\mathbf{\Delta\, \Theta_{n2n1} = \Theta_{n2} - \Theta_{n1}} \tag{5}$$

characterizes the increase of the response forces average efficiency and can be used as **operational efficiency characteristic** for the evaluated information system**.** Characteristic $\mathbf{\Delta\Theta_{n2n1}}$ in fact describes usefulness of the information system for the response/support forces.

Because our knowledge about surroundings before getting data from the information system and after getting data has a random character, we can write the following equations for average efficiency characteristics $\mathbf{\Theta_{n1}}$ and $\mathbf{\Theta_{n2}}$

$$\begin{aligned} \mathbf{\Theta_{n1}} &= \mathbf{\Sigma\ \Theta_{n1m} * P(m)}\ , \\ \mathbf{\Theta_{n2}} &= \mathbf{\Sigma\ \Theta_{n2m} * P(m/\wedge m)}\ , \end{aligned} \tag{6}$$

where $\mathbf{\Theta_{n1m}}$ and $\mathbf{\Theta_{n2m}}$ are efficiency characteristics of acting/operation alternatives $\mathbf{n_1}$ and $\mathbf{n_2}$ in the surrounding conditions **m** respectively, **m=0, 1,…, M.**

Response forces always try to choose the acting/operation alternative $\mathbf{n_2}$ that provides maximum value for the expression $\mathbf{\Sigma\ \Theta_{nm} * P\ (m/\hat{}m)}$ for all possible alternatives **n.**

We can generalize very important practical conclusions from the facts mentioned above. Information systems can have positive operational efficiency and real usefulness if and only if all of the three following conditions are present:

- Response forces have more than one acting/operation alternative. In other words, original alternative $\mathbf{n_1}$ is not unique for supporting forces.
- After getting information from the information system and better understanding of the surroundings, it is clear that the alternative $\mathbf{n_2}$ rather than alternative $\mathbf{n_1}$ is more efficient. In other words, if
$$\mathbf{\Theta_{n2} > \Theta_{n1}\ ,\quad n_2 \neq n_1\ .}$$
- Response forces have a real ability to change alternative $\mathbf{n_1}$ to alternative $\mathbf{n_2}$ in regime of almost real time and actually perform this alternative changing.

Even if only one of the mentioned above conditions is not fulfilled, the usefulness of the information system and its operational efficiency is zero. Using that information system for given response/supporting forces is just a waste of time, energy, and money.

2.1.4 Operational-economic efficiency characteristics

Design, manufacturing, use, and maintenance of the information system cost money. The decision making process involved in changing from alternative $\mathbf{n_1}$ to alternative $\mathbf{n_2}$ also costs money. Acting according to a new alternative $\mathbf{n_2}$ instead of alternative $\mathbf{n_1}$ can also require additional spending. All these factors have to be discussed during introduction and consideration of the operation-economic efficiency characteristics.

According to the general understanding of economic efficiency we can define the basic operational-economic efficiency characteristic for response/support forces as
$$\mathbf{E_n = \alpha * \Theta_n / C_n\ ,} \tag{7}$$

where $\mathbf{\Theta_n}$ is average efficiency characteristics for alternative **n** as in paragraph 2.1.3, $\mathbf{C_n}$ is the sum of all average costs that links to the operation alternative **n**, $\boldsymbol{\alpha}$ is a coefficient of proportionality. Characteristic $\mathbf{\Theta_n}$ is measured according to a tactical situation. $\mathbf{C_n}$ is measured in monetary units. Coefficient $\boldsymbol{\alpha}$ is measured in units that provide dimensionless value of the operational-economic efficiency characteristic $\mathbf{E_n}$**.**

If the original alternative $\mathbf{n_1}$ is changed to alternative $\mathbf{n_2}$ according to the data from the information system, the difference

$$\mathbf{\Delta\ E_{n2n1} = E_{n2} - E_{n1}} \tag{8}$$

characterizes increase of the response forces average efficiency and can be used as **operational-economic efficiency characteristic** for the evaluated information system**.** Characteristic $\mathbf{\Delta E_{n2n1}}$ in fact describes usefulness of an information system for the response/support forces in terms of economic efficiency. The higher is the value of $\mathbf{\Delta E_{n2n1}}$**,** the higher is the operational-economic efficiency of the evaluated information system.

For the end user of the information system, computing the characteristics $\mathbf{\Theta_n}$ and $\mathbf{C_n}$ is usually possible. But the value of coefficient $\boldsymbol{\alpha}$ is not so clear. That is why instead of the original/actual value $\mathbf{\Delta E_{n2n1}}$ it is more convenient to use a relative characteristic
$$\mathbf{\Delta_r\ E_{n2n1} = \Delta\ E_{n2n1} / E_{n1}\ .} \tag{9}$$

The relative characteristic $\mathbf{\Delta_r E_{n2n1}}$ does not depend on coefficient $\boldsymbol{\alpha}$**.** By plugging (7) and (8) into (9), we can get two very useful equations:
$$\mathbf{\Delta_r\ E_{n2n1} = (\Theta_{n2} / \Theta_{n1})*(C_{n1} / C_{n2})\ -1} \tag{10}$$

and $$\mathbf{\Delta_r E_{n2n1} = (1+ \Delta C_{n2n1} / C_{n1})^{-1} (\Delta \Theta_{n2n1} / \Theta_{n1} - \Delta C_{n2n1} / C_{n1})} \ , \tag{11}$$

Where $$\mathbf{\Delta C_{n2n1} = C_{n2} - C_{n1}}. \tag{12}$$

Equation (10) illustrates that from the operational-economic efficiency point of view, the evaluated information system is efficient/useful **($\Delta_r E_{n2n1} > 0$ and $\Delta E_{n2n1} > 0$)** if by changing from alternative $\mathbf{n_1}$ to alternative $\mathbf{n_2}$, operational efficiency $\mathbf{\Theta_n}$ grows more quickly than the corresponding costs $\mathbf{C_n}$ or, in other words, if

$$\mathbf{(\Theta_{n2} / \Theta_{n1}) > (C_{n2} / C_{n1})}. \tag{13}$$

In a similar way equation (11) illustrates that from the operational-economic efficiency point of view the information system is efficient/useful **($\Delta_r E_{n2n1} > 0$ and $\Delta E_{n2n1} > 0$)** if by changing from alternative $\mathbf{n_1}$ to alternative $\mathbf{n_2}$ the relative growth of the operation efficiency is higher than the relative growth of the corresponding costs or, in other words, if

$$\mathbf{\Delta \Theta_{n2n1} / \Theta_{n1} > \Delta C_{n2n1} / C_{n1}}\ . \tag{14}$$

If criteria (13) or (14) are not met, the information system is not efficient from the operational-economic efficiency point of view. If it is possible, it is better to spend money just on increasing the number of supporting forces instead of wasting money on the information system.

2.2 Practical computation results

In this paragraph we will consider the surrounding conditions that we can have in reality if we get any data from the information system. We will continue to discuss a simple detector (**^m=0, 1**) and we will base our conclusion on the paragraph 2.1 results. We will use the expressions (3) and (4) in our calculations. All characteristics that are discussed below depend on a priori probabilities **P(1)** and **P(0)**. They also depend on the commonly used and well known probability of detection $\mathbf{P_D}$ and the probability of false alarm $\mathbf{P_{FA}}$ that can be easily estimated during the preliminary field tests of the information system.

2.2.1 Probability of the correct detection

Probability of correct detection $\mathbf{P_{CD}}$ is one of the most important characteristics for the system end user. By definition, it is a conditional probability **P(1/^1).** Results of computing **P(1/^1)** for various $\mathbf{P_D}$, $\mathbf{P_{FA}}$, **P(1)** and **P(0)** are presented in Figure 1 – Figure 4 below.

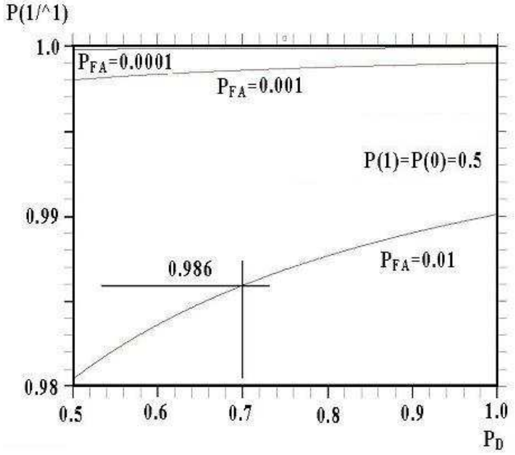


Figure 1. **P(1/^1)** versus $\mathbf{P_D}$ for various $\mathbf{P_{FA}}$.
P(1)=P(0) = 0.5

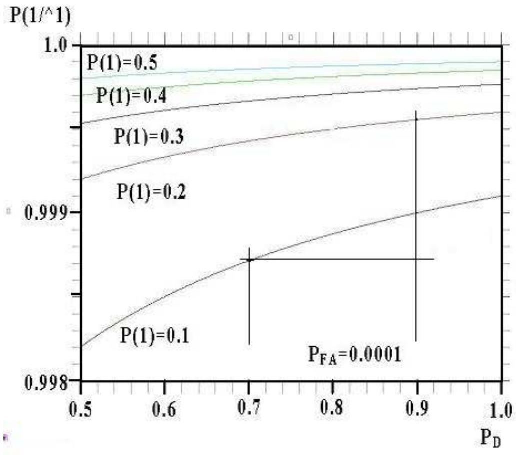


Figure 2. **P(1/^1)** versus $\mathbf{P_D}$ for various **P(1).**
$\mathbf{P_{FA} = 0.0001}$

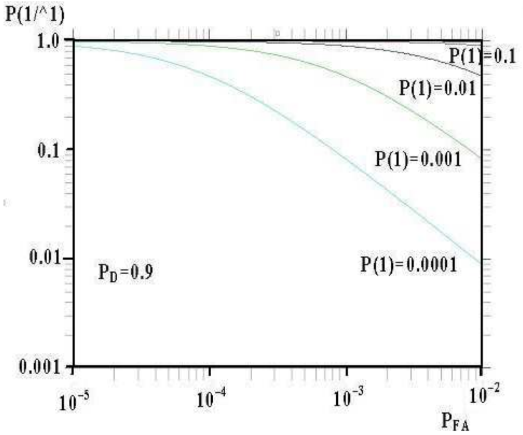


Figure 3. **P(1/^1)** versus **P_{FA}** for various **P(1).**
P_D = 0.9

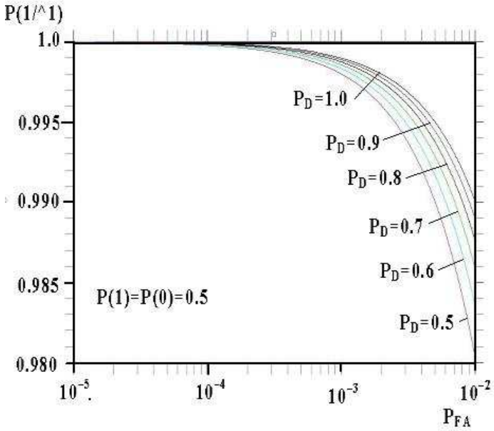


Figure 4. **P(1/^1)** versus **P_{FA}** for various **P_D.**
P(1)=P(0) = 0.5

Designers and end users can use Figures 1-4 for assessment of any practical tactical situation. Analysis of the data from Figures 1-4 allows making the following main general conclusions that are very important for information systems practical use:

- If an information system (simple detector in our case) generates an alarm, it always makes sense to send response forces to find and catch "bad guys". Because even if the detector is not so reliable and has "weak" characteristics **P_D =0.7, P_{FA} =0.01,** probability of the correct detection in this situation is very high: **P_{CD} = P(1/^1) = 0.986!** (See Figure 1.) We assume here that **P(1)=P(0) = 0.5.** It means according to Bayes' postulate that we do not have any specific a priori information about the target presence in the detection area.
- Reducing the false alarm rate (reducing probability **P_{FA}**) is much more important for designers than increasing probability of detection **P_D** in terms of increasing trustworthiness/reliability of the generated alarm and increasing probability of correct detection **P_{CD} = P(1/^1).** (See Figures 1, 4.)
- Very important in terms of increasing trustworthiness/reliability of the generated alarm is a priori knowledge about possible target presence. Increasing a priori probability **P(1)** from **0.1** to **0.2** can give higher increase of **P_{CD}** than increasing probability of detection **P_D** from **0.7** to **0.9**, for example**.** (See Figure 2.)

2.2.2 Probability of false detection (real false alarm)

Probability of false detection **P_{FD}** by definition is a conditional probability **P(0/^1).** (See paragraph 2.1.2.) That probability in fact characterizes real false alarm rate during practical usage of the information system in any tactical situation. Results of computing **P(0/^1)** for various **P_D**, **P_{FA}**, **P(1)** and **P(0)** are presented in Figure 5 – Figure 7 below.

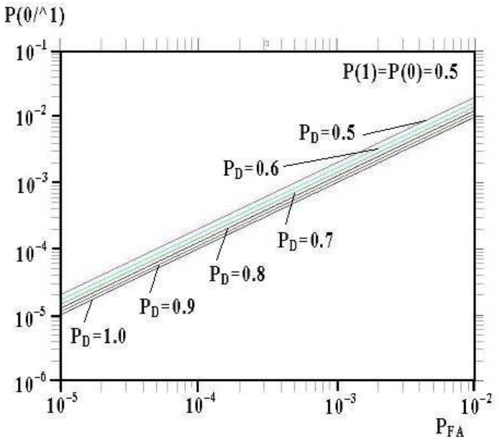


Figure 5. **P(0/^1)** versus **P_{FA}** for various **P_D.**
P(1)=P(0) = 0.5

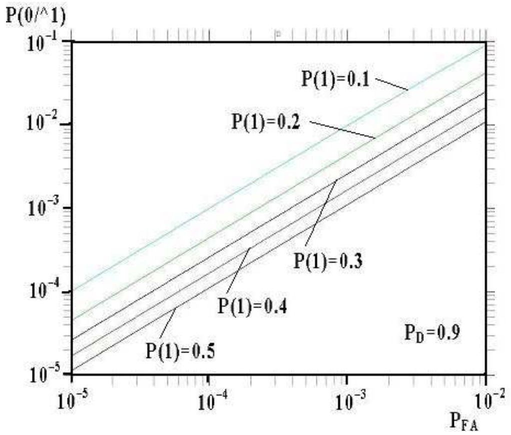
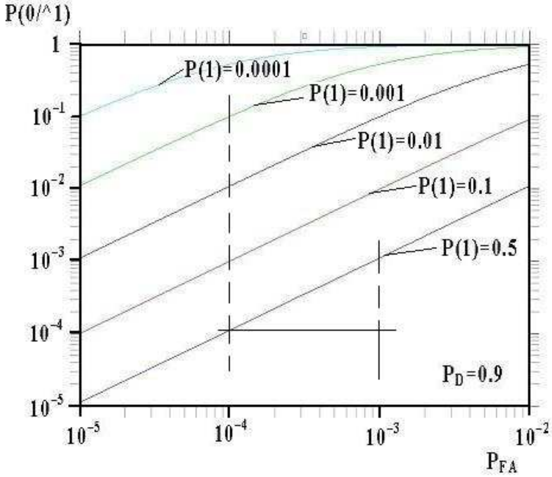


Figure 6. **P(0/^1)** versus **P_{FA}** for various **P(1).**
P_D = 0.9



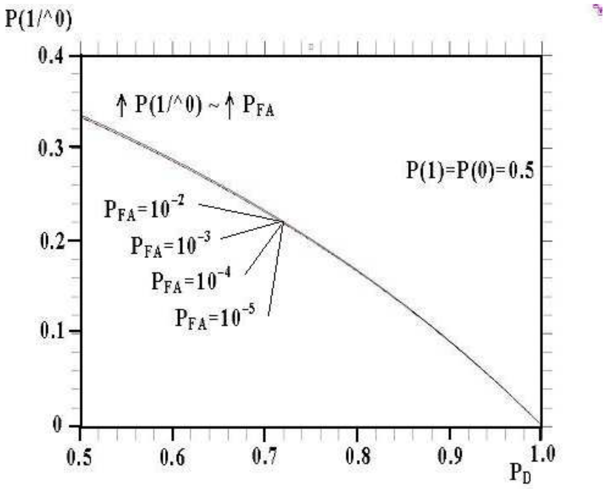


Figure 7. **P(0/^1)** versus $\mathbf{P_{FA}}$ for various **P(1).** $\mathbf{P_D = 0.9}$

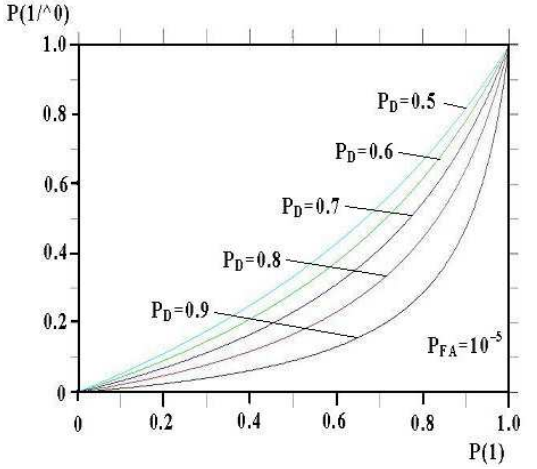
Figure 8. **P(1/^0)** versus $\mathbf{P_D}$ for various $\mathbf{P_{FA}}$**.** **P(1)=P(0) = 0.5**

Analysis of the data from Figures 5-7 allows making the following main general conclusions that are very important for information systems practical use and for decision making for response forces:

- Probability of the false detection $\mathbf{P_{FD}}$**=P(0/^1)** almost linearly depends on traditional false alarm probability $\mathbf{P_{FA}}$. (See Figure 5, 6.)
- Even if the traditional false alarm probability $\mathbf{P_{FA}}$ is low ($\mathbf{P_{FA}\sim10^{-5}}$), but a priori probability of target presence is low as well (**P(1)**~ $\mathbf{10^{-4}}$), the probability of false detection (real false alarm) is high enough ($\mathbf{P_{FD}}$**=P(0/^1)~0.1**). That means that a priori information is very important for the response forces decision making. (See Figure 7.)
- For increasing the trustworthiness/reliability of the generated alarm and reducing probability of the real false detection $\mathbf{P_{FD}}$ **= P(0/^1),** increasing a priori probability about target presence **P(1)** has actually the same importance as reducing the traditional false alarm rate (reducing probability $\mathbf{P_{FA}}$). (See Figure 7.)

2.2.3 Probability of false undetection

Probability of false undetection $\mathbf{P_{FUD}}$ by definition is a conditional probability **P(1/^0).** (See paragraph 2.1.2.) It characterizes the probability of target undetection in a real tactical situation in case of using the evaluated information system. This probability is very important for computing the real detection ability by using a multilayer structure of detection system. Results of computing **P(1/^0)** for various $\mathbf{P_D}$, $\mathbf{P_{FA}}$, **P(1)** and **P(0)** are presented in Figure 8 – Figure 10.



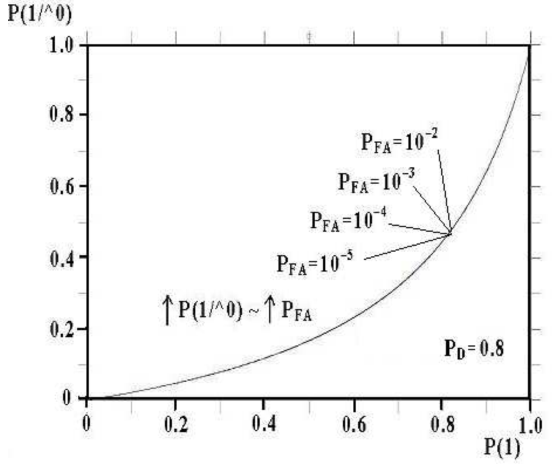


Figure 9. **P(1/^0)** versus **P(1)** for various $\mathbf{P_D}$**.** $\mathbf{P_{FA}=10^{-5}}$

Figure 10. **P(1/^0)** versus **P(1)** for various $\mathbf{P_{FA}}$**.** $\mathbf{P_D}$**=0.8**

Analysis of the data from Figures 8-10 allows making the following main general practical conclusions:

- Probability of false alarm $\mathbf{P_{FA}}$ actually does not have any influence on false target undetection for various a priori data about target presence. (See Figures 8, 10.) With increasing probability of detection $\mathbf{P_{D,}}$ influence of $\mathbf{P_{FA}}$ is reducing and becomes practically insignificant.
- In case of low a priori chance of target presence (**P(1)≤0.1**), probability of false target undetection **P(1/^0)** reduces almost linearly with reducing probability **P(1)**.
- If, for example, the probability of detection is $\mathbf{P_D=0.7}$**,** and we do not have any data about target presence (**P(1)=P(0) = 0.5**), the probability of false target undetection is about **0.235,** which is lower than typically assumed for mentioned data $\mathbf{1\text{-}P_D=1\text{-}0.7=0.3}$**.** For a double layer usage of the aforementioned detector, the probability of false target undetection is $(\mathbf{0.235})^2 \approx \mathbf{0.055}$, which is lower than typically calculated $\mathbf{(0.3)^2 = 0.09}$**.**

3. CONCLUSIONS

This article presents and discusses a system approach to efficiency estimation and evaluation of the various security, intelligence, surveillance and reconnaissance systems as well as unattended ground sensors. The presented approach aims at the end result of the system's function and usage. Proper analysis has to be based on defining and assessment of initial and final goals of the information system use. It is very useful to consider and evaluate three main levels of the efficiency estimation: level of the **information efficiency,** level of the **operational efficiency,** and level of the **operational-economic efficiency.** Taking into account all three levels allows making a reasonable and correct comparison of different information systems at all stages of their life cycle.

Practical efficiency characteristics of the information system help the end user to choose among many systems and then use the selected system in the most efficient way. The entire set of efficiency characteristics defined in this paper is actually stochastic. Corresponding computing procedures and equations are simple enough and can be used for practical purposes every time. It is important to note that the final value of the introduced **information efficiency** characteristic depends on a priori knowledge about possible target presence in the system responsibility/detection area as well as on commonly used and well known from preliminary system testing characteristics like probability of detection and probability of false alarm and also on specific results/data that are generated by information system itself. In addition, **operational efficiency** characteristics and **operational-economic efficiency** characteristics depend on tactical acting/operation alternatives and corresponding costs.

In this paper the most important results are analyzed for a detector such as a simple detector that well represents a variety of unattended ground sensors. Analysis results clearly show that using only traditional efficiency characteristics like commonly used probability of detection and probability of false alarm without taking presented results into account can drastically mislead the end user. The described approach finally allows setting up reasonable technical and structural requirements for information systems and makes trustworthy comparison and practical application planning of such systems. It also allows finding forward-looking perspective ways of systems development.

In the future we are planning to design more detailed mathematical models for various tactical situations and practical applications.

ACKNOWLEDGEMENTS

Dr. Edward M. Carapezza of DARPA is acknowledged for general support of the presented security and defense research. Dr. Daniel J. Pisano of Deming & Pisano LLC is acknowledged for his recommendations and discussion of the presented results. Dr. Lidia Pakhomova of Security&Defense Research LLC is acknowledged for her contribution in editing this manuscript.

REFERENCES

[1] Pakhomov, A., "System for detecting intruder", United States Patent, # 6,529,130, Mar. 4, 2003.
[2] Pakhomov, A., "Perimeter system for detecting intruders", United States Patent, # 6,664,894, Dec. 16, 2003.

[3] Speller, K., E. and Yu, D., "A Low Noise MEMS Accelerometer for Unattended Ground Sensor Application," Proc. SPIE 5417, 63-72 (2004).
[4] Crickmore, R., I., Nash, P., J. and Wooler, J., P., "Fiber optic security systems for land- and sea-based applications," Proc. SPIE 5611, 79-86 (2004).
[5] Pakhomov, A. and Goldburt, T., "Seismic Systems for Unconventional Targets Detection and Identification," Proc. SPIE 6201, 466-477 (2006).
[6] Pakhomov, A. and Goldburt, T., "New seismic unattended small size module for footstep and light and heavy vehicles detection and identification," Proc. SPIE 6562, 656216 (2007).
[7] Pakhomov, A. and Goldburt, T., "Zero false alarm seismic detection and identification systems,“ Proc. SPIE 6943, 694317 (2008).
[8] Shimazu, R., Berglund, V., Falkofske, D. and Krantz, B., "MicroSensor Systems: Detection of a Dismounted Threat," Proc. SPIE 5611, 144-155 (2004).
[9] Edwards, C. and Robinson, C., "Networked Enabled Sensors for the Future Soldier in Urban Warfare," Proc. SPIE 5611, 168-175 (2004).
[10] Van Dijk, G., J.A. and Maris, M., G., "Wireless sensor network for mobile surveillance systems," Proc. SPIE 5611, 185-191 (2004).
[11] http://plato.stanford.edu/entries/bayes-theorem/