

Countering the Terrorist Threat to Water: Using Intelligent On-line Monitoring: Today!!!!

By Dan Kroll Chief Scientist and Karl King Chief Technologist
Hach Homeland Security Technologies

ATTACKS ON WATER: FACT OR FICTION?

Scene 1 A small Midwestern city somewhere in the United States:

The man had been watching CNN now every day for months waiting for the message. He knew he was not the only one poised to strike. There were others like him scattered throughout the country. He had been waiting over a year for the message from Ossama. Some reports said that the leader had been killed in the earthquake in Pakistan but he didn't believe it and was diligent in checking the news everyday for the message.

At last a new message! "*CNN reports that al Jezeera has received a copy of a new taped message from Ossama bin Laden.*" Was this the tape that contained the code to strike imbedded in the message or another false alarm? Other messages had come without the all-important code to begin the attack. Would this be the one? He quickly went to his laptop computer and searched on the Internet for the full text of the message. There it was. "*The swimmer in the sea does not fear rain.*" That was the signal for him and the other cells to strike.

He quickly accessed the Internet and purchased tickets back home for early the next morning. He went to the basement of the rented house and checked the hookup of the pump to the water pipe. All appeared to be in order. He had already disabled the backflow prevention device that could have thwarted his plans. He spent the rest of the evening mixing and dissolving the chemicals he had been stockpiling for the past several months in the large tank hooked to the pump. When all was prepared he went back upstairs and set the alarm for 4:30. His flight was at 9 AM.

He awoke with a smile on his face. He had rested well. After getting dressed and loading his bag in the car, he went back down to the basement and turned on the pump. At that point he gave a little laugh knowing full well that he would be half way around the world before the first casualties began to exhibit symptoms. He was a small part of the great plan in which he and others would simultaneously attack water systems across the country this morning.

The rented pump kicked into action slowly injecting the toxic stew the terrorist had concocted into the pipes that supplied the water for the house. Slowly the poison pushed out into the distribution system. Within a few moments it had reached the main water trunk line beneath the street in front of the house and began its deadly spread throughout the distribution system.

Scene 2: 5:00 AM Home of the local water utility manager:

The pleasant aroma of fresh coffee and frying bacon spread through the house. There was nothing like a leisurly breakfast to begin the morning. His pager began to buzz as soon as he sat down. It was the line indicating a water quality excursion being detected by the on-line monitoring platforms he had recently persuaded the city fathers to install. He quickly went to his laptop computer to see what the alarm details were. These alarms had happened in the past. Usually when he pulled up the screen it was just a spike

in turbidity caused by a road crew jack hammering above the pipes or something of that nature. The system usually identified the excursion as a typical plant event or as an unknown that warranted further investigation. As the system had been deployed for several weeks, these types of alarms were becoming less frequent as common plant events were learned and classified by the system. As he pulled up the screen he could immediately recognize that this event was different.

The usual alarm signal was around 2-4 when it went off and they once had one as high as 7 when they had added the wrong concentration of caustic at the water treatment plant. This one however was over 30 and was flashing a tentative identification of an organophosphate pesticide. He quickly went to the phone and dialed the field technician on duty. "Jack this is Bill. The monitoring alarm is going off down at the 4th street monitoring station. I've never seen one quite like this. Go down and see if there is something wrong with the instruments. Maybe some kids got in and messed with them. Take the test kit along too and run a pesticide test strip right away if there is nothing obviously wrong with the instruments. They are indicating a possible pesticide incursion. Call me back when you get any info."

Twenty minutes later the phone rang. It was Jack. He had made it to the station. The instruments appeared normal and showed no signs of tampering, so he had run a pesticide test. It indicated a positive for acetochlinesterase inhibitors an indicator of possible contamination with pesticides or nerve agents. The total organic carbon (TOC) reading on the on-line instruments was also pegged out and the chlorine residual was down to zero. Something serious was going on.

"OK Jack. Take some samples to the lab for further analysis. I am not going to wait. I am going to initiate the emergency response protocol immediately. The 4th street station is the only one going off so far. Start looking for responses from other stations and get those samples tested right now." In a matter of minutes reverse 9-11 calls had gone out to all local residents not to come into contact with or drink the water. Local police and fire officials began to go door to door in the indicated neighborhoods to spread the news. Local television and radio stations carried the warning.

This city was lucky. Only a few residents were exposed before the warning went out. The hospital was informed of the tentative classification of the toxin before the first patients arrived so proper treatment to counteract the toxins could be applied immediately. No one died. Bill also gave the order shortly after the initial confirmation by test kit to isolate that portion of the water supply. Only a small portion of the city was affected.

Dozens of other cities targeted that day were not so lucky. They were not equipped with advanced monitoring technology. They relied upon occasional grab samples and customer complaints to indicate problems in the distribution system. Their first indication that an attack was occurring was when very sick people began to show up at the hospital. No warnings were issued. There was no reason to suspect that the water supply was causing the illnesses. With no information to go on, in many cases treatment was delayed. 10's of thousands were made ill and hundreds died. The unwarned systems were not able to isolate the attack. To compound the horrendous loss of life they were stuck with wide spread contamination in their systems that would end up costing millions to clean and refurbish. One city in the desert southwest had to be evacuated. Lawn

sprinklers had disseminated the persistent toxic compound used in that attack into the air and on to the soil. The clean up would take years.

Some critics will maintain that scene 1 is nothing more than pure fiction suitable as a script for an episode of "24" and that the type of monitoring system described in scene 2 is a far off dream. These so called experts are simply ill informed. Studies conducted by researchers from the U.S. Air Force, the U.S. Army Corps of Engineers and Hach Homeland Security Technologies (HST) have shown that an attack on drinking water distribution systems can be mounted for between \$0.05 and \$5.00 per death, using rudimentary techniques, and amass casualties in the thousands over a period of hours. The technology to mount such an attack is well within the capabilities of terrorists. That water supplies are a target is also reinforced by the fact that domestic terrorist and fringe groups have shown continued interest in using a Chemical, Biological, or Radiological (CBR) agent in their attacks and terrorist groups have also exhibited interest in water supply systems. The present state of on-line monitoring is such that the ability to detect such attacks in a timely manner, so that response actions can be put into play in a rapid fashion, is not a "pipe" dream but exists today.¹

OUR WATER SUPPLIES ARE VULNERABLE.

The realization that our water supplies are vulnerable to sabotage is not a recent discovery made after the attacks of 9/11. As early as 1941, FBI Director J. Edgar Hoover wrote, "Among public utilities, water supply facilities offer a particularly vulnerable point of attack to the foreign agent, due to the strategic position they occupy in keeping the wheels of industry turning and in preserving the health and morale of the American populace. Obviously, it is essential that our water supplies be afforded the utmost protection."² The US Military also recognized the threat prior to 9/11. The historic department of defense policy that requires domestic military base to rely on local utility infrastructure whenever possible was recognized as a threat by Major D. C. Hickman in his visionary report issued in September of 1999 entitled "*A Chemical and Biological Warfare Threat; USAF Water Systems at Risk.*"³ There is a long history of water being vulnerable to such attacks. See Table 1.

These incidents and others indicate that water supplies are recognized as a viable and desirable target by terror minded individuals. Water attack is a recognized and documented means of inflicting mass casualties. Mass casualties are a stated goal of Al Qaeda. Suleiman Abu Ghaith one of Osama bin Laden's closest friends and allies, said on an Islamic website that the terrorists planned to attack the US with chemical or biological weapons. September 11 was "*only a start. We have the right to kill 4 million Americans - 2 million of them children - and to exile twice as many and wound and cripple hundreds of thousands. It is our right to fight them with chemical and biological weapons, so as to afflict them with the fatal maladies that have afflicted the Muslims because of the Americans' chemical and biological weapons.*"⁴

Table 1. Chronology of Water Related Terrorism Incidents¹

Year	Description of Incident
1968	Yippies threaten the Democratic National Convention with plans to dump LSD into water supplies.
1970	Plans by the radical Weathermen to steal biological weapons from Ft. Detrick, Maryland to contaminate a major water supply are exposed.
1972	A plot by ecoterrorist group R.I.S.E. to poison urban water supplies around Chicago.
1977	North Carolina reservoir sabotaged with poisonous chemicals.
1979	Two separate incidents of chemical poisoning cause 2,008 illnesses in Virginia and Oregon.
1980	Attempted extortion of a Lake Tahoe casino with threat to poison water.
1980	Water mains in Pittsburgh deliberately contaminated with weed killer
1983	After threats to poison water supply in Louisiana traces of cyanide found.
1983	Israel uncovers Israeli Arab plot to poison Galilee water with "an unidentified powder
1985	Plutonium discovered in New York City's drinking water after a threat o contaminate the water supply.
1987	In the Philippines, 19 died and about 140 are hospitalized after accepting water and sweets from unknown persons
1990's	US government was plagued by series of creditable threats of a looming VX attack on the water supplies of the Nation's Capital. These threats were taken seriously enough that the government commissioned and funded research into a dedicated on-line VX detector. Several were deployed.
1991	There was an anonymous letter sent to the officials of Kelowna, British Columbia. The letter threatened the city's water supplies with biological contaminants. The motive was associated with the Gulf War.
1992	An attack against the Turkish Air Force base in Istanbul. The water tanks on the base were found to contain potassium cyanide (50 mg/L). The Kurdish Peoples Workers' Party (PPK) were responsible.
1993	A meeting of Islamic Fundamentalist groups occurred in Tehran, Iran. At this meeting, one of the proposals discussed was the idea of poisoning the water supplies of major cities in the west.
1994	A Moldavian General threatened to contaminate the water supply of the Russian 14 th Army Group with mercury. After his dismissal, the mercury was not recovered.
1999	Three threatening letters were received by public figures in Britian. The letters demanded the withdrawal of British troops from Northern Ireland by 16 June. The author, Adam Busby, threatened to poison the United Kingdom's water supply with the herbicidal weed killer Paraquat if the British government did not comply with his demand
1999	Two juveniles were responsible for pouring a "bright red substance" into the water supply of the town of Grass Valley, California. The water treatment plant was forced to shut down causing a denial of service to the areas 2,300 residents
2000	It was reported that Chechen rebels planned to poison unknown water sources in Chechnya, Russia.
2000	A man was arrested for attempting to poison the water supply of a village in Turkey with insecticide.
2000	A condominium block in Singapore discovered that the water had been poisoned with kerosene and turpentine
2001	In British Columbia, a reservoir hatch was found open and an oily substance on the surface of the water. The 6,400 residents of Ladysmith were warned not to drink the water until the system could be flushed.
2001	In the Philippines, Abu Sayyaf threatened to poison the water supply of the town of Isabella. About a week later, the water supply is cut off when residents complain of a gasoline taste and odor in the water. Abu Sayyaf is blamed
2002	Al Qaeda arrested with plans to attack U.S. embassy water in Rome with "cyanide".
2002	Federal officials arrest two Al Qaeda suspects in Denver with documents about how to poison the country's water.
2002	Al Qaeda operatives arrested with plans to attack water networks surrounding the Eiffel Tower neighborhoods in Paris
2003	Jordan foils Iraqi plot to poison drinking water supplies from Zarqa feeding U.S. bases along the Eastern desert.
2003	FBI bulletin warns of Al Qaeda plans found in Afghanistan to poison U.S. food and water supplies
2003	A vial containing Ricin is found in a SC postal facility. Accompanying the vial is a note stating that the city's water supply will be contaminated unless certain demands are met. Subsequent testing reveals no Ricin in the water.
2004	In China, a man is arrested after dumping insecticide into a reservoir. 64 people were ill and 42 were hospitalized after the exposure. The man was a seller of water purification devices, and his motive was to increase sales
2004	A Sudanese man with Iranian intelligence contacts is captured carrying a very powerful poison in Iraq. The man was reportedly preparing to poison the water supply of Diwaniyah a city 100 miles south of Baghdad
2004	The FBI and Department of Homeland Security issue a bulletin warning that terrorists were trying to recruit workers in water plants as part of a plan to poison drinking water at the treatment plants
2005	Russian authorities, during a visit by President Bush, recovered liquid cyanide and other unidentified poisons intended for use by terrorists. The Russian Federal Security Services said, " <i>The use of these strong acting poisons in small doses in highly populated areas, in key installations and in reservoirs could have caused large numbers of victims.</i> "
2005	In an attempt to disrupt the second round of Iraqi elections in December, rumors swept Baghdad on Dec. 15 that the water supply had been poisoned only hours before polls were to open for national parliamentary elections. Residents were awakened at 1 a.m. when warnings about drinking water were broadcast through mosque loudspeakers. According to the article, the country's health minister, Abdel Mutalib Mohammed, issued a statement on television saying that there were no cases of poison in the water system and that the news was untrue

As an interesting side note, Karl King the co-author of this paper's wife, Daniela, is a native of Romania. During the revolution in Romania (Ceausescus overthrow) there were reports that the water supply in the western town of Timosoara had been poisoned with nerve agent. There were rumors that the same poisoning was to take place in Brasov, where Daniela lived, and the army (which supported the people) was deployed to protect the town's water tanks. So, a real attack with nerve agent is an historical fact.

HOW COULD AN ATTACK OCCUR?

When observing a typical municipal water supply system it is natural to assume that the main point of vulnerability to a CBR attack would be the introduction of an agent into the system at the source water (reservoir) or treatment plant. However; in order to create widespread casualties from an attack on the source water, the amount of contaminant required would, after taking dilution into account, be either too large to handle easily or be more expensive than other readily available terrorist weapons. Within the water industry, this concept is summarized by the phrase *dilution is the solution to pollution*. Blind acceptance and reliance upon this strategy for protecting water has delayed the recognition of the true danger, as it exists, little own the timely adoption of possible ways to mitigate the problem.

The concept of dilution providing security for the system initially held after 9/11 is rapidly becoming recognized as a fallacy. Government officials and industry experts are coming to realize that the crucial vulnerability to contamination is in the distribution system. By October 2003 a GAO report to the Senate stated that the distribution system was the area most vulnerable to attack.⁵ Conceding that an attack with CBR agents would most likely take place somewhere in the distribution system, several misconceptions about this type of attack still persist. Popular belief holds that such attacks require the assistance of several technicians, are expensive to carry out, and require complicated and expensive pumping equipment to inject contaminants into a pressurized system. More recent studies by the Army Corps of Engineers and Hach HST, among others, show that CBR attacks could in fact be carried out for 5 cents or less per lethal dose, that a single individual can obtain or produce effective contaminants in quantity, and that contaminants can be introduced into the distribution system with the aid of inexpensive and easy to obtain pumping equipment via a method called backflow attack.^{1,6,7,8,9}

WHAT IS A BACKFLOW ATTACK?

A backflow attack occurs when a pump is used to over come the pressure gradient that is present in the distribution system's pipes. This can be easily achieved by using pumps available for rent or purchase at most home improvement stores. After the pressure has been overcome and a contaminant introduced, Bernoulli effects pull the contaminant into the flowing water and the normal movement of water in the system acts to disseminate the contaminant throughout the network effecting areas surrounding the introduction point. The introduction point can be anywhere in the system such as a fire hydrant, commercial building or residence. See figure 2. While many access points are equipped with backflow prevention devices, it should be recalled that these are simply

physical deterrents that were designed to prevent accidental backflows and can be circumvented by a determined terrorist.

Studies conducted by the US Air Force and Colorado State University have shown backflow attacks to be a very effective means of contaminating a system.⁸ A few gallons of highly toxic material was enough, if injected at a strategic location via continuous feed, to contaminate an entire system supplying a population of 150,000 people in a matter of a few hours. A terrorist could launch such an attack and be on a plane out of the country before the first casualties have begun to show up.



Figure 2. All distribution systems are vulnerable to backflow attacks.

While the threat from Islamic terrorists is dire, it is not the only threat. Domestic terrorists and disgruntled employees may represent a scenario just as serious and possibly more likely. Even though threat of deliberate attack gets a lot of attention, the greatest vulnerability to water quality in the distribution system is not from intentional contamination but accidental contamination due to mistakes made in systems operation or failure of aging infrastructure. Do to the meager monitoring that is currently being done in the distribution system many of these types of problems remain undetectable until they result in a catastrophic failure or a disease outbreak.

Currently, monitoring of drinking water supplies in the distribution system is limited. Previous to the terrorist threat, it was not a priority. 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. Such an ability would also serve the purpose of mapping a system for clean up, and after words, it could be used as a forensic tool to identify the source of an event. The development of such a monitoring system was listed as by a panel of experts and industry leaders as a top priority in enhancing water security.⁵ Hach HST has spent considerable time and resources over the past several years in meeting the challenges entailed in developing just such a system.

WATER ANALYSIS PRESENTS MANY CHALLENGES.

A common misconception concerning analysis in water held by many in the scientific community is that the system is stable with little variation over time or from

location to location. This is probably due to most analysts that are not specifically involved in water research being exposed to laboratory grade de-ionized water as the norm when running experiments. In the real world, even after treatment, there is great diversity in the water found in distribution systems. For a parameter as simple as pH that we would expect to be around 7 ± 1 pH units, the diversity is much greater and can run from 3 to near 11 pH units. Also in a given system there is great heterogeneity over time in basic conditions such as pH, turbidity, conductivity, etc. Figure 3 is representative of the diversity that can be found in the real world in these types of parameters over time.

On top of the great diversity of water quality that may be present in the distribution system, the general environment is also very harsh. The water conditions may be corrosive or scaling in nature. This can lead to degradation of anything placed in the system or the formation of a coating of various types of materials. There is also present in most pipe systems something known as biofilm. This is a thin layer of bacteria and their associated slime that coats the inside of pipes and anything else present in the system. This layer of growth can coat sensors and render them unable to function properly. It can also clog small tubes and pipes used to draw off samples resulting in erroneous readings. Any detection system designed to function over long periods of time in the distribution system must be capable of handling these harsh conditions. There is also the problem of aging infrastructure. Many of the water pipes in our major cities are over 100 years old and are occluded with rust, crumbling concrete and other debris. This raises concerns for instillation and sampling for a distribution system monitoring platform as well as the functioning of many of the new and emerging technologies involving micro fluidic microprocessors and other nanotechnologies that are trying to gain market acceptance.

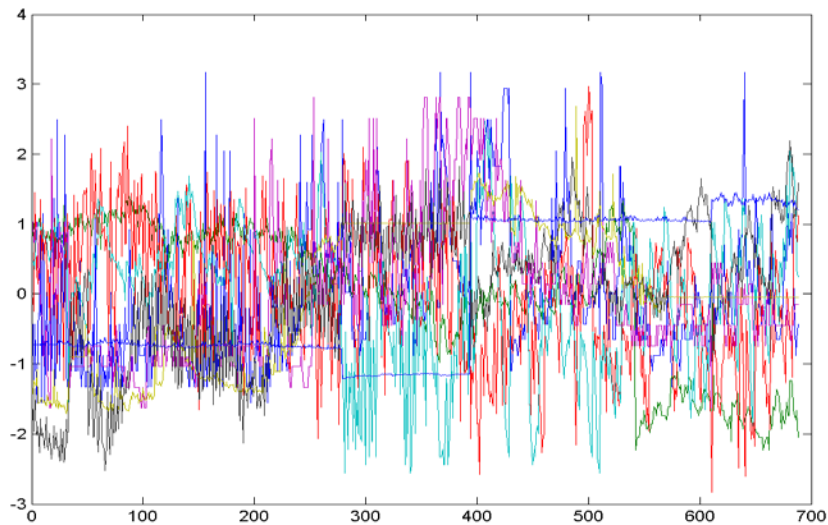


Fig. 3 Real world data can be complex and variable.

WHAT SHOULD A MONITORING SYSTEM DETECT?

One of the problems when designing such a monitoring system for water is the vast number of chemical agents that could be utilized by a terrorist to compromise a water supply system tends to preclude monitoring on an individual chemical basis. Chemical warfare agents such as VX, Sarin, Soman, etc.; commercially available

herbicides, pesticides and rodenticides; street drugs such as LSD and heroin; heavy metals; radionuclides; cyanide and a host of other industrial chemicals could be exploited as weapons. There are also a variety of biological agents and biotoxins that could be problematic. Which of the myriad possible agents would be the most likely to be deployed in a terrorist assault is still a matter of conjecture. To be truly effective a monitoring device needs to be able to detect any and all of the possible agents that could be encountered. A dedicated device capable of detecting anthrax for instance is interesting, but not very practical, as it could be thwarted by the terrorist use of another agent.

This need to detect such a wide variety of diverse contaminants requires a realignment of thinking from the traditional development of a sensor for a given compound or agent. Development of workable sensor arrays on a chip or other analytical instrumentation capable of detecting this variety is a definite challenge. An alternative approach is to use computer algorithms to detect and characterize changes in basic water quality parameters and to correlate these changes with threat agent introduction. This is the approach chosen by Hach HST and detailed in the remainder of this article.

HOW THE HACH HST SYSTEM WORKS

In the system designed by Hach HST, signals from 5 separate measurements of water quality (pH, Conductivity, Turbidity, Chlorine Residual, TOC) are processed from 5 separate measures into a single trigger signal in an event monitor computer system that contains the algorithms. The signal then goes through the baseline estimator, which is crucial in determining what is normal for that system at that time. A measurement of the change in the established baseline is then calculated. Then a weighting factor is applied to the various parameters based on experimental data for a wide variety of possible threat agents. The magnitude of the signal is then compared to a preset threshold level. If the signal exceeds the threshold, the trigger is activated.

The measurement of change that is derived from the trigger algorithm is then used for further classification of the cause of the trigger. The direction of the change in the 5-space world in which it is measured relates to the agents characteristics a.k.a. fingerprint. Seeing that this is the case, laboratory agent data can be used to build a threat agent library of these fingerprints. A profile from the monitor can be compared to agent fingerprints in the threat agent library to see if there is a match within a tolerance. This system can be used to classify what caused the trigger event. This system can also be very useful in developing a learning based system for classifying normal operational events that may be significant enough in magnitude to activate the trigger. When such an event occurs, the profile for the vector causing it is stored in a plant library that is named and categorized by the system operator. When the event trigger is set off the library search begins.

The agent library is given priority and is searched first. If a match is made, the agent is classified. If no match is found in the agent library, the plant library is then searched and, the event is identified if it matches one of the fingerprints in the plant library. If no match is found in the plant library either, the event is classified as an unknown and can be named if an investigation determines its cause. This is very significant because no profile for a given event need be present in the libraries for the system to trigger. This gives the system the unique ability to trigger on unknown threats. Also, the existence of the plant library with its ability to learn plant events results in a substantial and rapid decrease in

unknown alarms over time. The developed system has been subjected to strenuous testing in both laboratory and field scenarios and has been found to be an effective tool for surveillance of the distribution system.

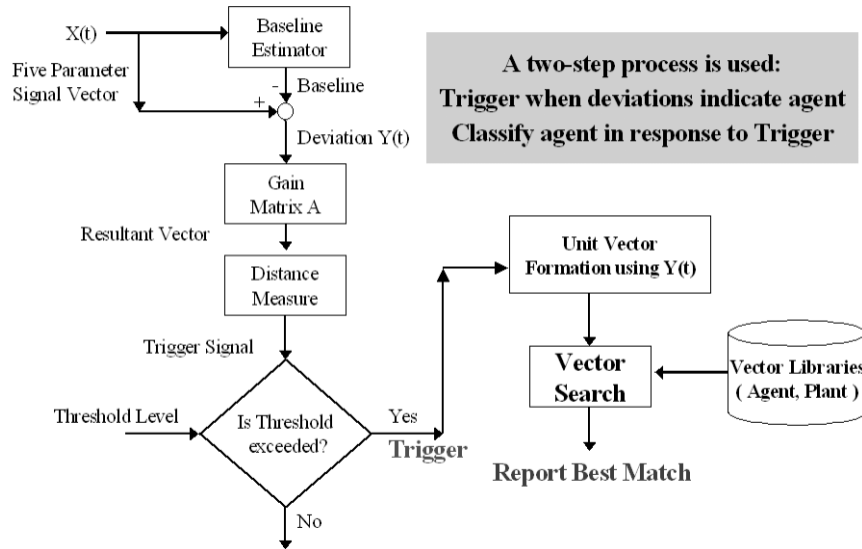


Fig 2. The use of intelligent algorithms with standard bulk parameter monitoring equipment allows for a robust system that is capable of triggering on and classifying a wide diversity of threat agents including unknown events.

SYSTEM TESTING AND DEPLOYMENT

Battelle EPA ETV Verification Testing¹⁰

In the fall of 2004, the developed technology was submitted for testing to the EPA Environmental Technology Verification (ETV) testing program run by Battelle. The ETV Program develops testing protocols and verifies the performance of innovative technologies that have the potential to improve protection of human health and the environment. The tested technologies were evaluated for accuracy of instrument readings versus reference methods, ability to maintain integrity during long term deployment, system to system variability, ability to respond to contaminants, and classification of unknown contaminants (The Hach system was the only one evaluated for ability to classify contaminants). The complete ETV report and an explanation of the report can be down loaded at http://www.hach.com/fmmimghach?/CODE:ETV_EMTS-WDMP92661//true and <http://www.hach.com/fmmimghach?/CODE:ETVEXP-HACHHST9203|1//true>

Contaminant Injection:¹⁰

During this phase of the test the instruments were installed in a recirculating pipe loop. Various contaminants were injected to determine if they altered the baseline response pattern of the instruments. Similar injections were performed after the long-term deployment test to ascertain if there had been any degradation of instrument response. A number of different contaminants were injected including *E. coli*, Aldicarb, arsenic trioxide and nicotine. All contaminants responded with changes in at least some of the instrument readings.

Long-term deployment, accuracy and inter-unit variability:¹⁰

During this phase of the testing, the systems were operated continuously for 52 days with only normal maintenance, such as reagent replenishment, being performed. During the course of the test, instruments were regularly compared to reference instruments. At the end of the 52 days a second response to contaminant injection procedure was performed. The results of the extended deployment study indicate that the system can be effectively deployed for long periods of time with only routine maintenance. Two Hach units were compared, using data collected from reference samples throughout the verification test to determine whether similar results were generated. All results were good.

Contaminant classification:¹⁰

During the final stage of the verification test thirteen contaminants (See Table 6) were injected at a concentration of approximately 15 mg/L, in duplicate, into a 1500 foot straight line pipe and allowed to flow past the monitoring sensors. Every contaminant injection resulted in the system exceeding the trigger threshold and producing a corresponding agent alarm. Each minute-by-minute search of the agent library can result in more than one agent being identified. For both Hach Units, the agent alarms occurred as few as eight times and as many as 79 times during the 20-minute injection periods. No agent alarms occurred outside of the 20-minute injection periods. If the system recognized deviations from the baseline, the agent library identified and recorded these deviations as “unknown” event. Due to the dynamic nature of the leading and trailing edges of the injected contaminant, it is possible that an injection event generated alarms other than the known injected contaminant. Table 6 shows all contaminant injections classified according to the fraction of agent alarms attributable to the correctly classified injected contaminant. The data is depicted concisely by classification rates divided into five levels: Level 5 – greater than 70%, Level 4 – between 31% and 69%, Level 3 – between 1% and 30%, Level 2 – injected contaminant not identified but other contaminants were identified, and Level 1 – no injections detected.

Table 6. Contaminant Classification Results

Contaminant	Injection 1		Injection 2	
	Unit 1	Unit 2	Unit 1	Unit 2
Aldicarb	4	4	4	4
Arsenic trioxide	2	2	2	2
Colchicine	4	4	4	4
Dicamba	4	5	5	5
Dichlorvos	4	3	3	2
<i>E. coli</i>	3	2	4	2
Ferricyanide	5	5	5	5
Fluoroacetate	5	5	4	4
Glyphosate	4	3	2	2
Lead nitrate	5	5	5	5
Mercuric chloride	4	4	4	4
Methanol	4	4	4	3
Nicotine	2	2	2	2

From the tests conducted on Hach Version 1 System, weak results were obtained for Methanol and Dichlorvos, while poor results were obtained for Glyphosate, Nicotine, Arsenic Trioxide and *E. coli*. The data from the tests on VERSION 1 of the Hach HST technology at the EPA center were recorded at the time of the tests. The Event Monitor Trigger System also acts as a data logger and provides a copy of the sensor signals recorded during the tests. This situation afforded us the ability to analyze failures detected in the VERSION 1 tests, improve and upgrade software, and then replay new versions of the technology to test for efficacy. A variety of causes were found to affect the test results of VERSION 1.

Because of a misunderstanding, the original Version 1 threat agent library included Round-UP Herbicide (a form of glyphosate), while the ETV protocol used pure glyphosate. When pure Glyphosate was added to the agent library in Version 3, the system correctly classified the agent.

HHST had previously tested nicotine (in house, and at ECBC) with good results. However, the data from the ETV test facility revealed that the excessive mixing method employed prior to injection had caused the nicotine base to react with the carbon dioxide in the air, changing the chemical nature of the contaminant. The Agent Library was improved by adding a signature for reacted nicotine, and Version 3 shows the positive test results. These two examples demonstrate the sensitivity of the system, and how the comprehensive data structure of its Agent Library derives its classification accuracy.

In addition while first developing the Agent Library, HHST employed bench-scale chlorine analyzers that contained EDTA (a metal sequestering agent) as a reagent component, whereas the EMTS sensor panel includes chlorine analyzers that do not use this substance. The EPA/ETV tests revealed this flaw, and VERSION 3 includes upgraded library signatures. Signatures for some other agents were examined for tabular errors and those were corrected as needed. This second set of test results could not be included in the ETV report, as any re-testing was not a part of the original test protocols. Following analysis and upgrades, two succeeding algorithm versions were produced; the test results from VERSION 3 is summarized in Table7.

Table 7. Classification Results from Algorithm version 3

Contaminant	Injection 1		Injection 2	
	Unit 1	Unit 2	Unit 1	Unit 2
Aldicarb	4	4	4	4
Arsenic trioxide	4	5	4	5
Colchicine	4	4	4	4
Dicamba	4	3	5	5
Dichlorvos	2	2	3	3
<i>E. coli</i>	4	3	4	3
Ferricyanide	5	5	5	5
Fluoroacetate	5	5	5	5
Glyphosate	4	4	4	4
Lead nitrate	5	5	5	5
Mercuric chloride	5	5	5	5
Methanol	4	4	4	3
Nicotine	4	4	4	4

Edgewood Chemical and Biological Command (ECBC) Testing

The purpose of this effort was to challenge water distribution systems and sensors, with agent simulants and real threat agents, in order to characterize the response of the distribution system and Early Warning System to agents. Agent concentrations and water solutions were varied to allow for the development and demonstration of distribution methodologies and performance data acquisition. In addition, this work evaluates the effectiveness of Hach Homeland Security Technologies real-time detection technology and provides important information necessary for the U.S. Army to perfect its theories of operation and response mechanisms. The scope of the work performed during these tests was two fold. The first part of the test was to perform beaker studies on agents that are not available for use in the Hach Laboratories in Colorado such as VX, Sarin, Soman, Ricin and Anthrax etc. The second part of the testing protocol called for verification of signatures in a flowing loop to validate the transfer of the beaker signature data to real world scenarios. See figure 3.

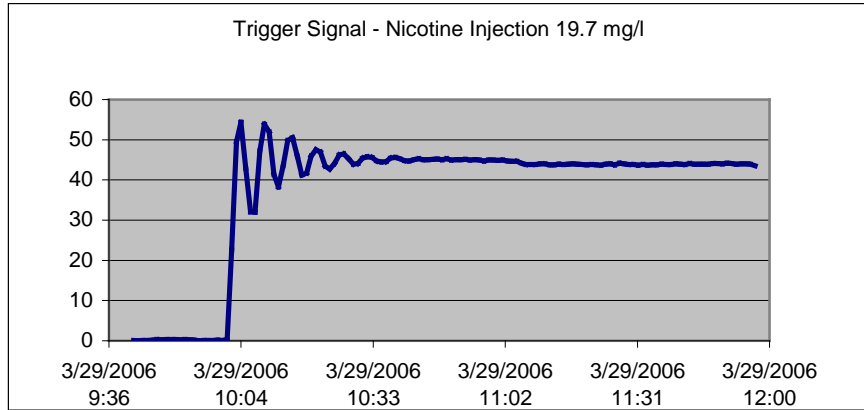


Fig 3. Flow loop testing verified transfer of fingerprints to a more realistic water sample scenario. Real-time loop tests were run on nicotine, ricin, anthrax and methanol.

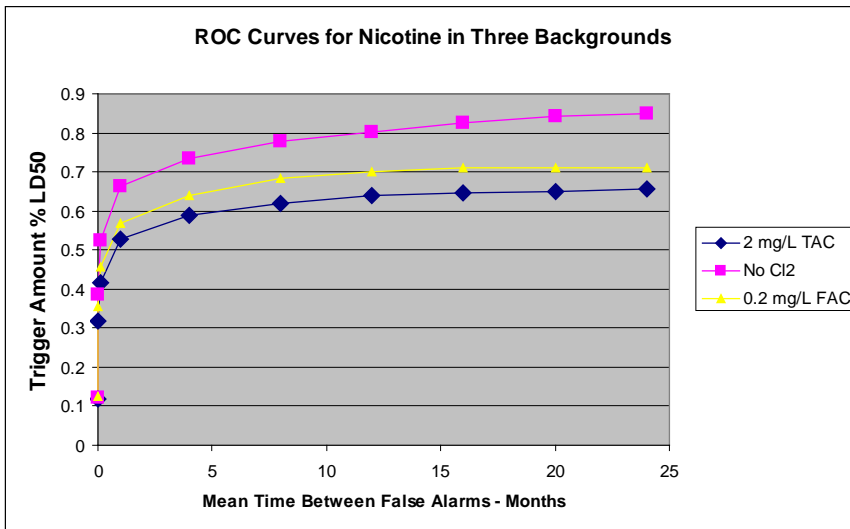
The results of this effort were that all fingerprints were successfully developed. Minimum detection limits and receiver operator curves were generated for all agents tested. It was also found that the fingerprints developed from the lab work could be successfully transferred to a flowing system by successfully triggering and classifying agents in the flow loops. Because of security concerns and confidentiality, only selected nicotine test data is provided in graphs 1 and 2 .

The test concentration of nicotine was 19.7 mg/L. In a single test run, nicotine was recognized by the system, with detection angles ranging from 0.94 degrees (essentially a perfect match) to 9.84 degrees (a weak match). The fluctuating trigger signal is due to the mixing dynamics of a recirculating loop.

Graph 1 Nicotine Injection in Loop



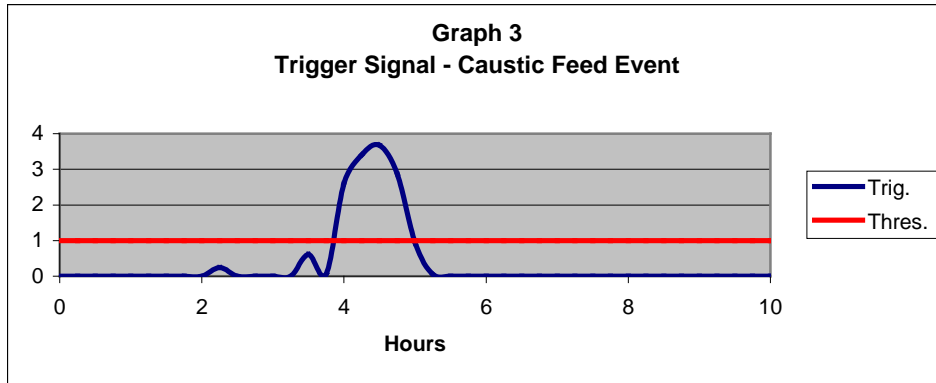
Graph 2 ROC Curve for Nicotine.



In generating the ROC curves for nicotine the trigger level threshold was set from between 0.36 and 1.26. This demonstrates that the trigger level can be set to detect very low levels of nicotine, well below the LD-50, and still have a very low false alarm rate.

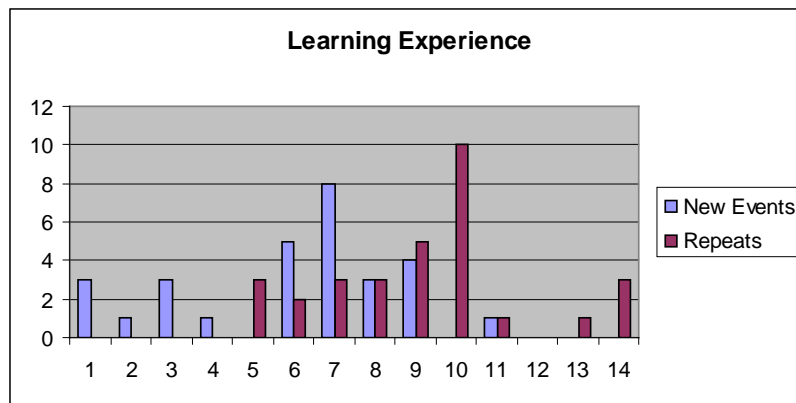
Real World Testing

The described system has been deployed in a variety of real world venues across the United States to determine theories of deployment and response and to verify robustness of the trigger and learning ability. To date over 120,000 hours of real world data has been monitored and evaluated. Several actual (non-terrorist) incidents have been recorded and learned such as roadwork, rain events, pipe burst, pressure events, caustic overfeeds, etc. An example is the caustic over feed event depicted in Graph 3. Graph 4 shows a very noisy real world situation and demonstrates how quickly the system can learn commonly occurring unknown events to help reduce their occurrence.



In this situation, the water utility plant used caustic feed to control the water pH. Misdelivery of a more concentrated form of the caustic resulted in the feed of excess caustic. The pH and conductivity of the water deviated enough to trigger a Plant Event for the system to “learn” and identify its reoccurrence.

Graph 4. Learning Experience Rate at a Field Site



The data in this case represent a real world deployment situation that had very noisy water quality. In this scenario there were 26 unique trigger events in the first 11 days of operations. All were fingerprinted and learned by the system. 11 of the events were repeated. This demonstrates that common events are rapidly learned by the system resulting in a rapid decrease in unknown alarms.

CONCLUSION

The designed and tested system makes use of an integrated array of robust common water quality monitoring sensors coupled with interpretive algorithms to recognize and classify significant water quality deviations. Extensive in house and 3rd party verification testing as well as extensive deployment at field sites has demonstrated the suites ability to fill the analytical gap that currently exists for distribution network monitoring and serve the purpose of an early warning system in the water distribution network. Hopefully the systems unique ability to learn will result in not only increased safety from terror related events but will morph into an operational tool that will find everyday use in improving water quality operations and ensure a better quality drinking water product to consumers.

REFERENCES

- 1) Kroll, Dan. 2006. "Securing the Water Supply. Protecting a Vulnerable Resource." PennWell Publishers. Tulsa, OK.
- 2) Hoover, J.E. 1941. Water supply facilities and national defense. *Journal of the American Water Works Association*. 33:11:1861
- 3) Hickman, Maj. Donald C, USAF, BSC, 1999 "A Chemical and Biological Warfare Threat: USAF Water Systems at Risk," Counter Proliferation Paper No. 3, USAF Counter Proliferation Center, Air War College.
- 4) Lines, A. 2002. *Daily Mirror*. "Al Qaeda: We'll Kill 4 Million More Americans" 14 June 2002.
- 5) GAO-04-29 "Drinking Water Security: Experts' views on how future federal funding can best be spent to improve security"; October 2003
- 6) Kroll, Dan.2003. Mass casualties on a budget. Confidential paper. Hach HST.
- 7) Army Corps of Engineers. 2003. Calculations on threat agents, requirements, and logistics for mounting a successful backflow attack.
- 8) Allman. Timothy. 2003. Drinking water distribution system modeling for predicting the impact and detection of intentional contamination, Masters Thesis, Colorado State University, Dept of Engineering, Fort Collins Colorado, Summer.
- 9) Ginsberg Mark, V. Hoch and D. Kroll. 2005. Terrorism and the security of water distribution systems. *Sword and Ploughshares*. January.
- 10) ETV Report. <http://www.epa.gov/etv/pdfs/vrvs/600etv06006/600etv06006.pdf>