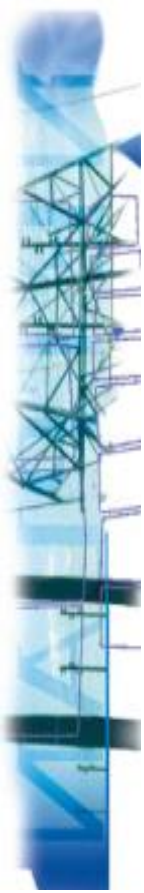




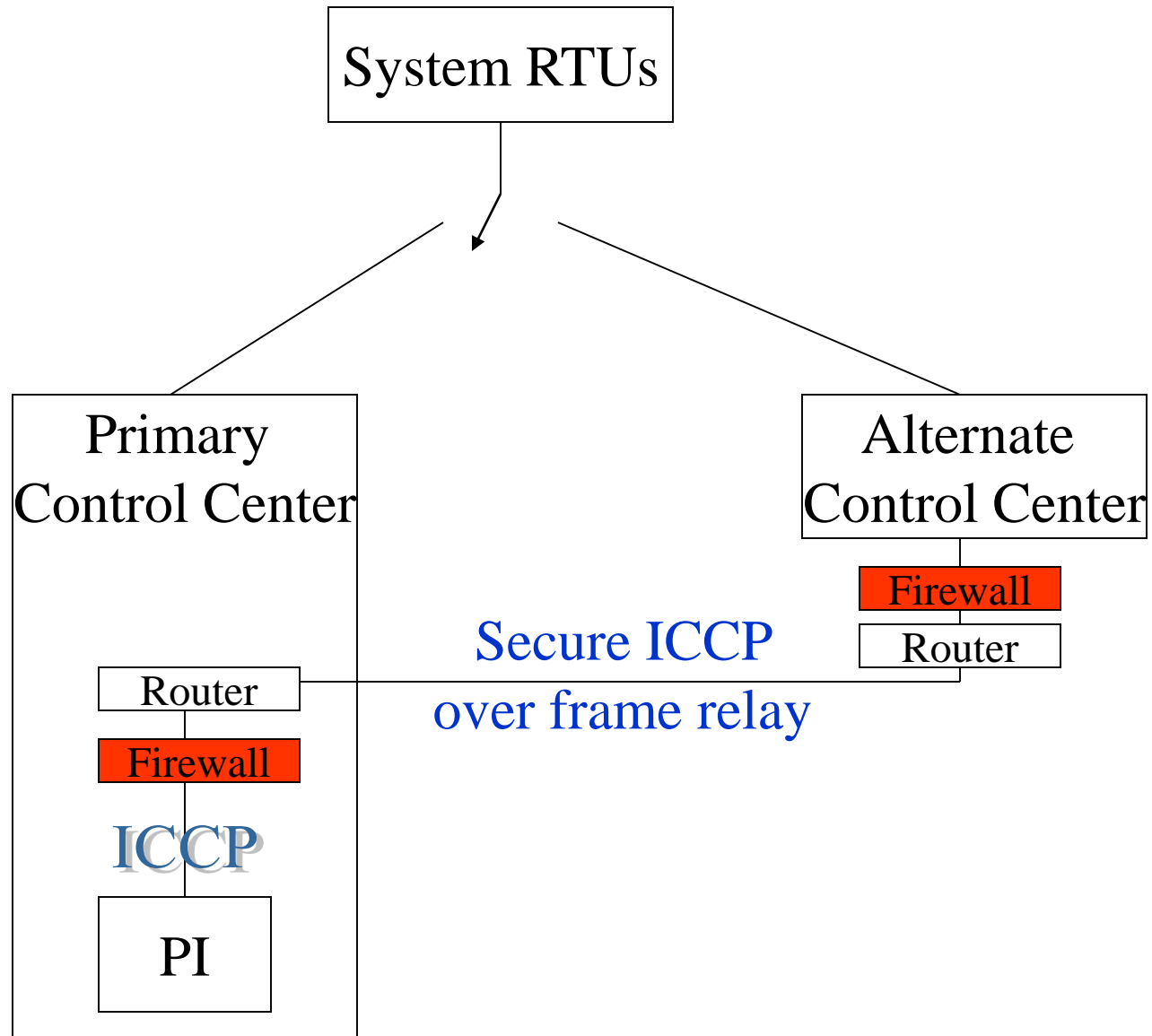
Security and ICCP/TASE.2

An Interoperability Report from
August 2003

Why Use ICCP to PI?

- 
- ICCP servers exist on the SCADA system.
 - The new PI ICCP will support multiple associations and bi-directional data transfers.
 - ICCP is easy to secure with more security on the way
 - To date, we have had no problems with our ICCP interface using 5000 tags at 10 seconds

Possible Configuration



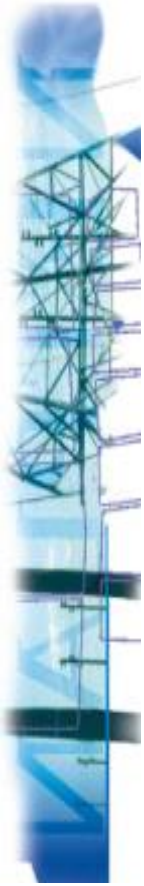
Specified Secure Profiles

OSI Reference Model

Application
Presentation
Session
Transport
Network
Data Link

ACSE (ISO/IEC 8650) + ACSE Authentication Definitions MMS (ISO/IEC 9506)		
ISO Presentation (ISO 9576) ASN.1 (ISO/IEC 8824/8825)		
ISO Session (ISO 8327)		
Transport		ISO Transport (ISO/IEC 8073) Transport Class 4
		SSL/TLS ISO Transport Layer Security (ISO/IEC 10736)
Network		ISO Network (ISO 8473) ES/IS (ISO 9542)
	RFC 1006	
	SSL/TLS	
	TCP (RFC 793)	
Data Link	IP (RFC 791) ARP (RFC 826)	
	Logical Link Control (ISO 8802)	
	Media Access Control (ISO 8803)	

Implementations and testing

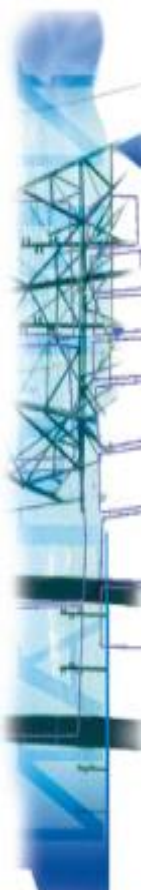


Specification Theory

- ACSE is used for Application Authentication
- TLS is used for Node Authentication and to provide encryption.

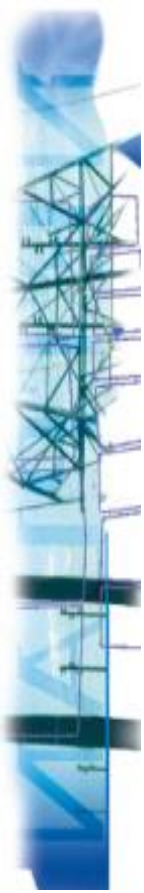


Tests for ACSE IOP

- 
- Proper certificate acceptance.
 - Seal testing (forward and backward time skew)
 - Acceptance of only configured Certs
 - Reject invalid calling/called certificates
 - Reject non-configured certificate

All test run between pairs where both act as Calling and called (14 tests total).

Tests for TLS IOP

- 
- Client, Server, Combo certificate acceptance.
 - Acceptance of Certs from a known CA
 - Acceptance of only configured Certs
 - Rejection of Certs/connection of unknown CA.
 - Rejection of non-configured Certs.
 - Key renegotiation
 - Cipher-suite negotiation

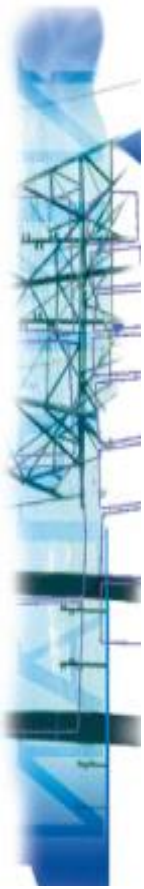
All test run between pairs where both act as
Calling and called (18 tests total).

Combined Tests

- No security (backward compatibility)
- Both TLS and ACSE Security enabled.
- Simultaneous Secure/Non-Secure associations.
- Don't Care configuration (accepts any combination).
- OSI exchange unaffected.

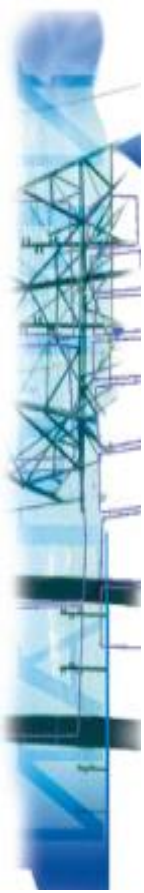
10 tests involved at a minimum.

IOP Information

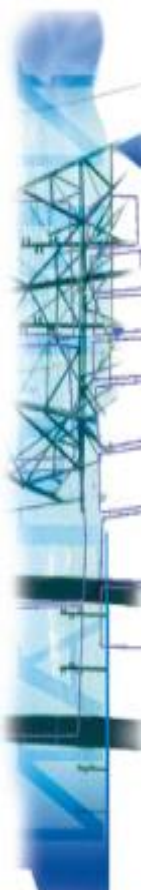


ICCP Vendor	Stack/Security Used
Alstom	SISCO
GE	SISCO
LiveData	LiveData
Siemens	SISCO
SISCO	SISCO

Problem Resolution

- 
- Problems were diagnosed
 - Corrected
 - Consumed 11-14 hours of IOP time.
 - Caused other vendors to re-execute some tests.

General Test Results



	Alstom	GE	LiveData	Siemens	SISCO
Alstom ⁽¹⁾		Passed	Passed	Passed	Passed
GE	Passed		Passed	Passed	Passed
LiveData ⁽²⁾	Passed	Passed		TLS only ⁽³⁾	Passed
Siemens ⁽¹⁾	Passed	Passed	TLS only ⁽³⁾		Passed
SISCO	Passed	Passed	Passed	Passed	

(1) - IOP ICCP DB configuration issue

(2) - Some TLS test cases skipped

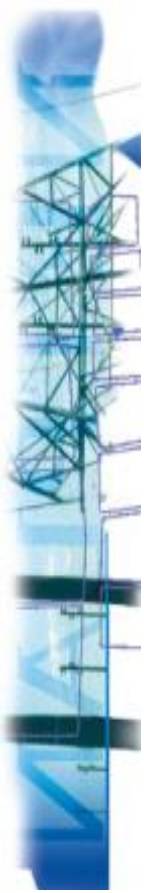
(3) - Complete suite not executed due to lack of time

Lessons Learned

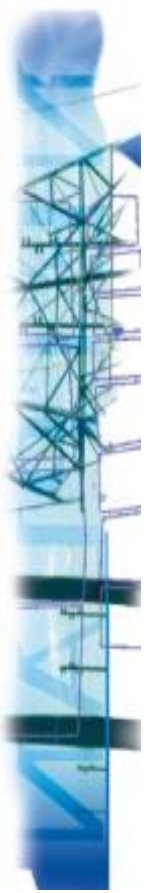
- Attempt to perform testing in advance (over Internet) failed.
 - IT staffs would not open up required ports.
- Calling and called testing was critical to finding certain issues.



Other lessons learned

- 
- Tool set needs to be augmented
 - Participants gained an understanding of how to configure and debug secure implementations.
 - Determined need to take IOP tests and construct a guide for deployment.

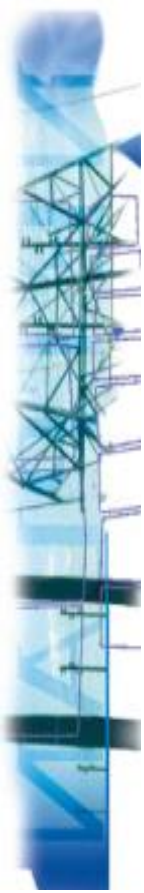
Observer Tools

- 
- Kema UniCA analyzer
 - Provided MMS/ICCP decoding and association setup/dataset transfer validation
 - Did not display SSL/TLS exchanges.
 - Gave inaccurate decodes when decoding the ACSE Authentication and certificates.

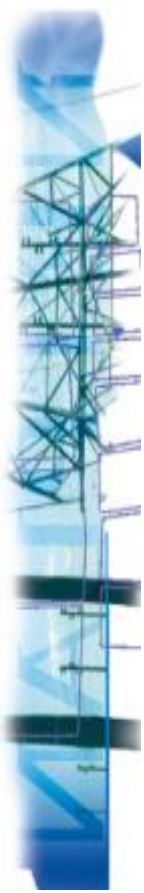
- Ethereal
 - Able to observe/display SSL/TLS exchanges.
 - Does not decode above transport (e.g. no MMS/ICCP decoding).

Became an integral tool for the observers.

Summary

- 
- IOP was successful
 - Problems with implementations were found and corrected.
 - Specification was enhanced to be more precise.
 - Observers were satisfied with the overall test, test methodology, and results.

What's Next

- 
- WECC DEWG will address deployment requirements at its November meeting.
 - NERC DEWG will address deployment requirements at its November meeting.
 - NERC Cyber Security 1200 Re-Write group will address ICCP security after the scoping group completes its work.

Observers

Dave Ambrose
(WAPA)

Glenn Sheffer
(NYISO)

Kevin Perry
(SPP)

