ETM® System Functional System Test

<Customer Name>

SecureLogix Corporation
13750 San Pedro Avenue, Suite 820
San Antonio, TX 78232
Main: (210) 402-9669
FAX: (210) 402-6992

Document Revision 1.2
July 10, 2015

System Acceptance Test Plan Revision History		
Date of Change	**Committed By**	**Description**
1/30/14	Jane Byrne	Validated test plan for site
9/4/14	Jane Byrne	Reworked Appendix A
7/10/2015	Jane Byrne	Added Call Recorder test section

I. Table of Contents

II. Introduction

A. Goals and Objectives

This document defines the Functional System Test (FST) for the ETM System. The FST was designed to validate the installation and configuration of the ETM System hardware and application software. ETM System tools are used to verify that hardware and software components are operating properly.

The purpose of the FST is to gain formal signoff that the SecureLogix installation tasks have been completed and the system has been accepted by the Customer.

B. Statement of Scope

The focus of the FST is on fundamental system functions of the ETM System; i.e. database connectivity, communications between distributed elements, ETM Appliance physical interface wiring, dial plan file configuration, etc. Operational configuration, such as ETM System voice firewall rules and alerts, are outside the scope of this FST.

C. Major Constraints

1. Full Operational Capability (FOC)

All known hardware or system configuration issues must be resolved at least four (4) hours prior to commencement of the FST.

A dry run of the FST is highly recommended.

2. Customer Witness

A customer representative will be expected to endorse individual test results. The customer therefore, should designate one or more witnesses to observe the entire FST.

3. Changes to This Document

All revisions to this document carried out after commencement of the FST must be approved in writing by both SecureLogix and the customer.

D. Supporting Equipment

1. Telephone

At minimum, a telephone connected to the customer's voice network with a known phone number must be available in order to make test calls. Inbound and outbound calls (depending upon Customer's voice network) may be necessary.

2. Destination Phone Numbers

A predetermined list of destination number(s) for test calls. These calls do not have to be answered.

III. Test Plan

A. Functions to be Tested

The following system functions will be validated during the FST:

- Basic ETM System Server Operation
- ETM System Console Client Data Network Communications
- ETM Platform Appliance Data Network Communications
- Voice Network Interface Configuration and Operation
- Usage Manager Report Server Communications
- Call Recorder Feature Configuration and Operation

B. Testing Strategy

1. Basic ETM System Server Operation

The ETM Management Server and the ETM Report Server platform as well as the Oracle RDBMS platform will be shutdown and restarted to ensure that the Oracle database and ETM System application services start normally. This test verifies that the following items are configured correctly:

a) Auto Startup at Boot

The Oracle database, the ETM Management Server, and the ETM Report Server applications should start up automatically when the server host is booted. Incorrect configuration of either the Oracle database or ETM Server application's startup files or services could prevent the ETM Servers from starting correctly.

b) License File

The server application will not start without a valid license file.

c) Database Availability

The ETM Management Server application will not start if the supporting Oracle database is not available and configured correctly.

d) ETM Server Configuration Parameters

The ETM Management Server and ETM Report Server applications' configurable parameters are stored in the

"twms.properties" file. Incorrect configuration of this file can prevent appliance to server connections, client to server connections, client to report server connections, and server to database connections.

2. ETM System Console Client Data Network Communications

An ETM System Console client session will be initiated from a platform other than the ETM Management Server or Oracle server to verify that the ETM Management Server is configured to accept external connections. Successful initiation of an ETM System Console client session verifies that the following items are configured correctly.

a) Customer's Data Network Configuration

The distributed components of the ETM System rely on the customer's data network for essential communications. If the network configuration settings defined within the ETM System Console client or ETM Management Server are incorrect or if the customer's network is incorrectly configured, the ETM Console Client will not be able to communicate with the ETM Management Server.

b) ETM System Console Client Port Configuration

The ETM Management Server listens for incoming ETM Console connections on a port defined in the "twms.properties" file. Misconfiguration could prevent ETM Console client connections.

c) DES Key Strings

The ETM Management Server application uses shared configuration and keys to authenticate ETM System Console client connection requests and to encrypt all client session data during transmission. The server and client strings must be identical or the client session cannot be initiated.

3. ETM Platform Appliance Data Network Communications

ETM Platform Appliances communicate with the ETM Management Server using TCP/IP protocols over the customer's data network. Each ETM Appliance "card" will be actively polled for status. A response indicating good card status verifies that the following items are configured correctly.

a) Physical Data Cabling

With physical ETM Platform Appliances (for TDM environments for example), data network cabling was installed to interconnect each device with the customer provided data network. Faulty or improperly installed cabling will prevent a device from connecting to the ETM Management Server.

b) DES Key Strings

The ETM Platform Appliances use a DES key string to authenticate with the ETM Management Server and encrypt packet payload while in transit. An ETM Platform Appliance cannot connect to the ETM Management Server if the DES Key strings do not match.

c) ETM Platform Appliance Port Configuration

The ETM Management Server listens for incoming ETM Platform Appliance connections on a port defined in the "twms.properties" file. Misconfiguration could prevent ETM Platform Appliance connections.

d) Customer's Data Network Configuration

The distributed components of the ETM System rely on the customer's data network for essential communications. If the network configuration settings defined within the ETM Console client or ETM Management Server are incorrect or if the customer's network is incorrectly configured, the ETM Console Client will not be able to communicate with the ETM Management Server.

e) Span Licensing

The availability of the Span interface on ETM Appliances reflects the licensing purchased by the customer. The count should match.

4. Voice Network Interface Configuration and Operation

The ETM Platform Appliance is configured at installation to monitor designated voice circuits. Tests will be performed to ensure no ETM System installation-induced errors are occurring on the voice network. Successful completion of these tests will verify that the following parameters are configured correctly.

a) Physical Telco Interface Cabling

In TDM environments, cabling was installed to insert each ETM Appliance between the commercial demarcation and the PBX. Faulty or improperly installed cabling will result in excessive error rates or the inability to process calls.

b) Circuit Characteristics

Incorrect configuration of the basic voice network details within the ETM Platform Appliance may result in excessive error rates, alarms, or the inability to process calls.

c) Call Detail Interpretation

Test calls will be placed on monitored circuits to ensure that call start, end, and addressing digits are interpreted correctly.

Default Span NPA - Each span is configured with a default NPA that is used in dial plan processing.

Channel Map Configuration - Incorrect configuration of the extension, incoming format, outgoing format, or format precedence in the span channel map could result in the generation of erroneous source or destination numbers.

Dial Plan Files - Dial plan files must be correctly configured and installed on each span.

5. Usage Manager Report Server Communications

The ETM System Usage Manager tool will be started and a sample report will be retrieved to verify that the ETM Report Server is available. Successful report generation verifies that the following items are configured correctly.

a) Report Server Configuration

The ETM Report Server listens for incoming connections on a port defined in the “twms.properties” file. Misconfiguration could prevent report server connections.

b) Report Generation

The ETM Usage Manager is the reporting application for the ETM System. Running a report and verifying properly formatted information will ensure analytical operations have access to all collected call details.

6. Call Recorder Feature Configuration and Operation

This is an optional section to be executed where the ETM Call Recorder feature has been licensed and installed. The ETM Collection Server and\or the ETM Web Manager tools will be started and sample recordings will be made to verify that call recordings are available and are of adequate sound quality. Successful call recordings verify that the following items are configured correctly.

a) ETM Management Server License

The Call Recorder feature must be included as a licensed feature within the twms.license file.

b) ETM Appliances

When the Call Recorder feature is licensed, the ETM Appliance(s) display settings specific to the Call Recorder feature, allowing them to direct media to an ETM Call Recording Cache (CRC) module. If these appliances settings are not properly configured, call recordings will not be made.

c) ETM Call Recording Cache (CRC)

The ETM CRC module may be deployed as a dedicated purpose server appliance (such as the ETM 5160) or co-reside on an appliance server with another application (such as with SIP or UTA applications). The CRC module must be configured to accept media streams from recording enabled spans. If desired, the CRC may also be configured to forward call recordings to a Collection Server. If the CRC is not configured properly, call recordings will not be made.

d) ETM Collection Server

If included as part of a project, the Collection Server is an application that is installed on a server. It will receive call recording files from one or more CRC modules and organizes the audio files in a fashion conducive to file searches and file archiving. The Call Recorder application must be configured to accept files from the appropriate CRC modules. If incorrectly configured, recorded calls will remain on the CRC.

e) ETM Web Application

If included as part of a project, the ETM Web Application is an applet that may be installed in a number of supported

web servers. It enables authorized users to access recorded calls that reside on one or more CRC modules. The ETM Web application must be properly configured to access CRC modules. If incorrectly configured, the user will not be able to access call recordings.

C. Test Record Keeping

Test result forms are found in Appendix A or Appendix B. Each individual test has a corresponding result Pass/Fail indicator. Any exceptions or comments must be entered in the provided section.

IV. Test Procedure

A. Functions to be Tested

The following general system functions will be tested during the FST:

- Basic ETM System Server Operation
- ETM System Console Client Data Network Communications
- ETM Platform Appliance Data Network Communications
- Voice Network Interface Configuration and Operation
- Usage Manager Report Server Communications
- Call Recorder Feature Configuration and Operation

B. Testing Procedure

1. Basic ETM System Server Operation Test

NOTE: This test will restart the ETM Management Server causing all ETM System Console client sessions to disconnect. Please notify all ETM System users before starting this test.

a) Preparation

Login to the server host and execute the following:

- From Windows Explorer or My Computer on the ETM Management Server host, navigate to the ETM System installation directory (Example: C:\Program Files\SecureLogix\ETM) and delete any files in the directory that are of the form:

  server-fatal-etm.log

  or

  server-fatal-etm-hhmmMMDDYYYY-N.log

b) Restart the ETM Management Server and Oracle Database Host Server Platforms

On both server platforms, restart Windows.

START | SHUTDOWN | RESTART

The servers will shutdown then restart.

c) Verify ETM Management Server Application Startup

Upon restart of the ETM Management Server platform, login to the operating system and wait two (2) minutes before verifying that there are no server fatal logs in the root of the ETM installation directory (e.g. <installation path>\ETM, or by default, C:\Program Files\SecureLogix\ETM).

From Windows Explorer or My Computer, navigate to the ETM System installation directory and go to the ps sub-directory.

Example: C:\Program Files\SecureLogix\ETM\ps

Verify the presence of an ETM lock file and note the modify date and time which should be within one minute of the current system time.

Wait one (1) minute and repeat the timestamp check on the lock file. Verify that the modify time on the lock file has incremented at least one minute. This indicates that the ETM Management Server is running and properly updating the lock file.

d) Verify Oracle Database Application Startup

Upon restart of the Oracle Database server platform, login to the operating system. Open the Windows Services management tool.

Open a run box. 
Type services.msc and press return.

Navigate to the Oracle services and verify both the listener service and the database created for the ETM System are both running.

2. ETM System Console Client Data Network Communications Test

a) Start the ETM System Console Client

Start the ETM System Console Client application from a properly configured workstation (other than on the server

host platform) and login using any valid ETM System user account.

b) Verify Session Connection

Verify that the Performance Manager properly initializes and will display the Firewall Policies, IPS Policies, Span Groups, Telco Configuration, and Platform Configuration branches.

3. ETM Platform Appliance Data Network Communications Test

a) Preparation

Expand the “Platform Configuration” node so that each “card” installed at the location under test is visible.

b) Validate Card Connectivity

Verify the quantity of ETM Appliances and ETM card sets displayed in the GUI matches what was physically installed.

c) Validate Card Operational Condition

Verify that the card icon next to each listed Controller Card is green. Excluding approved exceptions, there should be no additional icons visible at the card level.

Valid exceptions are as follows:

- “offline” to indicate spans that have been purchased and licensed, but are not connected to a telco span\trunk.
- T1 alarm bell (yellow, blue, or red) indicating a known telco error that has not yet been corrected by the customer. This is not an ETM System failure; it is correctly indicating the status of the span\trunk.

d) Validate Span Licensing

Expand each card to display the spans below. Verify the total count of spans visible in the GUI is equal to the number of licenses purchased for that location.

NOTE: An ETM 1024 analog appliance requires one purchased license but displays two (2) spans within the Performance Manager tree.

e) Validate Span Operational Condition

Excluding approved exceptions, verify there are no icons next to displayed spans.

Valid exceptions are as follows:

- "offline" to indicate spans that have been purchased and licensed, but are not connected to a telco span\trunk.
- T1 alarm bell (yellow, blue, or red) indicating a known telco error that has not yet been corrected by the customer. This is not an ETM System failure; it is correctly indicating the status of the span\trunk.

4. Voice Network Interface Configuration and Operation Test

a) Preparation

Locate each span under the Span Group node that is installed at the location under test and perform the following steps for each.

b) Reset Error Counters

Individually open the "Health and Status" tool for each span that is not in a telco error state or offline and locate the button to clear the Cumulative statistics.

Clear the stats and note the time on the test result sheet.

c) Error Counter Values

Allow a minimum of one (1) hour to elapse between the counter reset for an individual span in the previous step and the reading of that span's counter in this step.

Individually open the "Health and Status" tool for each span and review the Cumulative statistics counters.

Note any spans that are taking errors and log reason.

NOTE: The ETM System reports errors observed on the span. All errors are not service affecting. Many are common during normal operation. Each ETM Platform Appliance was validated at the time of install by a local PBX technician. It is then assumed any incrementing error counters during this test are related to the voice network, are

properly reported by the ETM System, and must be addressed by the customer.

d) Call Detail Interpretation

Activate the Call Monitor tool on the span to be tested.

For two-way spans, one incoming and one outgoing test call will be made. For one-way trunks, a single test call will be made in the appropriate direction.

Place the test call and find it on the channel monitor. Verify that the call start time, source phone number (if available), and destination phone number present correctly. End the call and verify that the call end time is correct.

5. Usage Manager Report Server Connection Test

a) Start the Usage Manager Report Tool

At the ETM System Console main screen, select and open the Usage Manager. Verify that the report tool starts up and displays its opening screen.

b) Generate a Report

(1) Create Report

From the Public node, right mouse click to create a new General Element. Use the following to define the specified settings on each tab.

General:	Report Element Name - <User Defined> Data Specification – Summary Only Table Layout – Size for page Table Style – Summary Columns Graphic Options – Minimize display of summary data
Detail:	Switch Span In/Out

	Source Raw Destination Destination Call Details Local Start Time Call ID
Summary:	Call ID – Count
Group:	Switch – Ascending/Normal, Order By Group, Display all Span – Ascending/Normal, Order By Group, Display all In/Out – Ascending/Normal, Order By Group, Display all Source– Ascending/Normal, Order By Group, Display all Raw Destination– Ascending/Normal, Order By Group, Display all Destination– Ascending/Normal, Order By Group, Display all Call Details– Ascending/Normal, Order By Group, Display all Local Start Time– Ascending/By Minute (By Second also ok), Order By Group, Display all
Order:	No Order
Chart:	No Chart
Trend:	No Trend
Filter:	Any Call Record

Save the Element using any appropriate name.

Create a report template containing the created element. To improve the readability of the report, adjust the page layout to landscape with a 0.5” border on all sides.

Run the report over the most recent full business day.

(2) Verify Results

The report will display information from all install locations, represented by the switch field. The data output lists the total number of calls on each span, sorted by call direction and source with the corresponding raw and interpreted destination number, start time, and call detail flags.

The report lists the total number of calls on each span, sorted by call direction and source with the corresponding raw and interpreted destination number, start time, and call detail flags.

Note: Depending upon the voice network, source numbers may not be available.

Verify that the raw destination numbers were correctly interpreted. It isn't necessary (or possible) to verify every listed number, instead check blocks of similar numbers. For example, all of the "1-800" calls will be listed in a contiguous block, just check that the first numbers in the block were correctly interpreted and flagged, and then skip to the next block.

Flags to be verified are:

- FREE – Toll-free numbers (1-800, 1-877, etc.)
- LOC – Local calls
- LD – Long distance calls
- INTL – International calls

The following table contains a sample of data in the specified report format.

Span	In/Out	Source	Raw Destination	Destination	Call Details	Local Start Time-By Minute	Count
Span:1	Inbound	[1](210)5554926	2105559611	[1](210)5559611	LOC	04/09 14:14	2
Span:1	Outbound	[1](210)5559611	3035552809	[1](303)5552809	LD	04/09 14:17	1

V. Appendix A – Acceptance Test

A. ETM System Functional System Test Results

	MS Startup		DB Startup	
	Pass	**Fail**	**Pass**	**Fail**
3.2.1 Basic ETM System Server Operation Test				

	Verify Session Connection	
3.2.2 ETM System Console Client Data Network Communications Test	**Pass**	**Fail**
Remote Client System #1		
Remote Client System #2		
Remote Client System #3		

	Card Connectivity		Card Operational Condition		Span Licensing		Span Operational Condition	
3.2.3 ETM Platform Appliance Data Network Communications Test	**Pass**	**Fail**	**Pass**	**Fail**	**Pass**	**Fail**	**Pass**	**Fail**
ETM 1012 Appliance								
Span 1								
ETM 3200								
Cardset #1								
Cardset #2								
Cardset #3								
Cardset #4								

	Error Counters		Call Detail Interpretation	
3.2.4 Voice Network Interface Configuration and Operation Test	**Pass**	**Fail**	**Pass**	**Fail**
Analog Span 1				
Digital Span 1				
Digital Span 2				
Digital Span 3				
Digital Span 4				
Digital Span 5				

Digital Span 6				
Digital Span 7				
Digital Span 8				
Digital Span 9				
Digital Span 10				
Digital Span 11				
Digital Span 12				
Digital Span 13				
Digital Span 14				
Digital Span 15				
Digital Span 16				

	Create Report		Verify Results	
	Pass	**Fail**	**Pass**	**Fail**
3.2.5 Usage Manager Report Server Connection Test				

B. Exceptions and/or Comments:

VI. Appendix B – Signature and Formal Acceptance

This Functional System Test was Executed on:	
Date _____	Time _____

Customer Representative:	SecureLogix Representative:
Name (Printed) _____	Name (Printed) _____
Signature _____	Signature _____
Title _____	Title _____