Theory of Operation for the Building Sentry One system

BPSI's Sentry One products are a sensor-based system that detect a defined spectrum of toxic compounds as well as a library of radiological isotopes and select biological agents on a continuous 24/7/365 basis. Through the integration with programmable logic controllers and sensor arrays, linked to a PC infrastructure with multi-layer communications protocols, the Sentry One product solution offers a dynamic set of customized security measures. The Sentry One architecture simply mesh into existing systems, in a seamless process. The Sentry One solution is a mechanical system installed in areas of CBRN concern (example being a commercial office building and the Building Sentry One (BSO) being deployed) for monitoring, both directly and/or remotely, airborne toxins in the building and its HVAC system. The BSO then enacts a sequence of alerts and mechanical protocols to isolate toxins and prevent their distribution in order to disrupt the desired outcome of targeted terrorist activity, prevent loss of life, preserve building assets, and to provide an early warning system in real-time. The BSO is an autonomous backbone system installed as an all-in-one building retrofit and integrates directly into existing building management systems (BMS). The BSO has been designed in modular fashion to support continued advances in sensory technology, with a "Plug and Play" overlay technology. No known similar systems exist. BSO is the only technology that fully integrates sensory technology into a market ready building retrofit product, with embedded building controls, logic, software, mechanical protocols and remote monitoring with multiple security means to prevent tampering and false positive or false negative readings.

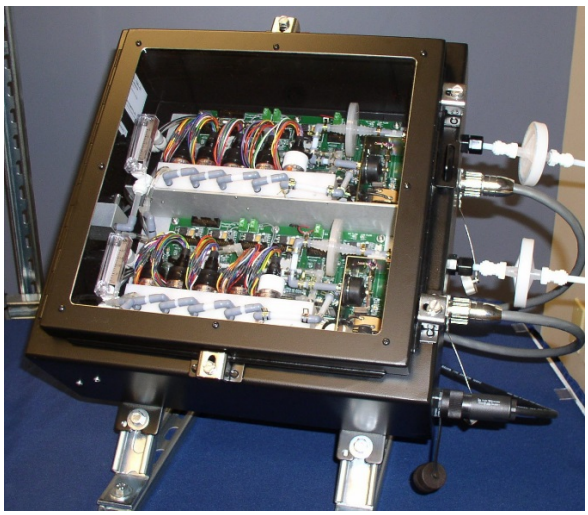
Overview: The Building Sentry One (BSO) is a system that is comprised of:

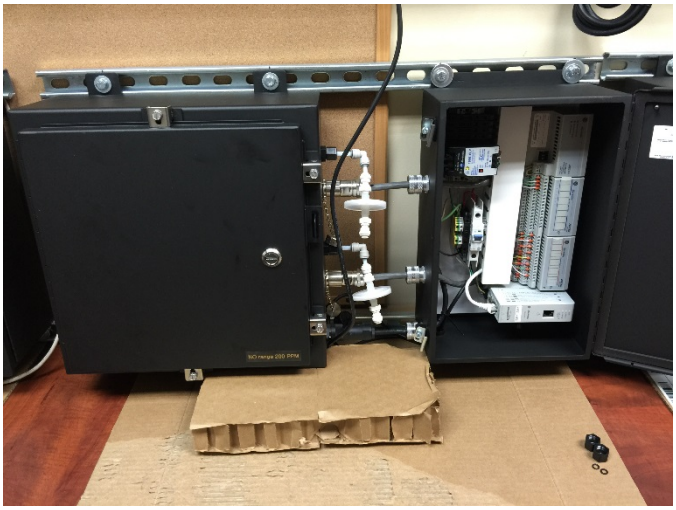
- Building Sentry One main brain cabinet (BSO)
- Chemical Sensor Array (CSA) with field PLC cabinet
- Operator Interface Computer (OIC)
- Radiation Area Detector (RAD) – optional
- Chemical Warfare Agent Monitor (WAM) – optional
- Biological – optional

For the purpose of this paper, only the BSO, CSA and OIC are being used and is the case for the most recent 420 job.

BSO: The BSO is a PLC based sensor system where the outputs of the CSA are translated using the Allen Bradley Factory Talk software and custom programming.

CSA: Each Chemical Sensor Array contains 2 separate sensor engines comprised of 5 analog sensors each with a 4-20 mA output totaling 10 analog outputs. In addition, each CSA has 2 air flow switches per array that are digital (open/closed) totaling 4 digital outputs. The CSA's are connected to a small remote i/o panel by way of 19 pin cables where the conductors of the cables are landed on the corresponding PLC land points. Power is brought into the small remote i/o panel powering both the PLC and CSA devices. Depending on distance (300ft), there will be or not be a fiber port for connecting the CSA to the BSO via an Ethernet or Fiber port located on the i/o panel.





OIC: The Operator Interface Computer HMI into the BSO system and is multi-level password protected. The BSO system will operate in the absence of the OIC but there would be no idea what is going on inside the system without it. On this, there is a port within the BSO that a CAT5/6 cable is connected between the BSO and the OIC as long as it is less than 300 ft otherwise another option would need to be figured out.

More Detail:

OIC: The OIC is password protected with 3 levels: 1- the start-up brings the system to a "default" level where the operator can only view what is going on with the system yet has no ability to acknowledge alarms, make set-point changes or anything else. 2- with the system on, logging into the system as a user defined person will allow one the ability to acknowledge alarms, make set-point changes, bypass sensors, bypass filters etc. 3- this level is only for BPSI and partner engineers. This allows access to the code side which the customer never receives.

CSA: The sensors within the CSA are knows as Electro-Chemical (EC) sensors and are individually targeted at a specific chemical. Because of their physical make-up, they have what is called a cross-sensitivity towards other chemicals because many chemicals share the same compounds. Each CSA has 2 separate sensor engines of the same design – they each have (5) EC Sensors of the same target gas. The reason for this is to virtually eliminate false alarms. In order for an actual alarm to take place, both engines need to react before the BSO closes the chemical detection dry contact that clients use to enact their post detection protocols. In addition, there are (2) sample draw air pumps that pump air from the environment being protected to the CSA sensor engines. The reason for (2) pumps is also for redundancy and each engine has its own dedicated pump. There are (2) air flow switches in-line with each pump that delivers the sample to the sensor engines. The first one will close at 70% flow +/- which will be treated as the "time to change your filter alert" and the second will close at 40%+/- which is "your filter must be replaced" alert – each of these being one of the actions of the BSO programming.

BSO: The BSO interprets all the data coming from the CSA and takes action based on many output scenarios which are programmed using the Rockwell software then generates a graphical interface to the OIC so we can see what is going on within the system. Many of those are as follows (to the best of my ability):

- If 1 of any or more sensors goes out of range for more than 10 minutes, an alert is sent to the OIC. I believe the deviation is above 4 mA + 3 or 5 mA. It's in the program.
- If 1 or any or more sensors drops below 3.5mA for a period of time, the same "Low level" alert is enacted – I also believe this is 10 minutes
- If any 1 of the same sensors in both engines exceed the set-point, an alarm is sent to the OIC and the BSO closes the dry contact within the BSO. Since we have had zero false alarms in over 2 million instrument hours of operation, this is a bad day happening.
- If power is dropped from any device and all readings go to zero, I believe there is a lost power alert that is displayed on the OIC. If there is a power outage on the BSO and the user has not purchased the UPS option, the system will simply go down. It is programmed to self-start after a power failure and re-arm itself to the "default" level.
- The client once logged in to the non-default user setting has the ability to set the trigger points from 4 to 20 mA. When they set the trigger point, it will be the trigger point for whatever chemical chosen and on both sensor engines.
- If anything fails in the BSO system, the properly password entered user has the ability to "bypass" certain devices. For example, if a sensor failed on 1 of the arrays, instead of not being protected for that particular gas until repaired because both sensors would not be able to hit the trigger point together, the user could simply bypass the failed sensor and by default, the 1 remaining sensor would now be placed as master and could trigger a shutdown by itself. Almost all components have the ability to be bypassed.
- During the startup process, if each and every component is not functioning properly, the system will not allow the user to arm the system. In all aspects that would cause this, it should be displayed on the OIC what is not allowing the system to start. Once the issue is found, repaired and or bypassed if applicable, the system will start.
- On the front panel, there are 2 lock key switches, 1 that allows the user to "Arm" the system and the other to put the entire system in "bypass" which is completely different than the internal bypassing of a component. The ARM switch allows the user to bring the system live and any detection will shut the building down. The BYPASS key is used for periodic maintenance – the "bypass on" setting does not allow the shutdown dry contacts to engage because the conductor that powers the shutdown contact coil goes through this switch. The purpose for this is allowing maintenance without taking the system down.
- All alarms, alerts and problems are kept in the Alarm History part of the program