



Developer's Workshop: Session C
CIP Safety™ Conformance Testing 2017

David Crane
ODVA

February 22, 2017

Session Overview

- Functional Safety
- CIP Safety Protocol
- Conformance Testing Process
- CIP Safety Conformance Test
- Test Guidance
- Available CIP Safety CCTs and TSP locations

Functional Safety

- IEC¹ defines “safety” as
 - Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment.
- IEC further defines “functional safety” as
 - The part of the overall safety that depends on a system or equipment operating correctly in response to its inputs.
- IEC 61508
 - Functional safety of E/E/PE safety-related systems
 - Probability of dangerous failure (PFD_{AV} , PFH)
 - SIL – Safety integrity level – e.g., SIL 3 $\rightarrow 10^{-8} \leq PFH < 10^{-7}$

¹International Electrotechnical Commission; <http://www.iec.ch/functionalsafety/>


Functional Safety

- IEC 61508 is the basis for many other international standards that target application and product sectors; for example:
 - IEC 62061 Safety-Related Electrical Control System (SRECS)
 - IEC 61511 Safety Instrumented Systems (SIS)
 - ISO 13849 Safety of machinery (SRP/CS)
 - PLe vs. SIL 3
- IEC 61784-3 “Functional safety fieldbuses”
 - Defines Functional Safety Communication Profiles (FSCP)
 - Uses the “black channel” approach (61508-2 subclause 7.4.11.2)
 - CIP Safety is defined as FSCP 2/1 (61784-3-2)

- Provides a stated probability of failure for the network layer
 - PFH is average frequency of dangerous failures per hour
 - Network PFH (1%) part of overall PFH
 - $10^{-10} < \text{PFH} < 10^{-9}$ required for a SIL 3 data communications channel
- CIP Transport Class 0 Messaging
- Real time format (Vol 1 3-6, 7-3.6.10)
- Certified by TÜV Rheinland

CIP Safety Protocol

Certificate



No.: 968/EL 373.03/15

Product tested	CIP Networks Library Volume 5, CIP Safety Edition 2.12	Certificate holder	ODVA, Inc., 4220 Varsity Drive, Suite A Ann Arbor, MI 48108 USA
Type designation	CIP Safety on DeviceNet, CIP Safety on EtherNet/IP, CIP Safety on SERCOS		
Codes and standards	IEC 61784-3:2010 EN ISO 13849-1:2008 + AC:2009 IEC 61508 Parts 1-7:2010		
Intended application	The CIP Networks Library, Volume 5; CIP Safety Edition 2.12, November 2015 meets the requirements of the IEC 61784-3. It can be used as a safety communication layer in applications up to SIL 3 according to IEC 61508 and EN ISO 13849-1 for Category 4 / PL e and enables vendors to build CIP Safety devices for DeviceNet, EtherNet/IP and SERCOS in compliance with these standards.		
Specific requirements	The design, development and suitability of devices for use in safety related applications has to be approved. The network conformance testing has to be performed for individual devices.		
Valid until	2020-12-10		

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/EL 373.03/15 dated 2015-12-10.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

Köln, 2015-12-10

S. Hüb
Dipl.-Ing. Stephan Hüb

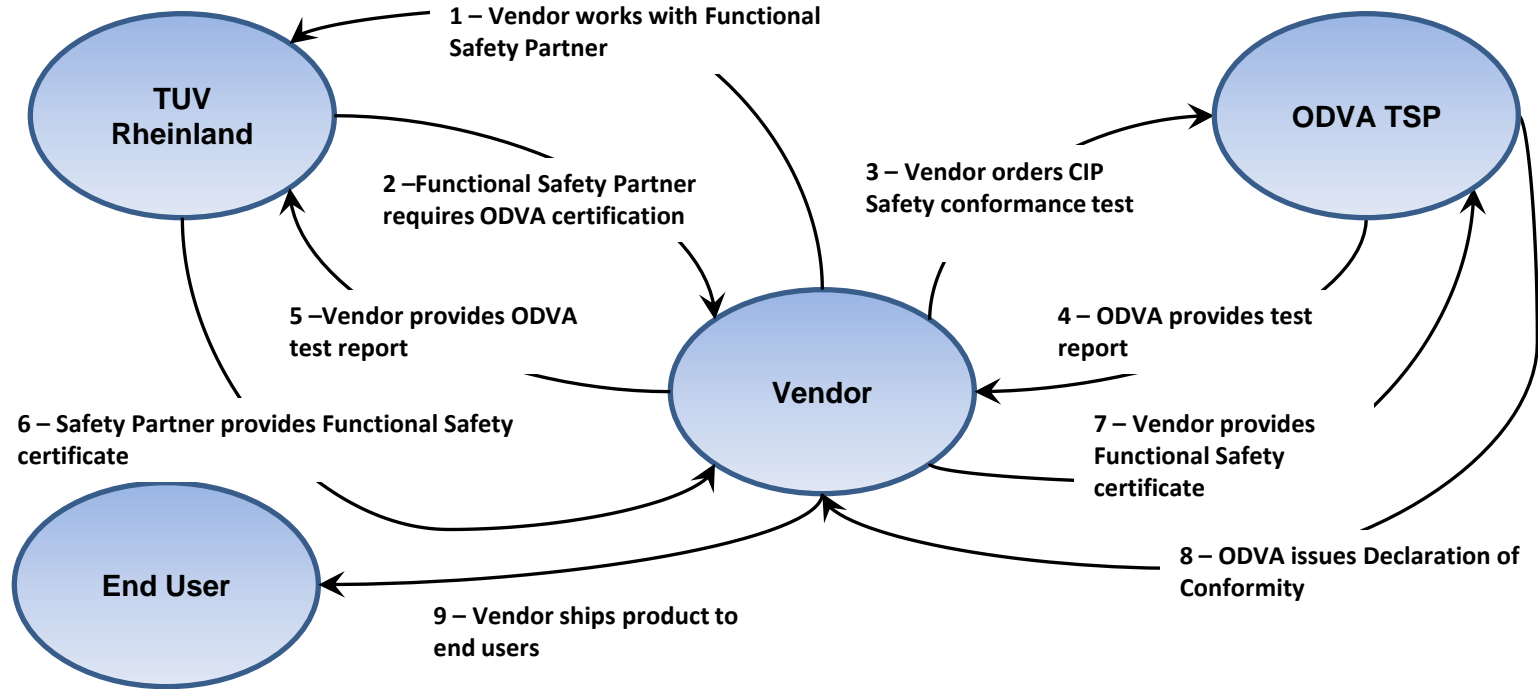
www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

Conformance Testing Overview

- Purpose of Conformance Testing
 - Satisfy ODVA Terms of Usage (TOU)
 - Obtain ODVA Declaration of Conformity (DOC)
- Prerequisites to CT
 - Current specification and software subscriptions
- Prepare for the lab test by running CT during development
- Procure test by placing an order on the ODVA website
- Provide required info and materials
- Participate by attending the lab test
 - Highly recommended for first-time and originator DUTs
- Pass the test to receive final test report and DOC
 - CIP Safety requires additional coordination between Vendor and ODVA

CIP Safety Conformance Testing Process



CIP Safety Conformance Test

- Includes all relevant sections of Standard Conformance Test
 - A standard test order is not needed for safety products
 - A standard test order IS needed for non-safety product variants
- Establishes conformance to the Safety Test Plan
 - Does not establish *functional safety* of the device
- Software installation provides CIP Safety test guidance
 - Readme
 - Sample Test Report
 - User's Guide – Appendix E

CIP Safety Conformance Test

- Implements automated safety protocol tests
 - Vol 5 Appendix F-3
- Includes CIP object test adaptations for safety
 - Vol 5 chapters 5 & 6
 - Safety-specific profiles and objects
 - Changes to standard objects (e.g., SNN attribute)
- Accommodation required for manual tests
 - QoS, ACD, DLR, TimeSync
- Dynamic Interoperability Test
 - Required for originators
 - Run if time permits for targets

CIP Safety Test Plan

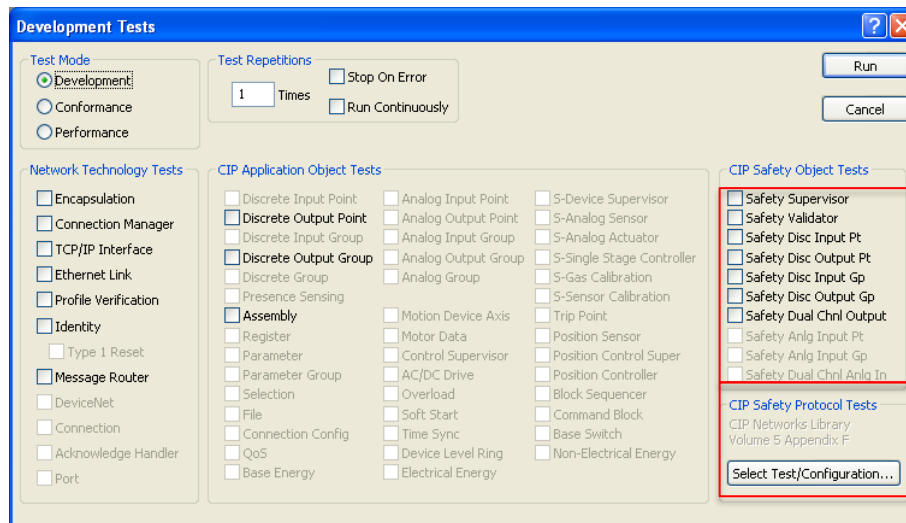
- Volume 5 – Appendix F
 - Links to traceable requirements (FRSxxx, SRSxxx)
 - Includes “Black Box” and “White Box” tests
 - **Black Box** – tests that can be externally verified
 - Volume 5 Appendix F-3
 - Automated test scripts
 - e.g., TST101 SafetyClose Processing by Targets
 - **White Box** - tests that require visibility into the implementation
 - Verified by the product developer
 - e.g., code inspection, design review, etc.
 - Volume 5 Appendix F-4
 - e.g., TST93 – Safety Device Hardware Validation Tests



Test Guidance – CIP Safety Protocol Test Software

“Standard” Protocol Test

- CIP Network specific tests
- CIP Object tests
 - Safety-specific profiles and objects
 - Impact to existing objects
 - CIP object extensions for safety
 - (Vol 5 chapters 5 & 6, Pub 170)
- CIP Safety object tests
 - e.g., Safety Supervisor



Safety Protocol Test

- “Black Box” tests are automated
- “White Box” tests must be performed by Vendor

Test Guidance – CIP Safety Test Selection

CIP Safety Object Tests

- ☐ Safety Supervisor
- ☐ Safety Validator
- ☐ Safety Disc Input Pt
- ☐ Safety Disc Output Pt
- ☐ Safety Disc Input Gp
- ☐ Safety Disc Output Gp
- ☐ Safety Dual Chnl Output
- ☐ Safety Anlg Input Pt
- ☐ Safety Anlg Input Gp
- ☐ Safety Dual Chnl Anlg In

CIP Safety Protocol Tests

CIP Networks Library
Volume 5 Appendix E

Select Test/Configuration...

Safety Tests

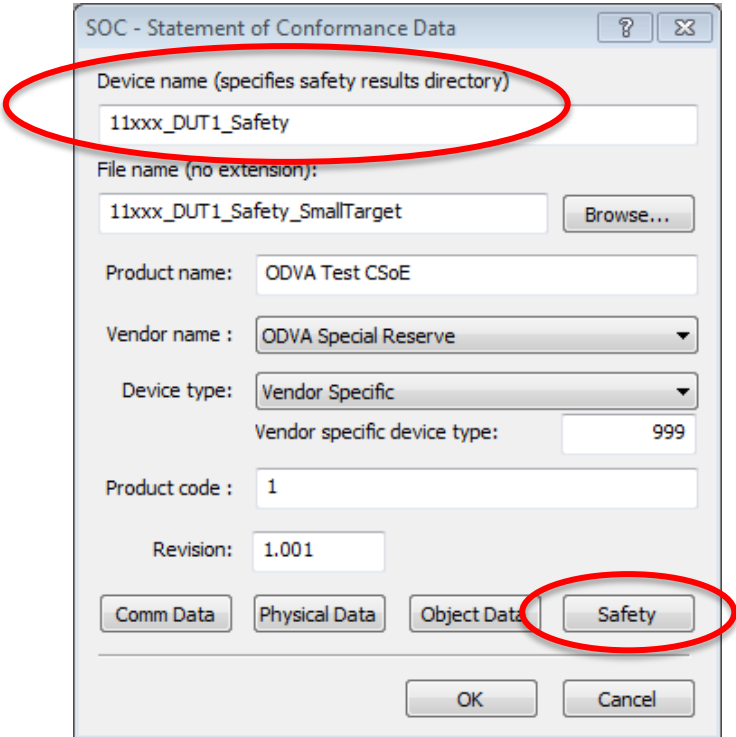
Device configuration: Single-cast producing target Safety Format: Extended

Test Number	Test Name
<input type="checkbox"/> 3	Connection Initialization Test
<input type="checkbox"/> 4	Connection Parameters CRC Negative Test
<input type="checkbox"/> 5	Type 2 SCID Test
<input type="checkbox"/> 6	Electronic Key Mismatch
<input type="checkbox"/> 13	Producer CRC and PID/CID Test
<input type="checkbox"/> 16	Producer Packet Generation Mode Byte
<input type="checkbox"/> 21	Producer Run/Idle Usage
<input type="checkbox"/> 22	Producer Ping Count Usage
<input type="checkbox"/> 32	Producer Time Coordination No-response Test
<input type="checkbox"/> 42	Configuration UNID
<input type="checkbox"/> 43	Input Type 1 Connection Establishment Test
<input type="checkbox"/> 48	Identity Object
<input type="checkbox"/> 52	Propose/Apply TUNID and Reset Commands
<input type="checkbox"/> 53	Configuration Lock/Unlock
<input type="checkbox"/> 54	Configure_Request
<input type="checkbox"/> 55	SNCT Configuration Process
<input type="checkbox"/> 56	Setting Passwords
<input type="checkbox"/> 58	Safety Validator Diagnostics

OK Cancel

Test Guidance – Safety STC

- Two changes to the STC for safety
- Safety results directory
 - This should be constant thru all test runs
 - Vary file name to manage multiple STCs
- Safety Characteristics
 - Device configurations and
 - Connection endpoints and sizes



SOC - Statement of Conformance Data

Device name (specifies safety results directory):
11xxx_DUT1_Safety

File name (no extension):
11xxx_DUT1_Safety_SmallTarget Browse...

Product name: ODVA Test CSoE

Vendor name: ODVA Special Reserve

Device type: Vendor Specific
Vendor specific device type: 999

Product code: 1

Revision: 1.001

Comm Data Physical Data Object Data **Safety**

OK Cancel

Test Guidance – Safety STC

- Device Behavior
 - Input/Output
 - Controller
- Connection Info
 - Target/Originator
 - Consumer/Producer
 - Single/Multi-cast
 - Connection Endpoints
 - Provide one STC per required test configuration (small & large connection sizes)
- SafetyOpen Types
- TUNID/NodeID/SNN
- (optional) Config file
- Originator target config file

Safety Characteristics

Device Behavior

☒ Input ☐ Controller

☒ Output ☐ Bridge

☐ Safety Reset Switch

Safety Connection Type(s)

Originator

☐ Single Cast Producer

☐ Single Cast Consumer

☐ Multi - Cast Consumer

Target

☒ Single Cast Producer

☒ Single Cast Consumer

☒ Multi - Cast Producer

Safety Open Type(s)

☒ Type 1 (Config) ☒ Type 2 (SCID) ☒ Type 2 (SCID=0)

Safety I/O Data

1 Consumed Size 6 Produced Size 15 Max Consumers

6 RPI Min 1000 RPI Max 1 RPI Tick

Active Safety Data

Safety Network Configuration Tool (SNCT)

☐ Originator ☒ Target Config File

Target Configuration Data File

Safety Open Application Path(s)

	Config	Consumed	Produced
Class:	4	4	4
Instance:	864	0x234	884
Null Instance:	199	199	199
Attribute:			
Connection Point:			

System Unique Identifiers

	DUT UNID	Test UNID
SNN Date	4	4
SNN Time	100	100
NodeID	0xc0a80178	0xc0a80101

Safety Protocol Version

2.0

OK Cancel

Test Guidance – Safety Configurations

- Clarification of the meaning of Produce/Consume
- Input/Output
 - TSCP = Target Single-cast Producer (i.e., INPUT)
 - TSCC = Target Single-cast Consumer (i.e., OUTPUT)
 - TMCP = Target Multicast Producer
- Meaning “reversed” for Originator DUTs
 - OSCP is a CIP consuming connection (i.e., OUTPUT)
 - OSCC is a CIP producing connection (i.e., INPUT)

Test Guidance – Safety Log Files

10968_1734IE4S_SA6_20120427_Safety.log

[illegible]

Test script console output

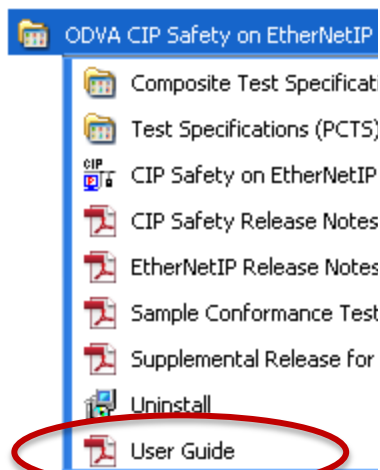
SPTe Rollup html

[illegible]

Test Guidance – Pass/Fail

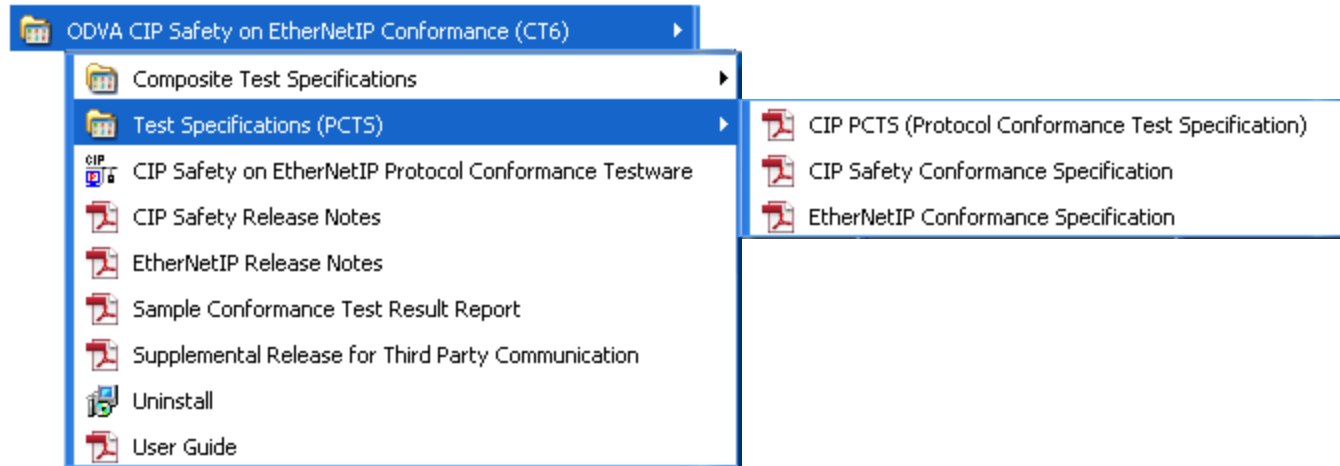
```
11078_ConformSafety.log - Notepad
File Edit Format View Help
18538
-----
18539 Extended Format Producer Time Coordination Response Failure Test
18540 Testware Revision = 1.01 08/24/04
18541 -----
18541 116) Extended Format Producer Time Coordination Response Failure Test
18542 <Test number = 116>
18543 Receive skipped: No Response Expected
18544 (Log messages suppressed: 15 in 0.110s)
18545 1> *** Producer Time Coordination Response Failure with Extended Format :: Connection not es
18546 2> *** Producer Time Coordination Response Failure with Extended Format :: Not all configure
18547 3> *** Producer Time Coordination Response Failure with Extended Format :: Test did not run
18548 ***** Found 3 Errors *****
18549 <Test Result status = Fail crc = x1F71B76E>
18550 </Test>
18550 End: Extended Format Producer Time Coordination Response Failure Test Test
18551 ***** Found 3 Errors in Extended Format Producer Time Coordination Response Failure Test Test
18552
-----
18553 Extended Format Producer Single-Cast
18554 Testware Revision = 1.01 08/24/04
18555 -----
18555 121) Extended Format Producer Single-Cast
18556 <Test number = 121>
18557 Receive skipped: No Response Expected
18558 (Log messages suppressed: 15 in 0.107s)
18559 <Milestone test="121" milestone="0" comment="Connection Established" />
18560 <Milestone test="121" milestone="1" comment="First Packet Verified" />
18561 <Milestone test="121" milestone="2" comment="Ping Count Multiplier Verified" />
18562 <Milestone test="121" milestone="3" comment="EPI Rate Verified" />
18563 <Milestone test="121" milestone="4" comment="Test Completed" />
18564 Test Passes
18565 <Test Result status = Pass crc = x2F2E48B2>
18566 </Test>
18566 End: Extended Format Producer Single-Cast Test
18567 Extended Format Producer Single-Cast Test Passes
18568
```

Test Guidance – Installed Documentation

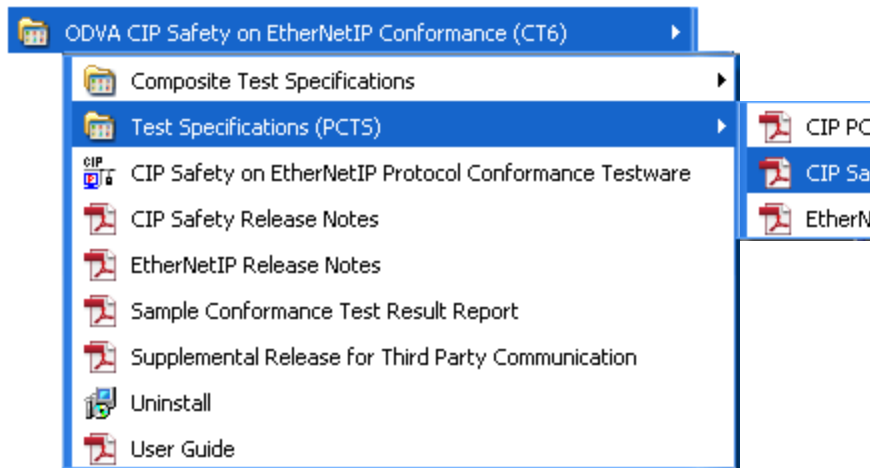


Appendix E	59
<i>CIP Safety Adaptation for Conformance Testing</i>	59
Before You Begin	59
CIP Safety Conformance Software Removal	59
CIP Safety Conformance Software Installation	60
CIP Safety Conformance and Python	64
Editing Safety Configuration Data	65
STC File Per Connection Type	70
CIP Safety Test Plan	71
Select Test/Configuration	72
Interpret Safety Test Results	73
About .SNCT Files	84
Create a .SNCT File	84
About .CFG Files	87
Create a .CFG File	87

Test Guidance – Installed Documentation



Test Guidance – Installed Documentation



2. CIP Safety Object Tests

This chapter specifies the conformance tests for CIP objects defined in the CIP Safety Specification, CIP Networks Library Volume 5 (ODVA PUB00085).

A template for use in developing CIP Conformance test specifications is provided in PUB00166 Appendix A.

Some testing specifications related to CIP Safety are contained in the common and network-specific test specification documents. For more information, please see the referenced document:

CIP Conformance Test Specification (ODVA PUB00166)

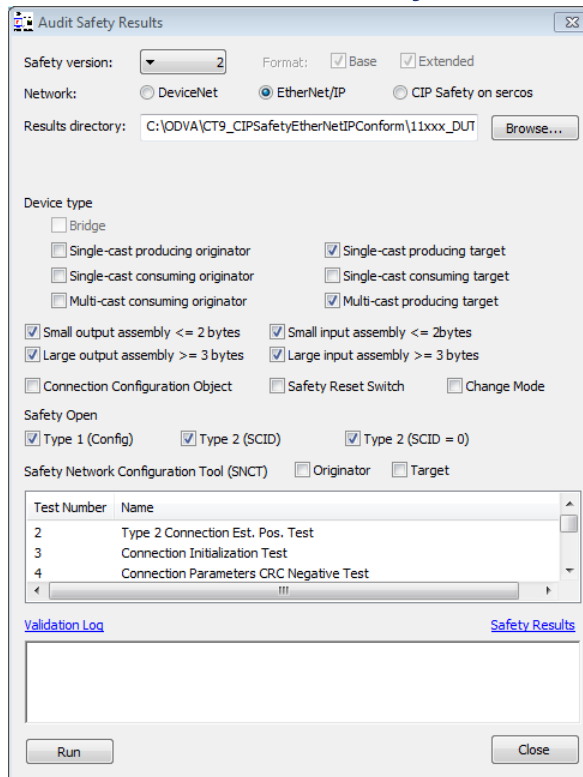
CIP Conformance Test Specification: DeviceNet Adaptation (ODVA PUB00167)

CIP Conformance Test Specification: EtherNet/IP Adaptation (ODVA PUB00168)

Object Code	For information about this Object Test:	Go to this page:
x01	Identity	8
x03	DeviceNet	9
x09	Discrete Output Point	10
x39	Safety Supervisor	11
x3A	Safety Validator	31
x3B	Safety Discrete Output Point	35
x3C	Safety Discrete Output Group	39
x3D	Safety Discrete Input Point	43
x3E	Safety Discrete Input Group	47
x3F	Safety Dual Channel Output	51
x49	Safety Analog Input Point	55
x4B	Safety Dual Channel Analog Input	62
x4C	SERCOS III Link	66
xF3	Connection Configuration	69
xF5	TCP/IP Interface	77

Test Guidance – Safety Results Audit Tool

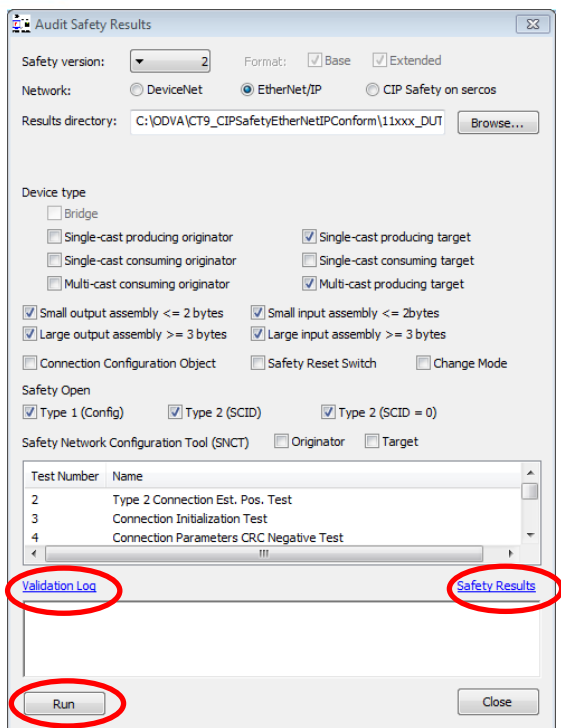
- Analyzes all safety logs
- Multiple test passes required
 - Target Configurations
 - I/O size \leq 2bytes
 - I/O size \geq 3 bytes
 - Originator Configurations
 - Connection size variation
 - Single/Multi-Cast
 - Vendor-specific configuration



The screenshot shows the 'Audit Safety Results' dialog box. It includes settings for Safety version (dropdown), Format (Base and Extended checkboxes), Network (DeviceNet, EtherNet/IP, and CIP Safety on sercos radio buttons), and Results directory (text field with a Browse button). The Device type section contains checkboxes for Bridge, Single-cast producing/consuming originator, Multi-cast consuming originator, Single-cast producing/consuming target, and Multi-cast producing target. There are also checkboxes for Small and Large output/input assembly sizes. Safety Open settings include Type 1 (Config), Type 2 (SCID), and Type 2 (SCID = 0). Safety Network Configuration Tool (SNCT) has Originator and Target checkboxes. A table lists test numbers and names: 2 (Type 2 Connection Est. Pos. Test), 3 (Connection Initialization Test), and 4 (Connection Parameters CRC Negative Test). At the bottom, there are links for 'Validation Log' and 'Safety Results', and 'Run' and 'Close' buttons.

Test Number	Name
2	Type 2 Connection Est. Pos. Test
3	Connection Initialization Test
4	Connection Parameters CRC Negative Test

Test Guidance – Safety Results Audit Tool



Audit Safety Results

Safety version: Format: ☒ Base ☒ Extended

Network: ☐ DeviceNet ☒ EtherNet/IP ☐ CIP Safety on sercos

Results directory: C:\ODVA\CT9_CIPSafetyEtherNetIPConform\11xxx_DUT

Device type

☐ Bridge

☐ Single-cast producing originator ☒ Single-cast producing target

☐ Single-cast consuming originator ☐ Single-cast consuming target

☐ Multi-cast consuming originator ☒ Multi-cast producing target

☒ Small output assembly <= 2 bytes ☒ Small input assembly <= 2 bytes

☒ Large output assembly >= 3 bytes ☒ Large input assembly >= 3 bytes

☐ Connection Configuration Object ☐ Safety Reset Switch ☐ Change Mode

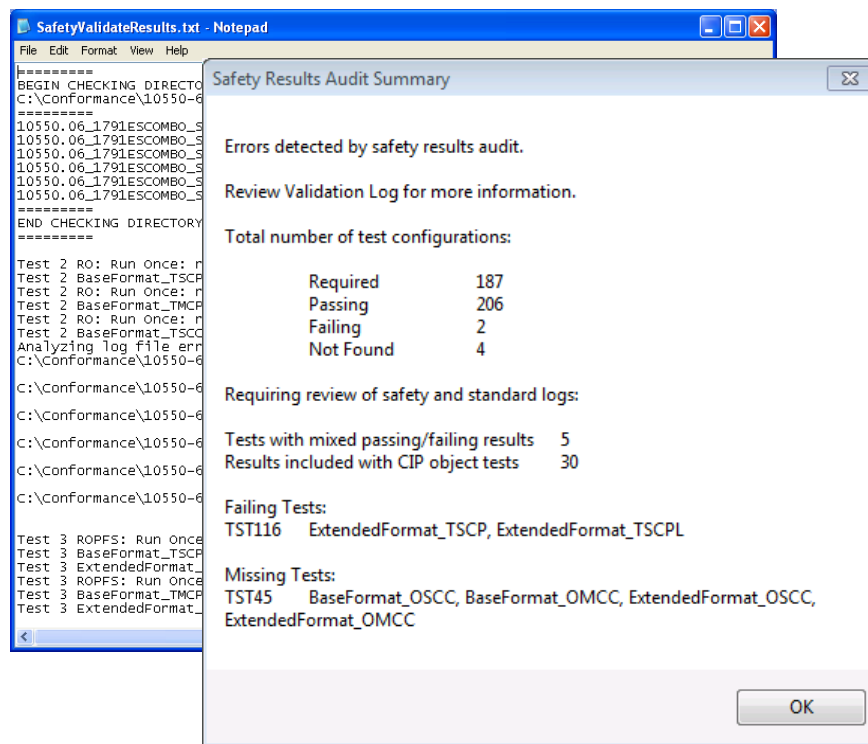
Safety Open

☒ Type 1 (Config) ☒ Type 2 (SCID) ☒ Type 2 (SCID = 0)

Safety Network Configuration Tool (SNCT) ☐ Originator ☐ Target

Test Number	Name
2	Type 2 Connection Est. Pos. Test
3	Connection Initialization Test
4	Connection Parameters CRC Negative Test

[Validation Log](#) [Safety Results](#)



SafetyValidateResults.txt - Notepad

```

=====
BEGIN CHECKING DIRECTORY
C:\Conformance\10550-6
=====
10550.06_1791ESCOMBO_S
10550.06_1791ESCOMBO_S
10550.06_1791ESCOMBO_S
10550.06_1791ESCOMBO_S
10550.06_1791ESCOMBO_S
10550.06_1791ESCOMBO_S
=====
END CHECKING DIRECTORY
=====
Test 2 RO: Run Once: n
Test 2 BaseFormat_TSCP
Test 2 RO: Run Once: n
Test 2 BaseFormat_TMCP
Test 2 RO: Run Once: n
Test 2 BaseFormat_TSCC
Analyzing log file err
C:\Conformance\10550-6
C:\Conformance\10550-6
C:\Conformance\10550-6
C:\Conformance\10550-6
Test 3 ROPFS: Run Once
Test 3 BaseFormat_TSCP
Test 3 ExtendedFormat_
Test 3 ROPFS: Run Once
Test 3 BaseFormat_TMCP
Test 3 ExtendedFormat_

```

Safety Results Audit Summary

Errors detected by safety results audit.

Review Validation Log for more information.

Total number of test configurations:

	Required	187
Passing	206	
Failing	2	
Not Found	4	

Requiring review of safety and standard logs:

Tests with mixed passing/failing results 5

Results included with CIP object tests 30

Failing Tests:

TST116 ExtendedFormat_TSCP, ExtendedFormat_TSCPL

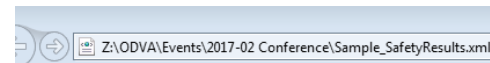
Missing Tests:

TST45 BaseFormat_OSCC, BaseFormat_OMCC, ExtendedFormat_OSCC, ExtendedFormat_OMCC

Test Guidance – Safety Results Audit Tool

- [Sample SafetyResults.csv](#)
- [Sample SafetyResults.xml](#)

STATUS	TEST	FORMAT	CONF	SPEL
Found	TST101	BaseFormat	TSCP	
Found	TST13	BaseFormat	TSCP	
Found	TST14	BaseFormat	TSCP	
Found	TST16	BaseFormat	TSCP	
Found	TST17	BaseFormat	TSCP	
Found	TST20	BaseFormat	TSCP	
Found	TST21	BaseFormat	TSCP	
Found	TST22	BaseFormat	TSCP	
Found	TST2	BaseFormat	TSCP	
Found	TST31	BaseFormat	TSCP	
Found	TST3	BaseFormat	TSCP	
Found	TST4	BaseFormat	TSCP	
Found	TST58	BaseFormat	TSCP	
Found	TST5	BaseFormat	TSCP	
Found	TST6	BaseFormat	TSCP	
Found	TST101	ExtendedFormat	TSCP	
Found	TST109	ExtendedFormat	TSCP	
Found	TST113	ExtendedFormat	TSCP	
Found	TST116	ExtendedFormat	TSCP	
Found	TST121	ExtendedFormat	TSCP	
Found	TST13	ExtendedFormat	TSCP	
Found	TST16	ExtendedFormat	TSCP	
Found	TST3	ExtendedFormat	TSCP	
Found	TST4	ExtendedFormat	TSCP	
Found	TST58	ExtendedFormat	TSCP	
Found	TST5	ExtendedFormat	TSCP	
Found	TST6	ExtendedFormat	TSCP	
Skipped	TST6	ExtendedFormat	TSCP	
Found	TST6	ExtendedFormat	TSCP	
Found	TST101	BaseFormat	TSCPL	



```

<?xml version="1.0" encoding="utf-8" ?>
<testresults>
- <test>
  <runreq>RO</runreq>
  <number>2</number>
  <cfg>TSCP</cfg>
- <CRCs>
  <crc>0xEED1E4F3</crc>
</CRCs>
  <Result>Pass</Result>
  <ResultCRC>0xEED1E4F3</ResultCRC>
</test>
- <test>
  <runreq>RO</runreq>
  <number>2</number>
  <cfg>TSCPL</cfg>
- <CRCs>
  <crc>0xEED1E4F3</crc>
</CRCs>
  <Result>Pass</Result>
  <ResultCRC>0xEED1E4F3</ResultCRC>
</test>
- <test>
  <runreq>RO</runreq>
  <number>2</number>
  <cfg>TMCP</cfg>
- <CRCs>
  <crc>0xEED1E4F3</crc>
</CRCs>
  <Result>Pass</Result>
  <ResultCRC>0xEED1E4F3</ResultCRC>
</test>
- <test>
  <runreq>RO</runreq>
  <number>2</number>

```

Available CIP Safety CCTs

- DeviceNet
 - CT7 DS (CT26 DN)
- EtherNet/IP
 - CT8 ES (CT12 EN)
- Sercos III
 - CT1 SS
- Planned updates in 2017 – Release candidates available
 - CT8 DS (CT28 DN)
 - CT9 ES (CT14 EN)
 - CT2 SS

Planned updates in 2017

- Release of new safety software subscriptions in first half of 2017
 - Improvements related to Originator testing
 - Improved support for non-SNCT devices
 - Fixes for unexpected stack behaviors
- Next software subscription
 - Improve safety results audit to cover all tests and eliminate manual checking
 - Add coverage for Safety Motion objects
 - Support ongoing specification changes

Available CIP Safety TSPs

- Ann Arbor (ODVA Technology and Training Center)
 - CIP Safety on EtherNet/IP, DeviceNet, Sercos III
 - Target and Originator
- Magdeburg TSP (University of Magdeburg)
 - CIP Safety on EtherNet/IP
 - Target
- Stuttgart TSP (University of Stuttgart ISW)
 - CIP Safety on Sercos III
 - Target
- Yokohama TSP and Shanghai TSP (TRJ, TRS)
 - No CIP Safety testing at the present time

Opportunities For Additional Training

- ODVA Quickstart Seminars
- CIP Safety One Day Training
 - in conjunction with TÜV Rheinland HW/SW FS Engineer Training and Exam



THANK YOU

THANK YOU