

The Congress of Chairs Facilitates Multiple Standards Activities

Bill Rush, Chair

*March 6, 2007
Atlanta, Georgia*

**The Goal Is A “Single Point Of Contact For
Standards Information”**

The CoC Facilitates Standards Use

- ◆ **CoC Is “Congress of Chairs”**
- ◆ **Seeking More Compatible Standards**
- ◆ **By Sharing Ideas Informally**
- ◆ **And Sharing Results With Users**

Agenda For Today's Meeting

- ◆ **Glossary Status**
- ◆ **Activity Status Web Site Demonstration**
- ◆ **Web Site And Communication Update**
- ◆ **Reports Of Group Chairs**
- ◆ **Open Discussion On Helping Coordinate**

CoC Combines Contributed Glossaries

- ◆ **Groups Submit Glossaries**
- ◆ **We Combine New Glossary With Others**
- ◆ **Publish All Definitions, Even Conflicts**
- ◆ **List Conflicts, Inform Group**
- ◆ **14 Standards Combined To Date**

Approved Security Function	A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either specified in an approved standard, or adopted in an approved standard and specified either in an annex of the approved standard or in a document referenced by the approved standard, or specified in the list of approved security functions.	1, 10
Archive	See key management archive.	10
Area Control Error (ACE)	The instantaneous difference between a Balancing Authority's net actual and scheduled interchange, taking into account the effects of Frequency Bias and correction for meter error.	34
Asset	An entity that may have value to someone. Assets may be tangible or intangible. Examples are people, a facility, materials, equipment, information, business reputation, an activity or operation such as manufacturing, the environment, and the community.	32
Attack	Attempt to gain unauthorized access to a system's services, resources, or information, or the attempt to compromise an Information System's integrity, availability, or confidentiality. [CNSS]	12
Attack	Hostile action taken by an adversary to obtain access to an asset and use it to achieve their objectives.	32
Authentication	A process that establishes the origin of information, or validates an entity's identity ¹ .	10
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSS]	12
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.	14, 15
Authentication	The process used to verify user identity.	39
Authentication Code	A cryptographic checksum based on an approved security function	1, 10

Learn What Standards Are Available

- **CoC Has A List Of**
 - Standards And Sponsors
 - Status (Planned Through Complete)
 - User Needs The Standard Meets
- **CoC Is The Most Complete Available List**
- **Chairs Spot Conflicts, Users Find Status**
- **List, Glossary At <https://pcsforum.org/groups/59/>**

Control Systems Standards Activities Database

[List All](#) | [Search](#) | [Add](#) | [Activity Help](#)

We welcome your recommendations for improvement, please use the [feedback form](#)

PCSF Congress of Chairs List of Cyber Security Activities.

Title	Sponsor	Data Manager	Support Item	AC	UC	DI	DC	RDF	TRE	Status	Date Last Updated
 Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan	 AGA	 Dr. William Rush	 AGA 12, Part 1	 ✓	 ✓	 ✓	 ✓	 ✗	 ✓	 Complete	 2006-08-18
 Cryptographic Protection of SCADA Communications, Part 2: Retrofit Link Encryption for Asynchronous Serial Communications	 AGA	 Dr. William Rush	 AGA 12, Part 2	 ✓	 ✓	 ✓	 ✓	 ✗	 ✓	 In Progress	 2006-08-11
 Cryptographic Protection of SCADA Communications, Part 3: Networked Systems	 AGA	 Dr. William Rush	 AGA 12, Part 3	 ✗	 ✗	 ✗	 ✗	 ✗	 ✗	 Not Started	 2006-08-11

About PCSF
Participants
Governance Body
News
PCSF Report
Calendar of Events
PCSF User Account
Terms of Use

Interest Groups
Working Groups

Working Group Deliverables
Reference Library



WWW
pcsforum.org

Search

The Status Project Provides Updated Status Of Other Groups

- ◆ **Track Process Control Security Work**
 - Identify Sponsor And Point Of Contact
 - Show Work Product (*Standard, Guide, Recommended Practice, Report, Technical Paper, Etc.*)
 - End User Requirements Addressed
 - Status Of Work
 - Qualifying Remarks

Control Systems Standards Activities Database

[List All](#) | [Search](#) | [Add](#) | [Activity Help](#)

We welcome your recommendations for improvement, please use the [feedback form](#)

PCSF Congress of Chairs List of Cyber Security Activities.

Title	Sponsor	Data Manager	Support Item	AC	UC	DI	DC	RDF	TRE	Status	Date Last Updated
 Cryptographic Protection of SCADA Communications, Part 1: Background, Policies, and Test Plan	 AGA	 Dr. William Rush	 AGA 12, Part 1	 ✓	 ✓	 ✓	 ✓	 ✗	 ✓	 Complete	 2006-08-18
 Cryptographic Protection of SCADA Communications, Part 2: Retrofit Link Encryption for Asynchronous Serial Communications	 AGA	 Dr. William Rush	 AGA 12, Part 2	 ✓	 ✓	 ✓	 ✓	 ✗	 ✓	 In Progress	 2006-08-11
 Cryptographic Protection of SCADA Communications, Part 3: Networked Systems	 AGA	 Dr. William Rush	 AGA 12, Part 3	 ✗	 ✗	 ✗	 ✗	 ✗	 ✗	 Not Started	 2006-08-11

About PCSF
Participants
Governance Body
News
PCSF Report
Calendar of Events
PCSF User Account
Terms of Use

Interest Groups
Working Groups
Working Group Deliverables
Reference Library



WWW
pcsforum.org

Search

Web Site & Communication Update

- ◆ **CoC Website Organized 2 Years Ago**
- ◆ **Not Meeting Needs**
- ◆ **Replaced In October 2006**
- ◆ **Only Marginal Improvement**
- ◆ **Hope For New Site**
- ◆ **Hold Time Investment Until New Site Up**

Chair Summaries Of Activities

- ◆ **DNP3**
- ◆ **Digression On IEC Committees**
- ◆ **IEC TC57 WG19**
- ◆ **IEC TC 65 WG 10**
- ◆ **AGA 12**

The PCSF Congress of Chairs –
DNP3 Secure Authentication Status

Andrew West, Chair DNP TC

March 7, 2007
Atlanta, Georgia

DNP3 Secure Authentication



- ◆ **The DNP3 SCADA protocol is managed by the DNP Users Group**
- ◆ **DNP3 is a widely used SCADA protocol**
 - Used in >75% North American electric utilities
 - Used in >30% of electric utilities worldwide
 - Adopted by water industries in UK & Australia
- ◆ **New: Authenticate “critical” messages**

DNP3 Security Status

- ◆ **Secure authentication proposal adopted Feb 6, 2007 at DNP UG Annual Meeting**
 - In progress since 2002, most work since 2005
- ◆ **Adds authentication info (Hashed key)**
 - No overhead to “non-critical” messages
 - Lightweight overhead for “critical” messages
 - Periodic (typical ~10 minute) key changes

DNP3 aligns with IEC 62351-5

- ◆ **Same team working on DNP3 and IEC 62351-5**
 - IEC standard still under development (~Q4 '07?)
- ◆ **Info Listed On PCSF Activity Status Web Site**
 - https://www.pcsforum.org/activities/list_activities.php
- ◆ **Specification available to DNP UG Members now at <http://www.dnp.org>**

What Is Next For DNP3?

◆ Trial implementations under way

- Discussing validation with Pacific Northwest National Laboratory
- Expect to ratify specification with little or no change

◆ Extensions for remote key management

- Allow remote addition & removal of users, etc.
- Very difficult to allow use of certificates in SCADA

◆ Test procedures

A Digression On IEC Committees

- ◆ **International Electrotechnical Commission**
 - TC Is Technical Committee
 - WG Is Working Group
- ◆ **TC 57 Is Electric Power (Non-Nuclear)**
- ◆ **TC 65 Is Security**

The PCSF Congress of Chairs –

IEC TC57 WG19 Status

Paul Skare, Chair

March 7, 2007
Atlanta, Georgia

My Standard Helps Electric Utilities

- ◆ **International Electrotechnical Commission**
- ◆ **Electric utilities' control systems**
- ◆ **Architecture**
- ◆ **Harmonization across IEC TC57 standards**
- ◆ **Technical Oversight/Review Board for TC57**

My Standard's Status

- ◆ **Working security via WG15**
- ◆ **New Reference Architecture coming out**
 - Adds VLPGO concepts
 - Adds Intelligrid references
- ◆ **Promoting harmonized security approach with TC57 all WGs; IEEE P1686, P1689, AGA 12, and TC65**

My Standard Coordinates With Others

- ◆ **Included In Combined Glossary? In the IEC TC57 glossary, first draft released for review to IEC national committees**
- ◆ **Listed On PCSF Activity Status Web Site? IEC TC57 explained there.**
- ◆ **Other Committees views**
 - Working through liaisons in WG15, EPRI, DNP UG,
 - CIM inputs from CIM User Group
 - 61850 inputs from UCA International User Group
- ◆ **Maybe We Want To Work With Others? Must follow IEC rules – can apply for category D alliance, and can work via liaison relationships.**

Continue the work!

- ◆ **IEC standards must be purchased**
 - Can only share drafts with approved bodies
- ◆ **Service Oriented Architectures now included in Reference Architecture**
- ◆ **Reviewing glossary**
- ◆ **Will review common quality codes**
- ◆ **Will accept inputs from other groups – liaison relationships as well as Category D possible**

The PCSF Congress of Chairs –

AGA 12 Status

Bill Rush, AGA 12 Chair

March 7, 2007
Atlanta, Georgia

AGA 12 Protects Exposed SCADA Communications

- ◆ **American Gas Association**
- ◆ **Gas, Water, Electric, Process Control**
- ◆ **12-1: Security Posture, Test, Background**
- ◆ **12-2: Serial, Asynchronous Retrofit Links**
- ◆ **Specifies Business Justification, Interoperability**

AGA 12 Status

- ◆ **12-1 Balloted, Gas Recom'ned Practice**
- ◆ **12-2 “Working Notes” On Internet**
 - Reviewed By Sandia
 - Used To Build Interoperable Units
 - Still Needs Editing, Balloting
- ◆ **2 Manufacturers Offer Modules Designed For AGA 12-2 Compliance**

AGA 12 Coordinates With Others

- ◆ **Included In Combined Glossary**
- ◆ **Other Committees Are Reviewing**
 - **IEEE P1689 – Part 1 For Electric**
 - **IEEE P1711 - Part 2 For Electric**
 - **Offered To AwwaRF, On Web Site**
- ◆ **ISA Adopting Some Basic Requirements**

AGA 12 Still Needs Work

- ◆ **12-2 Needs Editing, Balloting**
- ◆ **Need Conformance Test Protocol**
- ◆ **Need Better Key Management**
- ◆ **Need Forensics, Attack Detection**
- ◆ **12-3 And 12-4 (High Speed Network And Embedded Specification) Not Started**

Discussion On Helping Coordinate

- ◆ **Submit Your Glossary**
- ◆ **Add Your Group To Activity Status Site**
- ◆ **Are Reports Of Group Chairs Useful?**
- ◆ **Two “New” Topics As Projects**
 - **The “Right Classification/Search” Criteria?**
 - **Coordinating Requirements Documents?**