|  |  |  |
| --- | --- | --- |
| Thruput logo red on white | | |
| **Thruput Limited,** 6 Whitworth Road, Marston Trading Estate, Frome, Somerset, BA11 4BY, United Kingdom | | |
| E: sales@thruput.co.uk | T: +44 1373 300 818 | W: www.Thruput.co.uk |

**TSP (C#)**

**Software Development Notes**

**Work in Progress**

This document is the copyright of the Thruput Limited. No material may be reproduced, copied, translated or modified without the express written permission of Thruput Limited.

Sentineltm, MIDAStm, *The Graphix Factory*tm and TruePixeltm are trademarks of Thruput Limited

Thruput products are fully dvi_logo and **VESA** Compliant.

**Contents**

[1 Summary 3](#_Toc20297234)

[1.1 References 3](#_Toc20297235)

[1.2 Development Environment 3](#_Toc20297236)

[1.3 The build process 3](#_Toc20297237)

[1.4 The release process 3](#_Toc20297238)

[1.5 Work still to do 3](#_Toc20297239)

[2 Work performed by Release 4](#_Toc20297240)

[2.1 Release 1.7 – 20/09/2019 4](#_Toc20297241)

# Summary

This document started on contains an overview of the design and development work performed on the C# version of the TSP Suite since 20th September 2019.

## References

The ‘Issue #’ numbers refer to the unique numbers in the Issue Tracker Spreadsheet stored on the server in the folder \\192.168.11.250\Testing\IssueTracker.

.

## Development Environment

The impound tools was developed using:

Visual Studio 2019 – Community Edition

The source code folder was:

E:\Chris\Work\SoftwareDevelopment\TSP (C#) Vx.x.x

Source control (SVN)

http://192.168.11.250/repos/Software/S900\_Sentinel\_VideoRecorder/src/branches/Sentinel\_Recorder\_Vx.x.x

## The build process

Open SentinelTechnicalSupervisor.sln

Select Release

Build/Rebuild

Open Installer/installer.iss and compile

## The release process

After developer testing place the installation and the updated release notes in :

\\192.168.11.250\Testing\1) Work in Progress\yyyy-mm-dd\xxxxxxxxxx

Circulate an email for it to be tested

Once testing is complete copy the folder to :

\\192.168.11.250\Testing\2) Complete\\yyyy-mm-dd\xxxxxxxxxx

Ensure that everything is under source control including this document.

## Work still to do

# Work performed by Release

## Release 1.7 – 20/09/2019

The requirement is to implement Issue # 23 - Clear all alarms and warnings on a channel when placing it into maintenance mode

### Version Number

The release number was bumped up to 1.7 from 1.5.3, with agreement from Paul to skip over the not used version 1.6 which used the codemeter software licensing system.

Change the version numbers iun the assemblyinfo in ConfigureTSP and TechnicalSupervisor properties.

Change the version number in installer/installer.iss

Change the version number in installer/etc/Readme.txt

### Code investigation

The maintenance modes are changed in Form4.button4\_Click

##### The Maintenance log update

The update to the maintenance log occurs at line 1908 of ConfigInterface.cs.

So one solution would be at this point to also clear any alarms for that channel

This is executed in a background worker thread so that the main GUI is not blocked.

##### Clearing Alarms for a channel

To clear all alarms the following SQL statement is executed:

UPDATE eventLog SET acknowledged=1 WHERE (level >= 2) or (level < 0)

So I would assume that the command therefore is:

UPDATE eventLog SET acknowledged=1 WHERE channel = the channel id

##### Clearing Alarms for a full system

The channel number comes through as if it is the whole system – which really means the NAS it is talking to. So in this case simply clear acknowledge all alarms.

I.e. UPDATE eventLog SET acknowledged=1

So the code is:

//CRR 20/09/2019 Issue #23 - Clear current alarms on a channel if it's maintenance mode is being set to true

if(item.active)

{

string ClearAlarmSQL;

string ClearAlarmReply;

if (item.channel < 0)

{

ClearAlarmSQL = String.Format("UPDATE eventLog SET acknowledged=1"); // Acknowledge all Alarms on the NAS

}

else

{

ClearAlarmSQL = String.Format("UPDATE eventLog SET acknowledged=1 WHERE channel = {0}", item.channel.ToString()); // Acknowledge alarms for the specific channel

}

if (!Execute(ClearAlarmSQL, out ClearAlarmReply))

ret = false; // Failed to get a reply..

}

Released to :

Folder: \\192.168.11.250\testing\_rw\1) Work in Progress\2019-09-20 - Pre Release TSP (C#) version 1.7 9 (Clear Alarm when apply Maint Mode)

## Release 1.7 – 20/09/2019

The requirement is to implement Issue # 25 –

The C# TSP can delay up to 60 seconds before showing the correct status on the various items. Can this be reduced or eliminated ?

These tests were performed on an old version of the TSP . They will retest on the latest.

## Version 1.8ALPHA Experimental

The brief from Mike is to extract the records from the Logs.DB eventLog the same way that the TSP does and display in ‘dos box’ .

## Version 1.8 – Full SNMP functionality

Version 1.8 was released for testing together with SNMPAgent 2 on 4/12/2019 .

The Sentinel Technical Supervisor supports the following command line options:

-config <configuration folder> Specify the configuration folder

If this is not specified a default folder is used

-d Enable debug

-h Display help and exit

-i Install a new configuration

This can be used in conjunction with the -config option

-l <log folder> Place a copy of the events into the specified log folder

-snmp Collect the event log via snmp

-u Uninstall the configuration

This can be used in connjunction with the -config option

-v3 Use the encrypted SNMP v3 protocol

## Version 1.8.0.3 – Simplified the MIB and added time events were collected

Version 1.8.0.3 was released for testing together with SNMPAgent 2.0.0.3 on 4/11/2019

## Version 1.8.0.4 – Read the SNMP configuration from a file.

-xml filename needs to be added to the command line options

The options to be in the configuration file are:

-config <configuration folder> Specify the configuration folder

If this is not specified a default folder is used

-d Enable debug

This can be used in conjunction with the -config option

-l <log folder> Place a copy of the events into the specified log folder

-snmp Collect the event log via snmp

-v3 Use the encrypted SNMP v3 protocol

Example XML file:

<?xml version="1.0" encoding="utf-8" ?>

<thruput>

<tsp>

<debug>Y</debug>

<logfolder>c:\temp\logs</logfolder>

<usesnmp>Y</usesnmp>

<snmpv3only>Y</snmpv3only>

~~<snmpusername>agentAuthPriv</snmpusername>~~

~~<snmpauthpassword>auth</snmpauthpassword>~~

~~<snmpprivpassword>priv</snmpprivpassword>~~

</tsp>

</thruput>

### Notes from discussion on 22/01/2020

**Logging in/out and Usernames and passwords**

1. In future users will need to log into the SNMP TSP with a username and password
2. The usernames and passwords will be used to authenticate the communications with the SNMPAgent
3. An invalid username and password will result in no communication with  the SNMPAgent.
4. There will be an option to logout from the SNMP TSP
5. No timeout to force a logout is required on the SNMP TSP
6. There will be a button on the SNMP TSP where the user may clear alarms on the monitored servers (NASs). However the alarms will only be cleared if the user has entered the correct username and password.
7. The SNMPAgents will maintain a list of usernames, passwords and a definition of the priotity of each user.
8. User priorities are:

‘Normal User’: Only view Alarm and Warning events

‘Super User’: View Alarms, Warnings and Information events

‘Administrator’ : View Alarms, Warnings and Information events  and acknowledge all alarms

**Information returned from the SNMPAgent**

1. The SNMPAgent will now also return unacknowledged events for devices that are in maintenance mode in response to a ‘GET’ statement. Previously events for devices in maintenance mode were ignored.
2. An additional field will be added to the event data being returned by the SNMPAgent which will define if the device is in maintenance mode or not.

**SNMP TSP**

1. The SNMP TSP will filter out the SNMP messages for devices in maintenance mode before updating the SNMP TSP mimic display.

**C# TSP**

1. No changes are proposed.

**Possibly for the future**

1. A local ‘maintenance’ or ‘muted’ mode which can be used to ‘silence’ and not display errors for specified device on the local SNMP TSP  ( and C# TSP ? ) . A box will be popped up over the mimic display of the device indicating it is in ‘maintenance’ or ‘muted’ mode.
2. Provided an audit of users logging in and out.

### Notes from discussion on 3/2/20

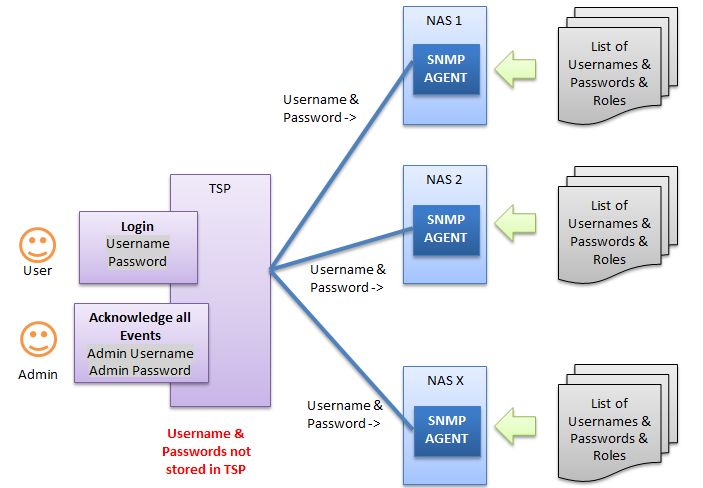
* The SNMP TSP can be run up and opened without a user logging in – However the objects on the Mimic display will be shown in grey and a message saying something like “Not Logged In” will be displayed.
* Upon a successful login the username will be displayed on the Mimic display
* The SNMP TSP will keep a text file log of the user logins
* When the user logs in the TSP will display a ‘please wait icon’ and attempt to connect to the SNMPAgents on the connected NAS devices.
* On the sucessful connection to one or more NAS devices the mimic display will then indicate the status of each device.
* If some NAS devices respond and some do not then the Mimic display will show those devices which do not respond in grey.
* An additional GET item will be added to the SNMP MIB called ‘AckAllEvents’ which when requested with a GET command with the correct user credentials will acknowledge all of the unacknowledged events in that NAS.
* It is also proposed to add an additional GET item to the SNMP MIB called ‘VerifyUser’ which will be used to check that the passed user credentials are correct or not.
* The SNMPAgent will keep a log of requests to ‘acknowledge all events’.
* The usernames, passwords and roles are stored on the NAS in a simple text file, eg:

james abcdefgh normal

jane abcdefgh super

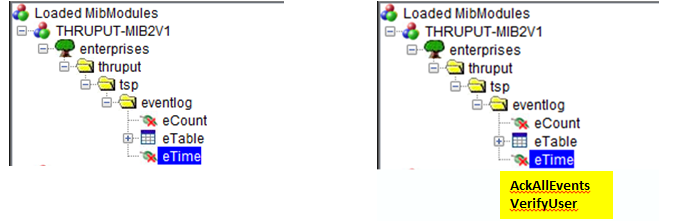
jack abcdefgh admin

I created the following diagram as I thought it would be useful during the discussion:



Suggested modifications to the SNMP MIB

**Current Proposed**



Please let me know if I have missed anything.

|  |  |  |
| --- | --- | --- |
| Best regards | | |
|  | | |
| **Chris Ringrow** | | |
|  | | |
|  | | |
|  | **Thruput Limited**  6 Whitworth Road,  Marston Trading Estate, Frome,  Somerset, BA11 4BY, United Kingdom. | T: +44 1373 300 818  W: [www.thruput.co.uk](../../../../../Neil/Dropbox/Sales%20Documents/Master%20Documents/Thruput%20New%20Blank%20Master%20documents/Frome%20-%20Not%20ready%20for%20use/www.thruput.co.uk)  E: [chris.ringrow@thruput.co.uk](mailto:chris.ringrow@thruput.co.uk) |

### Discussion with Mike and Paul 03/02/2020 at 15:00

* The logon screen, logout screen, user names and passwords are only to be added to the SNMP version of the TSP
* The user will be presented with a login screen when the SNMP TSP starts up and the mimic display will not be shown until they successfully log in.
* When the user logs out the login screen will be displayed which will hide the mimic display.
* Once the user has successfully logged in the mimic display will be shown with all of the Mimic objects being initially coloured green.
* Ensure that the released version of the SNMPAgent has a default administrator username, eg:
* Username: administrator
* Password: administrator
* Role: Administrator