

Broad Spectrum On-Line Security Monitoring for the Detection and Classification of Bio/Chem Events in Drinking Water Distribution Systems

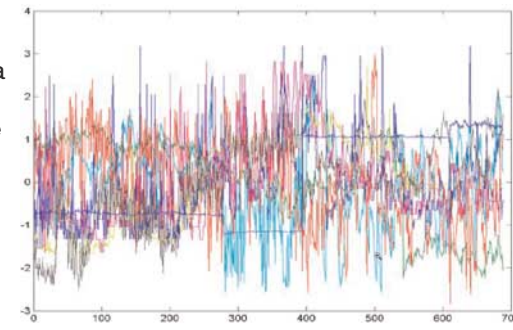
Dan Kroll and Karl King, Chief Scientists, Hach Homeland Security Technologies

Introduction

Drinking water distribution systems, as they are currently configured, are vulnerable to attack. While most supply sources are limited in their vulnerability due to the volume involved, the distribution systems remain a vulnerable and tempting target as stated in a recent GAO report to congress, listing the distribution system as the largest security risk.

THE PROBLEM WITH REAL WORLD DATA.

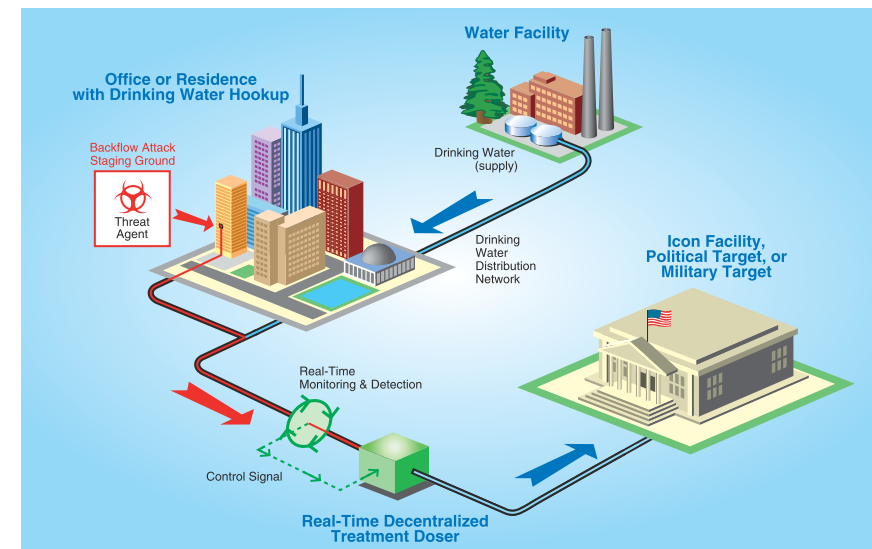
Real world baseline data indicates significant fluctuations can occur on a regular basis. The challenge is to differentiate between the changes that are seen as a result of the introduction of a contaminant and those that are a result of everyday system perturbation?



Real World Auto-Scaled Data

CAN COMMON PARAMETER MONITORING BE USED IN NEW WAYS TO DETECT AND IDENTIFY SYSTEM INCURSIONS?

Backflow events are not just theoretical; they have already taken place. In addition to terrorist attacks, domestic accidents have resulted in illness and death.



A Typical System Can Be Easily Compromised Through a Backflow Event

Hypothesis

The developed system employs an array of common analytical instrumentation, coupled with advanced interpretive algorithms to provide detection/ identification-response networks capable of enhancing system security.

WHAT SENSORS TO USE...AND WHY.

Sensor selection was based on reliability and ability to measure fundamentally different characteristics of threat agent substances.

SENSOR SET SELECTED

pH.....acid/ base relationships

Conductivity (electrolytic)ionic concentrations

Chlorinedisinfectant levels, oxidant reduction

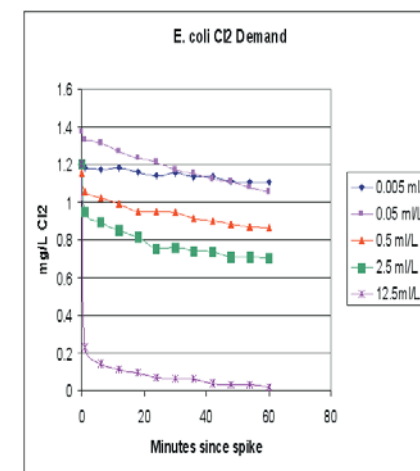
Turbidityparticles in water (bio agents)

Total Organic Carboncarbon content of organic molecules

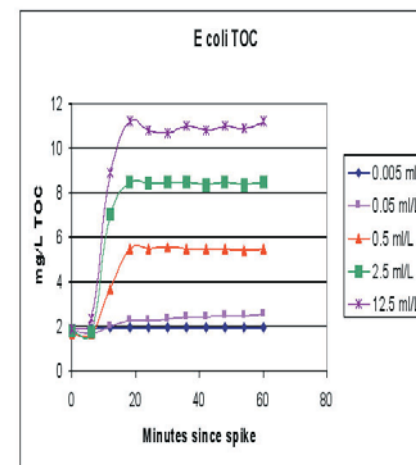
ORP - NOT SELECTEDbecause it is unstable and prone to poisoning in long-term installations

TYPICAL RESPONSE DATA.

All of the tested agents showed a distinct change in one or more of the measured parameters. As an example some of the data for *E.coli* is presented below.



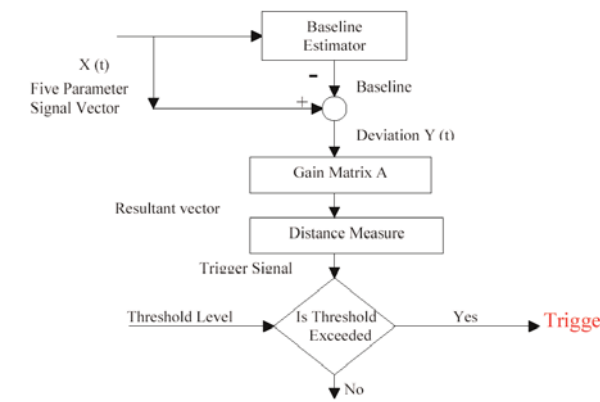
18-hour old *E.coli* cultures grown in EC media.



Implementation

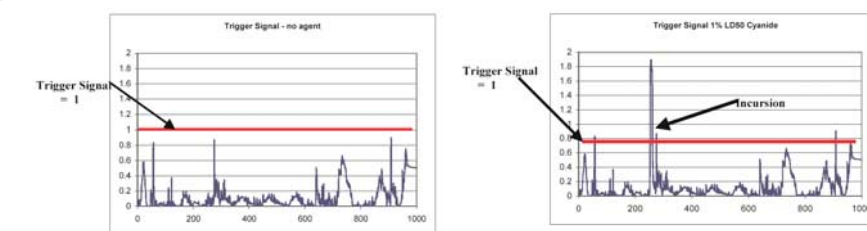
The signals from all of the instruments are processed from a 5-space vector to a scalar trigger signal in an event monitor. The signal then goes through the proprietary baseline estimator. A deviation of the signal from the estimated baseline is derived, a gain matrix is applied, and compared to a threshold level. If the signal exceeds the threshold the trigger is activated.

HOW THE SYSTEM TRIGGERS AN EVENT.



SIMULATION OF AGENT ADDITION.

Real world data was obtained from several sites and used to test the system.



HOW WELL DOES THE SYSTEM WORK?

The system has the ability to trigger and classify at very low concentrations when exposed to the compounds of interest. The table below lists the % of LD-50* for various compounds at which the system triggers and at which it is capable of making a classification.

Agent	% LD-50 to Trigger	% LD-50 to Classify
Aflatoxin	0.37	1
Aldicarb	0.66	0.7
Cyanide	0.5	0.15
Nicotine	0.8	3.3
Oxamyl	2.5	2.6
Sodium Fluoroacetate	1	4.8
Strychnine	0.7	1.5

*The LD-50 is defined as the amount of the compound that would kill 50% of the population of adult males with a weight of 70 kg after consuming 1 liter of water.

Testing

If for some reason one of the instruments were to fail, what would be the effect on the system's ability to trigger on a given agent? The effect of losing an instrument or deploying a system without the full array of sensors is dependent upon what agent is present. The table below lists a number of potential contaminants along with the sensors.

WHAT IS THE EFFECT OF LOSING A PARAMETER?

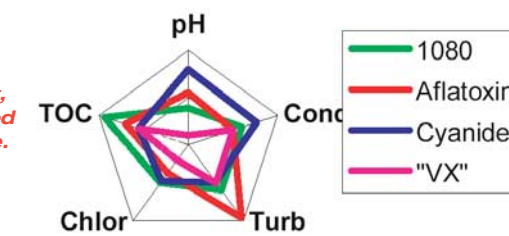
Ratio: concentration needed for trigger with parameter absent/ concentration needed with parameter present.

Agent	Turb	pH	Cond	Chlorine	TOC
Thallium*	1	1.27	4.32	1	1
Cyanide	1	1.18	1.03	1	2.9
VX	1	1	1	1.05	8.5
Methomyl	1	1	1	1.14	8.8
Aflatoxin	1	1	1	1.18	4.5
<i>E. Coli</i>	1	1.08	1	1.1	5.8
Arsenic*	1.56	1.13	1	1	1
Nicotine	1	1.15	1	1.32	2.3

*no carbon

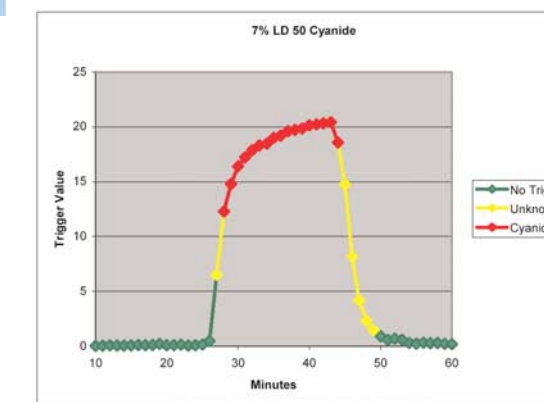
RADAR PLOT OF AGENT DEVIATIONS.

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.



Each vector results in a vector angle in n-space that, from the research conducted so far, appears to be unique.

TESTING THE COMBINED DETECTION/IDENTIFICATION SYSTEM.



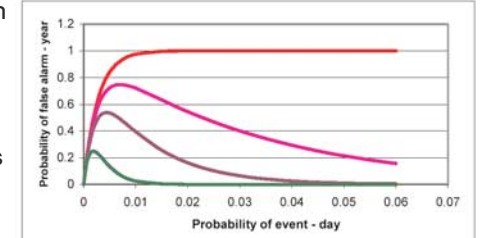
Multiple methods were used for testing the combined system, including spreadsheet models and Monte Carlo simulation. Finally the system was verified with lab tests using Cyanide, Sodium Fluoroacetate (1080), Nicotine, and Aflatoxin.

Trigger Signal for Cyanide Slug Flow at 7% of LD-50

Analysis

REDUCTION OF FALSE POSITIVES VIA HACH LEARNING ALGORITHM

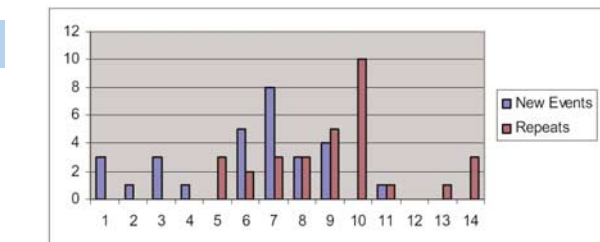
The unknown alarm rate when the system is tracking real world data is quite low. The system is equipped with a learning algorithm, so that as unknown alarm events occur over time the system has the ability to store the signature that is generated during the event.



Learning period = 0, 30, 90, 365 days
P(unknown event) = P(not learned)*P(event)

LEARNING EXPERIENCE.

Events that occur frequently will be quickly learned while rare or singular events will take longer to learn. This should result in a fairly rapid drop off in the number of unknown events as common events are quickly learned.



There were 26 unique events over 11 days of operation. All were learned, 16 of them were repeated.

Conclusion

The system described uses 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 use of a unique system for estimating the baseline in real world systems allows for the identification of small deviations from normal readings. 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. Laboratory procedures on over 80 agents to date have shown no significant overlap of profiles. 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, and hopefully most systems will never need the security capabilities of the system. In addition, the system provides many operational benefits useful in evaluating day-to-day system health and operational parameters.