EnvisaLink™ TPI Programmer's Document

DEVELOPER DOCUMENTATION

VERSION 1.08
February 10, 2017

1.0 Overview

The EnvisaLink™ Third Party Interface (TPI) consists of a set of commands and responses designed to allow third-party command and control applications to interface directly with the EnvisaLink™ module and in turn the security system, over a TCP/IP connection.

The goal in releasing this programmer's interface is not only to allow existing home-automation software greater interaction with the EnvisaLink module, but also to encourage the development of third-party applications on mobile platforms.

2.0 Connecting to the Envisalink™

2.1 Hardware Connections

Please refer to Envisalink installation or “Quick Start” document.

2.2 TCP Connection

The Envisalink acts as a server for the TCP connection and the user application is the client. The Envisalink listens on port 4025 and will only accept one client connection on that port. Any subsequent connections will be denied.

The Envisalink will close the connection if the client closes its side.

To initiate a connection, the application must first start a session by establishing a TCP socket. Once established the TPI will send a 5053 command (See section 3.0 for a detailed description of the protocol) requesting a session password.

The client should then, within 10 seconds, send 005 login request. The 005 command contains the password which is the same password to log into the Envisalink's local web page. Upon successful login, the Envisalink's TPI will respond with the session status command, 505, and whether the password was accepted or rejected. If a password is not received within 10 seconds, the TPI will issue a 5052 command and close the TCP socket. The socket will also be closed if the password fails.

Once the password is accepted, the session is created and will continue until the TCP connection is dropped.

Note, as with all network communications, it is possible the TCP socket could be lost due to a network disruption, or an exception at either the client or server end. Application programmers are advised to include some handling for dropped connections. The Poll command (000) is a useful command to test of the connection is still alive. Alternately, an application could watch for the period time broadcast (510) which is issued by the panel every 4 minutes.

Enivsalink 3 vs Envisalink 4 Difference
The Envisalink 3 only supports 6 ASCII digits for a password but the Envisalink 4 supports 10.

IMPORTANT: Envisalink Application Firewall
As of Envisalink 4 (1.0.102) and Envisalink 3 (1.12.180) the Envisalink has an internal firewall that will block all TPI connections that originate outside of the network segment it resides upon. This is to protect users who expose their Envisalinks to the public Internet either by mistake or ignorance. This feature can be **disabled** by changing the default user's password from “user” to any other password, 4 characters or longer.

3.0 Detailed Description of the Feature Set

3.1 Communications Protocol

All data is sent as hex ASCII codes. The transmission from will consist of the following:

CCC DDD…DDD CKS CR/LF

CCC => 3 Digit Command
This tells the module or the application what to do. Commands are 3 characters long. For example, the Status Command (001) would be sent as hex ASCII codes ‘30 30 31’. See the following tables for a list of supported commands.

DDD…DDD => Data Byte(s)
This is the data that may be needed for the command. For example, after the Partition Arm command (030), the application must specify which partition should be armed (1-8). The following tables show what the data requirements are for each command. Some commands, like the User Closing, have space holding zeros. In this case all 4 digits are sent even though this module ever uses only two.

CKS => Checksum
The checksum is calculated by adding the hex value of all command and data digits, and truncating the result to 8 bits. The upper and lower nibbles of the result are converted to ASCII characters before sending. For example, a Partition Alarm on partition 3 would be sent like this:

The command and data fields contain: 6 5 4 3
The ASCII codes for this would be: 36 35 34 33
36 + 35 + 34 + 33 = D2. Since the result is already 8 bits we don’t have to worry about the length and simply send it.

Format	Command	Data	Checksum	CR/LF
Code	6 5 4	3	D 2	CR LF
ASCII	36 35 34	33	44 32	0D 0A

CR/LF => Carriage Return & Line Feed
Each transmission is followed with a carriage return (hex ASCII 0D) and a line feed (hex ASCII 0A) to indicate the end of a transmission.

3.2 Application Commands

Description	Command	# of Data Bytes	Data Bytes
Poll The TPI will respond with a Command Acknowledge code. Note: The POLL command will also reset the Envisalink's network watch-dog timer. If there is no communications with the Envisalerts servers for a period of 20 minutes, the Envisallink will reboot. Sending the TPI POLL command will reset this timer. Useful if the module is not connected to the Internet or firewalled.	000	0	
Status Report The TPI will send updates for all general zone, partition, and trouble status to the Application (Troubles will be limited to indicating the status of the Trouble LED on a keypad). Only the partitions that have been detected, and their trouble states, will be displayed. Please see section 3.5 for more information.	001	0	
Dump Zone Timers This will dump the internal Envisalink Zone Timers. See command 615	008	0	
Network Login The command is sent by the client after it has created a TCP connection to the TPI to open a session. The TPI will respond with command 505 if the login was successful. The password is the same as the local Envisalink password for the web page.	005	1-6	Password, case sensitive
Set Time & Date The TPI will change the time and date to that sent by the application. Please note it may take up to 4 minutes for this command to be reflected on all the keypads on the security system.	010	10	hhmmMMDDYY
Command Output Control The TPI will activate the selected Command Output	020	2	Partition (1-8) Output (1-4)
Partition Arm Control The TPI will attempt to arm the selected partition. The partition will be armed in AWAY mode (no zones bypassed).	030	1	Partition (1-8)
Partition Arm Control – Stay Arm The TPI will attempt to stay-arm the selected partition.	031	1	Partition (1-8)
Partition Arm Control – Zero Entry Delay The TPI will attempt to arm the partition with zero entry delay.	032	1	Partition (1-8)
Partition Arm Control – With Code The TPI will attempt to arm the selected partition by using a User Code. This is equivalent to entering a User Code while the partition is in the Ready mode.	033	7	Partition (1-8) Code (4-6 digit)
Partition Disarm Control The TPI will attempt to disarm the selected partition. This command can also be used to acknowledge alarms on a partition. Sending the Partition Disarm command will silence any alarms as well as disarm the partition.	040	7	Partition (1-8) Code (4-6 digit)
Time Stamp Control Sending a '1' (ON) will cause the TPI to prepend all TPI commands with an 8 digit timestamp followed by a single space (0x20). For backwards compatibility the default state is OFF. Note, the timestamps do not form part of the packet format and hence are not included in the checksum.	055	1	On/Off (1,0)
Time Broadcast Control Sending a '1' (ON) will cause the TPI to periodically transmit system time broadcasts (TPI COMMAND 550). The default state is OFF.	056	1	On/Off (1,0)
Temperature Broadcast Control Sending a '1' (ON) will cause the TPI to periodically transmit the interior	057	1	On/Off (1,0)

and exterior temperatures (TPI COMMANDS 561,562). The default state is OFF. This applies to the EMS-100 only. Use command 080 to force a 561 report with the STAT50 et al.			
Trigger Panic Alarm This command emulates the FAP (Fire, Ambulance, Police) panic keys on a DSC keypad. Send this command, with 1, 2, or 3, will cause an immediate alarm. This assumes the panel is properly programmed to allow such events to occur.	060	1	1 = Fire 2 = Ambulance 3 = Police
Single Keystroke – Partition 1 This command is provided for backwards compatibility. 071 is the preferred command. Send a single keystroke on Partition 1 only. NOTE: Any other characters other than those listed are ignored but the TPI still responds with a 500 if the checksum is good. This is for backwards compatibility with other interfaces.	070	1	ASCII(0..9, *,#,A)
Send Keystroke String (Max: 6 Keystrokes) This command allows the application to send a keystroke string as if the user pressed the equivalent key sequence on an existing keypad. WARNING: There is no error checking for state of the panel so the application must know what mode the panel is beforehand, before sending key presses.	071	2-7	Partition (1-8) ASCII(0..9, *,#)
Enter User Code Programming This command will cause the partition to enter user code programming (*5) mode if the partition isn't already busy.	072	1	Partition (1-8)
Enter User Programming This command will cause the partition to enter user code programming (*6) mode if the partition isn't already busy.	073	1	Partition (1-8)
Keep Alive Sending this command will reset the timer on the panel so it doesn't timed out. Useful when working in zone bypass mode or user account mode.	074	1	Partition (1-8)
Request Interior HVAC broadcast This command will force the Envisalink to issue TPI command 651, regardless of whether there is HVAC enabled.	80	0	
Code Send This command is used whenever there is a need to send a code. The command, such as command output, will be sent to the module and the module will then send command 900 to tell the user to enter an access code. This command transfers this code. *NOTE:* The code entered will be sent to the partition that sent the 900 request. The TPI remembers which partition the code request came from when sending 200: Code Send.	200	4-6	Access Code (4-6)

3.3 TPI Commands

Description	Command	# of Data Bytes	Data Bytes
Command Acknowledge A command has been received successfully	500	3	Previous CMD received
Command Error A command has been received with a bad checksum	501	0	
System Error An error has been detected. See section 5.4 for a list of error codes	502	3	000-255 (error code)
Login Interaction Sent during session login only. 3 = Request for password, sent after socket setup 2 = Time out. You did not send a password within 10 seconds. 1 = Password Correct, session established 0 = Password provided was incorrect	505	1	0 = Fail 1 = Successful 2 = Timed_Out 3 = Password Request
Keypad LED State – Partition 1 only Outputed when the TPI has detected a change of state in the Partition 1 keypad LEDs. Bit 7 – BACKLIGHT LED Bit 6 - FIRE LED Bit 5 - PROGRAM LED Bit 4 - TROUBLE LED Bit 3 - BYPASS LED Bit 2 - MEMORY LED Bit 1 - ARMED LED Bit 0 - READY LED	510	2	Byte (HEX) indicating LED state (ON/OFF).
Keypad LED FLASH state – Partition 1 only Outputed when the TPI has detected a change of state in the Partition 1 keypad LEDs as to whether to flash or not. Overrides 510. That is, if 511 says the PROGRAM LED is flashing, then it doesn't matter what 510 says. Bit 7 – BACKLIGHT LED Bit 6 - FIRE LED Bit 5 - PROGRAM LED Bit 4 - TROUBLE LED Bit 3 - BYPASS LED Bit 2 - MEMORY LED Bit 1 - ARMED LED Bit 0 - READY LED	511	2	Byte (HEX) indicating LED state (ON/OFF).
Time/Date Broadcast Outputs the current security system time.	550	10	HH:MM MM/DD/YY
Ring Detected The Panel has detected a ring on the telephone line. Note: This command will only be issued if an ESCORT 5580xx module is present.	560	0	
Indoor Temperature Broadcast If an ESCORT 5580TC is installed, and at least one ENERSTAT thermostat, this command displays the interior temperature and the thermostat number. For other thermostats you must request this command by using API command 080. *NOTE: The three digit temperature is a decimal representation of a signed byte. (0 – 255) representing -127 to 127 degrees. MSB is sign bit.*	561	4	Thermostat (1-4) Temperature (XXX)

Outdoor Temperature Broadcast If an ESCORT 5580TC is installed, and at least one ENERSTAT thermostat with an external temperature sensor, this command displays the exterior temperature and the thermostat number. *NOTE: The three digit temperature is a decimal representation of a signed byte. (0 – 255) representing -127 to 127 degrees. MSB is sign bit.*	562	4	Thermostat (1-4) Temperature (XXX)
Zone Alarm A zone has gone into alarm	601	4	Partition(1-8) Zone (001-064)
Zone Alarm Restore A zone alarm has been restored	602	4	Partition(1-8) Zone (001-064)
Zone Tamper A zone has a tamper condition	603	4	Partition(1-8) Zone (001-064)
Zone Tamper Restore A zone tamper condition has been restored	604	4	Partition(1-8) Zone (001-064)
Zone Fault A zone has a fault condition	605	3	Zone (001-064)
Zone Fault Restore A zone fault condition has been restored	606	3	Zone (001-064)
Zone Open General status of the zone.	609	3	Zone (001-064)
Zone Restored General status of the zone.	610	3	Zone (001-064)
Envisalink Zone Timer Dump This command contains the raw zone timers used inside the Envisalink. The dump is a 256 character packed HEX string representing 64 UINT16 (little endian) zone timers. Zone timers count down from 0xFFFF (zone is open) to 0x0000 (zone is closed too long ago to remember). Each “tick” of the zone time is actually 5 seconds so a zone timer of 0xFFFE means “5 seconds ago”. Remember, the zone timers are LITTLE ENDIAN so the above example would be transmitted as FEFF.	615	256	HEX string of 64 little endian UINT16 words
Bypassed Zones Bitfield Dump This command is issued upon leaving Zone Bypass programming (*1 on the keypad). It is a 16 character HEX string representing an 8 byte bitfield. This bitfield indicates which zones are currently in bypass. A “1” indicates the zone is in bypass. The lower 8 zones are in the first position of the bitfield. The developer can force this dump by using the keystring commands to enter and leave zone bypassing. i.e. “*1#” **Enivsalink 3 vs Envisalink 4 Difference** This command is currently only available on the Envisalink 3 with firmware revision 1.12.182 and higher.	616	16	HEX string of 8 bytes
Duress Alarm A duress code has been entered on a system keypad	620	4	0000 cannot trace user
[F] Key Alarm A Fire key alarm has been activated	621	0	
[F] Key Restore A Fire key alarm has been restored (sent automatically)	622	0	
[A] Key Alarm An Auxillary key alarm has been activated	623	0	
[A] Key Restoral An Auxillary key alarm has been restored (sent automatically)	624	0	
[P] Key Alarm A Panic key alarm has been activated	625	0	
[P] Key Restore A Panic key alarm has been restored (sent automatically)	626	0	
2-Wire Smoke/Aux Alarm A 2-wire smoke/Auxiliary alarm has been activated	631	0	
2-Wire Smoke/Aux Restore A 2-wire smoke/Auxiliary alarm has been restored	632	0	

Partition Ready Partition can now be armed (all zones restored, no troubles, etc). Also issued at the end of Bell Timeout if the partition was READY when an alarm occurred.	650	1	Partition (1-8)
Partition Not Ready Partition cannot be armed (zones open, trouble present, etc)	651	1	Partition (1-8)
Partition Armed Partition has been armed – sent at the end of exit delay Also sent after an alarm if the Bell Cutoff Timer expires Mode is appended to indicate whether the partition is armed AWAY, STAY, ZERO-ENTRY-AWAY, or ZERO-ENTRY-STAY.	652	2	Partition (1-8) Mode (0,1,2,3)
Partition Ready – Force Arming Enabled Partition can now be armed (all zones restored, no troubles, etc). Also issued at the end of Bell Timeout if the partition was READY when an alarm occurred.	653	1	Partition (1-8)
Partition In Alarm A partition is in alarm	654	1	Partition (1-8)
Partition Disarmed A partition has been disarmed	655	1	Partition (1-8)
Exit Delay in Progress A partition is in Exit Delay	656	1	Partition (1-8)
Entry Delay in Progress A partition is in Entry Delay	657	1	Partition (1-8)
Keypad Lock-out A partition is in Keypad Lockout due to too many failed user code attempts.	658	1	Partition (1-8)
Partition Failed to Arm An attempt to arm the partition has failed	659	1	Partition (1-8)
PGM Output is in Progress *71, *72, *73, or *74 has been pressed	660	1	Partition (1-8)
Chime Enabled The door chime feature has been enabled	663	1	Partition (1-8)
Chime Disabled The door chime feature has been disabled	664	1	Partition (1-8)
Invalid Access Code An access code that was entered was invalid	670	1	Partition (1-8)
Function Not Available A function that was selected is not available	671	1	Partition (1-8)
Failure to Arm An attempt was made to arm the partition and it failed.	672	1	Partition (1-8)
Partition is Busy The partition is busy (another keypad is programming or an installer is programming)	673	1	Partition (1-8)
System Arming in Progress This system is auto-arming and is in arm warning delay	674	1	Partition (1-8)
System in Installers Mode The whole system is in installers mode. If you did not enter Installers through the TPI, you will be locked out of most options	680	0	
User Closing A partition has been armed by a user – sent at the end of exit delay	700	5	Partition (1-8) User (0001-0042)
Special Closing A partition has been armed by one of the following methods: Quick Arm, Auto Arm, Keyswitch, DLS software, Wireless Key	701	1	Partition (1-8)
Partial Closing A partition has been armed but one or more zones have been bypassed.	702	1	Partition (1-8)
User Opening A partition has been disarmed by a user	750	5	Partition (1-8) User (0001-0042)
Special Opening A partition has been disarmed by one of the following methods:	751	1	Partition (1-8)

Keyswitch, DLS software, Wireless Key			
Panel Battery Trouble The panel has a low battery	800	0	
Panel Battery Trouble Restore The panel's low battery has been restored	801	0	
Panel AC Trouble AC power to the panel has been removed	802	0	
Panel AC Restore AC power to the panel has been restored	803	0	
System Bell Trouble An open circuit has been detected across the bell terminals	806	0	
System Bell Trouble Restoral The bell trouble has been restored	807	0	
FTC Trouble The panel has failed to communicate successfully to the monitoring station	814	0	
FTC Trouble Restore The panel has resumed communications	815	0	
Buffer Near Full Sent when the panel's Event Buffer is 75% full from when it was last uploaded to DLS	816	0	
General System Tamper A tamper has occurred with one of the following modules: Zone Expander, PC5132, PC5204, PC5208, PC5400, PC59XX, LINKS 2X50, PC5108L, PC5100, PC5200.	829	0	
General System Tamper Restore A general system Tamper has been restored.	830	0	
Trouble LED ON This command shows the general trouble status that the trouble LED on a keypad normally shows. When ON, it means there is a trouble on this partition. This command when the LED *transitions* from OFF, to ON.	840	1	Partition (1-8)
Trouble LED OFF This command shows the general trouble status that the trouble LED on a keypad normally shows. When the LED is OFF, this usually means there are no troubles present on this partition but certain modes will blank this LED even in the presence of a partition trouble. This command when the LED *transitions* from ON, to OFF.	841	1	Partition (1-8)
Fire Trouble Alarm	842	0	
Fire Trouble Alarm Restore	843	0	
Verbose Trouble Status This command is issued when a trouble appears on the system and roughly every 5 minutes until the trouble is cleared. The two characters are a bitfield (similar to 510,511). The meaning of each bit is the same as what you see on an LED keypad (see the user manual). They are bit 0 = Service is Required bit 1 = AC Power Lost bit 2 = Telephone Line Fault bit 3 = Failure to Communicate bit 4 = Sensor/Zone Fault bit 5 = Sensor/Zone Tamper bit 6 = Sensor/Zone Low Battery bit 7 = Loss of Time	849	2	1 HEX byte
Code Required This command will tell the API to enter an access code. Once entered, the 200 command will be sent to perform the required action. The code should be entered within the window time of the panel.	900	0	
Command Output Pressed This command will tell the API to enter an access code. Once entered,	912	2	Partition (1-8) Command(1-4)

the 200 command will be sent to perform the required action. The code should be entered within the window time of the panel.			
Master Code Required This command will tell the API to enter a master access code. Once entered, the 200 command will be sent to perform the required action. The code should be entered within the window time of the panel.	921	0	
Installers Code Required This command will tell the API to enter an installers access code. Once entered, the 200 command will be sent to perform the required action. The code should be entered within the window time of the panel.	922	0	

NOTES:

3.4 Special USER/MASTER Code Requirements

Some TPI commands will require a user code in order to execute. An example would be command output (CMD 020). The TPI does not know of the code requirement *a priori. S*o if a code is required by the panel, the TPI will issue a 900 command to indicate to the application that a 4-6 digit code must be entered.

Arming, disarming and functions that require codes to execute should follow this simple protocol.

1. Select the function (arm, disarm, output) by sending the appropriate command.
2. If a code is required, the TPI will send command 900.
3. The TPI must then respond with command 200 containing a valid user code.

If no code is required there will be no need for command 200. The application will have the panel's time window for entering the access code. If a command 200 is issued to the TPI outside of the panel's window, system error 26 (Command not Required) will be issued.

3.5 Special Considerations for some TPI Commands

While almost all the commands the TPI issues are event driven, that is to say they are issued in response to either some API command or some event within the scope of the security system, not all are. Some commands simply reflect the status of certain systems and therefore are only issued when a change of state is encountered. For example, command **650** tells the API that that the indicated partition is **READY**. Because this is really state information, it is only sent when the partition state transitions from another state, i.e. **PARTITION_IN_ALARM,** to the **READY** state. This also applies to Zone states.

The commands in particular are:

609, 610, 650, 651, 652, 654, 655, 656, 657, 670, and 671

The further impact of this situation is that upon power-up, the TPI is not immediately aware of state of all the zones. It is only when the TPI detects a *change* in the state will it know the true state and issue the appropriate change-of-state command listed above. Particular attention must be paid to the output of the API Command 001 (STATUS) as the state information it presents may be erroneous with respect to zone status if the TPI has recently been added to the security system bus. It is because the TPI has not seen a state transition yet and therefore must report the default state for zones; **READY** and **CLOSED** respectively. This does not apply to Partition Troubles, and Partition states. The panel updates the TPI with this information whenever it is idle so it is almost always available right after power-up.

3.6 Installers Mode - Warning

Using the TPI commands 070 and 071, you can conceivably put the panel into installers mode (*8). The danger here is that when in installers mode most of the commands are locked out so you could end up dead-locking yourself with the only way out of installers being to power cycle the panel.

3.7 TPI (502) Error Codes

The TPI command, 502 (system error), provides the application programmer a lot of information on the inner workings of the TPI, and the DSC security system in general. The following is the list of currently supported error codes and are self-explanatory. In cases where a BUSY or BUFFER_OVERRUN code are encountered, the application should retry after a small delay period. Commands prefixed by “API” indicate that the exception came from a command issued by the application, all others stem from either the TPI, or the panel.

ERROR CODE	DESCRIPTION
0	No Error
1	Receive Buffer Overrun (a command is received while another is still being processed)
2	Receive Buffer Overflow
3	Transmit Buffer Overflow
10	Keybus Transmit Buffer Overrun
11	Keybus Transmit Time Timeout
12	Keybus Transmit Mode Timeout
13	Keybus Transmit Keystring Timeout
14	Keybus Interface Not Functioning (the TPI cannot communicate with the security system)
15	Keybus Busy (Attempting to Disarm or Arm with user code)
16	Keybus Busy – Lockout (The panel is currently in Keypad Lockout – too many disarm attempts)
17	Keybus Busy – Installers Mode (Panel is in installers mode, most functions are unavailable)
18	Keybus Busy – General Busy (The requested partition is busy)
20	API Command Syntax Error
21	API Command Partition Error (Requested Partition is out of bounds)
22	API Command Not Supported
23	API System Not Armed (sent in response to a disarm command)
24	API System Not Ready to Arm (system is either not-secure, in exit-delay, or already armed)
25	API Command Invalid Length
26	API User Code not Required
27	API Invalid Characters in Command (no alpha characters are allowed except for checksum)

Version 1.0.8 Changes

– Added command 815

–