U.S. DEPARTMENT OF ENERGY

PNNL-22511-1

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Conformance Tool High Level Design Document

IEC 61850 Cyber Security Acceleration Project

TW Edgar

May 2013

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor Battelle Memorial Institute, nor any of their employees, makes **any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights**. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof, or Battelle Memorial Institute. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

**Available to DOE and DOE contractors from the
Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062;
ph: (865) 576-8401
fax: (865) 576-5728
email: reports@adonis.osti.gov**

**Available to the public from the National Technical Information Service,
U.S. Department of Commerce, 5285 Port Royal Rd., Springfield, VA 22161
ph: (800) 553-6847
fax: (703) 605-6900
email: orders@ntis.fedworld.gov
online ordering: http://www.ntis.gov/ordering.htm**

This document was printed on recycled paper.

(9/2003)

This Page Left Intentionally Blank

Contents

Figures

Acronyms and Abbreviations

CEDS	Cybersecurity for Energy Delivery Systems
ICS	Industrial Control System
IDE	Integrated Development Environment
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
PNNL	Pacific Northwest National Laboratory
SCADA	Supervisory Control and Data Acquisition
SSL	Secure Sockets Layer
SUT	System Under Test
TLS	Transport Layer Security
TMW	Triangle MicroWorks

1.0 Introduction

This document is the high level design document for the Pacific Northwest National Laboratory (PNNL) IEC 62351-3, 4 and 6 standards conformance test software toolkit.

1.1 Document Purpose, Scope, and Intended Audience

1.1.1 Document Purpose

This document should clearly communicate the design choices for the PNNL IEC 62351-3, 4 and 6 standards software conformance test software toolkit (Fire) for the CEDS IEC Cyber Security Acceleration project. This document will be used to focus and drive the development of a prototype system.

1.1.2 Document Scope

This document provides the high level vision of the software conformance test software toolkit’s design and its necessary components. This document is intended to be followed by a low level design document that provides the detail necessary for a software development team to develop a prototype.

1.1.3 Intended Audience

This document is intended to provide a consistent understanding of project deliverables for project members and partners.

1.2 Software Purpose, Scope, and Intended Users

1.2.1 Software Purpose

The software tool described in this document provides a test suite for testing conformance of vendor software and hardware that implements the IEC 62351-3, 4 or 6 security standards. This tool is designed to provide an implementation of semi-automated tests, both positive and negative, to assist industry in developing IEC 62351-3, 4 and 6 standards conforming and interoperable products. This tool is not designed for certification efforts and does not provide any guarantee of assurance in protocol interoperability.

1.2.2 Software Scope

This document defines the software architecture to implement and execute conformance tests. This software is only for conformance testing of equipment implementing the IEC 62351-3, 4 and 6 security standards. This document is an implementation of the conformance tests defined in the IEC 61850 Cyber Security Acceleration Project’s *IEC 62351 Conformance Tests* document.

1.2.3 Intended Software Users

The intended users of this software are power industry vendors developing equipment to the IEC 61850 for substation automation and IEC 62351-3, 4 and 6 standards.

2.0 Problem Space

Cyber security is a crucial aspect of communications for Supervisory Control and Data Acquisition (SCADA) and Industrial Control System (ICS) communication. Current practice provides a wealth of strong cryptographic mechanisms to provide information assurance. However, cryptographic strength is often undermined by implementation details. Security standards are developed to provide a common definition that is strong and provides interoperability between implementations. It is crucial to perform conformance testing to ensure that capabilities defined by the standard are implemented correctly and that no additional capabilities are provided that could undermine the security of the system.

3.0 Protocol Overview

3.1 IEC 61850

IEC 61850 is an international standard providing design guidance for a multi-layered substation network automation architecture. IEC 61850 and related standards are being developed to aid in the ease of installation of Intelligent Electronic Devices (IEDs). Previous industry protocols required the engineer or technician to have an intimate knowledge of how each device was configured and connected. Using IEC 61850 for substation automation, the data will provide enough information to allow easy and automated connection to a network and the overall control system.

3.2 IEC 62351

IEC 62351 is a suite of international standards under development. When published, it will provide guidance on securing messages being passed by IEDs. The parts specifically being tested as part of this project are:

- Part 3: Profiles including TCP/IP
- Part 4: Profiles including MMS
- Part 6: Security for IEC 61850

4.0 Testing

Due to software architectural considerations, categorizing positive and negative tests separately is beneficial for document clarity. Following are definitions for positive and negative tests in the context of this document.

4.1 Positive Testing

Positive testing is the process of validating that an implementation operates as expected; i.e., show that it does what it is supposed to do.

4.2 Negative Testing

Negative testing is the process of validating that an implementation doesn't execute outside the bounds of design; i.e., show that the implementation does not do anything that it is not supposed to do. In the context of this document, negative testing refers to performing tests that attempt to communicate with a device in a configuration outside of the bounds defined within the IEC 62351-3, 4 and 6 standards.

5.0 Software Architecture

5.1 Software Dependencies

The IEC 62351-3, 4 and 6 conformance testing software tool (Fire) depends upon the Triangle MicroWorks (TMW) Anvil and Hammer software tools, the accompanying IEC 61850 libraries and the TMW software's ability to create and run flowcharts. The TMW software flowcharts will be the user interface that ties the tools of conformance testing software together.

Due to the IEC 62351-3, 4 and 6 standard's dependency upon IEC 61850 for substation automation, it should follow that an IEC 62351-3, 4 and 6 conformance tool would require an implementation of IEC 61850. The TMW Anvil and Hammer tools are IEC 61850 conformance testing tools for server and client devices and provide the necessary foundation to create an IEC 62351-3, 4 and 6 conformance testing tool.

5.2 Overall Design

The Fire tool consists of a set of conformance test workflow files, a set of command line executables, and configuration and operation documentation. These files and executables require the TMW Anvil and Hammer tools. TMW provides workflow scripting within their IEC 61850 tool suite. This scripting ability provides the capability to define a workflow of processes and validation checks. In addition, this scripting capability provides a means to execute external software as part of the workflow. The conformance test workflow files defined in this document are TMW flowchart source files. Each flowchart file implements a specific conformance test defined in the IEC 61850 Cyber Security Acceleration Project's *IEC 62351 Conformance Tests* document. These source files are executed within the appropriate TMW tool to perform a conformance test. When and where the TMW tool does not provide the necessary functionality to cover a conformance test task, external executables will be provided that will be called by the conformance test workflows. Finally, conformance tests will require the system under test (SUT) to be precisely configured. As the method and process to configure equipment varies greatly between vendor and product line, it is unreasonable to expect the tool to automatically configure devices. Therefore, accompanying guidance and configuration profiles will be provided for each conformance test workflow. Figure 1 depicts the overall architecture of the conformance tool.

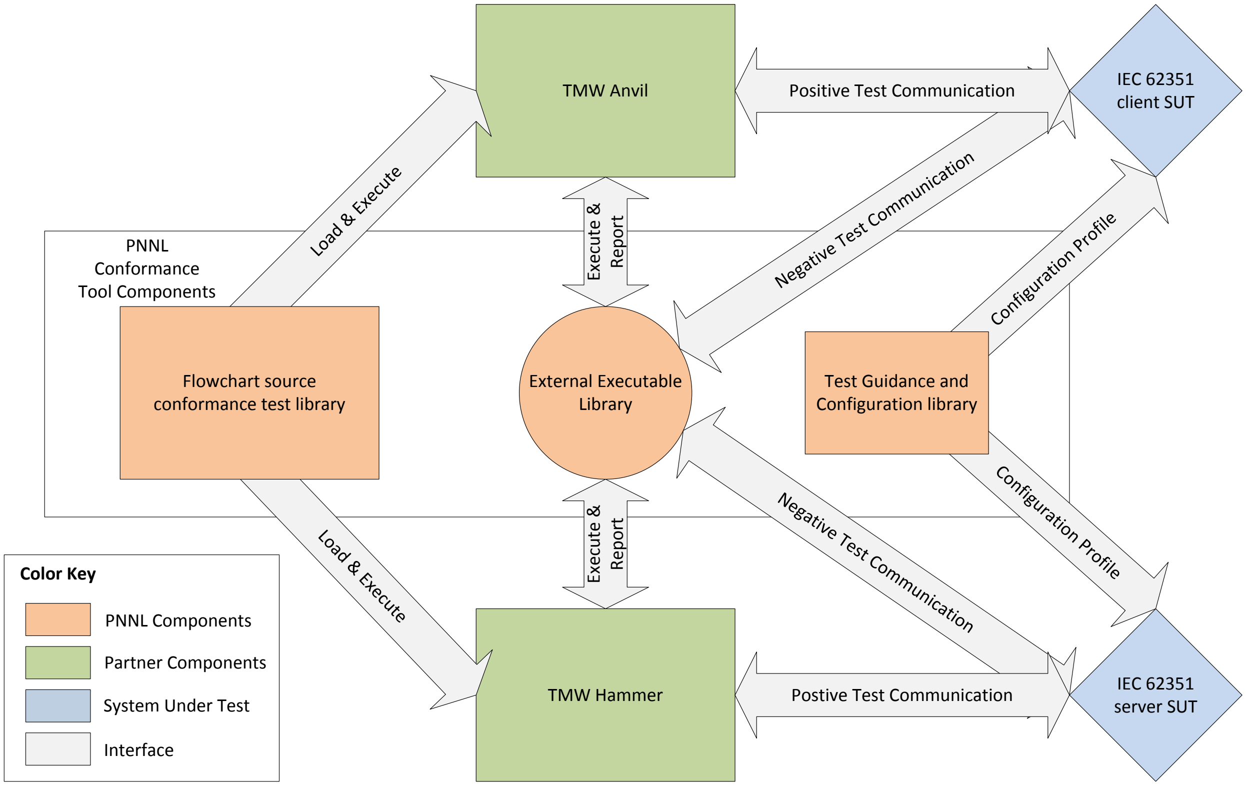


Figure 1: Conformance Tool High Level Architecture

To execute a conformance test, the user will read the accompanying guidance document and configure the SUT appropriately for the specific test. Next, the user will load a flowchart source file into the appropriate TMW application. Once the test is executed, the TMW application will run through the work flow of the test, configuring itself, communicating with the SUT, and evaluating the responses against expected results. If the test requires capability beyond those provided by the TMW applications, external applications will be executed at the appropriate locations to provide the necessary data to complete the conformance tests. The results of the test will be logged. A separate tool will be provided to generate a final conformance testing report at the end of the execution of tests.

5.3 Positive Testing

The TMW Anvil and Hammer tool provides implementations of IEC 62351capabilities. Therefore, the majority of positive tests can be defined completely within the Flow Chart IDE scripting.

5.4 Negative Testing

The TMW Anvil and Hammer tools do not provide access to underlying cryptographic libraries. Therefore, it is necessary to provide external executables that enable cryptographic functions that are not supported by conforming tools.

6.0 Software Conformance Workflow

6.1 Configuration Workflow

The battery of conformance tests will evaluate all of the possible configurations of an IEC 62351-3, 4 and 6 compliant device. Therefore it is necessary that the SUT be configurable in multiple ways. In order to do this, a process is required to correctly configure the SUT prior to each conformance test. This section will describe the high level workflow of the PNNL conformance tool for a user configuring a SUT in preparation for a conformance test.

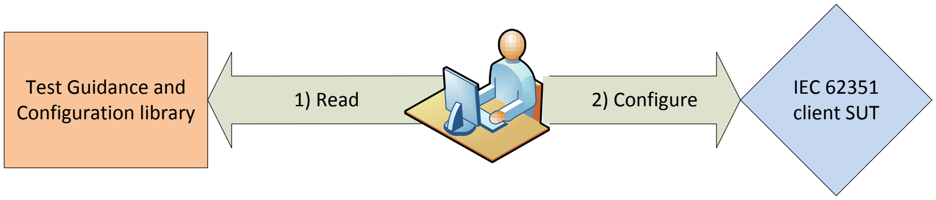


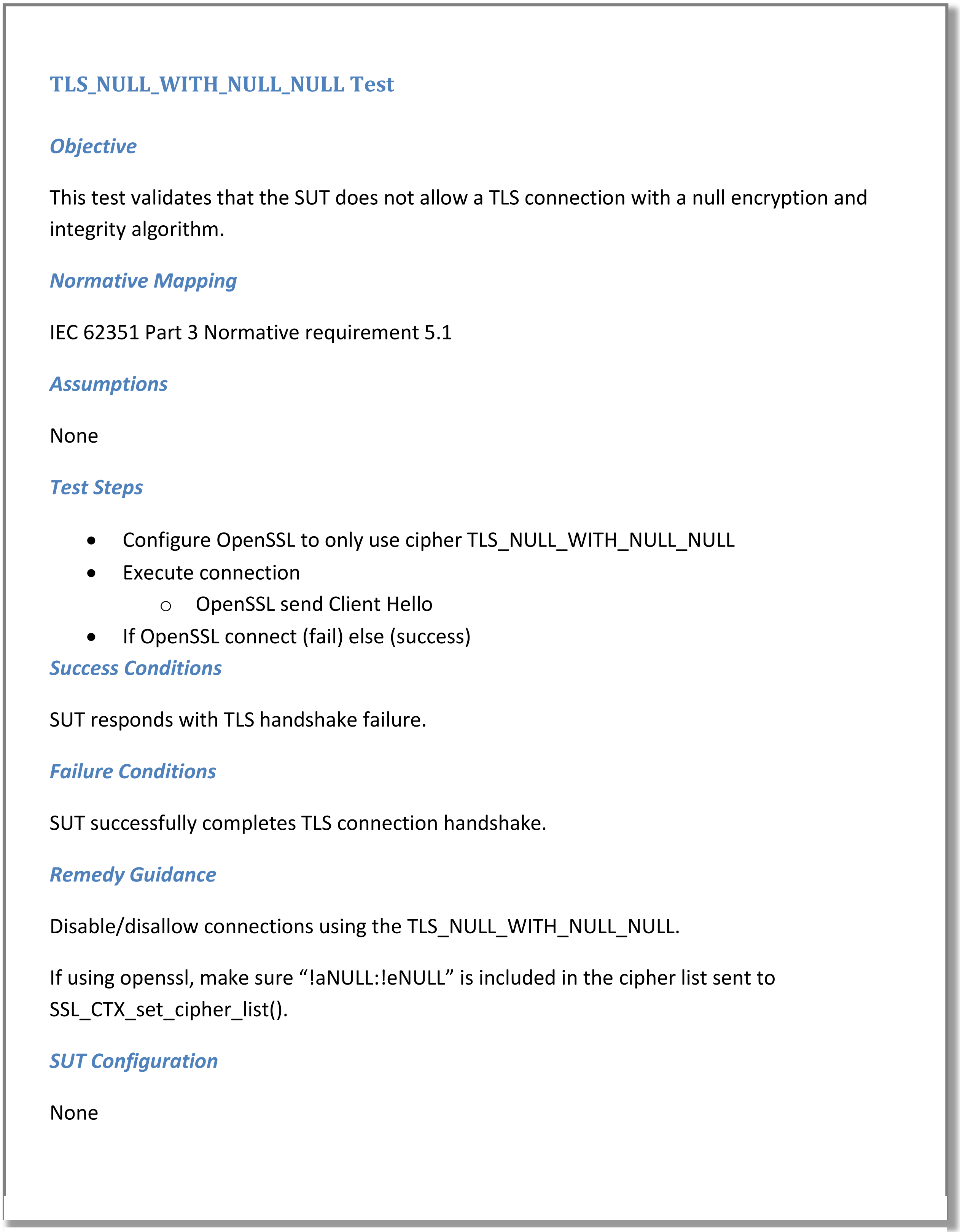
Figure 2: Configuration High Level Workflow

6.1.1 Selecting a Test

The first step is selecting a specific conformance test to execute. The tool provides a library of conformance tests that span multiple documents of the IEC 62351 standard suite (e.g. parts 3, 4 and 6). Depending on the device type and conformance level of the SUT, only a subset of conformance tests in the library will be applicable. Select the desired test from the library.

6.1.2 Test Guidance and Configuration Profile

Every conformance test in the library will have an accompanying *Test Guidance and Configuration Profile* document. This document will explain the objective of the test and contain a mapping to a normative standard requirement, any assumptions the tool makes about the SUT, what steps are executed, success and failure conditions, guidance on remedying failure conditions, and a SUT configuration profile. **Error! Reference source not found.** shows an excerpt from an example *Test Guidance and Configuration Profile* document.



TLS_NULL_WITH_NULL_NULL Test

Objective

This test validates that the SUT does not allow a TLS connection with a null encryption and integrity algorithm.

Normative Mapping

IEC 62351 Part 3 Normative requirement 5.1

Assumptions

None

Test Steps

- Configure OpenSSL to only use cipher TLS_NULL_WITH_NULL_NULL
- Execute connection
  - OpenSSL send Client Hello
- If OpenSSL connect (fail) else (success)

Success Conditions

SUT responds with TLS handshake failure.

Failure Conditions

SUT successfully completes TLS connection handshake.

Remedy Guidance

Disable/disallow connections using the TLS_NULL_WITH_NULL_NULL.

If using openssl, make sure “!aNULL:!eNULL” is included in the cipher list sent to SSL_CTX_set_cipher_list().

SUT Configuration

None

Figure 3: Example *Test Guidance and Configuration Profile* Document

The test objective describes what about the SUT is being tested. This is different than mapping to the standard because some normative requirements require multiple tests for complete validation.

The normative standard requirement states the standard and normative requirement reference that is the basis for a test.

Next is a list of assumptions that were made because of any ambiguity of the standard.

The test steps list the process steps and checks that are implemented and executed by the test. This information provides transparency into the test process and helps determine where and why a test failed or troubleshoot any errors if the assumptions were inaccurate for the SUT.

The success and failure conditions lists the different ways a SUT can pass and fail a test and describes what each condition means in the context of the test.

The remedy guidance offers potential items to evaluate or avenues to fix each failure condition. These are only provided to assist in pinpointing where an implementation could have failed conformity, but it is not guaranteed that the advice offered is the correct reason a device is responding improperly.

Finally, the SUT configuration profile lists the IEC 62351-3, 4 and 6 configuration variables that are pertinent for this test and how their values should be configured in the SUT. Some tests will require additional configuration files that will be referenced in this section of the *Test Guidance and Configuration Profile* that are included with the PNNL conformance test tool.

6.1.3 SUT Configuration

Due to the varied methods and tools required to configure IEC 62351-3, 4 and 6 capable devices, a SUT must be configured manually.

6.2 Positive Test Workflow

All conformance tests are equivalent from the user’s perspective. However, for the purpose of the design, there are conformance tests that can be fully implemented with the capabilities provided by the TMW tools and those that cannot. This section describes the workflow for the set that can be fully implemented using the TMW tools.

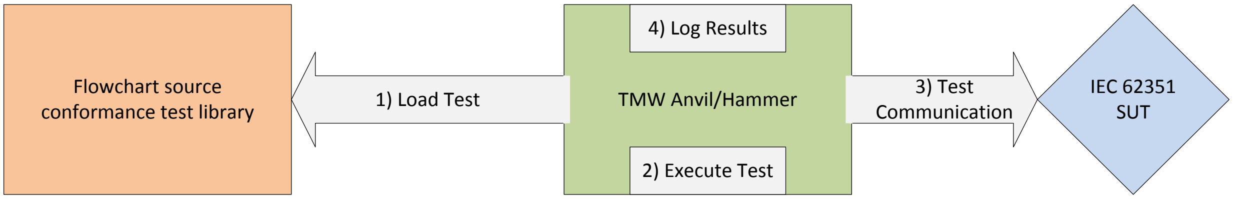
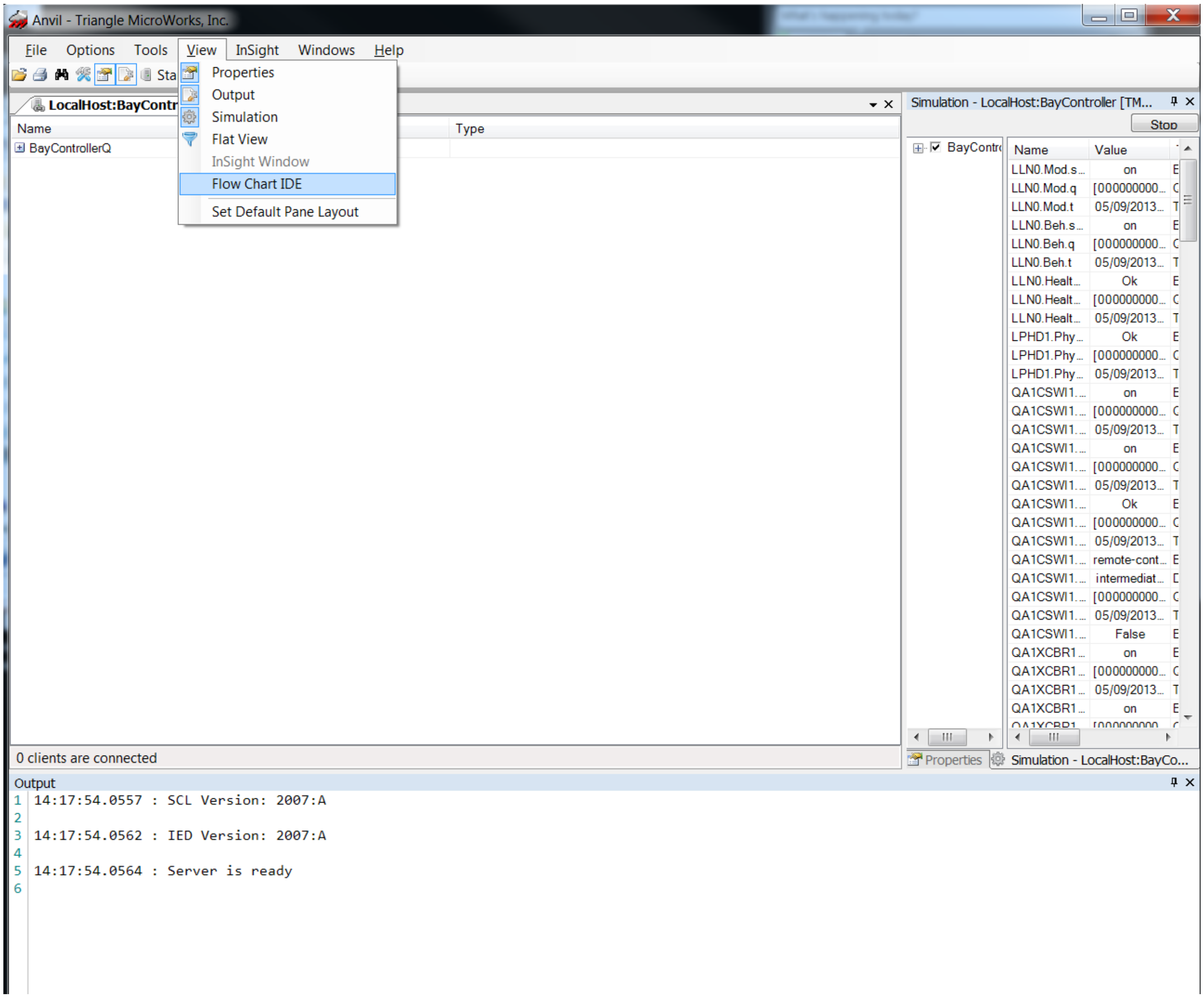


Figure 4: Positive Test High Level Workflow

6.2.1 Loading a Test

Loading a conformance test is merely loading a flowchart source file in one of the TMW products. This section documents the workflow to load a test.



0 clients are connected

Name	Value	
LLN0.Mod.s...	on	E
LLN0.Mod.q	[000000000...	C
LLN0.Mod.t	05/09/2013...	T
LLN0.Beh.s...	on	E
LLN0.Beh.q	[000000000...	C
LLN0.Beh.t	05/09/2013...	T
LLN0.Healt...	Ok	E
LLN0.Healt...	[000000000...	C
LLN0.Healt...	05/09/2013...	T
LPHD1.Phy...	Ok	E
LPHD1.Phy...	[000000000...	C
LPHD1.Phy...	05/09/2013...	T
QA1CSWI1....	on	E
QA1CSWI1....	[000000000...	C
QA1CSWI1....	05/09/2013...	T
QA1CSWI1....	on	E
QA1CSWI1....	[000000000...	C
QA1CSWI1....	05/09/2013...	T
QA1CSWI1....	Ok	E
QA1CSWI1....	[000000000...	C
QA1CSWI1....	05/09/2013...	T
QA1CSWI1....	remote-cont...	E
QA1CSWI1....	intermediat...	D
QA1CSWI1....	[000000000...	C
QA1CSWI1....	05/09/2013...	T
QA1CSWI1....	False	E
QA1XCBR1...	on	E
QA1XCBR1...	[000000000...	C
QA1XCBR1...	05/09/2013...	T
QA1XCBR1...	on	E
QA1XCBR1	[000000000	C

```
14:17:54.0557 : SCL Version: 2007:A

14:17:54.0562 : IED Version: 2007:A

14:17:54.0564 : Server is ready

```

Figure 5: TMW Flow Chart IDE Menu Item

Flowchart source files are a special case in the TMW tools and require opening a window separate from the main window. The user can select the Flow Chart IDE from the View menu.

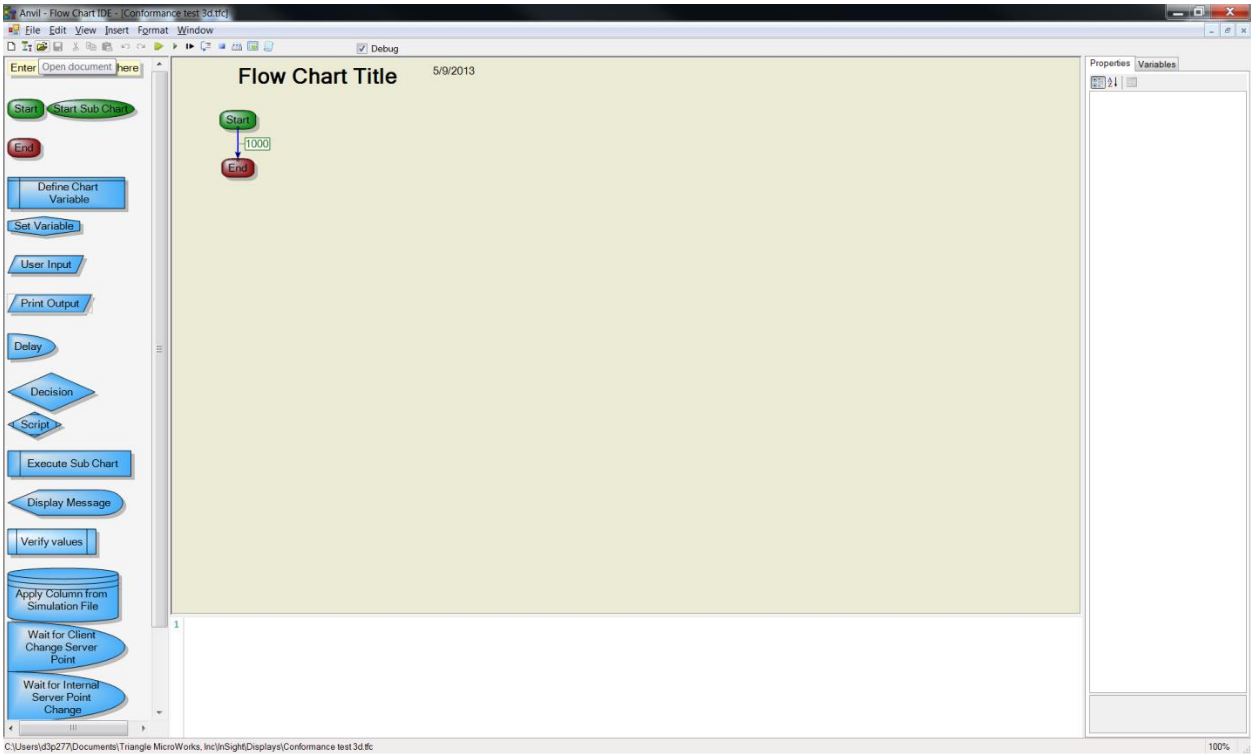
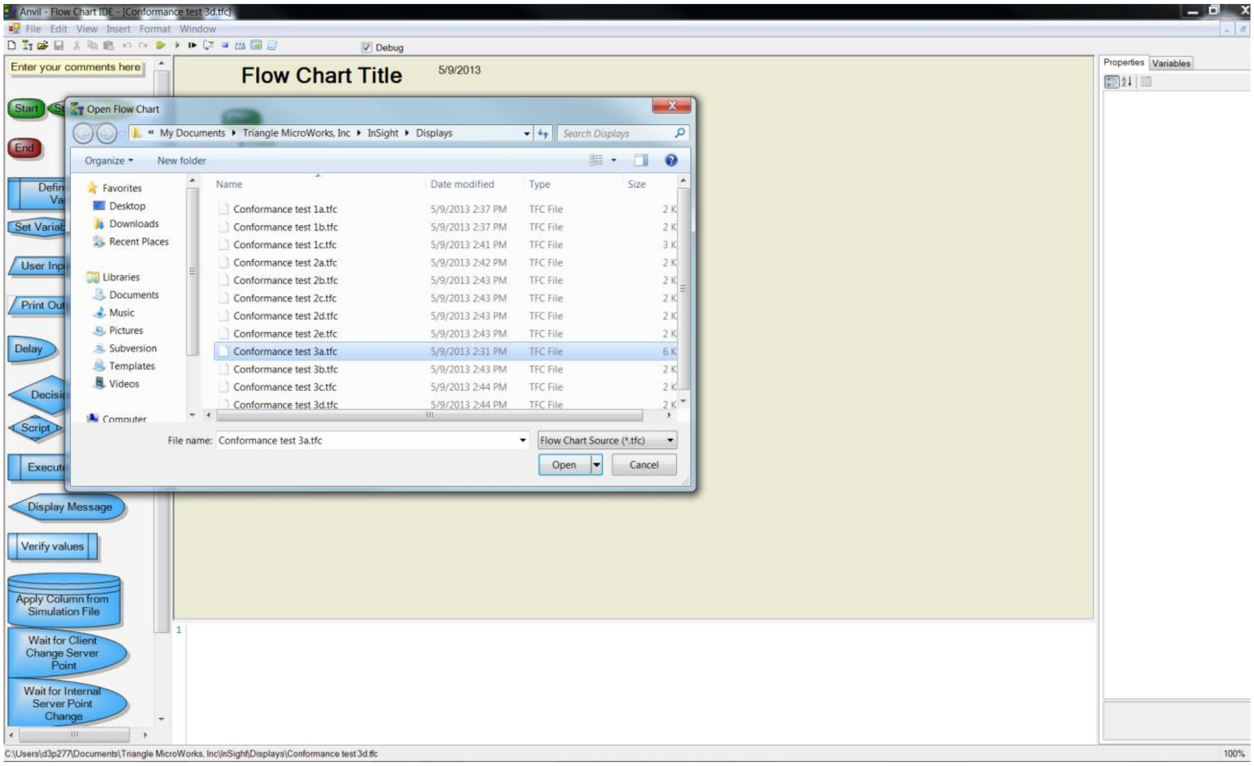


Figure 6: TMW Flow Chart IDE

The TMW flow chart IDE allows for process flow creation and is the environment in which the conformance tests have been created. From here the user would use the File menu to open a document.



Name	Date modified	Type	Size
Conformance test 1a.tfc	5/9/2013 2:37 PM	TFC File	2 K
Conformance test 1b.tfc	5/9/2013 2:37 PM	TFC File	2 K
Conformance test 1c.tfc	5/9/2013 2:41 PM	TFC File	3 K
Conformance test 2a.tfc	5/9/2013 2:42 PM	TFC File	2 K
Conformance test 2b.tfc	5/9/2013 2:43 PM	TFC File	2 K
Conformance test 2c.tfc	5/9/2013 2:43 PM	TFC File	2 K
Conformance test 2d.tfc	5/9/2013 2:43 PM	TFC File	2 K
Conformance test 2e.tfc	5/9/2013 2:43 PM	TFC File	2 K
Conformance test 3a.tfc	5/9/2013 2:31 PM	TFC File	6 K
Conformance test 3b.tfc	5/9/2013 2:43 PM	TFC File	2 K
Conformance test 3c.tfc	5/9/2013 2:44 PM	TFC File	2 K
Conformance test 3d.tfc	5/9/2013 2:44 PM	TFC File	2 K

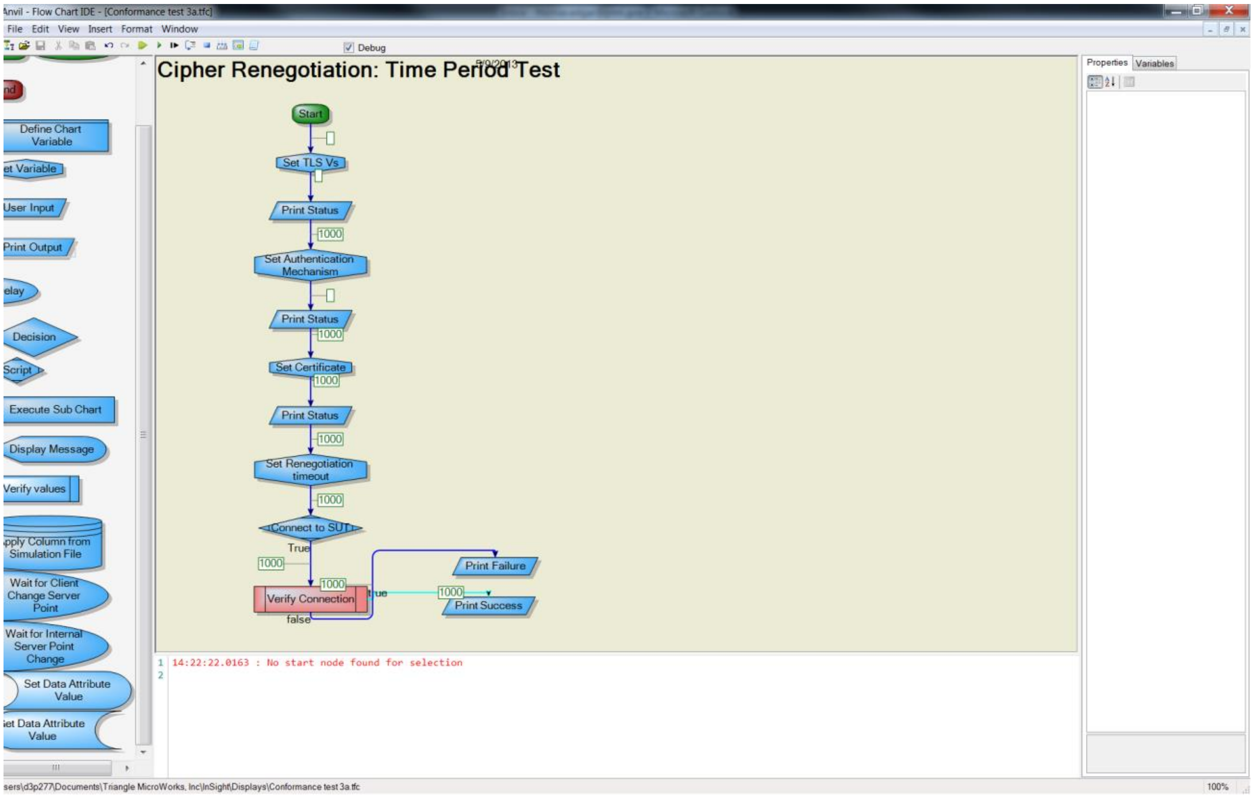
File name: Conformance test 3a.tfc

Flow Chart Source (*.tfc)

C:\Users\d3p277\Documents\Triangle MicroWorks, Inc\InSight\Displays\Conformance test 3d.tfc

Figure 7: Open Conformance Test Flow Chart Source File

The user selects the appropriate conformance test document from the test library.


Anvil - Flow Chart IDE - [Conformance test 3a.tfc]
File Edit View Insert Format Window
☑ Debug
Cipher Renegotiation: Time Period Test
Start
Set TLS Vs
Print Status
1000
Set Authentication Mechanism
Print Status
1000
Set Certificate
1000
Print Status
1000
Set Renegotiation timeout
1000
Connect to SUT
True
1000
1000
Verify Connection
false
true
1000
Print Failure
Print Success
Define Chart Variable
et Variable
User Input
Print Output
elay
Decision
Script
Execute Sub Chart
Display Message
Verify values
pply Column from Simulation File
Wait for Client Change Server Point
Wait for Internal Server Point Change
Set Data Attribute Value
iet Data Attribute Value
Properties
Variables
sers\d3p277\Documents\Triangle MicroWorks, Inc\InSight\Displays\Conformance test 3a.tfc
100%

```
1  14:22:22.0163 : No start node found for selection
2
```

Figure 8: Example Positive Conformance Test

Once the conformance test is loaded, the steps to execute the test are displayed in the central window.

6.2.2 Execute Test

In the TMW flow chart IDE, the play button will execute the conformance test. This will start the automated process of testing a SUT for conformity to a specific aspect of the IEC 62351-3, 4 and 6 standards. As the test executes, it will provide feedback on status and results in the text area. If an error occurs, feedback will be provided on what part of the test failed and include any troubleshooting data.

6.2.3 Test Communication

Depending on the test, varied communication will be sent to the SUT to gather responses. These responses will be evaluated against the expected responses as defined by the IEC 62351-3, 4 and 6 standards. The communication with the SUT is the actual conformance testing.

6.2.4 Log Results

To provide a holistic picture of the SUT's conformity, the results from each conformance test will be logged in a manner that can be automatically combined into a report detailing each test run, the pass/fail results, and any guidance to remedy failed tests.

6.3 Negative Test Workflow

Negative conformance tests will appear the same from a user's perspective; however, from a technical design viewpoint they follow a different workflow than the positive tests. The first two steps follow exactly the same path as the positive testing; however, the change in workflow occurs within the execution of the conformance tests and the communication. Refer to the Positive Test Workflow section for descriptions of the shared states as only the deviated states are described in this section. Figure 9 shows the entire workflow for negative tests.

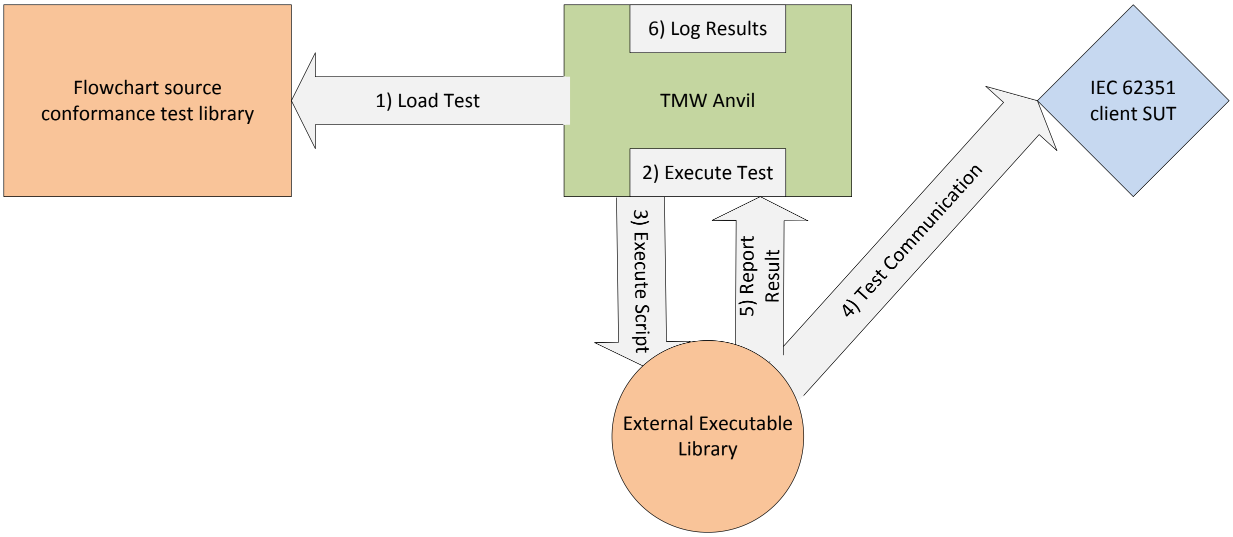


Figure 9: Negative Test High Level Workflow

6.3.1 Execute Script

As with a positive test, a negative test workflow will be displayed within the flow chart IDE when loaded. Negative tests distinctly differ by inclusion of calls to executables external to the TMW applications. These external executables provide capabilities that are unsupported by the TMW tools but necessary to execute negative tests. The goal of negative tests is to test devices to ensure that they do not support nonconforming capabilities, and as such, it is required that the conformance tool be able to execute non-conforming behavior. Therefore, external executable scripts are provided as part of the conformance tool to enable this non-conforming behavior. The TMW tools will execute the external scripts at appropriate positions in the conformance test. Figure 10 shows an example negative test with a call to an external executable. This test attempts to perform a TLS connection with a SUT with a NULL security profile configured; this is not allowed by IEC 62351-3.

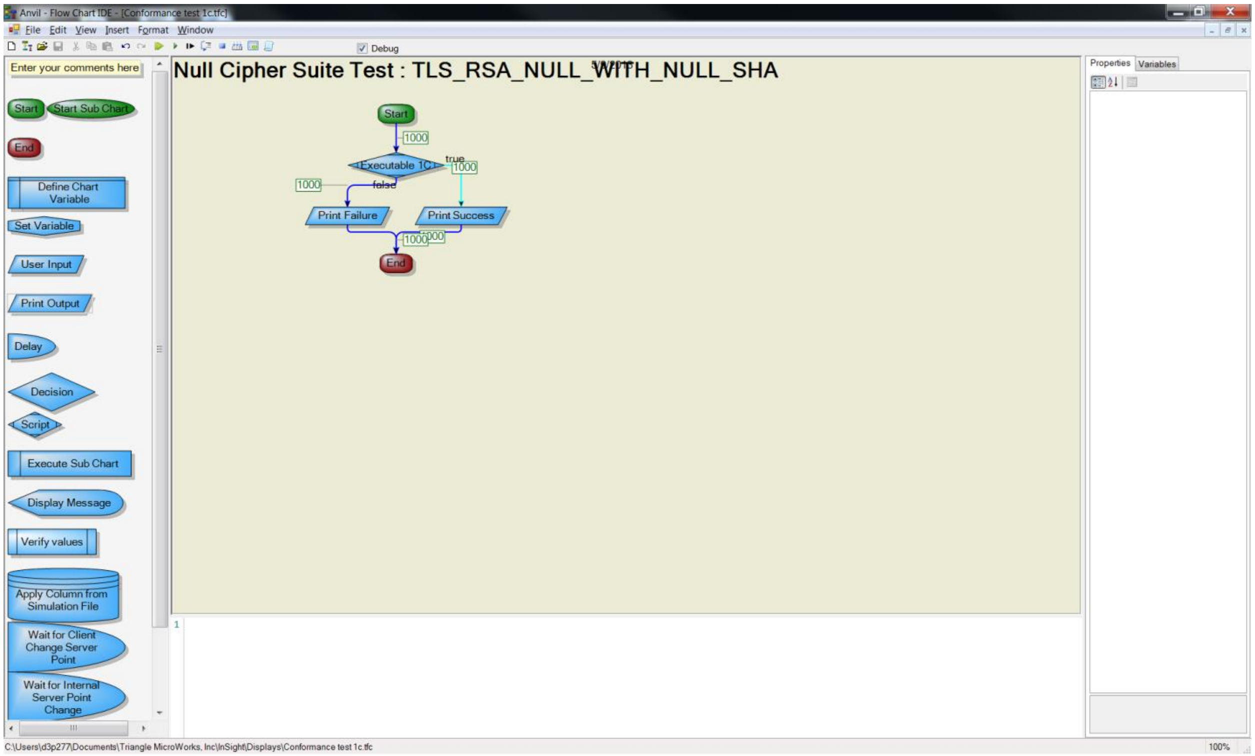

Anvil - Flow Chart IDE - [Conformance test 1c.tfc]
File Edit View Insert Format Window
☑ Debug
Enter your comments here
Start
Start Sub Chart
End
Define Chart Variable
Set Variable
User Input
Print Output
Delay
Decision
Script
Execute Sub Chart
Display Message
Verify values
Apply Column from Simulation File
Wait for Client Change Server Point
Wait for Internal Server Point Change
Null Cipher Suite Test : TLS_RSA_NULL_WITH_NULL_SHA
Start
1000
Executable 1C
true
1000
1000
false
Print Failure
Print Success
1000
1000
End
Properties
Variables
C:\Users\d3p277\Documents\Triangle MicroWorks, Inc\InSight\Displays\Conformance test 1c.tfc
100%

Figure 10: Example Negative Test with Call to External Executable

6.3.2 Test Communication

As the required testing for a negative test is outside of the capabilities of the TMW tools, all communication to the SUT will come from the external executables. The OpenSSL and GnuTLS libraries are leveraged to create the communication capabilities necessary to perform the negative tests.

6.3.3 Report Results

At the end of their execution, the external executables will report status back to the TMW tool. This will include status for errors, successful tests, and failed tests. The conformance tests are designed to understand status messages in order to generate the appropriate feedback and logging within the TMW tools.

7.0 User Interface

The TMW tool user interfaces will provide the entirety of the user interface for the conformance tool.

8.0 References

1. IEC 61850 (all parts), Communication networks and systems in substations
2. IEC 62351-1, Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues

3. IEC 62351-2, Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms
4. IEC 62351-3, Power systems management and associated information exchange– Data and communications security – Part 3: Communication network and system security – Profiles including TCP/IP
5. IEC 62351-4, Power systems management and associated information exchange – Data and communications security – Part 4: Profiles including MMS
6. IEC 62351-6, Power systems management and associated information exchange – Data and communications security – Part 6: Security for IEC 61850
7. Triangle MicroWorks IEC 61850 Test Suite (Anvil and Hammer) www.trianglemicroworks.com/
8. OpenSSL Cryptography and SSL/TLS Toolkit www.openssl.org
9. GnuTLS Transport Layer Security Library www.gnutls.org/