and monitoring. In addition to the safety data captured in phase IV trials, all serious, unexpected AEs that occur in the general population that uses the drug must be reported to the sponsor and to regulatory agencies. New or unexpected serious AEs, which are rare, can usually be detected only in postmarketing phase when relatively large numbers of patients use the drug compared to the numbers treated in clinical trials.

One should note, however, that assessment of safety when a drug is widely used is difficult because patient and physician AE reports are *ad hoc* (spontaneous), and the extent of drug usage in the population is usually unknown. Often, once a drug is available, anecdotal evidence and spontaneous reports lead to the perception that usage is associated with an unexpected safety problem. Such perception can lead to a reanalysis of the clinical trial data, additional clinical trials for safety, review of regulatory spontaneous reporting databases, or active surveillance programs.

Various statistical approaches to the identification of potential safety issues (risks) have been proposed using routine databases such as the US food and drug administration (FDA) spontaneous reporting system. For example, Bayesian data mining has been proposed to identify compounds or classes of compounds with safety risks [4–7].

One should note that active postmarketing surveillance can be planned *a priori* or when potential safety issues are identified during drug development. For example, active surveillance is often planned for vaccines that are generally given to healthy subjects, and in many cases to children [8].

References

[1] Chow, S.-C. & Liu, J.-P. (2004). Safety assessment, in *Design and Analysis of Clinical Trials: Concepts and Methodologies*, 2nd Edition, Wiley-Interscience, New York, p. 562–601.

[2] Ellenberg, S.S., Fleming, T.R. & DeMets, D.L. (2003). *Data monitoring Committees in Clinical Trials: A Practical Perspective*, John Wiley & Sons, Chichster.

[3] DeMets, D.L., Furberg, C.D. & Friedman, L.M. (2005). *Data Monitoring in Clinical Trials: A Case Studies Approach*, Springer, New York.

[4] DuMouchel, W. (1999). Bayesian data mining in large frequency tables with an application to the FDA spontaneous reporting system, *The American Statistician* **53**, 177–190.

[5] O'Neill, R.T. & Szarfman, A. (1999). Bayesian data mining in large frequency tables with an application to the FDA spontaneous reporting system: discussion, *The American Statistician* **53**, 190–196.

[6] Louis, T. & Shen, W. (1999). Bayesian data mining in large frequency tables with an application to the FDA spontaneous reporting system: discussion, *The American Statistician* **53**, 196–198.

[7] Madigan, D. (1999). Bayesian data mining in large frequency tables with an application to the FDA spontaneous reporting system: discussion, *The American Statistician* **53**, 198–200.

[8] Iskander, J.K., Miller, E.R., Pless, R.P. & Chen, R.T. (2004). *Vaccine Safety Postmarketing Surveillance: the Vaccine Adverse Event Reporting System*, Centers for Disease Control and Prevention, Department of Health and Human Services. Document 130012.

JUDITH D. GOLDBERG AND BENJAMIN LEVINSON

Safety Pyramid ***see*** Near-Miss Management: A Participative Approach to Improving System Reliability

Sampling and Inspection for Monitoring Threats to Homeland Security

Since the events of September 11, 2001, there has been increased emphasis on monitoring and surveillance to detect and prevent further terrorist attacks. While significant resources have been devoted to the *mechanics* of screening (e.g., improved X-ray equipment, chemical "sniffers"), considerably less attention has been paid to quantifying the efficacy of these surveillance programs.

Given the high volumes of passengers, containers, mail items, and various other inter and intracontinental "movements" an important consideration is the identification of a level of inspection that balances cost, inconvenience, detection success, and

probability of "false triggering". From a statistical perspective, the answer is partly provided by the theory and methods of statistical process control (SPC) and elementary probability theory. However, biosurveillance, syndromic surveillance (*see* **Syndromic Surveillance**), and counterterrorism surveillance (*see* **Managing Infrastructure Reliability, Safety, and Security**; **Game Theoretic Methods**; **Public Health Surveillance**) are fundamentally different from monitoring activities for quality assurance in an industrial manufacturing process. Unlike the industrial setting, where there is generally good information on the performance of the manufacturing process (e.g., percent defective, proportion of nonconforming or "out-of-spec" items), monitoring in the context of bio/homeland security is characterized by extreme uncertainty. For example, because of the nefarious activities of terrorist organizations, security and intelligence organizations do not always know what it is they are looking for. As terrorists become increasingly sophisticated in their modes of attack, our uncertainty in both the likelihood of an attack and which sentinels to monitor increases. Furthermore, considerations of cost and logistics mean that we could never hope to reduce the likelihood or probabilities of such events to zero.

Given both these constraints and uncertainties, one is thus faced with the problem of how best to sample and inspect objects that potentially represent a threat to homeland security ([1] and references therein). These objects could be, for example, containers entering shipping ports with concealed threats such as biological agents, radioactive material or weapons [2]; water reservoirs with threats of contamination; or aircraft with bombs and/or terrorists on board.

Various techniques can be used to model risks and uncertainty [3–5] associated with homeland security, including classical max–min theories, worst-case scenarios (*see* **Premium Calculation and Insurance Pricing**; **Risk Measures and Economic Capital for (Re)insurers**), expert opinion (*see* **Risk in Credit Granting and Lending Decisions: Credit Scoring**; **Operational Risk Modeling**; **Reliability Demonstration**), and Bayesian [6] methods (*see* **Repair, Inspection, and Replacement Models**; **Imprecise Reliability**; **Lifetime Models and Risk Assessment**; **Bayesian Statistics in Quantitative Risk Assessment**). More recently, Information Gap decision theory has been applied to monitoring for homeland security [1, 7, 8].

We present here a simple model for sampling and inspecting generic "objects" to detect threats to homeland security. The model yields rules of thumb that could be used by decision makers to set (upper) limits on the number of objects to be inspected for a given or desired level of risk, or to estimate levels or limitations to risk as a function of the number of objects inspected. The approach can be generalized in various ways, for example, to take account of imperfect detection rates [9] and several monitoring protocols [10] when the underlying probabilities of threats are subject to info-gap uncertainty.

A Model for Sampling and Inspection

Suppose that there are N objects entering an inspection point (e.g., a container port) over a time period of t units (e.g., t weeks), and that n of these objects are sampled and inspected for a particular threat T.

Define p to be the probability that an object contains a T and θ to be the probability that a T is detected if one is present. Assuming that there are no clustering effects or serial correlations, the probability that precisely k of those objects inspected contain a T *and* are detected, *and* that the remaining $N-k$ objects contain no T is $(p\,\theta)^k(1-p)^{N-k}$. Multiplying this expression by $\binom{n}{k}$, the number of ways of choosing k from n, and summing over $k = 0, 1, \ldots, n$ gives an expression for the probability that no T passes undetected over some time period t. The compliment of this probability, *viz*,

$$P_N(n,t) = 1 - [1 - p(1-\theta)]^n\,[1-p]^{N-n} \quad (1)$$

is then the probability that at least one T passes through the inspection point undetected in time t.

Ideally, one would like to minimize $P_N(n,t)$, which is easily seen from equation (1) to occur when $n = N$, i.e., when every object is inspected – which is obvious, although not achievable in practice. Furthermore, since N and n are increasing functions of time t, it follows from equation (1) that $P_N(n,t)$ approaches unity for large t except when $\theta = 1$ and $n = N$. In other words, regardless of the precise values of p, θ, n, and N(except $\theta = 1$ and $n = N$), at least one threat T will eventually pass through the inspection point undetected. To limit risks to homeland security, for example, by imposing a (small) upper bound on $P_N(n,t)$, it is thus clear that one must

impose limits on import volumes (N) over specified time periods (t). For example, if we require

$$P_N(n, t) \leq \pi_c \ll 1 \tag{2}$$

with π_c some specified small number, we deduce from equations (1) and (2), by rearranging equation (1), and taking logarithms that

$$n \log\left(1 + \frac{p\theta}{1-p}\right) + N \log(1-p) \geq \log(1-\pi_c) \tag{3}$$

Assuming $p \ll 1$ (and $\pi_c \ll 1$), we can use the linear approximation $\log(1+x) \approx x (|x| \ll 1)$ to rewrite equation (3) as

$$N \leq \frac{\pi_c}{p(1-f\theta)} \tag{4}$$

where

$$f = \frac{n}{N} \tag{5}$$

is the inspection fraction which we assume, for illustrative purposes, to be a constant.

It follows from equation (4) that the import volume has a finite upper bound except, as noted, when $f = \theta = 1$. In practice, of course, $\theta < 1$ so that regardless of the precise values of π_c, p, θ, and f, equation (4) implies that limits must be imposed on import volumes if one wishes to reduce the chance of threats passing inspection points undetected [2]. It is also clear from equation (4) that if one wishes to increase the upper limit on N for given π_c, or equivalently, decrease the lower limit on π_c for given N, one should choose the largest possible value of the inspection fraction f in equation (5) that is consistent with economic and other constraints. The problem, of course, is that precise values for these limits depend on p and θ which are themselves unknown and uncertain. Nevertheless, equation (4) provides a simple rule of thumb that decision makers could use in practice, using, for example, what-if or worst-case scenario estimates for p and θ.

As an example, suppose that economic constraints limit inspection fractions to 75%, and worst-case estimates are $p = 10^{-4}$ and $\theta = 2/3$. For this scenario, equation (4) gives

$$N \leq \sim 2\pi_c \times 10^{+4} \tag{6}$$

Thus, if we require $\pi_c = 10^{-2}$, say, then equation (6) implies $N \leq 200$; this presumably would impose severe restrictions on the (unit) time period over which one satisfies the likelihood constraint of equation (2). Similarly, if say, 1000 objects pass through an inspection point every month, the condition imposed by equation (2) is only achievable over a 2-month period ($N = 2000$) when $\pi_c \geq 1/10$. In other words, in this scenario over a 2-month time frame, one can only be assured that there is not more than a 1 in 10 chance of at least one threat passing undetected.

Discussion

In this article, we have presented a simple model for sampling and inspection of objects for threats to homeland security. An important general conclusion is that unless one inspects every object entering an inspection point, and unless one has perfect detection rates, at least one threat will eventually pass through the inspection point undetected. We thus need to impose limits on import volumes and periods to limit the chances of threats passing undetected. The simple model presented here can be generalized and extended in various ways by using info-gap decision theory [7] to model uncertainties in the underlying probabilities of threats being present and detected in import objects [1]. In info-gap terminology, the inequality represented by equation (2) is only one of many possible performance requirements that decision makers may consider in arriving at so-called robust-optimal solutions [1] in which there are trade-offs between desired levels of performance and immunity to uncertainty [7]. Generalized info-gap models for homeland security are the subject of ongoing research [9, 10].

References

[1] Moffitt, L.J., Stranlund J.K. & Field, B.C. (2005). Inspections to avert terrorism: robustness under severe uncertainty, *Journal of Homeland Security and Emergency Management* **2**(3), 1–17 Art 3, http://www.bepress.com/jhsem/vol2/iss3/3.

[2] Harrold, J.R., Stephens, H.W. & van Dorp, J.P. (2004). A framework for sustainable port security, *Journal of Homeland Security and Emergency Management* **1**(2), 1–21 Art 12, http://www.bepress.com/jhsem/vol1/iss2/12.

[3] French, S. (1986). *Decision Theory: An Introduction to the Mathematics of Rationality*, Ellis Horwood, Chichester.
[4] Render, B., Stair Jr, R.M. & Hann, M.E. (2003). *Quantitative Analysis for Management*, Prentice Hall, Englewood Cliffs.
[5] Burgman, M.A. (2005). *Risks and Decisions for Conservation and Environmental Management*, Cambridge University Press.
[6] Ouchi, F.A. (2004). *Literature Review on the Use of Expert Opinion in Probabilistic Risk Analysis*, World Bank Policy Research Working Paper 3201, World Bank, World Bank Institute.
[7] Ben-Haim, Y. (2006). *Information-Gap Decision Theory: Decisions Under Severe Uncertainty*, 2nd Edition, Academic Press, San Diego.
[8] Yoffe, A. & Ben-Haim, Y. (2006). An Info-Gap approach to policy selection for bio-terror response, *IEEE International Conference on Intelligence and Security Informatics, ISI 2006*, San Diego, pp. 554–559, May.
[9] Fox, D.R. & Thompson, C.J. (2007). *Risk and Uncertainty in Bio-Surveillance Having Imperfect Detection Rates*, Proceeding 56th session International Statistical Institute, Lisbon Portugal, pp. 22–29.
[10] Thompson, C.J. & Fox, D.R. (2006). Robust monitoring and resource allocation among anti-terrorist protocols, In preparation.

COLIN THOMPSON AND DAVID R. FOX

Scenario Simulation Method for Risk Management

In financial risk management, two types of risk measurements are commonly used. The first type measures the sensitivities of portfolio value to some particular market variables. Usually, a portfolio's risk profile can be described by a large number of those sensitivities. Examples include delta, gamma, and vega (*see* **Risk-Neutral Pricing: Importance and Relevance**; **Weather Derivatives**; **Default Risk**; **Statistical Arbitrage**) in options portfolios, or duration and convexity (*see* **Asset–Liability Management for Life Insurers**) in bond portfolios.[a] The second type is more comprehensive as it calculates the probability distribution of the portfolio value at a given horizon. This then provides common risk measures that summarize the portfolio risk, such as the widely used value at risk (VaR) (*see* **Risk Measures and Economic Capital for (Re)insurers**; **Credit Scoring *via* Altman Z-Score**; **Compliance with Treatment Allocation**), defined as the maximum loss from an adverse market movement with a specified probability over a period of time.

Among the commonly applied methods to estimate VaR, the simplest is "delta approximation" (*see* **Simulation in Risk Management**). The method, however, critically depends on two assumptions: the normality assumption of portfolio value, and the linearity assumption of the relationship between transactions' prices and market variables. For most portfolios, especially for portfolios with options and/or embedded options (*see* **Options and Guarantees in Life Insurance**; **From Basel II to Solvency II – Risk Management in the Insurance Sector**), Monte Carlo simulation (*see* **Simulation in Risk Management**; **Structured Products and Hybrid Securities**; **Reliability Optimization**; **Uncertainty Analysis and Dependence Modeling**) is a more appropriate method. The difficulty with the Monte Carlo approach is its computational burden. To obtain a reliable estimate, the sample size has to be large. Since each sample requires a repricing of the entire portfolio, the required large sample size often makes the Monte Carlo approach impractical.

The scenario simulation method (*see* **Scenario-Based Risk Management and Simulation Optimization**) described here is a computationally efficient alternative to conventional Monte Carlo for multicurrency fixed-income portfolios. Following [1], the model approximates a multidimensional lognormal distribution of interest rates and exchange rates by a multinomial distribution of key factors. While it allows very large samples of correlated yield-curve (*see* **Structured Products and Hybrid Securities**; **Credit Migration Matrices**) joint scenarios, the number of scenarios in each currency is limited, which implies that the number of portfolio evaluations is limited.

Scenario simulation provides the entire distribution of future portfolio returns (see Figures 6 and 7). From this, not only VaR, but standard deviation and other measures of risk, such as the "coherent measures of risk" of Artzner *et al.* [2], can be computed. The scenario simulation model can be applied in