Since 1980, PROTECH has been designing, manufacturing, and marketing Perimeter Intrusion Detection Systems (PIDS) to protect personnel, property, and assets at sensitive sites. We manufacture systems that give early warning of potential threats at the perimeter. PROTECH offers a complete range of perimeter intrusion detection systems and technologies including – G-FENCE fence-mounted intrusion detection, infrared beam technology (invisible fences), PIRAMID dual technology motions sensors and video analytic object detection and tracking. Our technology can be integrated with monitoring applications including Protech's MAXIBUS, Smart Bridge, or Spectra.

For additional information, contact:

PROTECH/Protection Technologies, Inc.
529 Vista Blvd.
Sparks, NV 89434

Phone: +1 775 856-7333 | Fax: +1 775 856-7658
protechsales@protechusa.com
www.protechusa.com

# ALARM INFORMATION HUB

## DIVISION 28 – ELECTRONIC SAFETY AND SECURITY

## MasterFormat 2020

### 28 31 21 Area and Perimeter Intrusion Detection

**Notes to Specifier:**

1. Where several alternative parameters or specifications exist, or where, the specifier has the option of inserting text, such choices are presented in **<bold text>, where the parameter specified in [brackets] is the normal default.**

2. Explanatory notes and comments are presented in *italic* text.

# ALARM INFORMATION HUB

## PART 1 GENERAL

### 1.01 SUMMARY

A. Section includes a Maxibus hub (concentrator) for Perimeter Intrusion Detection Systems (PIDS).

B. Product - A component which provides centralization of alarm information from a network of sensors to a single point.

C. Related Requirements

1. 28 01 30 Operation and Maintenance of Security Detection, Alarm and Monitoring
2. 28 05 11 Cyber Security Requirements for Electronic Safety and Security
3. 28 06 30 Schedules for Security Detection, Alarm and Monitoring
4. 28 31 31 Intrusion Detection Interfaces

### 1.02 REFERENCES

A. Definitions

1. Modbus – A serial master-slave communications protocol initially published in 1979 for use with programmable logic controllers.
2. PEAP - A 802.1X authentication method using public key certificates on the server to authenticate clients with the server. PEAP authentication generates an encrypted TLS/SSL link between the client and the authentication server. Data exchanges are encrypted and stored in the link to ensure that the user identifiers are secured.
3. EAP-GTC (Generic Token Card) is an authentication method using cleartext to exchange authentication parameters between the client and the server. This authentication method uses single use, One-Time Tokens. This is a secure identifier exchange method. It is defined in RFC 2284.
4. EAP-MD5 – An _authentication method which verifies an MD5 hash of the user's password. This authentication method is frequently used in trusted networks. EAP-MD5 is defined in RFC 2284.
5. EAP-TLS (Transport Layer Security) is an authentication method using PKI (Public Key Infrastructure) and RADIUS server authentication, among others. It requires a client-side certificate to communicate with the authentication server. It is defined in RFC 5216. This method uses server-side certificates to perform the authentication between the clients and the server. Authentication does, nevertheless, rely on passwords.
6. The EAP-MS-CHAPv2 (Microsoft Challenge Handshake Authentication Protocol version 2) authentication method is used extensively in MICROSOFT systems. It requires a RADIUS server to be used as a backend authentication server and is defined in RFC 2759.

B. Reference Standards

1. Electromagnetic compatibility
   a. EU EMC Directives EN 55022, EN 55024
   a. FCC-47 CFR Part 15, Class B
2. IEEE 802.3 Ethernet

## 1.03 SUBMITTALS

A. Product Data
   1. Manufacturer’s printed or electronic data sheets
   2. Manufacturer’s installation and operation manuals

B. Shop Drawings
   1. Termination points and enclosures

## 1.04 QUALIFICATIONS

A. Manufacturer of system shall have a minimum of five (5) years experience in the design, manufacture, and successful implementation of perimeter sensing systems.

## 1.05 DELIVERY, STORAGE, AND HANDLING

A. Deliver the equipment system in the manufacturer’s original, unopened, undamaged container with identification labels intact.
   1. Ship and store the system protected from mechanical and environmental conditions as designated by the manufacturer and in a temperature environment of -32°F to +158°F (-0°C to +70°C)

## 1.06 WARRANTY

A. The Manufacturer shall provide a limited warranty for the system to be free of defects in workmanship and material under normal operating conditions for a period of two years from the date of product shipment.

- END OF SECTION –

## PART 2 PRODUCT

### 2.01 EQUIPMENT

A. Manufacturer: PROTECH/Protection Technologies, Inc.
529 Vista Blvd.
Sparks, NV 89434
Phone: +1 775 856-7333 | Fax: +1 775 856-7658
protechsales@protechusa.com
www.protechusa.com

B. Model: MAXIBUS UNIVERSAL

Smart Bridge

C. Alternates: None

### 2.02 GENERAL DESCRIPTION

A. The Alarm Information Hub (Maxibus Hub) shall centralize all system alarm information from sensing columns and other sensing systems provided by the Manufacturer and authorized third party systems.

*The MAXIBUS UNIVERSAL Hub provides processing capability for the following Protech systems through its 4 RS-485 COM ports:*

*G-FENCE 3000 control units (up to 16 per COM port)*

*G-FENCE 2400 control units (up to 4 per COM port)*

*MAXIRIS (up to 32 per COM port)*

*SOLARIS (up to 24 radio boards (1 radio per sensing column) and 64 control boards (1 per 5TX and 1 per 5RX beams) per COM port)*

*APIRIS Columns - up to 8 per COM port*

*Consult factory for compatible third-party systems.*

B. The Hub shall provide for remote configuration and maintenance of connected sensing elements, including detection of the sensors connected to the network, number of available contacts, and diagnostic information for each sensor.

C. Events – The Hub shall provide a detailed event log, including alarms, accessible through a web server.

1. For each event, the log shall maintain the following data:
   a. event timing to include date, hour, minute, and second
   b. specific device address triggered during an event, and type of event (e.g., intrusion, anti-climbing, tamper)

D. Settings

1. The Hub shall maintain the following settings in its memory:
   a. relay assignments
   b. site configuration
   c. its own settings
2. The Hub shall have the capability of exporting its settings to a file and restoring settings from a saved file.

E. Communications
1. The Hub shall connect to field sensing elements via Modbus RTU protocol over an RS-485 or radio connection.
a. Number of RS-485 COM ports: 2 or 4
1) RS-485 devices, including:
a) RS-485 field devices
b) radio controller units
i. The Hub shall detect automatically radio controllers and number of sensor columns for each radio controller
c) Alarm panels
2. The Hub shall provide an RJ45 Ethernet connection using Modbus TCP protocol, enabling the following capability:
a. Configuration via direct-connected PC
b. Remote network access via the web
c. Connection to a video management system.

*Smart Bridge is a software that connects PROTECH's MAXIBUS UNIVERSAL (and/or G-Fence 2400 Controllers) to various VMS software platforms. The Smart Bridge software resides on the VMS Event Server and connects up to 256 MAXIBUS Universal devices and/or G-Fence 2400 Controllers and sends alarm events to the VMS platform.*

3. Alarm outputs – The Hub shall be capable of providing alarm information via any of the following:
a. dry contact outputs automatically up to 136 available contact outputs.
b. Modbus over RS-485, with Hub functioning in Master or Slave mode
c. Modbus over Ethernet, with Hub functioning as Server or Client
1) Network speed: 100 Mbps

*The Hub has 8 on-board relay contact outputs and provision for up to 16 additional relay extension cards, each of which provides 8 additional relays. Maximally configured, 8 on-board relays and 128 expansion board relays are available.*

F. Web Server – The Hub shall have an integrated web server to support configuration and maintenance.
1. The web server shall be capable of the following:
a. assigning an administrator and securing access through login ID and password
b. setting the real time clock in the Hub
c. mapping one or more alarms to one or more relay contact outputs
d. setting Ethernet network parameters
e. configuring the COM ports for the sensing network(s)
f. displaying a log of events
g. displaying relay assignments
2. The web server shall be accessed via any web standard browser.
3. The web server interface shall be available in English, Spanish, or French.

G. Configuration and Maintenance Software
   1. Configuration and Maintenance software (“software”) shall be available as a PC-based graphical tool intended for configuration and basic monitoring of the system
   2. Functions
      a. Viewing sensing node (column) status
      b. Import a site layout in image file format
      c. Display all system components on a map
      d. Display the location of an intrusion alarm on a map
      e. Display a current event log
H. Cybersecurity
   1. Network Modbus TCP communication shall support the following:
      a. secure encrypted communication using Transport Layer Security (TLS) protocol.
      b. HTTPS and SSH certificates
      c. 802.1x port-based security with support for MD5, MSCHAPV2 and GTC authentication and TLS.
I. Electrical – Voltage: 12 VDC @ 230 mA
J. Operating temperature: 32°F to +131°F (0° C to +55° C)
K. Dimensions: See Attachment A

- END OF SECTION –

## PART 3 EXECUTION

### 3.01 INSTALLERS

A. The Contractor’s installers and technicians shall be factory trained and certified to install, service, and maintain the system.

B. Contractor personnel shall comply with all applicable state and local licensing requirements.

### 3.02 PREPARATION

A. Contractor shall insure that all products to be installed have been verified to possess the latest version of available firmware.

### 3.03 INSTALLATION

A. The Contractor shall adhere to all Manufacturer’s published installation procedures, diagrams, and guidance.

- END OF SECTION –

**ATTACHMENT A** Dimensions