

APU Integration Using XML Messages

Application Note

© Copyright 2021, **Fiber SenSys®**, **Inc.** all rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from **Fiber SenSys®, Inc.**, 6175 NW Century Blvd., Hillsboro, Oregon 97124, USA.

This application note is provided by **Fiber SenSys, Inc.** While reasonable efforts have been taken in the preparation of this material to ensure its accuracy, **Fiber SenSys, Inc.** makes no express or implied warranties of any kind with regard to the documentation provided herein. **Fiber SenSys, Inc.** reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of **Fiber SenSys, Inc.** to notify any person or organization of such revision or changes.

Fiber SenSys® is a registered trademark of **Fiber SenSys, Inc.**

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

Fiber SenSys, Inc. (FSI)
6175 NW Century Blvd.
Hillsboro, OR 97124
USA

Tel: 1-503-692-4430
Fax: 1-503-692-4410
info@fibersensys.com
www.fibersensys.com

Contents

Contents 3

Introduction 4

Additional sections **Error! Bookmark not defined.**

Appendix..... **Error! Bookmark not defined.**

Introduction

Most Fiber SenSys Alarm Processing Units (APUs) provide notification of alarms and sensor faults across a communications network. These APUs can be installed into a local-area network (LAN) to connect with an existing head end, or other annunciator/monitoring equipment. The physical network supported is 10/100 wired Ethernet and the networking protocol supported is TCP/IP.

This document describes how to integrate Fiber SenSys APUs with monitoring software such as an SMS/VMS/PISM system. In most cases, Fiber SenSys recommends using the Device SDK to integration with APUs. The SDK does not require a fee and is available for download from the Fiber SenSys website. The SDK has its own application note, APU Software Integration Using Device SDK (AN-ESW-008), which should be read instead of this document.

However, there are circumstances under which the Device SDK cannot be used. For example, it requires the use of the Microsoft Windows operating system. This document describes how software engineers can make use of the underlying XML protocol without use of the Device SDK.

Requirements

This application note is intended for software engineering personnel who have an operating knowledge of software engineering principles, the use of XML documents as communications messages, intensive knowledge about the software that will interpret the XML messages, and some previous experience with integrating alarm devices into that software.

Along with this document, you should have received a ZIP file containing XSD schema files.

If you do not have access to a physical APU for your initial implementation, you will also want to download the Device SDK from the Fiber SenSys website. Even though you will not be using the Device SDK for integration, it contains software that can simulate communication with an APU. Of course, testing with the actual APU model(s) supported by your application is recommended before deployment.

You will also want to download a copy of the APU Networking Application Note (AN-ESW-006) from the Fiber SenSys website. This document explains to system integrators how to install the APU on a network. It also describes how to configure APUs for incoming connections vs outgoing connections. This is important because you will want to indicate to system integrators how to configure the APU to make use of your software integration.

Concepts

Fiber SenSys manufactures a variety of “Alarm Processing Unit” devices (**APUs**). Each APU uses one or more fiber optic cables as sensing elements, processes data collected from the sensing elements, determines whether an intrusion is occurring, and reports the results. By

installing one or more APUs along with the appropriate fiber optic cables, customers can receive reports of intrusions along a perimeter.

Fiber SenSys has several different APU models. The differences between these models mostly do not affect integration, but there are some minor differences that will be described later. All APUs have the concept of a **zone**, which is a distinct region being monitored for intrusion. *Existing APUs can have 1-25 zones but no limit should be imposed on the number of zones per APU.* Each zone can be sensing properly or be in **fault**. When an intrusion is detected on a zone, it causes an **alarm** to be reported for that zone. The APU can also be placed in a secure enclosure with a switch attached to the door; when the door is opened, the switch is opened, and the APU reports that it is a **tamper** condition.

Other conditions of interest are a power failure on the unit, a failure on the communications port, or some other condition that causes the APU to be non-responsive. These failures cannot be reported by the APU (obviously) but must be detected by the monitoring software and reported as a **communications failure**.

Here is a summary of the primary conditions of interest:

Condition	APU or zone	When it begins	When it ends
Alarm	Zone	Intrusion identified	N/A
Fault	Zone	Failure to sense cable	Sensing restored
Tamper	APU	Enclosure opened	Enclosure closed
Comm. failure	APU	Monitor can't talk with APU	Communication restored

A later section will describe how the XML protocol describes these conditions.

Note: the 300 series APU has a light labelled 'event'. This 'event' concept is used for configuration purposes and is not reported to monitoring equipment.

*Note: the 500 series APU has a concept called **hyperzone**. A hyperzone is an intermediate node between the APU and one or more zones. Conditions reported on the hyperzone should be ignored.*

Communications Concepts

For the monitoring equipment to communicate properly with the APU, a TCP/IP connection must be made. This connection can either be made from the APU to the monitoring equipment (Active) or from the monitoring equipment to the APU (Passive). Often the monitoring equipment has a preference that determines which method the customers must use. Sometimes the monitoring equipment can support either method and leaves the issue up to the customer.

Current APUs support only a single connection at a time. Thus, simultaneous redundant connections are not possible. However, if redundant monitoring equipment is in use, a failover mechanism can be set up. (Documents describing this in more detail are available.)

Note: the XPort configuration web interface has been customized for Fiber SenSys and does not show all of the standard fields. However, the fields are available through telnet.

The protocol used by APUs conforms to the ICD-101B standard, developed by the Security Equipment Integration Working Group of the United States military. This standard, based on XML over TCP/IP, is used both for communications with many different types of sensors but also for exchange between multiple monitoring systems. Contact SEIWG¹ for access to the ICD-101B standard itself.

As implemented in Fiber SenSys APUs, the ICD-101B protocol has the following aspects:

- A handshake sequence that establishes the connection.
- A keep-alive mechanism that maintains the connection; this can also be used to detect a communications failure with the sensor.
- Report messages that inform the monitoring equipment of the other conditions of interest described above.

Overall, the protocol consists of a sequence of XML messages. A message consists of a complete XML document, including XML declaration. (Note: XML declarations to the APU are ignored; the character set is assumed to be ISO-8859-1.) Whitespace may occur between messages. The APU may send XML messages other than those described below²; such messages should be discarded.

Integration Design

The software design for integration depends on the monitoring software. However, a typical pattern is to add a module to the monitoring software that establishes and maintains communications with the APUs and translates any conditions of interest to the monitoring software's preferred inputs.

¹ <http://www.acq.osd.mil/ncbdp/nm/pseag/about/seiwig.html>

² In addition to other message types, an otherwise valid XML message may contain an invalid data sequence and fail to parse correctly. In particular, at one time users were allowed to enter device names that included XML characters such as '<' but did not escape such characters. Newer software prevents users from entering such names.

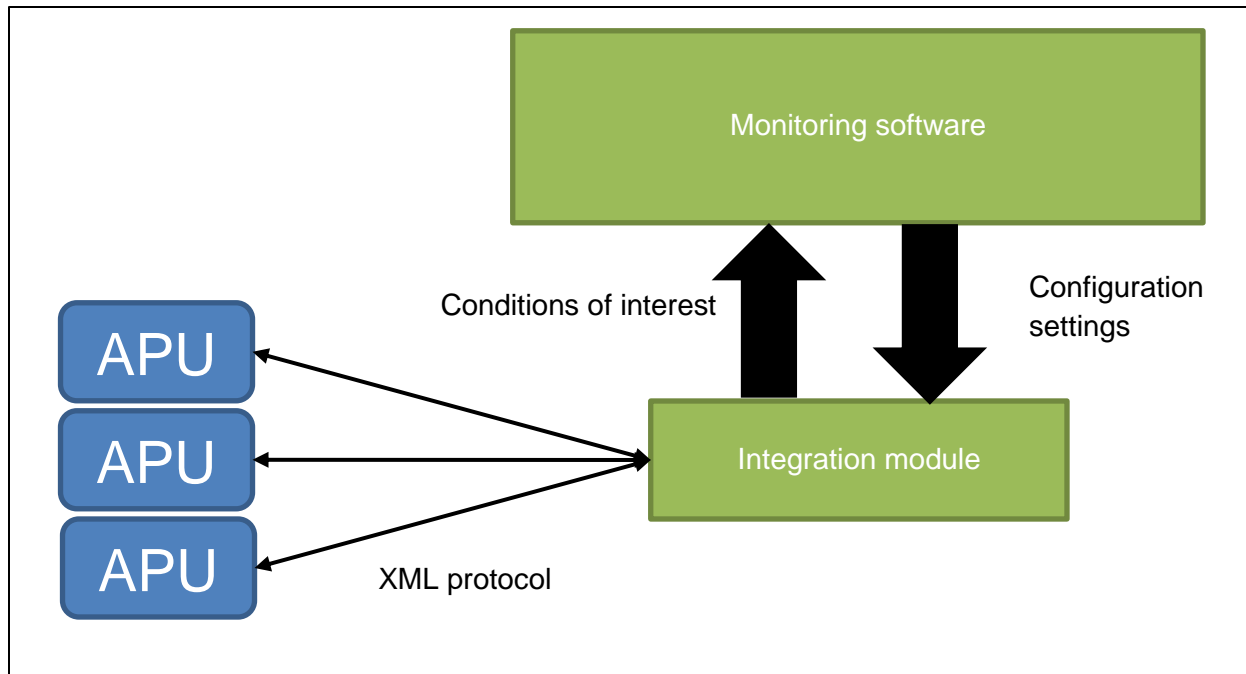


Figure 1: Typical integration design pattern

The integration module will need to support the following:

- APU's are TCP/IP devices.
 - They communicate over a TCP connection using XML messages.
 - This connection can either be to the APU (Passive) or from the APU (Active).
 - There is a “handshake” sequence that must be used to establish a connection.
 - There is a “ping” sequence that must be used to maintain the connection.
 - Each APU has a unique device name.
 - An XML message is sent when a detection or a change of APU state occurs³.
 - An APU contains one or more detection zones.
- Zones are sensing regions within the APU.
 - In XML messages, zones are described as sub-devices.
 - Each zone has a name that is unique within the APU.
 - An XML message is sent when a detection or a change of zone state occurs⁴.

Protocol Details

As mentioned before, APU's communicate using XML messages that conform to the ICD-101B standard. Fiber SenSys APU's use a subset of the standard messages.

Message types and usage

The messages that monitoring equipment should expect to receive are the following:

³ An example of APU state change is when an APU enters or leaves the tamper condition.

⁴ An example of APU zone state change is when the zone enters or leaves the cable fault condition.

- **PlatformStatusReport**, which describes the hierarchical structure of the APU along with the status of each part of the structure⁵.
- **DeviceStatusReport** and **DeviceDetectionReport**, which together indicate the conditions of interest (other than communications failure)⁶.
- **CommandMessage**, used for “Ping” messages.

You should have received XSD files that describe these messages in more detail. This document will describe the semantics of the messages.

Communications with Fiber SenSys APUs begins with a handshake sequence. It is important to follow this sequence correctly because otherwise the monitoring equipment will not be informed of previously entered conditions such as sensing fault or tamper.

To begin the handshake, establish a TCP/IP connection between the APU and the monitoring equipment. The monitoring equipment should then wait to receive a PlatformStatusReport⁷. This message indicates that the APU considers its previous connections closed and is ready for a new connection. It also provides the monitoring equipment with the DeviceName for the APU and the hierarchical structure and state of its zones. The monitoring equipment should react to this by sending a Ping request CommandMessage⁸.

The APU will respond to the Ping request by sending the following:

- A second PlatformStatusReport.
- (Sometimes) DeviceDetectionReport and DeviceStatusReport messages, depending on whether any zones are in sensing fault, the APU is in tamper, or an intrusion has (just now) occurred. These messages should be treated the same way as after the handshake is complete – see below.
- One or more DeviceConfiguration messages – ignore these.
- A Ping response.

Once the connection is established, the monitoring equipment should occasionally send a Ping request with the APU’s name to maintain the connection. After 130 seconds without receiving a Ping request, the APU will consider the connection closed and go back to waiting the handshake sequence.

If the APU does not reply to the Ping request, then the communications connection has failed and should be reported.

⁵ As of 2021, the existing 300 and 500 series devices do not report the status on the APU in the PlatformStatusReport. However, when the connection is established, these devices will follow the PlatformStatusReport with a DeviceStatusReport containing this information.

⁶ The DeviceStatusReport indicates changes in state and the DeviceDetectionReport indicates detections. The DeviceStatusReport XML structure is also used as a nested structure within a PlatformStatusReport message.

⁷ More information about and examples of PlatformStatusReports are included in the XSD file.

⁸ Examples of Ping request and response messages are included in the CommandMessage.xsd file.

While the connection is open, the APU will send out unsolicited DeviceDetectionReport and DeviceStatusReport messages to report intrusion alarm, sensing fault, and tamper conditions. The XSD files describe details of these structures but because these conditions are reported in different ways, this document will describe the messages that you should expect for various conditions.

Intrusion alarm

When an intrusion occurs on a zone, a DeviceDetectionReport message will be sent for that zone. See the DeviceDetectionReport.xsd file for an example.

As a reminder, intrusions are detections, not state changes. APUs do not have the notion of “being in” an ongoing alarm condition. When multiple messages are received it is because multiple alarms were generated.

Sensing fault

When a zone is unable to sense properly, both a DeviceDetectionReport and a DeviceStatusReport are sent. When sensing has been restored, a DeviceStatusReport will be sent *but* not another DeviceDetectionReport.

Here is a zone sensing fault example, starting with a 500 series APU zone going into fault. Note that this is reported by having the DeviceState change to the `Fault` state.

```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceDetectionReport>
  <DeviceDetectionRecord>
    <DeviceIdentification>
      <DeviceName>FD508-100913.HZONE-2.ZONE-006</DeviceName>
      <DeviceCategory>Sensor</DeviceCategory>
      <DeviceType>SPIDR Zone</DeviceType>
    </DeviceIdentification>
    <Detection>
      <ID>SZ00015</ID>
      <DetectionEvent>Fault</DetectionEvent>
      <UpdateTime Zone="GMT">2070-01-03T08:13:49.164</UpdateTime>
    </Detection>
  </DeviceDetectionRecord>
</DeviceDetectionReport>
<?xml version="1.0" encoding="UTF-8"?>
<DeviceStatusReport>
  <DeviceIdentification>
    <DeviceName>FD508-100913.HZONE-2.ZONE-006</DeviceName>
    <DeviceCategory>Sensor</DeviceCategory>
    <DeviceType>SPIDR Zone</DeviceType>
  </DeviceIdentification>
  <Status>
    <DeviceState>Fault</DeviceState>
    <CommunicationState>Fail</CommunicationState>
    <UpdateTime Zone="GMT">2070-01-03T08:13:49.165</UpdateTime>
  </Status>
</DeviceStatusReport>
```

```
</Status>  
</DeviceStatusReport>
```

When the zone comes out of fault, the DeviceState changes to the `Secure` state⁹:

```
<?xml version="1.0" encoding="UTF-8"?>  
<DeviceStatusReport>  
  <DeviceIdentification>  
    <DeviceName>FD508-100913.HZONE-2.ZONE-006</DeviceName>  
    <DeviceCategory>Sensor</DeviceCategory>  
    <DeviceType>SPIDR Zone</DeviceType>  
  </DeviceIdentification>  
  <Status>  
    <DeviceState>Secure</DeviceState>  
    <CommunicationState>OK</CommunicationState>  
    <UpdateTime Zone="GMT">2070-01-03T08:13:58.161</UpdateTime>  
  </Status>  
  <Detection>  
    <DetectionEvent>Other</DetectionEvent>  
    <Details>Internal line fault</Details>  
    <UpdateTime Zone="GMT">2070-01-03T08:13:58.161</UpdateTime>  
  </Detection>  
</DeviceStatusReport>
```

Similar messages will come from a 300 series APU.

Tamper condition

When a tamper conditions occurs on an APU, the APU will change to the `Tamper` state and a `DeviceStatusReport` message will be sent for that APU. See the `DeviceStatusReport.xsd` file for an example.

Configuration changes

When the APU's structure has been changed, such as a zone having been added or removed, or when the `DeviceName` on the APU has been renamed, then another `PlatformStatusReport` will be sent containing the new structure with the removed devices in the `Deleted` state.

Monitoring equipment must react to this message. There is no single best policy for this. Some sites and users prefer that the monitoring equipment automatically re-configure itself. Others require manual intervention to avoid unintended or unauthorized reconfiguration.

⁹ This assumes that there is not some other zone condition that would not be secure. As of 2021, the existing 300 and 500 series devices only report `Fault` and `Secure` state for zones, but monitoring equipment should be prepared to receive additional state types.

Testing Your Integration with APU Simulators

The Device SDK comes with APU simulator software. The simulators allow testing to be done without an actual APU. It only simulates the communication of APUs, not the logic involved in discovering intrusions. Each simulated APU needs a separate IP address. Because of this, the simulator software is broken up into a client and server. The separation of the client and server allows the simulated APUs to be run from a computer better equipped to handle more than one IP address while still allowing a developer to control the simulators remotely. The server is a simple console application that only prints out when a new simulator is created. The client is a GUI application that allows a user to add, remove or update simulators on the server.

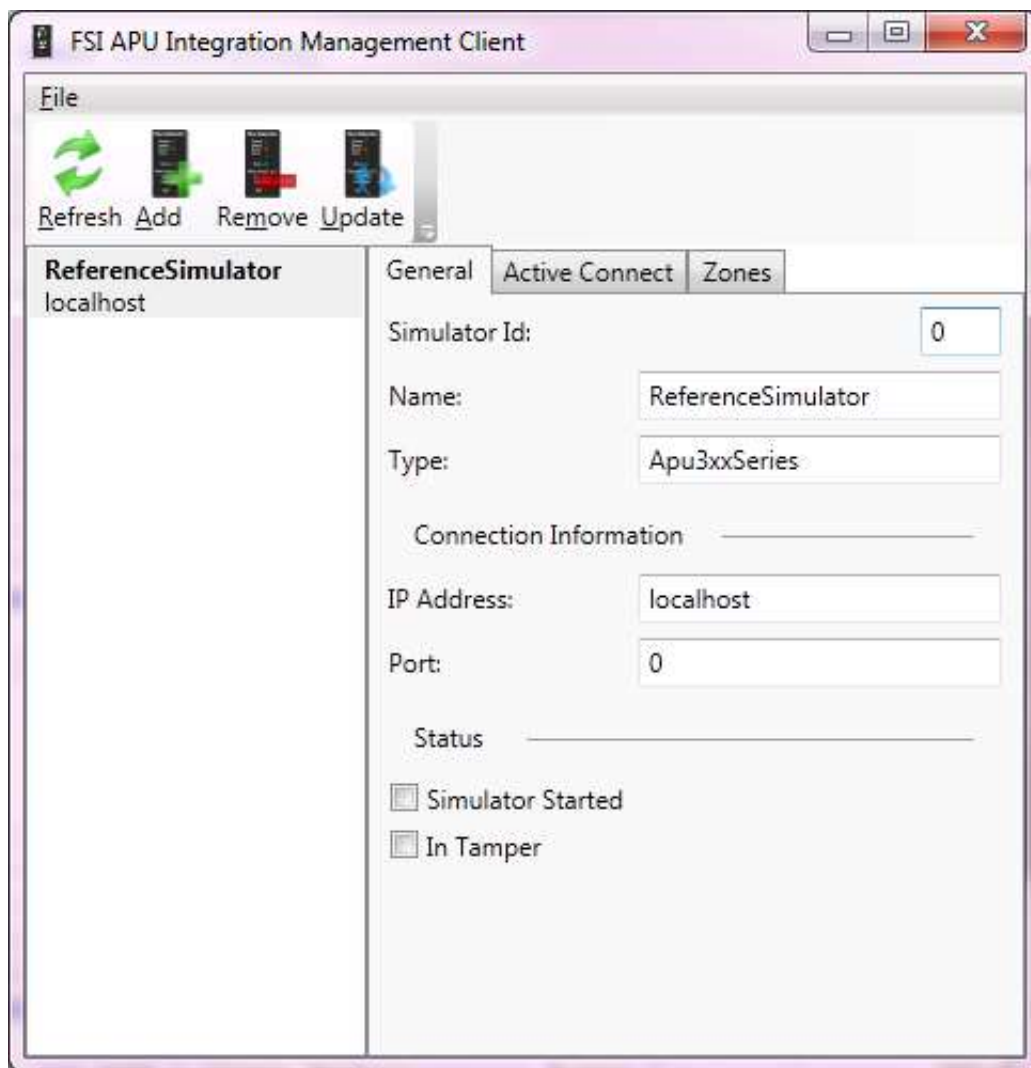


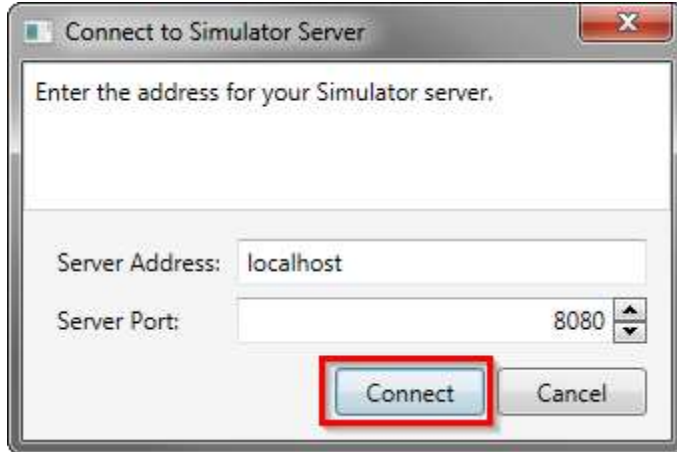
Figure 2 Simulator Client

Figure 2 Simulator Client shows the main window of the client. The various tabs in the main window contains check-boxes representing the different states of the simulator. Modifying a checkbox then clicking the Update button, will update the state of the simulator. For example under the Zones tab, modifying the Alarm checkbox of one or more of the channels and clicking

Update will cause the simulator to send out alarm messages to the connected integration software.

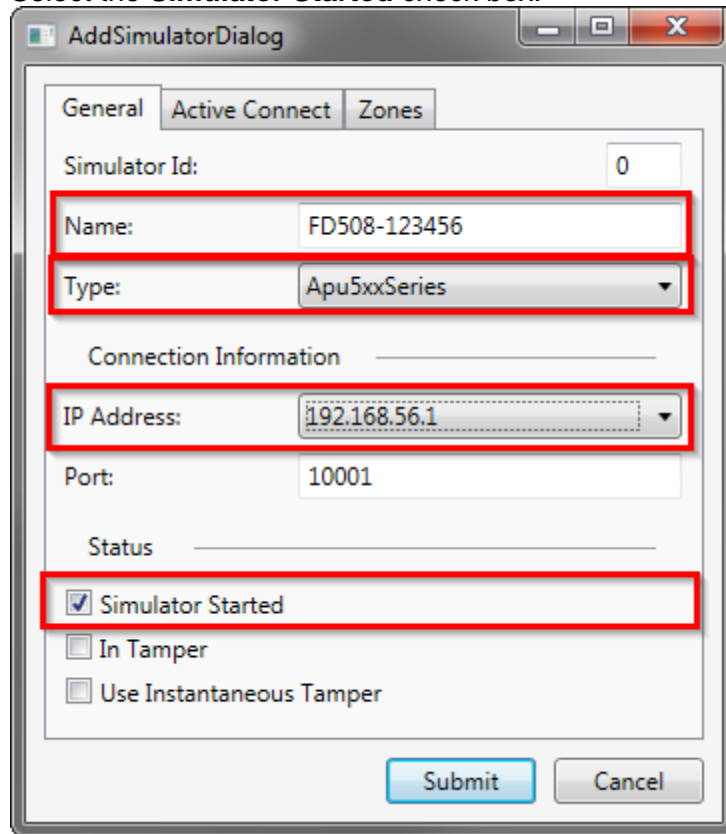
Using the Simulators

1. Start the server. The default location is {username}\Documents\Fiber SenSys\Device SDK\Simulators\Server\FSI.Simulators.Server.exe. The server can be minimized as there is no further interaction required for it.
2. Run the client. The default location is {username}\Documents\Fiber SenSys\Device SDK\Simulators\Client\FSI.Simulators.Client.exe
3. On **Connect to Simulator Server** click **Connect**.



4. Click **Add** to create a new simulated APU.
5. In the **AddSimulatorDialog General** tab:
 - a. Type the APU name in the **Name** box. An example name for a 500 Series APU is FD508-123456.
 - b. Click the desired APU type in the **Type** list. The main difference between 5xx and 3xx APUs is the 500 series has a concept called “hyperzones” in addition to zones.
 - c. Click one of the IP address from the **IP Address** list. An IP address will be listed for each interface on the computer. There can only be one simulated APU per interface. Provide this IP address to the Fiber SenSys Integrator software to connect to the emulator.

- d. Select the **Simulator Started** check box.



The screenshot shows the 'AddSimulatorDialog' window with the 'General' tab selected. The fields are as follows:

- Simulator Id: 0
- Name: FD508-123456
- Type: Apu5xxSeries
- Connection Information:
 - IP Address: 192.168.56.1
 - Port: 10001
- Status:
 - ☒ Simulator Started
 - ☐ In Tamper
 - ☐ Use Instantaneous Tamper

Buttons at the bottom: Submit, Cancel.

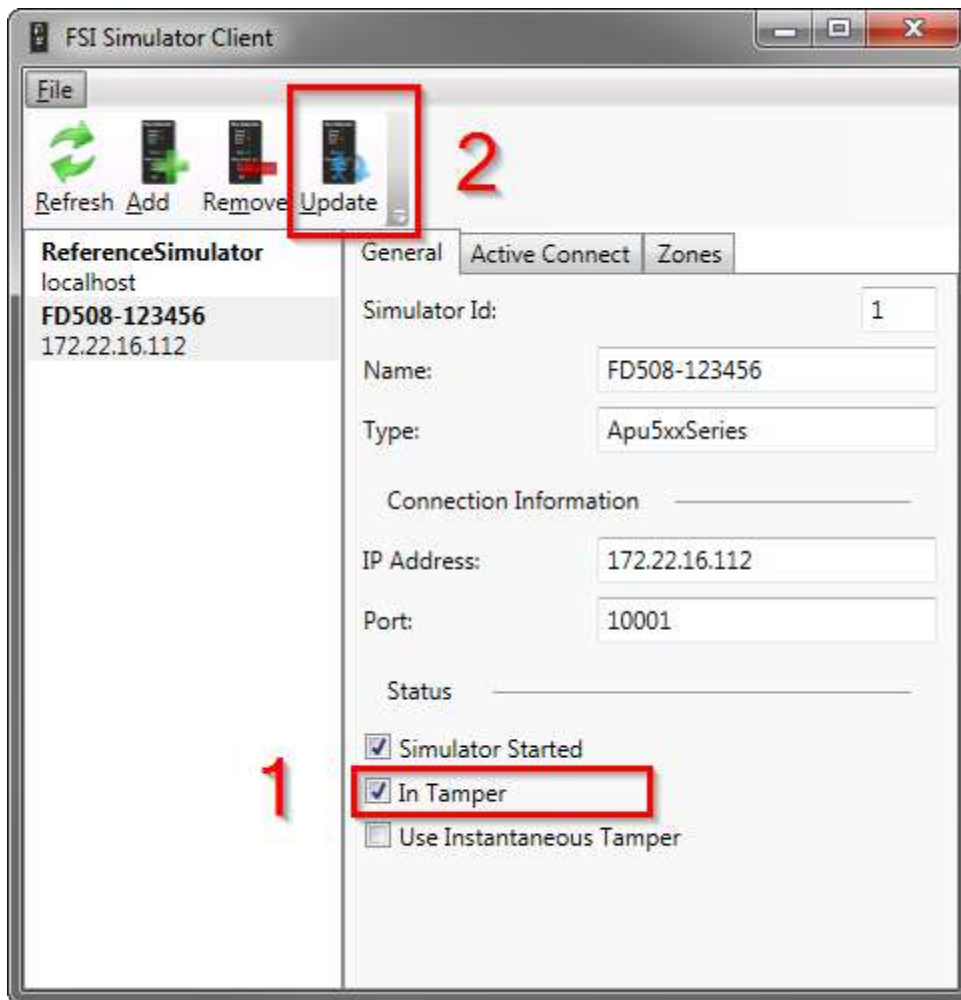
6. In the **Zones** tab use **Add Hyperzone** and **Add Channel** to add hyperzones and channels to the emulated APU. For 500 series APUs there must be one hyperzone. For

all APUs there must also be one channel.

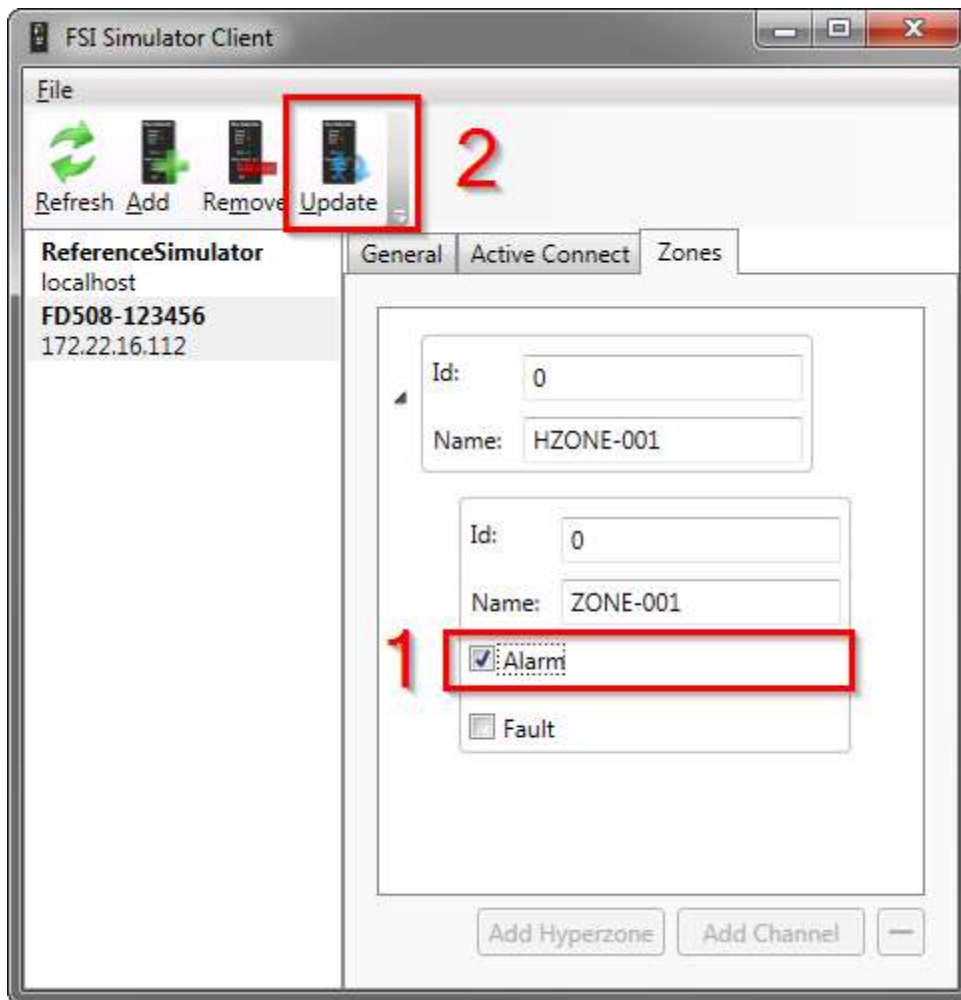
The screenshot shows the 'AddSimulatorDialog' window with the 'Zones' tab selected. It contains three zone entries. The first entry, with Id: 0, is highlighted in blue and has its 'Name' field (HZONE-001) highlighted with a red box. The second entry, also with Id: 0, has its 'Name' field (ZONE-001) highlighted with a red box. The third entry, with Id: 1, has its 'Name' field (ZONE-002) highlighted with a red box. Each zone entry includes checkboxes for 'Alarm' and 'Fault'. At the bottom of the dialog are buttons for 'Add Hyperzone', 'Add Channel', 'Submit', and 'Cancel'.

7. Click **Submit** to create the emulated APU.

Now various events can be simulated. To simulate a tamper select the **In Tamper** check box and click **Update**.



To simulate an alarm or fault go to the **Zones** tab and select **Alarm** or **Fault** for the desired zone. Click **Update** to apply and actually send the event.



Note: Don't forget to click **Update** after changing tamper, fault, or alarm check boxes.

For more information, please contact us at:

info@fibersensys.com

Tel: +1(503) 692-4430

Toll free (US) +1(800) 641-8150

www.fibersensys.com