CentrAlert

- Rack Mountable Electronics in Secure Control Room
- Zone Sensitivity Adjustment via ‘Class A’ PC
- Easily integrated to third Party Technologies
- No Power Requirements in the Field

The Centralised Processing Control Solution

System Architecture

Given a choice, many professionals would prefer to design their perimeter security systems with as little electronics as possible located in the perimeter area. There are many good reasons why this strategy is desirable, such as:

- increased system reliability
- increased system security
- field adjustments eliminated
- centralised processing and adjustment

Systems architectures which eliminate field-located electronic systems are inherently more reliable because the often-sensitive electronics are removed from environments where they may be subjected to extremes of temperature and humidity, as well as the destructive effects of lightning strikes.

System security is also enhanced if the architecture permits the location of expensive analysis equipment in secure buildings, safe from opportunist vandalism or intentional destruction.

Many high security sites, such as prisons and military establishments, are ever more conscious of the need to make cost savings in terms of security personnel. Given that access to the perimeters of such sites requires escort personnel, any system which eliminates the requirement for adjustment of field-based equipment is likely to be viewed a bonus by removing the need to provide escorts.

Centralised processing of signals from perimeter sensors allows more intelligent assessment of the potential causes by enabling techniques such as zone correlation and comparison. Adaptive filtering, in which interfering signals generated by weather activity are removed from one sensor, by subtraction of similar signals from an adjacent sensor becomes possible with centralised processing architectures.

Prior to the introduction of CentrAlert, system architectures offering such benefits simply were not available, largely due to the limitations of the sensors employed. Most intrusion detection sensors required localised signals processing to avoid the severe loss that would otherwise occur by transmitting unprocessed sensor signals to a centralised location.

Given the availability and performance of the DeFensor microphonic cable sensors and the Sensor Coil PIDS, these limitations are eliminated and the design of CentrAlert exploits the benefits of these sensors to the greatest effect.

For the first time, security system designers can discard compromise solutions by choosing the only system which provides the wide ranging, technically excellent solutions described here - CentrAlert.

The open architecture embodied in the design of the CentrAlert system allows Geoquip the freedom to offer a range of system configurations to fulfil customer requirements in the most technical effective way. This range is described as follows.

The Detection Engine (Master & Slave Racks)

At the heart of the CentrAlert PIDS is the Detection Engine, which is a centralised rack-mounting module housed within the plant or control room of the site to be monitored.
The module contains all the hardware necessary to perform the signal conditioning and analysis that result in alarm detection on up to 512 Sensor Inputs and 512 Auxiliary Inputs. It also incorporates optional Rugby Time Code Receiver and a keyswitch for operator authorisation.

The Detection Engine is based on a secure Embedded System Architecture, which provides sophisticated but highly reliable Digital Signal processing without any of the risks of viruses or other disruptions which a non-embedded platform may suffer.

Mounted alongside the Detection Engine are optional racks of Relays, providing for up to 512 contact outputs which may be freely configured in groups for automatic or manual switching in response to alarm events. A printer may also be attached directly to the Detection Engine to provide a logging record in the event of a computer failure.

Centralised Control

The Sensors

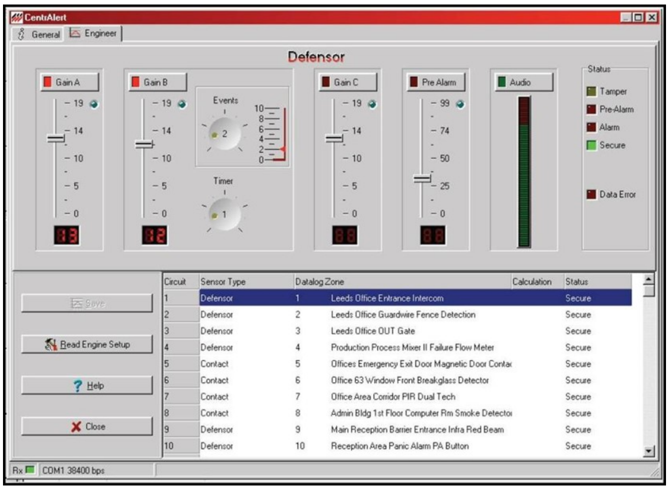
The Detection Sensors or Auxiliary Contact Inputs, located on the site perimeter, are connected to the Detection Engine via multi-pair cables, allowing up to 2.5km separation between the sensors and the control equipment. A Marshalling Box, mounted within the plant room, is provided to allow easy termination of the cables bringing the sensor signals in from the perimeter, and contains the Lightning Protection and RF Immunity modules which protect the detection equipment. The input signals are then transferred from this Marshalling Box to the Detection Engine via pre-made interconnecting cables.

The Control Computer Management System

The Control Computer is connected to the Detection Engine via a simple Serial Link. CentrAlert provides software protocols which allow access to all PIDS functions including sensitivity adjustments, enable/disable zones, etc and provided these protocols are implemented on the Control Computer Management System, full functionality can be made available to authorised personel charged with the operation of the CentrAlert system via the GUI provided by the Control Computer.

User management, logging of both alarms and engineering adjustments, and statistical alarm analysis techniques are all implemented, along with multi-level graphic site mapping to provide the operator with the visual aids necessary to manage the security requirements of a large site. It also provides audible warnings for the system events as well as automatic switching of appropriate sensor signals for Audio Verification of alarms.

The CentrAlert detection system is most often interfaced with Geoquip's GeoLog security management system or the Datalog modular security software. These programs provide most of the additional features normally associated with high security sites. Such equipment may include access control systems, video control systems, and associated hardware. By combining CentrAlert and GeoLog or Datalog, a powerful and flexible detection system and security management system is realised. The combination of a CentrAlert detection system and a GeoLog or Datalog security management system results in a seamlessly integrated solution with centralised control of the various components of a site's security system. Microwave Sensors, Infrared Systems, and other Perimeter Intrusion Detection Systems can be easily integrated with and annunciated at the CentrAlert.

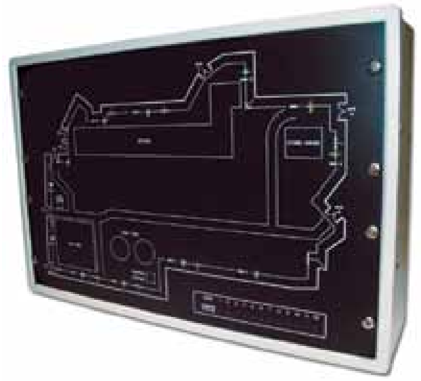


Circuit	Sensor Type	Datalog Zone		Calculation	Status
1	Defensor	1	Leeds Office Entrance Intercom		Secure
2	Defensor	2	Leeds Office Guardwire Fence Detection		Secure
3	Defensor	3	Leeds Office OUT Gate		Secure
4	Defensor	4	Production Process Mixer II Failure Flow Meter		Secure
5	Contact	5	Offices Emergency Exit Door Magnetic Door Contac		Secure
6	Contact	6	Office 63 Window Front Breakglass Detector		Secure
7	Contact	7	Office Area Corridor PIR Dual Tech		Secure
8	Contact	8	Admin Bldg 1st Floor Computer Rm Smoke Detector		Secure
9	Defensor	9	Main Reception Barrier Entrance Infra Red Beam		Secure
10	Defensor	10	Reception Area Panic Alarm PA Button		Secure

Rx COM1 38400 bps

Backup Systems

An optional Mimic-Annunciator panel may also be connected to the Detection Engine, providing a simple "Alarm Panel" style of user interface in sites where a computer screen is deemed inappropriate as the primary operator interface. This Mimic-Annunciator will still operate even in the unlikely event of a computer crash or failure, providing a fail-safe back-up to keep the site running while any computer problems are diagnosed and corrected. There is also a facility to allow the direct connection of a Logging Printer to the Detection Engine so that a full record of site activity is maintained even when the main Control Computer is off-line. Master/Slave and hot backup configurations are also possible.



Key Advantages of CentrAlert

CentrAlert

- Up to 512 Sensor Inputs
- Up to 512 Auxiliary Contact Inputs
- Up to 512 Relay Outputs
- Full lightning protection and RF immunity
- No sensitive equipment mounted on the perimeter
- Centralised adjustment of ALL system parameters
- New generation digital signal analysis based on highly-reliable Embedded Technology
- Seamless integration with the DeFensor & Sensor Coil PIDS
- Audio verification with storage option
- Simple installation, even in large sites
- Multiple levels of system redundancy-onboard log and printer run even when control computer is off-line and back-up Mimic Annunciator panel available

GeoLog & Datalog

- **Linux Operating System (GeoLog)**
  Linux systems offer enhanced reliability, stability and security compared with Windows based operating systems.
- **Distributed Workstation Server Architecture**
  Multiple workstation topology allows greater flexibility when designing event transaction processes and ensures fall-back capability in the event of hardware failure.
- **Full Redundancy Capability**
  Workstation networking over multiple communication links maximises system availability even after catastrophic hardware failure.
- **Existing Network Utilization**
  GeoLog and Datalog systems may use existing TCP/IP network links to minimise installation costs.
- **Fully Configurable Event Processing**
  Event acknowledgement process may be automatically or manually controlled in accordance with configurable routing tables.
- **Preset Event Processing Options**
  1. Fixed Routing
  Where routing of events between detection systems and operator workstations is in accordance with a fixed table of routes.

  2. Operator Driven Routing
  Where routing of events between detection systems and operator workstations is dynamically allocated on the basis of the speed of response of operators e.g. First responding operator deals with the event.

  3. Least Traffic Routing
  Where routing of events between detection systems and operator workstations is determined by the current event processing load and results in automatic selection of the least busy operator.
- **Context Sensitive Event Processing**
  Event routing may be instantly changed in response to changes in the security regime e.g. changes in threat levels, night/day transitions, weekend transitions, or specific time and date periods.
- **Context Sensitive Operator Permissions**
  Operator permissions may be dynamically changed in response to changes in the security regime as described above.
- **Full Control of Intrusion Detection Systems**
  Integrated detection system parameters may be altered as required from the central control point with fully traceable history of all parameter changes.

  Automatic parameter changes may be invoked in response to critical events such as detector tamper alarms.
- **Intrusion Detection System Zone Management**
  Zones may be allocated various status conditions including Disabled/Enabled, Inhibited/Secure, On Test/Secure.
- **Logical Fusion of Intrusion Detection Systems**
  Detection technologies may be logically combined to provide highest system performance under conditions where single detection technologies may be less effective.
- **High Level CCTV Integration**
  Software drivers are available for most CCTV matrices allowing automatic control of the CCTV system in response to detection system status changes.

  GeoLog and Datalog provide camera preset allocation capability along with flexible camera to monitor routing options.
- **3D Graphical Mapping**
  Three dimensional graphical imagery provides operators with greater clarity and event representation.
- **Web Style Help Files**
  Embedded links within Operator Help files enable actions to be implemented directly from help file texts.
- **Full Event Database Review Capability**
  Graphical and textual representation of event histories may be filtered by date/time and zone number.

Th Leader in Perimeter
Protection Solutions

DeTekion Security Systems, Inc.

DeTekion

Corporate Headquarters:
200 Plaza Drive
Vestal, New York 13850
Telephone 607 729-7179
Fax 607 729-5149
www.detekion.com