RETURN ON INVESTMENT FROM AUTOMATED, ADAPTIVE MONITORING ALTERNATIVES TO CONVENTIONAL, NON-ADAPTIVE SOLUTIONS: A FORMAL ANALYSIS

Financial Model Overview

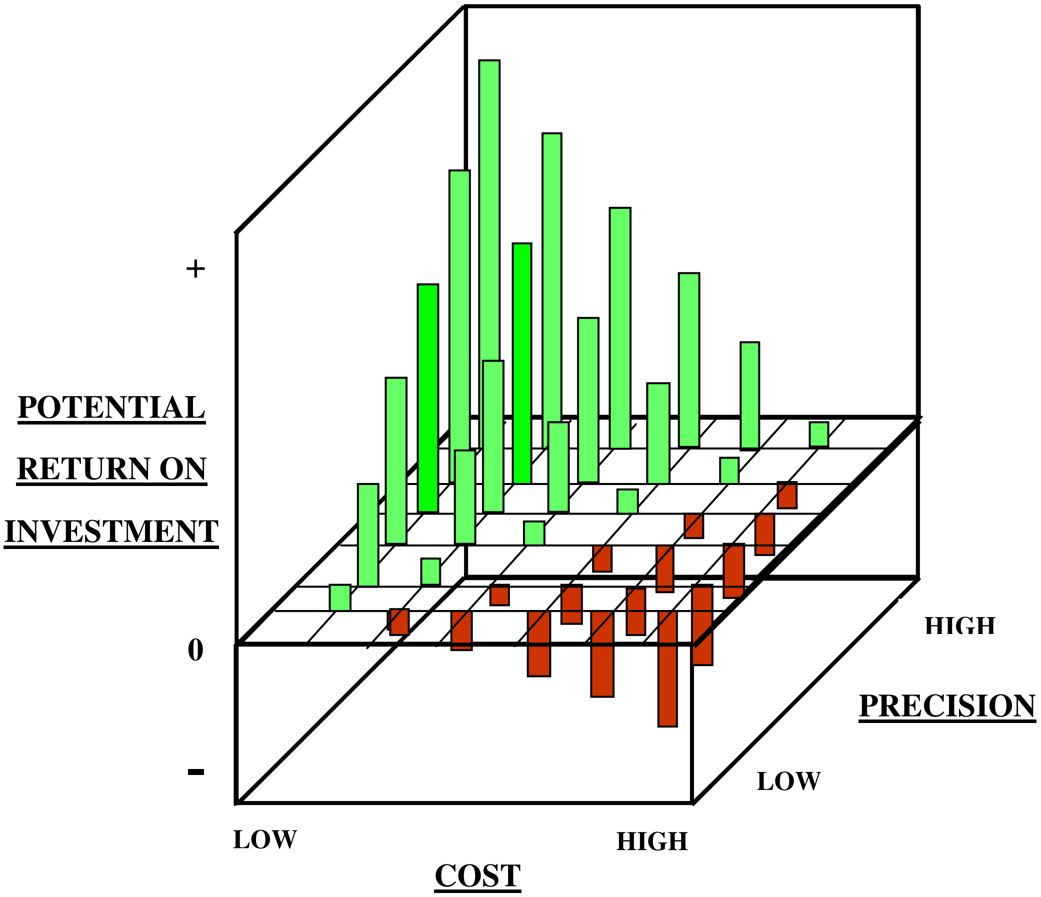

Figure 1. Potential ROI versus Monitoring Precision and Cost.

Figure 1 illustrates a financial model for investing in automated, adaptive (auto-adaptive) monitoring solutions, such as those offered by Brainlike, Inc. As the figure shows, monitoring return on investment (ROI) depends on two key variables, precision and cost. High ROI comes when maximum precision can be delivered at minimum cost. Even with high precision, only marginal ROI comes when costs are high. Likewise, even with low costs, only marginal ROI also comes precision is low. Negative ROI comes when both costs are high and precision is low.

Most conventional, non-adaptive monitoring solutions wind up either in the lower left portion or the upper right portion of Figure 1. Typically, monitoring adds only moderate value in the commercial sector, because commercial implementation is straightforward but imprecise. Alternatively, monitoring adds only moderate value in the defense sector, because defense implementation tends to be much more precise but much more costly. Conventional monitoring solutions that wind up in the upper left quadrant of the figure, like those offered by Brainlike Inc., are hard to find.

To illustrate how precision and cost figure into the ROI picture, results are provided below from a formal financial model that was applied to two scenarios. The ROI figures shown based on delivering one product over a five-year period, and they are risk-adjusted. The ROI figures were derived in terms of incremental ROI from adding auto-adaptive functionality to an existing, non-adaptive monitoring system. Here are the two scenarios:

- Scenario 1. Monitoring to prevent security checkpoint breeches or equipment breakdowns. Examples include border crossings, drug smuggling, equipment thefts, computer crashes, reactor scrams, and planes or boats violating restricted space. Target events occur infrequently, but they are costly. **For this first scenario, the financial model estimates a five-year, risk-adjusted ROI of $17 million**, against an initial investment of $200,000.
- Scenario 2. Monitoring to terrorism disasters at 10 major data centers. Target events under this scenario include airplane or ship bombings, chemical or biological poisonings, missile or troop attacks, and power, internet, or financial center disasters. Target events under this scenario occur much more rarely than under scenario 1, but they are far more costly. **For this first scenario, the financial model estimates a five-year, risk-adjusted ROI of $53 million**, against an initial investment of $200,000.

The formal model that produced these ROI figures and its parameter values are explained in the next section.

Financial Model Details

The names of these parameters and their values under scenarios 1 and 2 are given in Figure 2.

ROI Model Parameters	Scenario 1	Scenario 2
Annual number of monitoring time points	35,040	350,400
Annual expected number of alerts	3,285	100
Annual expected number of target events	120	2
Annual expected number of alerted target events with fixed threshold monitoring	60	1
Annual expected number of alerted target events with auto-adaptive monitoring	120	2
Cost of responding to one false alert	$100	$250,000
Cost of responding to one target event	$1,000	$5,000,000
Cost of not responding to one target event	$250,000	$50,000,000
Initial product development cost	$200,000	$200,000
Final product delivery cost	$200,000	$750,000
Operational design, integration, and testing cost	$500,000	$2,000,000
Annual licensing and maintenance savings	$100,000	$1,000,000
Post-year-one project cancellation probability	0.50	0.50
Post-year-two project cancellation probability	0.15	0.15
Operational deployment failure risk probability	0.10	0.10
Expected Five Year, Risk Adjusted ROI:	**$17,432,500**	**$53,587,500**

Figure 2. Estimated ROI for Two Selected Scenarios.

- Annual number of monitoring time points. A real-time system looking for unexpected activity every 15 minutes would generate 35,040 alerts, which is the assumed number under scenario 1. Ten times that number was used in scenario 2 to reflect a system that would be installed at 10 facilities.
- Annual expected number of alerts. This number depends on the number of alerts that could realistically initiate preventive action. For example, if a sailor on an eight-hour watch were monitoring sensors for unexpected activity such that an alert would result from further sensor investigation, the sailor could reasonably be expected to check out three alerts per shift. The resulting number of alerts that could be dealt with would be 3,285 per year, which was used under scenario 1. Ten times that number was used under scenario 2, to reflect a system that would be installed at 10 facilities.

- Annual expected number of target events. This could range from a very small number of potentially catastrophic events like ship bombings to a fairly substantial number of relatively minor events like security boundary breeches. Under scenario 2, two events per year in the 10 installations being monitored might be appropriate, while under scenario 1,120 events per year might be appropriate. These numbers are intended to reflect only events that are actionable, that is events that could be prevented if properly forewarned.
- Annual expected number of alerted target events with fixed threshold monitoring. This is one of two sensitivity parameters in the financial model. The model compares expected hit rates without auto-adaptive monitoring to expected hit rates with adaptive monitoring. For simplicity, an assumption has been made that a monitoring system exists that is not auto-adaptive, also known as non-stationary. The numbers reflect the assumption that about half the target events that could be detected in the field would indeed be detected by a non-stationary system. For scenario 1 with 120 target events per year, this leads to a value of 60. The same rationale suggests that one out the two annual scenario 2 target events would be uncovered quickly enough to initiate preventive action, using auto-adaptive monitoring.
- Annual expected number of alerted target events with auto-adaptive monitoring. This is the remaining sensitivity parameter in the financial model. Both scenarios assume that all target events will be uncovered with auto-adaptive monitoring. This assumption may seem strong at first, but it’s tied directly to target events being actionable. Assuming that auto-adaptive monitoring is the most precise monitoring possible in terms of identifying actionable target events, this perfect hit rate assumption makes sense — given that target event numbers are only those that are actionable.
- Cost of responding to one false alert. This amount reflects the cost of checking out a potential problem only to discover that it’s a non-problem. This number may range from a small amount associated with having an expert check out an equipment problem (along with the cost of staffing that expert) such as under scenario 1, to a much larger number associated with shutting down a portion of an airport or taking other action of a similar magnitude under scenario 2. The assumed value of $100 reflects the former case and $250,000 reflects the latter case.
- Cost of responding to one target event. This amount, which reflects the cost of taking effective preventive action, is typically an order of magnitude larger than its false-alert response counterpart. Scenario 1 examples — which would include preventing a computer crash, a reactor scram, a security barrier breech, or a high-jacking from happening — may require moving applications to another server, switching feed pumps, or sending out a security squad. Scenario 2 examples might be shutting down an airport or scrambling a fighter squadron. The parameters provided in Figure 2 reflect related costs under both scenarios.
- Cost of not responding to one target event. This parameter is the largest cost driver in the financial model. This cost was set at $250,000 under scenario 1 and $50 million under scenario 2. The scenario 1 figure might be too high for some events such as inadvertent, minor security zone crossings. However, it could easily be far too low for others, such as equipment or security breakdowns that result in costly incidents.

The selected scenario 2 figure could arguably be small or large, depending on particular scenario assumptions.

- Initial product development cost. This amount reflects initial contract funding, which was set at $200,000.
- Final product delivery cost. This value was set at $200,000 under scenario 1 and $750,000 under scenario 2.
- Operational design, integration, and testing cost. This amount reflects Phase III costs, which would support delivering a fully tested, auto-adaptive monitoring system. These costs have been estimated $500,000 under scenario I and $2,000,000 under phase II.
- Annual licensing and maintenance savings. This number reflects the difference between having the auto-adaptive system and an alternative system, which would require occasional tuning to satisfy novel and changing field conditions. The savings shown below under scenarios 1 and 2 assume that $100,000 per year would be saved per installation through continuous, auto-adaptive tuning.
- Post-Year-One Cancellation Probability. The expected ROI model includes adjustments for possible project cancellations. Under both scenarios, the assigned likelihood of 0.5 reflects an estimated 50% chance that contract support would end after year one.
- Post-Year-Two Project Cancellation Probability. Under both scenarios, assigned likelihood of 0.15 reflects an estimated 15% chance that contract support will terminate at the end of year two.
- Operational deployment failure risk probability. Under both scenarios, the assigned likelihood of 0.10 reflects an estimated 10% chance that after all screening, evaluation, and deployment work that has been completed, the system will still not add sufficient value to warrant operational use.