FEATURE BLAST

Federal Information Processing Standard (FIPS) 201 Solution

Product Description

TAC is proud to announce its solution for the U.S. Government Federal Information Processing Standard: FIPS 201. The Andover Continuum system from TAC has been enhanced in version 1.9 to include optional support for FIPS 201. This solution includes new controller firmware and options for the FIPS 201 ready NetController II, AC-1 modules and the ACX Series.

Features and Benefits

The FIPS support in Continuum v1.9 permits data to be synchronized between CyberStation and the IDMS/PIV systems and also distributes FIPS compliant data to controllers for access control decisions. FIPS compliant access control requires all NetController II, AC-1 and ACX Series controllers to be upgraded to the latest FIPS compatible firmware.

Second/Transitional FIPS Card Support

Until CyberStation 1.81, only one credential could be assigned to a single personnel record. Since the release of v1.81, a second credential (e.g. Prox or FIPS PIV card) could be assigned to each personnel object but only the first credential data could be sent down and supported at the controller level. Now with v1.9, data for both credentials can be downloaded to a controller that supports dual credentials. This feature is useful for sites transitioning from one card access system to a FIPS-compliant system. Use of dual credentials may be temporary or indefinite. Once a site is ready to solely use the second credential (e.g. FIPS PIV card), a simple change

t.a.c®
by Schneider Electric

can enforce that only the second credential is used to determine personnel access.

Note: This feature may also be used at non-FIPS sites and does not require the FIPS option when used solely with non-FIPS credentials.

Easily transition sites from one personnel credential type to FIPS-PIV cards with Continuum's "transitional" card support.

Personnel Import Utility (PIU) to PIV Middleware Data Synchronization

Import data from a FIPS approved Identity Management System (IDMS) / Personnel Identity Verification (PIV) middleware system. The FIPS support in CyberStation v1.9 permits data to be synchronized between Continuum and the IDMS/PIV systems.

Keep your personnel data up to date and synchronized with the FIPS approved Identity Management System (IDMS) / Personnel Identity Verification (PIV) middleware system.

Personnel Import Utility (PIU) Enhancements

The Personnel Import Utility launched in version 1.8 (which supported data import using LDAP) is enhanced to allow XML as a data source. TAC has included a standard XSLT transformation script that integrates with the PIV middleware from ImageWare Systems, TAC's preferred and tested PIV system for FIPS installations. The PIU synchronizes import and export of personnel data using XML. The PIU may exchange data from other systems that utilize XML by editing the XSLT transforms.

Use standards-based XML to import personnel objects from the PIV middleware system.

Additional Features included with the Andover Continuum Solution

The following features are not specified as required in FIPS 201 but are included in the Andover Continuum solution and will complement your FIPS 201 configuration for a more comprehensive system.

10/100 Base-T Ethernet with IPsec/IKE Encryption

Communication with the NetController II and ACX Series controllers is not only fast (supporting data transfer rate up to 100 Mbps) but secure with IPsec/IKE protocols for Network Security. Encryption (up to 168-bit using Triple DES) and authentication may be enabled for communications to and from Andover Continuum workstations and controllers. Andover Continuum utilizes Internet Protocol Security (IPsec) and Internet Key Exchange Protocol (IKE) to assure tamper-proof communications over the Ethernet between IP controllers and workstations.

Establish tamper-proof Andover Continuum Ethernet connections with IPSec/IKE encryption.

FIPS 140-2 Compliance

Although it is possible to have a site that is FIPS 201 compliant without FIPS 140-2 compliant access controllers, many specifications also require FIPS 140-2 compliant access controllers. To address this

additional requirement, TAC is in the process of listing the Continuum Network Security Module that is in the NetController II and ACX Series controllers. These will be certified as Level 2 FIPS 140-2.

Build your FIPS 201 system with Level 2 FIPS 140-2 ready products.[*]

*   Level 2 FIPS 140-2 certification of TAC products is in process.

Support for Area Lockdown

It is important to be able to contain potential threats when they are detected. The NetController II and ACX Series controllers can respond to Area Lockdown commands set from Andover Continuum software providing a quick method for sealing off areas. A simple click of a graphic or an automatic program response is all that is needed to disable card readers and exit requests in any given area. First responder personnel can still gain access to the area if their record is marked with "executive privilege".

Rapidly "lockdown" areas when potential threats are detected.
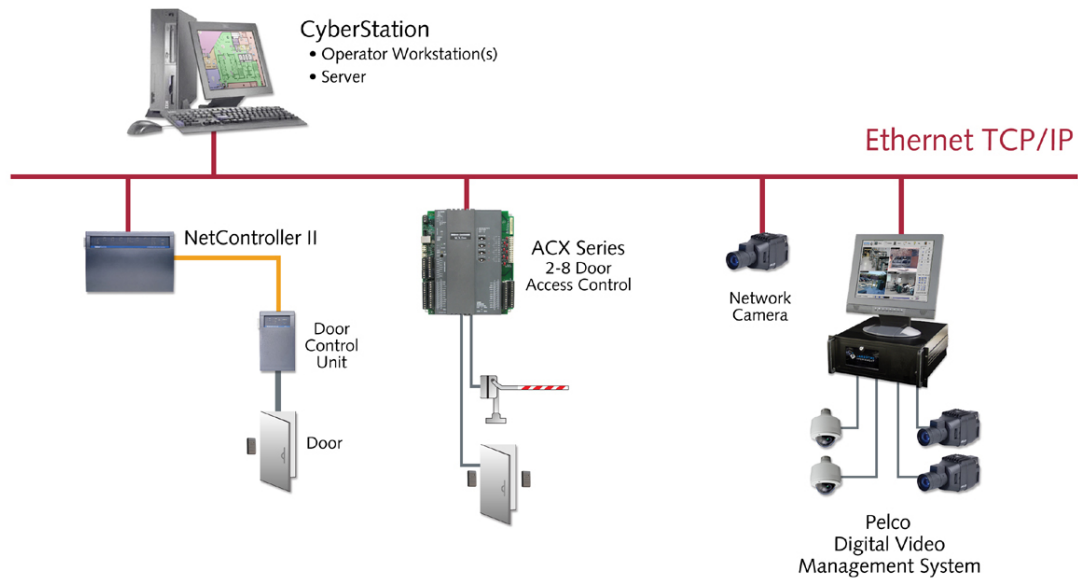

Condition "Threat" Level-based Access Rights

The NetController II and ACX Series controllers can adapt access rights to a change in condition or "threat" levels as the U.S. Department of Homeland Security refers to them. Each personnel record can be assigned a clearance level for each area to which a person has access. When the condition is more severe than the person's clearance level, access is automatically denied. The condition level may be set manually through Continuum software or automatically through a program. A program can even be written to monitor national threat levels and adjust Andover Continuum Condition Levels accordingly. Although the U.S. government only calls for five condition levels of threat, Andover Continuum is capable of assigning up to 255 custom condition levels for local security needs.

Automatically adjust access rights when condition and threat levels change.

Andover Continuum Security Architecture

The architecture below includes the products that make up the Andover Continuum security system; some of which are part of the TAC FIPS 201 solution. Whereas the Pelco Digital Video Management System (DVMS) is not part of the FIPS 201 solution, it does natively intergrate with CyberStation and complements the overall system for added security value.

t.a.c
by Schneider Electric