ALARM INTERNATIONAL INC

CSV IP Alarm Data Specification

For Alarm Communication Unit Manufacturers

Version 1.53

Presented by
Boyd Robinson
Alarm International Inc
10 west Terrace
Newton
Auckland
Tel : (09) 3030303
Fax : (09) 3020324
Email : Boyd@alarmnz.com
Web : http://www.Alarmnz.com

Table of Contents

TABLE OF CONTENTS 5
TABLE OF FIGURES 6
DOCUMENT HISTORY 6

1. OVERVIEW 7

2. DATA FRAME DESCRIPTION 7

3. ALARM COMMUNICATION UNIT IMLEMENTATION 8

4. ALARM CONCENTRATOR/RECEIVER IMPLEMENTATION 9

5. LIMITATIONS 9

6. DISALLOWED CHARACTERS………………………………………………………9

Table of Figures

None

Document History

Version	Status	Date	Comments
1	Draft	7th April 2006	First draft
1.1	1st Release	12th January 2007	Updated message structure to include authentication
1.2	2nd Release	9th February 2007	Altered example message format to ContactID
1.3	3rd Release	11th February 2007	Added Addendum – Disallowed characters in XML
1.4	4th Release	9th November 2007	Addendum – added , Disallowed character in XML
1.5	5th Release	30th November 2007	Document Re-Edited/Checked by Chief Eng (NRC)
1.53	5th Release rev.53	9thth April 2010	Clarifications regarding Multiple messages with a single session and XML coexistence strategy.

1. Overview

This document provides a description of the method used to transfer un-encrypted alarm data via TCP/IP from an ACU (alarm communication unit) to a CMS (Central Monitoring Station) alarm concentrator/receiver. CSV IP ALARM data uses basic authentication (optional) and immediately precedes the standard message format (account number followed by message data)

All CMS software applications include ASCII character translation tables and can represent the message data perfectly as long as the account number is clearly separated from the message. The Authentication fields are also separated from the message and used to access the CMS alarm concentrator/receiver when communicating over a public network.

2. CSV IP ALARM Data Frame Description

The IP alarm format consists of a standard TCP/IP data frame, the first two fields of the message between header and trailer are reserved to specify the ***username***, ***password*** (authentication) and the last two fields allocated for the ***account number*** (ACU identifier) and ***message data.*** (standard message content). A manufacturer could use their own data format or a well known industry standard dial up alarm formats like **Contact ID**, **SIA**, to describe message their content. Please note these CSV IP Alarm fields are separated with commas. (CSV)

All bytes in the message contain the necessary ASCII characters indicating the event as sent from the manufacturers ACU bound for the CMS. e.g a generic **Contact ID** message such as ***18113001003*** from an alarm communication unit with ***1234*** programmed as the account number and using "***Name***" for the username "***Password***" for the password would be encapsulated as:

<FrameHeader>
Name,***Password***,***1234***,***18113001003***
<Frame Trailer>

If no authentication is utilized in the same message then it would appear as:

<FrameHeader>
,,***1234,18113001003***
<Frame Trailer>

With dial up that would be have been decoded by the CMS as: **123418113001003**
or

1234 = Account
181 = new event
130 = burglary event type
01 = area
003 = zone

(see appendix 1 for other ContactID messages)

3. Alarm Communication Unit Implementation

Alarm transmission is designed to be a simple data logger and does not attempt to support "command and control" functions as these are proprietary to each manufacturer and normally form part of the ACU programming tool.

Designers will need to insure the minimum following fields are contained in their internal path parameters within the ACU memory, these include;

Primary login name,
Primary password,
Primary IP address,
Primary Gateway IP address,
Primary Subnet mask,
Primary Port number,
Primary Supervision Time (hh:mm)
Primary Supervision Character (ascii)

Secondary login name,
Secondary password,
Secondary IP address,
Secondary Gateway IP address,
Secondary Subnet mask,
Secondary Port number,
Secondary Supervision Time (hh:mm)
Secondary Supervision Character (ascii)

Upon detection of a status change the ACU would create a socket defined by the IP address and port number as specified in the ACU communication path parameters. If the ACU is unable to open a socket using the primary parameters it should attempt the same process using the alternate or secondary IP address and port number. If still unsuccessful it should re-attempt the socket creation a number of times for each socket (primary and secondary).

Once a socket is created events should be encapsulated in a data frame as per section 2 and sent to the destination network. The destination network shall return back or reflect the same message as it receives, this will provide a method of acknowledgement (kiss off). If the ACU does not receive this message within a pre-defined timeout period it shall re-transmit the signal.

Once the signal is successfully transmitted (including any other events in the buffer) the socket shall be disconnected.

4. ALARM Concentrator Receiver Implementation

Packets of data arriving at the alarm concentrator/receiver will be screened for the presence of valid authentication data or message data within the de-encapsulated data frame. If a valid packet has being received via TCP the lack of an error generated via the TCP session will indicate a valid transmission (message reflected correctly) – no additional handshake from the CMS will be used. The alarm concentrator/receiver can be engineered to take multiple CSV messages within a single session however the entire CSV message including authentication must be passed each time *(Name, Password, Account, Message data).* In such cases each CSV message is reflected consecutively within the same session and after at least 5 seconds without any message activity the alarm concentrator/receiver close the socket. If an invalid packet type is detected the data frame will be flushed from the buffer and no further processing will take place i.e. the socket will be forcefully disconnected.

5. Limitations

This document is a general design specification of the transfer of un-encrypted alarm data via TCP/IP. CSV IP Alarm does not attempt address security issues relating to the transport of un-encrypted data across the Internet, however if manufacturers or designers choose to utilize the login name/password fields or the message data field as a encryption string then such methods will need to be supported at the CMS concentrator/receiver. Generally it is recommended that security is handled outside the message layer via a more robust VPN methodology.

Oversize content within fields inside the data frame could expand the message beyond a standard 512 character TCP/IP packet length causing a small transmission delay so it is recommended to designers to not exceed this length for the most urgent messages.

6. Disallowed Characters

The message data field supports all legacy alarm formats and is ready for advanced M2M (machine to machine) XML IP ALARM formats that will follow into the future. Alarm concentrator/receivers that support panels that use disallowed characters will not be able to coexist with XML IP ALARM messages simultaneously and must be separated via Port or IP address.

The following 6 characters are reserved for XML/CSV statements and recommended to not be used within (inside) any Alarm IP ***Name***, ***Password***, ***Account, message data*** field:
<
>
&
‘
“
,

Appendix 1

Contact ID Communication Format:

18 SSSS QXYZ GG CCC K

18 = Uniquely identifies this format to the receiver and to an automation system, but not displayed on the printer

SSSS = 4 digit Subscriber ID
Q = Event qualifier, which gives specific event information
  1= New event or opening
  3 = New restore or closing
  6 = Previous event
YXZ = Event code (3 Hex digits see chart below)
GG = Group number (physical or logical, 2 Hex digits)
CCC = Device or sensor number(3Hex digits, event reports) or user number (Open/close report)
Note: The GG and CCC fields can contain 0 for a null (no information) field.

Contact ID Event Code Classification

Medical Alarm - 100
101 Pendant Transmitter
102 Fail to report in

Fire Alarms - 110
111 Smoke
112 Combustion
113 Water Flow
114 Heat
115 Pull Station
116 Duct
117 Flame
118 Near Alarm

Panics Alarms - 120
121 Duress
122 Silent
123 Audible

Burglar Alarms - 130
131 Perimeter
132 Interior
133 24 Hour
134 Entry/Exit
135 Day/Night
136 Outdoor
137 Tamper

138 Near Alarm

General Alarms - 140
141 Polling Loop Open
142 Polling Loop Short
143 Expansion Module Failure
144 Sensor Tamper
145 Expansion Module Failure

24Hr Non-Burglary -150 and 160
151 Gas Detection
152 Refrigeration
153 Loss of Heat
154 Water Leakage
155 Foil Break
156 Day Trouble
157 Low bottled GasLevel
158 High Temp
159 Low Temp
161 Loss of Air Flow

Fire Supervisory – 200 and 210
201 Low Water Pressure
202 Low CO_2
203 Gate Valve Sensor
204 Low Water Level
205 Pump Activated
206 Pump Failure

System Trouble – 300 and 310
301 AC Loss
302 Low System Battery
303 RAM Checksum Bad
304 ROM Checksum Bad
305 System Reset
306 Panel Program Changed
307 Self-Test Failure
308 System Shutdown
309 Battery Test Failure
310 Ground Fault

Sounder/Relay Troubles - 320
321 Bell 1
322 Bell 2
323 Alarm Relay
324 Trouble Relay
325 Reversing

System Peripheral Troubles - 330 and 340
331 Polling Loop Open
332 Polling Loop Short
333 Expansion Module Failure
334 Repeater Failure
335 Local Printer Paper Out
336 Local Printer Failure

Communication Troubles - 350 and 360
351 Telco 1 fault
352 Telco 2 fault
353 Long Range Radio
354 Fail to Communicate
355 Loss of Radio Supervision
356 Loss of Central Polling

Protection Loop Trouble - 370
371 Protection Loop Open
372 Protection Loop Short
373 Fire Trouble

Sensor Trouble - 380
381 Loss of Supervisory-RF
382 Loss of Supervisory -RPM
383 Sensor Tamper
384 RF Transmitter Low Battery

Open/Close - 400
401 Open/Close by User
402 Group Open/Close
403 Automatic Open/Close
404 Late to Open/Close
405 Deferred Open/Close
406 Cancel
407 Remote Arm /Disarm
408 Quick Arm
409 Keyswitch Open /Close

Remote Access - 410
411 Call Request Made
412 Success – Download Access
413 Unsuccessful Access
414 System Shutdown
415 Dialer Shutdown

Access Control - 420
421 Access Denied
422 Access Report by User
441 Stay Arming
451 Early Opening/Closing
452 Late Opening/Closing
453 Late to Open
454 Late to Close
455 Auto-Arm Failure

System Disable - 500 & 510

Sounder/Relay Disable - 520
521 Bell 1 Disable
522 Bell 2 Disable
523 Alarm Relay Disable
524 Trouble Relay Disable
525 Reversing Relay Disable

System Peripheral

Disable - 530 and 540 Communication

Disable - 550 and 560
551 Dialer Disable
552 RadioTransmitter Disable

Bypasses - 570
570 Zone Bypass
571 Fire Zone Bypass
572 24 Hour Zone Bypass
573 Burglary Zone Bypass
574 Group Bypass