

Safeguarding the Distribution System: On-line Monitoring for Security and Enhancing Operational Performance

By Dan Kroll
Chief Scientist, Hach Homeland Security Technologies
5600 Lindbergh Drive, Loveland, Colorado, USA
970-663-1377 ext. 2637

Introduction

Since the 9/11 attack on the US, the vulnerability of drinking water supplies to assault by terrorists has gained widespread attention. While most supply sources have limited vulnerability due to the massive volumes of water involved, the distribution systems remain an accessible and tempting target as was clearly stated in a recent General Accounting Office report to the US Congress. Terrorists could compromise a system through an assault anywhere in the distribution network through a backflow event. Due to the size and scope of the distribution system, this vulnerability cannot be addressed through enhancing physical security. Distributed monitoring is the only way to detect and mitigate the effects of such an attack.

- May 1983 – Israel uncovers Israeli Arab plot to poison Galilee water with “an unidentified powder”.
- February 2002 – Al Qaeda arrested with plans to attack U.S. embassy water in Rome with “cyanide”.
- December 2002 -- Al Qaeda operatives arrested with plans to attack water networks surrounding the Eiffel Tower neighborhoods, Paris
- April 2003 -- Jordan foils Iraqi plot to poison drinking water supplies from Zarqa feeding U.S. military bases along the Eastern desert.
- September 2003 -- FBI bulletin warns of Al Qaeda plans found in Afghanistan to poison U.S. food and water supplies.

The ability to detect an event in the distribution system and then identify it would be of incomparable value in responding to an incident in a timely and proper manner.

The general scientific consensus is that no practical, available, or cost-effective real-time technology exists to detect and mitigate intentional attacks or accidental incursions in drinking water distribution systems. Over the past several years a new approach has been developed to address the problems of distribution system monitoring. The developed system employs an array of common analytical instrumentation, such as pH and chlorine monitors, coupled with advanced interpretive algorithms to provide detection/classification-response networks that are capable of enhancing distribution system security and operations. The instrumentation has been challenged with, and found effective against a variety of agents including TICs (toxic industrial chemicals), TIMs (toxic industrial materials), and chemical and biological warfare agents.

The response of these various agents is not only adequate to detect the presence of a contaminant, but the responses elicited from the sensor array allows for the possibility of classification. Through the use of a searchable library of agent profiles, the system described is capable of providing not only an alarm, but also a classification of the likely cause. The profiles of over 80 of the most likely threat agents and common contaminants have been compiled. In addition, a proprietary baseline estimator dramatically and

immediately reduces unknown warnings due to regular fluctuations in operational parameters upon start-up. As time since deployment increases, the number of unknown deviations from baseline is rapidly reduced to near zero by the system's programmed ability to learn what is normal for a given operation.

Selection of Parameters to be Measured

When the system was developed there were a variety of possible answers to the question of what instrumentation technology to use, MEMs technology, lab on a chip, GC-MS, Raman Spectroscopy, etc. With the goal in mind of creating a cost-effective system that could be rapidly deployed and was both robust in operation and diverse in its ability to detect contaminants, it was decided to investigate the possibility of using a variety of well characterized, off-the-shelf sensors proven to be robust for field deployment in a multi-parameter array. The sensors chosen for investigation were pH, Conductivity, Chlorine Residual, Turbidity, and Total Organic Carbon (TOC). Data was collected for Oxidation Reduction Potential (ORP), but it was not used in the final system because the probes are unstable and prone to fouling in long term installations.

The Problem with Real World Data: Can We See the Candle Before the Sun?

Real world baseline data is not always as neat and tidy as a laboratory system. Significant fluctuations can occur on a regular basis in real world systems. The problem then becomes, can we differentiate between the changes that are seen as a result of the introduction of a contaminant and those that are a result of everyday system perturbation?

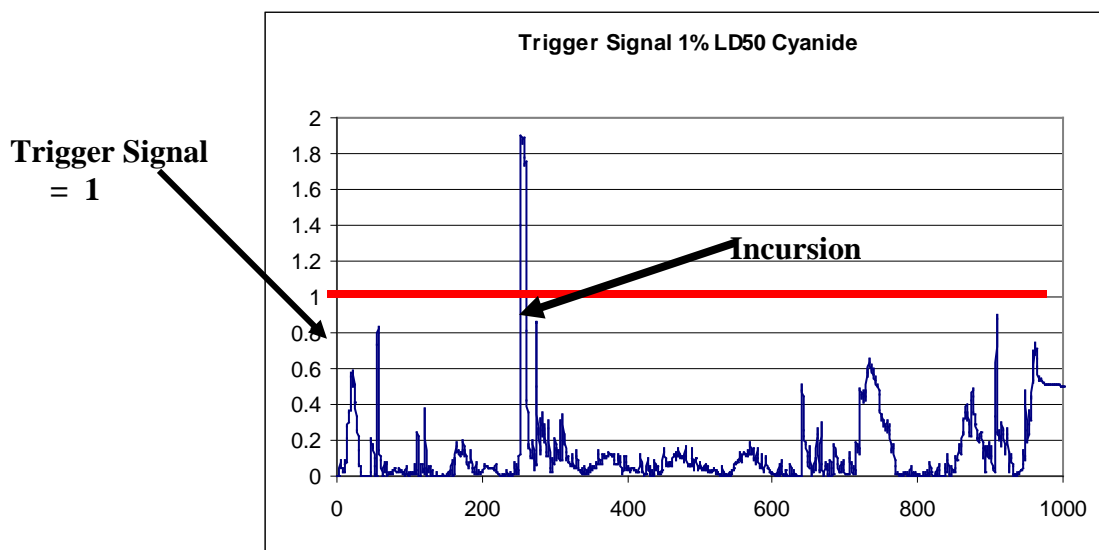
The secret to success, in a situation such as this, is to have a robust and workable baseline estimator. Extracting the deviation signals in the presence of noise is absolutely necessary for good sensitivity. Several traditional methods of baseline estimation were investigated and found to either degrade sensitivity or result in unacceptable numbers of false positives. Finally, a proprietary method was derived and found to be effective.

How the Trigger System Works

In the system as it is designed, the signals from all of the instruments are processed from a 5-space vector to a scalar trigger signal. The signal then goes through the proprietary baseline estimator. A deviation of the signal from the estimated baseline is then derived, a gain matrix is applied, and then compared to a threshold level.

Testing the Trigger System

Real world data was obtained from several sites and the most noisy data stream for each parameter was selected and used to test the system. Even with extremely noisy data the trigger signal typically remains below a threshold level set at 1. Therefore; during normal operation, with no agent present, the typical process deviation should not be large enough to produce a Trigger Signal > 1. However when the data for a cyanide incursion at 1% of the LD-50 or approximately 2.8 mg/L is superimposed on the system the trigger level of 1 is easily exceeded. See Below. Other contaminants exhibit similar results.

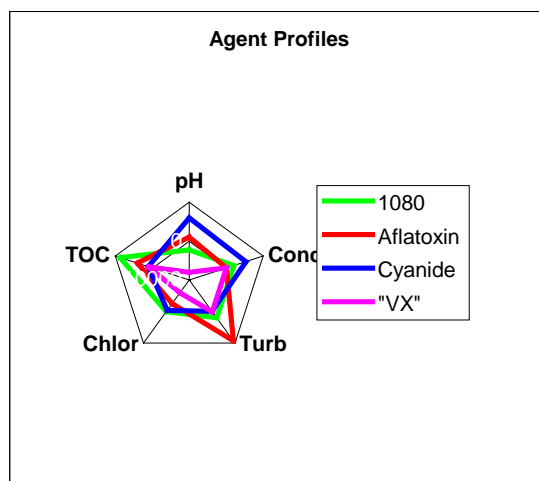


When the amount of cyanide in the system is increased to 10% of the LD-50 the results are even more dramatic.

Deviation/Classification Algorithm

The deviation vector that is derived from the trigger algorithm contains significantly more data than what is needed to simply trigger the system. The Deviation Vector's magnitude relates to concentration and Trigger Signal, while the Deviation Vector direction relates to the agent characteristics. Seeing that this is the case, laboratory agent data can be used to build a Threat Agent Library of Deviation Vectors. A Deviation Vector from the water monitor can be compared to Agent Vectors in the Threat Agent Library to see if there is a match within a tolerance. This system can be used to classify the agent when present. Each vector results in a vector angle in n-space that is representative of the class of chemical present. The graph below is a radar plot of some agent data that visually illustrates this point.

Graph 14. Radar Plot of Agent Deviations



The direction of the vector is unique for a given class of agent, allowing the algorithm to classify the cause of a trigger.

Fig. 3. Detection Algorithm Added to Trigger

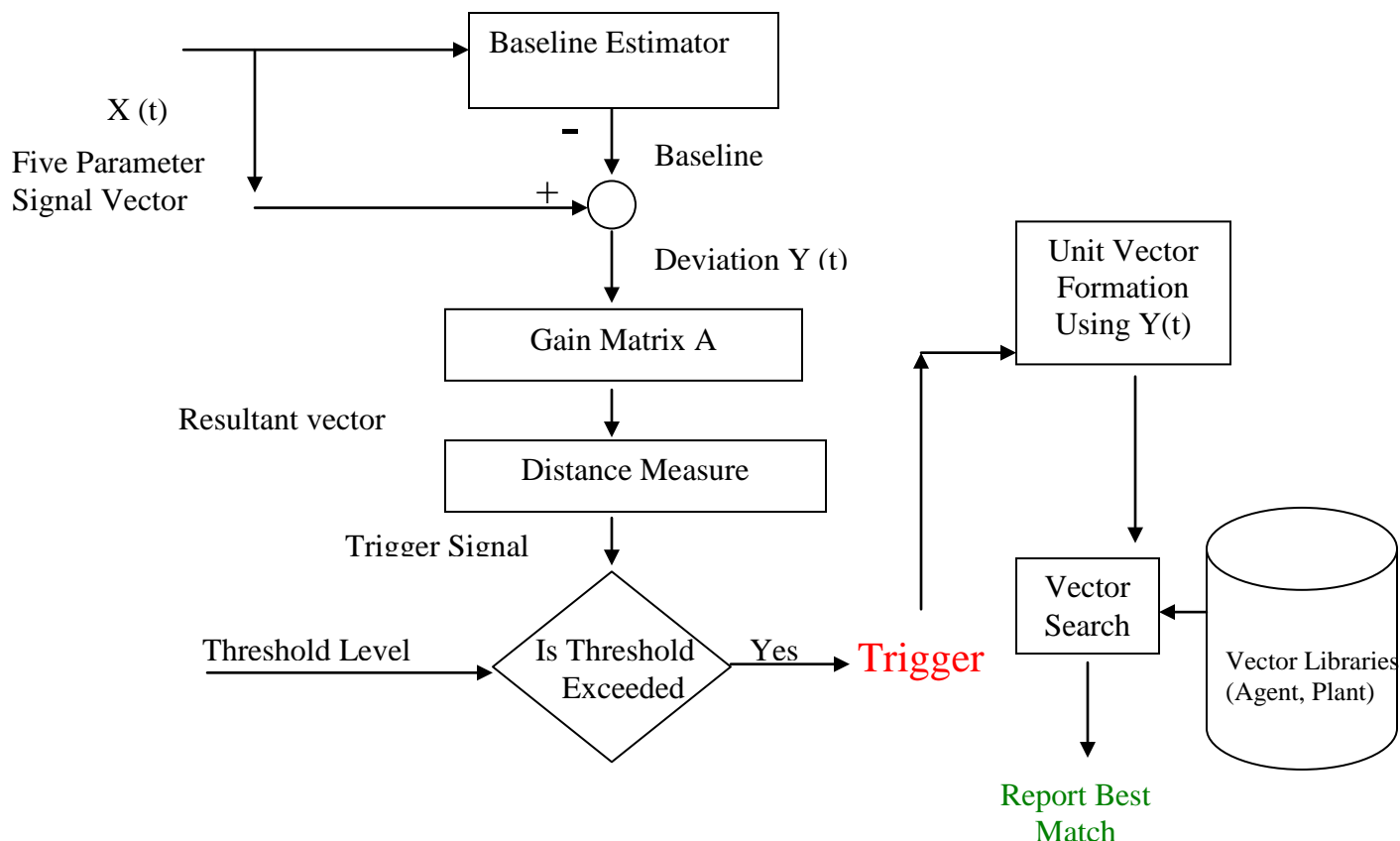


Table 4. MDLs for Selected Agents as a Percentage of LD-50

AGENT	TRIGGER	CLASSIFY
Aflatoxin	0.37	1.00
Aldicarb	0.66	0.70
Cyanide	0.50	0.15
Nicotine	0.80	3.30
Oxamyl	2.50	2.60
Sodium Fluoroacetate	1.00	4.80
Strychnine	0.70	1.50

Conclusion

The system described has made use of robust, off-the-shelf sensor technologies by placing them together in an array and using intelligent algorithms in a new and powerful manner to extract data that is of interest in devising an early warning system for water security. The system has been shown to be effective versus a wide variety of threat agents. The use of a unique system for estimating the baseline in real world

systems allows for the identification of small deviations from normal readings in water analysis parameters. This in turn leads to a system capable of triggering on these deviations. Once the system has been triggered, the algorithms have been shown to be capable of utilizing the unique profile represented by a threat agent's deviations to classify that threat agent or event type.

The system also has the capability to learn day-to-day deviations that are unique to a given system. Events that occur commonly will be rapidly learned, and the rate of unknown events will rapidly decrease. Over all, the system is an invaluable security tool for recognizing system incursions, but it has the ability to become much more than that. Hopefully most systems will never be in need of the security aspect of this system, but there are other dimensions to the system that should find use in any location. To date, most of the library work has been done on threat agents, but as time allows, the libraries will be expanded to incorporate common distribution system problems that may arise. Also, as an individual plant library recognizes deviations and the operators are able to identify them, the system will become a useful tool in evaluating the day-to-day system health and operational parameters.

The system is currently undergoing advanced testing using threat agents at the US Army's Aberdeen Proving Grounds and has recently undergone Environmental Technology Verification testing by Battelle at the USEPA's Test and Evaluation Facility in Cincinnati, Ohio.

The Algorithm resides in the Event™ Monitor Trigger System, which can take data from the Water Distribution Monitoring Panel or the PipeSonde In-pipe Sonde along with TOC. Installation with the sonde trades sensitivity for smaller size, lower cost and in-pipe installation.

