Argonne
NATIONAL
LABORATORY

… for a brighter future

# Control System Cyber Security Measures at the Advanced Photon Source

*Debby Quock, ANL Advanced Photon Source*

*ICALEPCS 2007 Control System Cyber-Security Workshop*

U.S. Department
of Energy

THE UNIVERSITY OF
CHICAGO

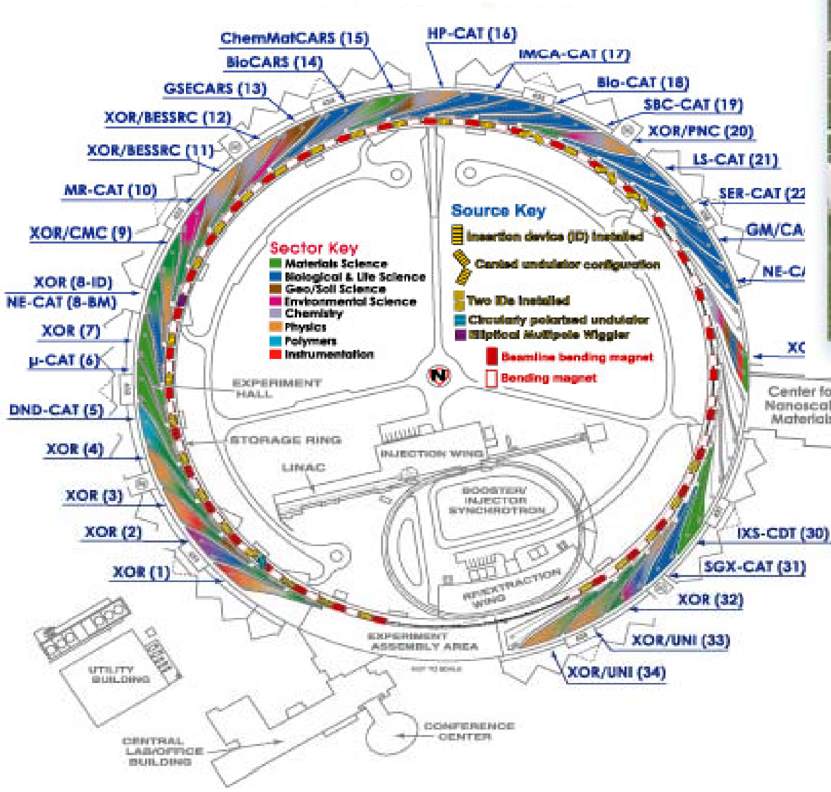
Office of
Science
U.S. DEPARTMENT OF ENERGY

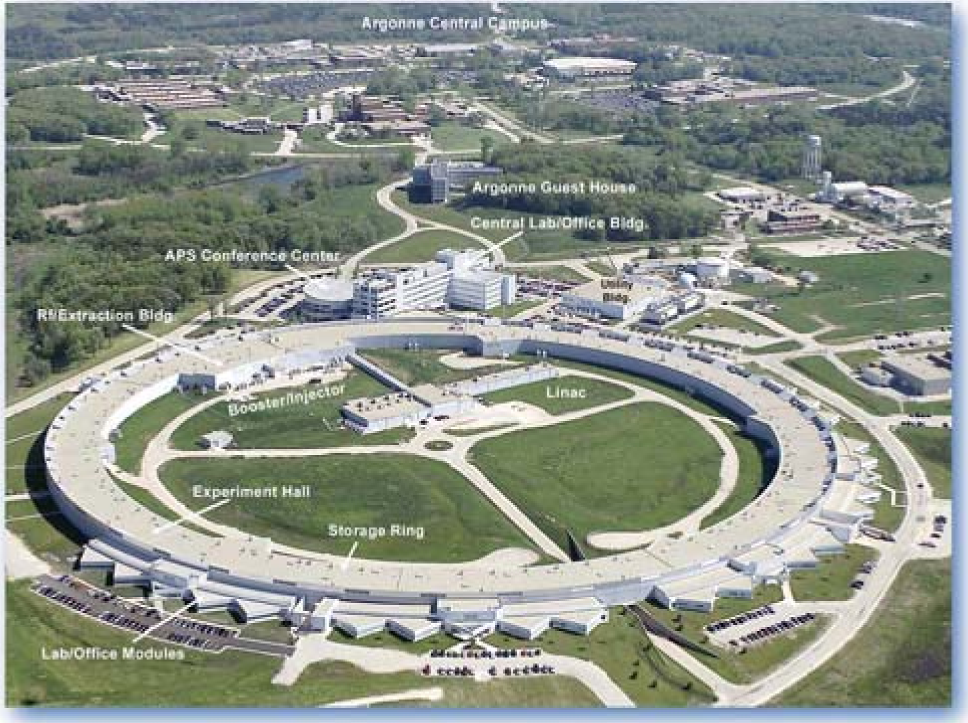
A U.S. Department of Energy laboratory
managed by The University of Chicago

# *Introduction*

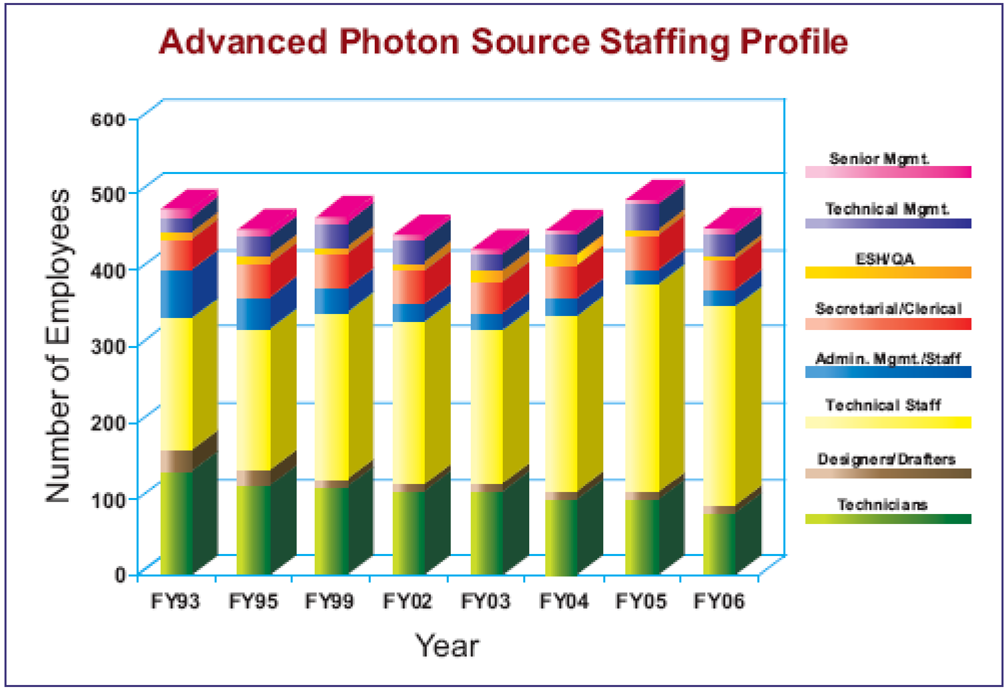
- Advanced Photon Source (APS) overview
- ANL and APS network architecture
- APS real-time control system
- APS control system related software applications
- Known cyber security issues and recommended strategies
- Future cyber security initiatives at APS

# Advanced Photon Source (APS)



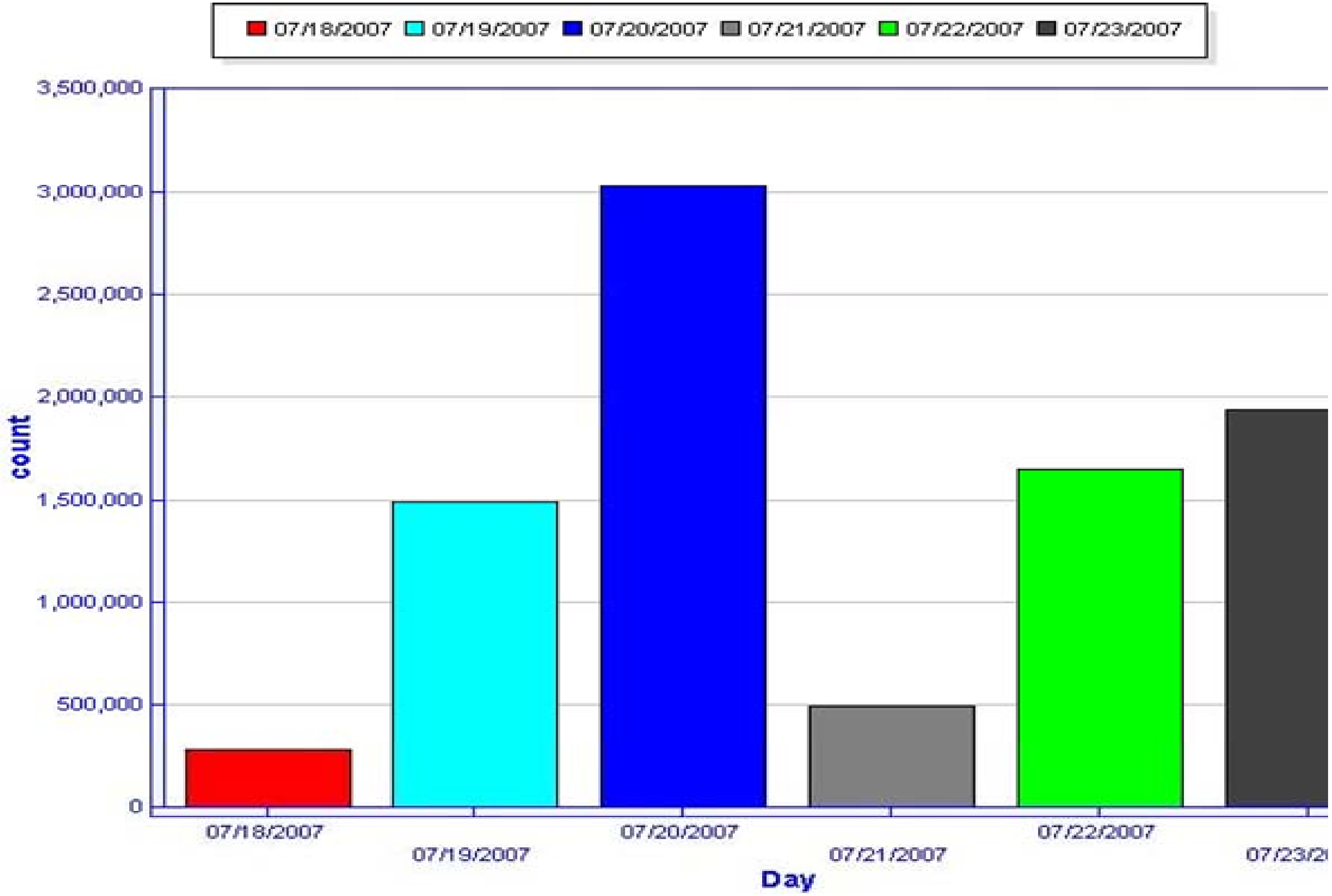


# Remote Access
# to APS Control System

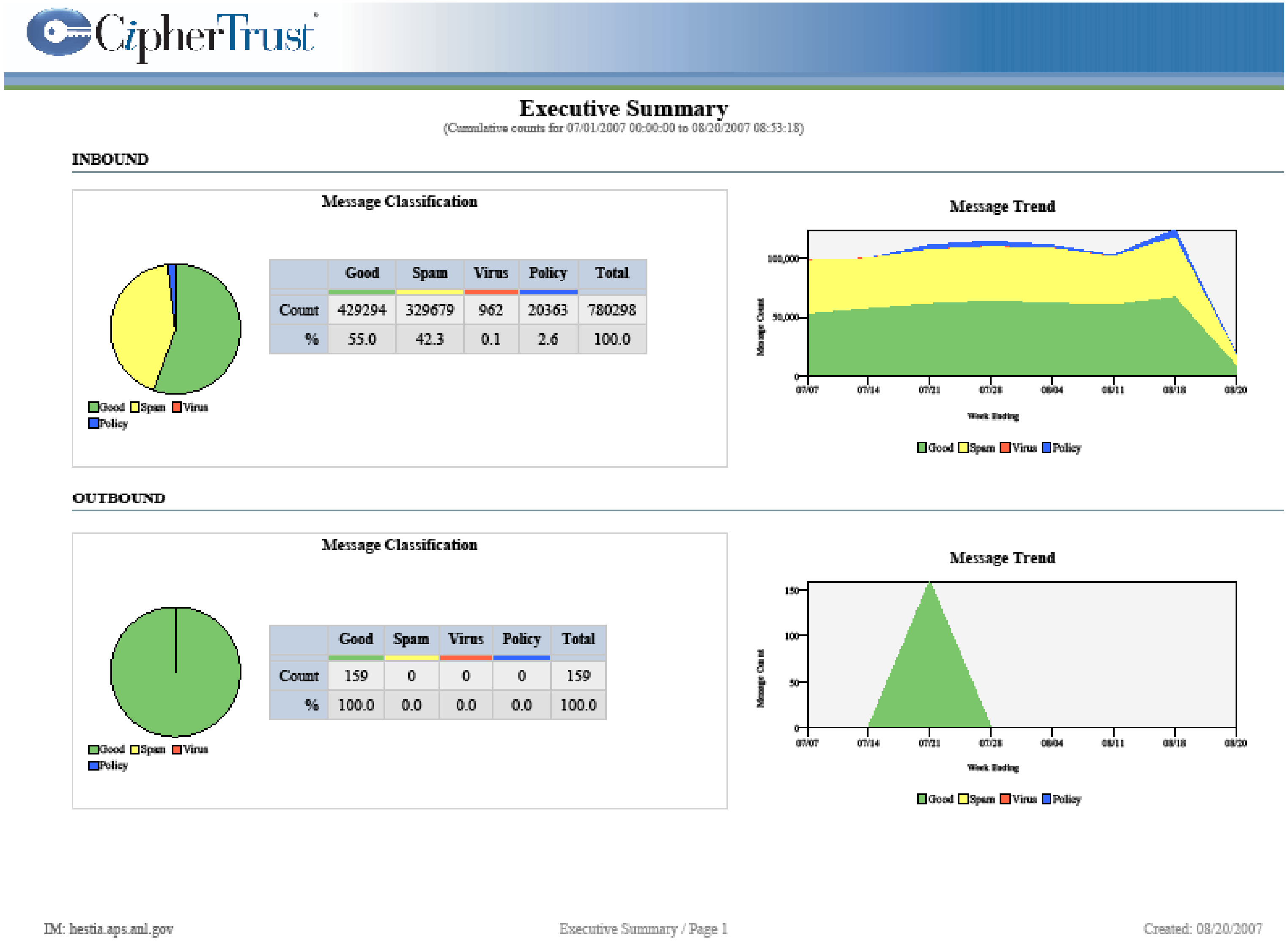


- Accessed by Scientists, Engineers, Operators, and Management
  - *For fiscal year 2006, the APS had 3,274 onsite unique users*
- Virtual Private Network (VPN)
  - *Offsite access from home and laptops*
- Secure Shell (SSH)
  - *For terminal window and file transfers*
- Modem
  - *APS modem pool system only supports PPP without callback*
- Portal Server
  - *Offsite access to email and files*
- AccessGrid
  - *Video and audio group-to-group interactions* [http://www.accessgrid.org](http://www.accessgrid.org)

# APS External Attacks



# APS Firewall Anti-Spam Summary



## Executive Summary

(Cumulative counts for 07/01/2007 00:00:00 to 08/20/2007 08:53:18)

### INBOUND

Message Classification

| | Good | Spam | Virus | Policy | Total |
|---|---|---|---|---|---|
| Count | 429294 | 329679 | 962 | 20363 | 780298 |
| % | 55.0 | 42.3 | 0.1 | 2.6 | 100.0 |

Message Trend

### OUTBOUND

Message Classification

| | Good | Spam | Virus | Policy | Total |
|---|---|---|---|---|---|
| Count | 159 | 0 | 0 | 0 | 159 |
| % | 100.0 | 0.0 | 0.0 | 0.0 | 100.0 |

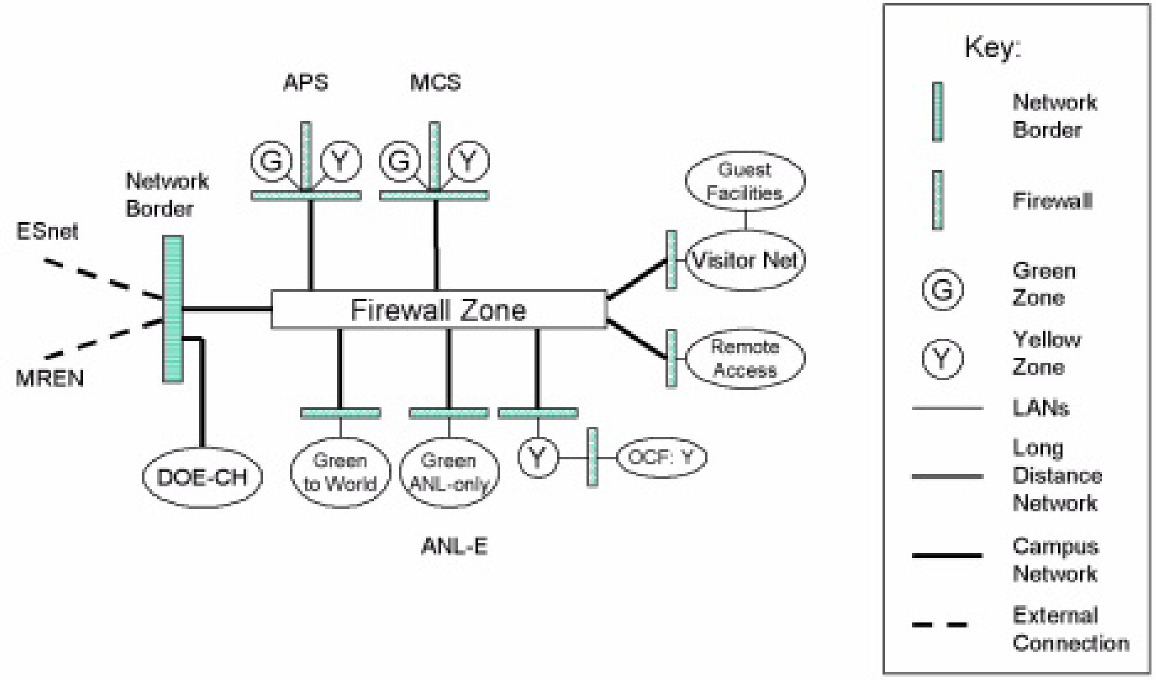
Message Trend

IM: hestia.aps.anl.gov

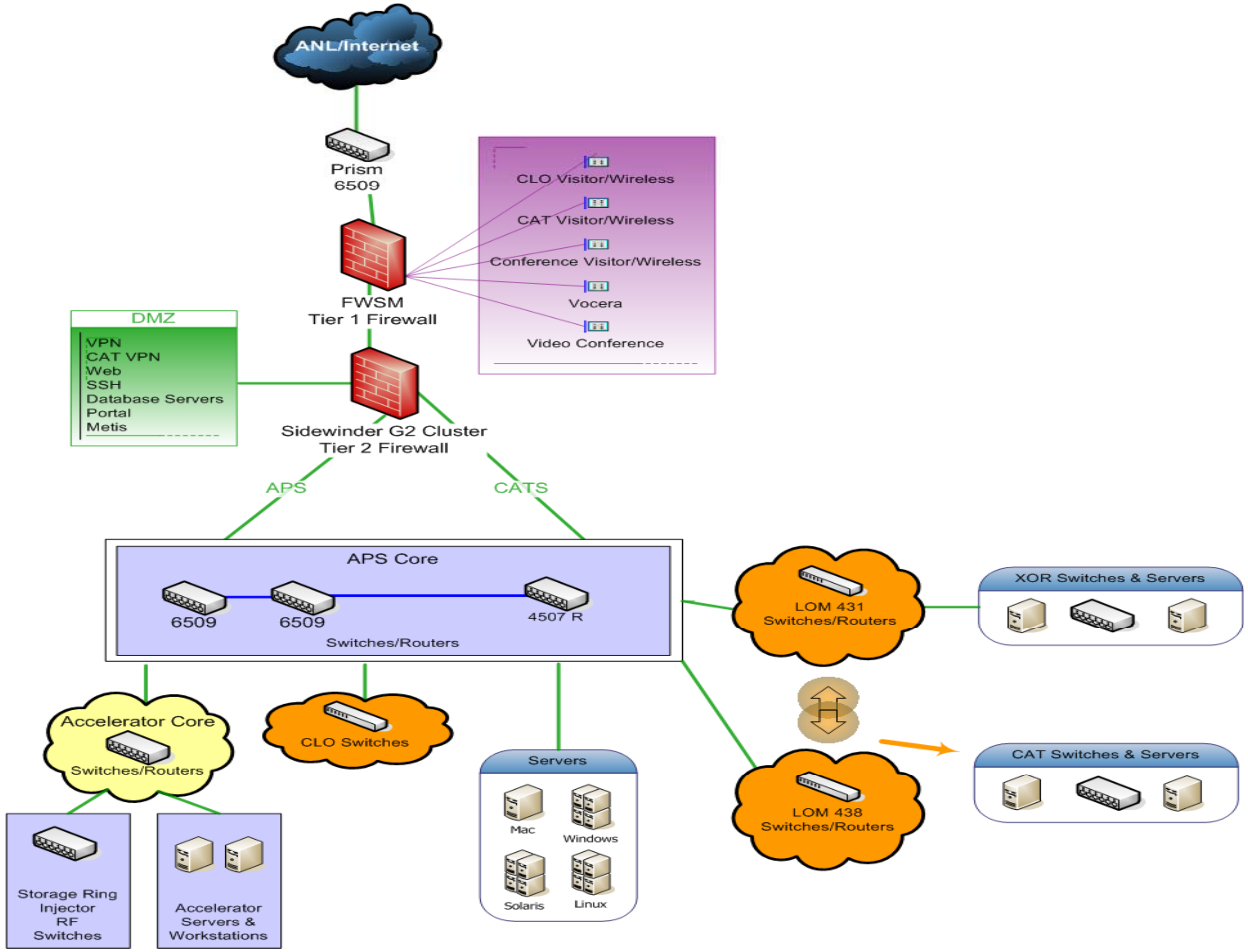
Executive Summary / Page 1

Created: 08/20/2007

# Argonne National Laboratory
# Network Boundaries and Protection



# APS Network



ANL/Internet
Prism
6509
FWSM
Tier 1 Firewall
CLO Visitor/Wireless
CAT Visitor/Wireless
Conference Visitor/Wireless
Vocera
Video Conference
DMZ
VPN
CAT VPN
Web
SSH
Database Servers
Portal
Metis
Sidewinder G2 Cluster
Tier 2 Firewall
APS
CATS
APS Core
6509
6509
4507 R
Switches/Routers
LOM 431
Switches/Routers
XOR Switches & Servers
Accelerator Core
Switches/Routers
CLO Switches
Servers
Mac
Windows
Solaris
Linux
LOM 438
Switches/Routers
CAT Switches & Servers
Storage Ring
Injector
RF
Switches
Accelerator
Servers &
Workstations

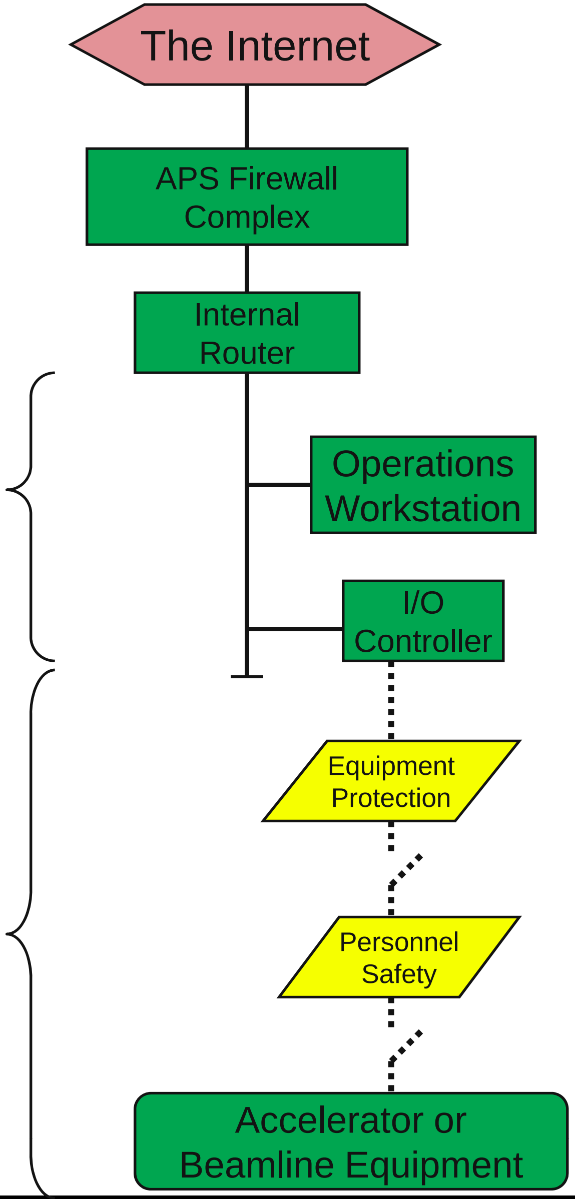
# APS Equipment Security Controls

*Overall:*

1. *Rigorous control systems and safety procedures.*
2. *Physical access required to override controls.*
3. *Computer security breach in worst case would result in facility downtime but no damage.*

Control operation network.

Equipment control systems. Many Installed throughout the complex. All equipment is controlled using this model.



Firewall controls - beyond Argonne standards.

Router creates internal-only control network.

Limited-access workstations; rigorous configuration management.

Custom systems, minimal access; rigorous configuration control.

No IP network; all signals are serial.

Hardcoded equipment parameters. Rigorous change management.

Hardcoded safety parameters. Rigorous change management. Physical key access required.

# APS Control System

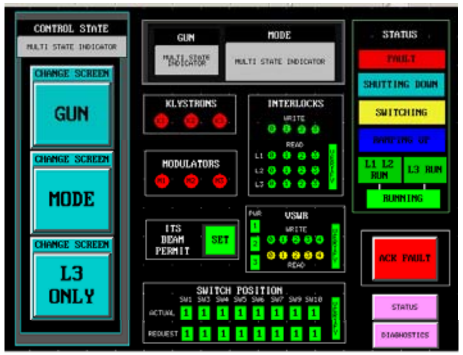
Accelerator IOC

- Linac, PAR, Booster and Storage Ring
  - 80 Workstations (Solaris, Linux, Windows, Apple Mac)
  - Approximately 300 distributed Input/Output Controllers (IOCs)
  - EPICS supervisory real-time controls software is interfaced by 96 PLCs, FPGAs, and Johnson Controls distributed control systems
  - More than 30,000 replaceable hardware components
  - Over 100,000 IOC points that are monitoring and controlling more than 450,000 technical parameters
  - Nearly 700 unique control system software applications
- Beamlines
  - Beam diagnostics control roughly 60 X-ray beams simultaneously with >500 ultra-high resolution beam position monitors, each resolving beam motion to a fraction the size of the period at the end of this sentence.
  - Nearly 100 remote computers collect data from the 500 monitors & re-steer the X-ray beams 1,500 times per second

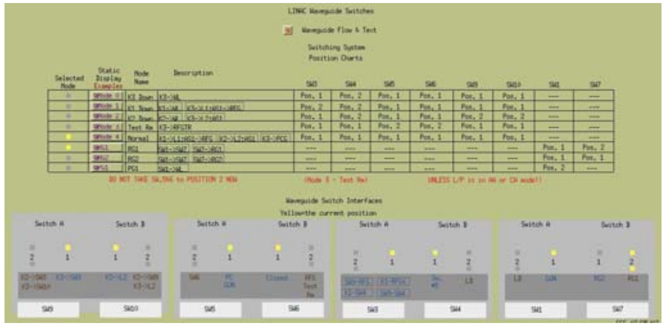
# EPICS Remote Control of PLC

## - EPICS Database Access Security by User, Group, Workstation

PLC Touch Screens with built-in logic for User Interface Control



MEDM displays monitor RF switch positions



LINAC Waveguide Switches

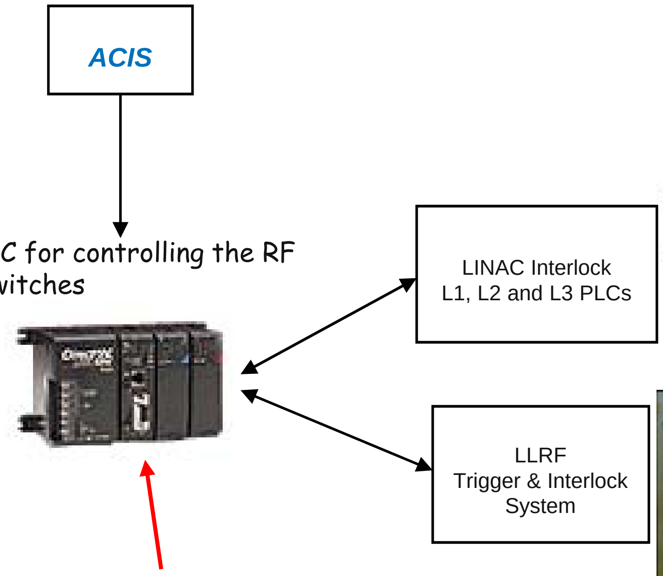
Waveguide Flow & Test

Switching System
Position Charts

| Selected Mode | Static Display Examples | Mode Name | Description | SW3 | SW4 | SW5 | SW6 | SW9 | SW10 | SW1 | SW7 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | Mode 0 | K3 Down | K3->[illegible] | Pos. 1 | Pos. 2 | Pos. 1 | Pos. 1 | Pos. 1 | Pos. 1 | --- | --- |
| | Mode 1 | K1 Down | K1->[illegible] K3->[illegible] | Pos. 2 | Pos. 2 | Pos. 1 | Pos. 1 | Pos. 1 | Pos. 1 | --- | --- |
| | Mode 2 | K2 Down | K2->[illegible] K3->[illegible] | Pos. 1 | Pos. 2 | Pos. 1 | Pos. 1 | Pos. 2 | Pos. 2 | --- | --- |
| | Mode 3 | Test Rm | K3->RFGTR | Pos. 1 | Pos. 1 | Pos. 2 | Pos. 2 | Pos. 1 | Pos. 1 | --- | --- |
| | Mode 4 | Normal | K1->L1:RG1->RFG K2->L2:RG2 K3->PCE | Pos. 1 | Pos. 1 | Pos. 1 | Pos. 1 | Pos. 1 | Pos. 1 | --- | --- |
| | RG1 | RG1 | SW1->SW7 SW7->RG1 | --- | --- | --- | --- | --- | --- | Pos. 1 | Pos. 2 |
| | RG2 | RG2 | SW1->SW7 SW7->RG2 | --- | --- | --- | --- | --- | --- | Pos. 1 | Pos. 1 |
| | PC1 | PC1 | SW1->[illegible] | --- | --- | --- | --- | --- | --- | Pos. 2 | --- |

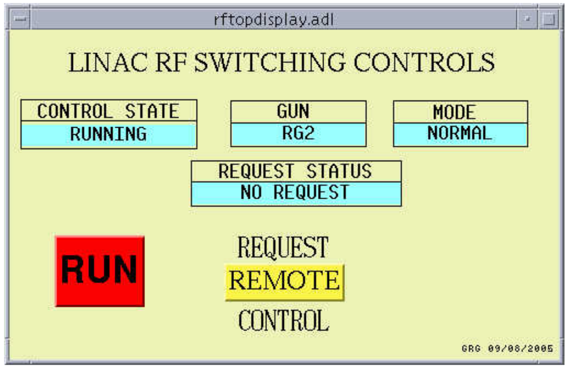
DO NOT TAKE SW5,SW6 to POSITION 2 NOW (Mode 3 - Test Rm) UNLESS L/P is in AA or CA mode!!

Waveguide Switch Interfaces
Yellow=the current position



PLC for controlling the RF Switches

Remote control from the Main Control Room
– MEDM displays with built-in logic



LINAC RF SWITCHING CONTROLS

CONTROL STATE: RUNNING

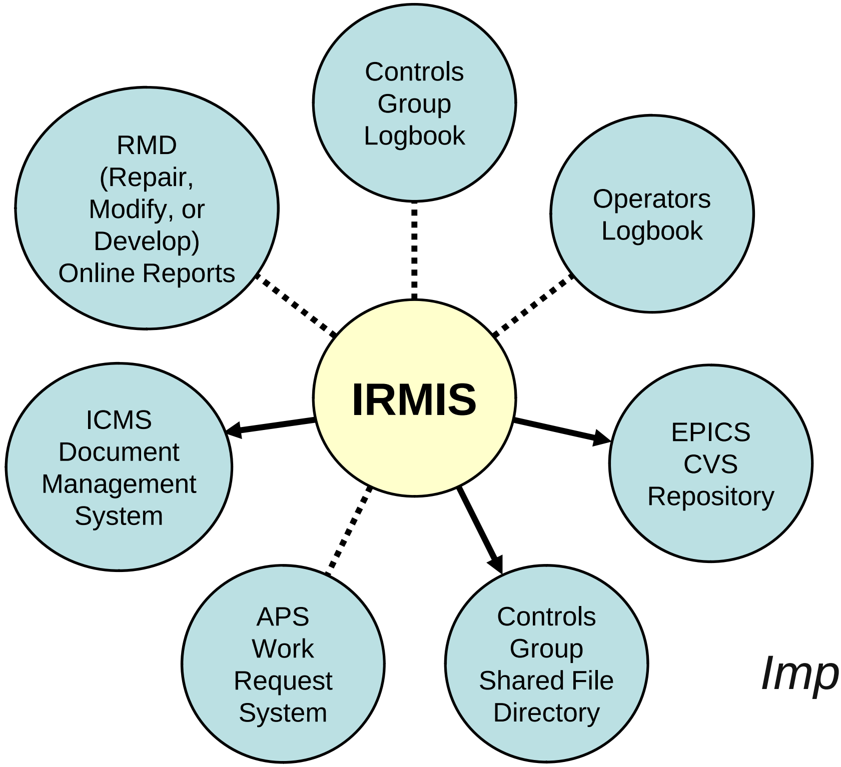
GUN: RG2

MODE: NORMAL

REQUEST STATUS: NO REQUEST

GRG 09/08/2005

# APS Control Systems-Related Software Applications



IRMIS

Controls Group Logbook

Operators Logbook

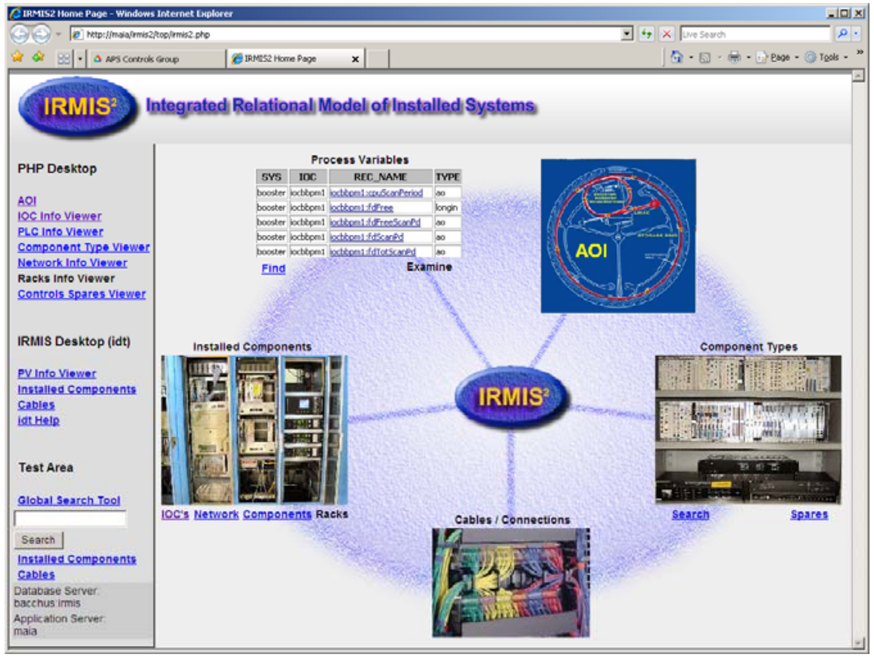
RMD (Repair, Modify, or Develop) Online Reports

ICMS Document Management System

EPICS CVS Repository

APS Work Request System

Controls Group Shared File Directory


IRMIS2 Home Page - Windows Internet Explorer
http://maia/irmis2/top/irmis2.php
Live Search
APS Controls Group
IRMIS2 Home Page
Page
Tools
IRMIS²
AOI
IRMIS²

Integrated Relational Model of Installed Systems

PHP Desktop

AOI
IOC Info Viewer
PLC Info Viewer
Component Type Viewer
Network Info Viewer
Racks Info Viewer
Controls Spares Viewer

IRMIS Desktop (idt)

PV Info Viewer
Installed Components
Cables
idt Help

Test Area

Global Search Tool

Search

Installed Components
Cables

Database Server: bacchus:irmis
Application Server: maia

Process Variables

| SYS | IOC | REC_NAME | TYPE |
|---|---|---|---|
| booster | iocbbpm1 | iocbbpm1:cpuScanPeriod | ao |
| booster | iocbbpm1 | iocbbpm1:fdFree | longin |
| booster | iocbbpm1 | iocbbpm1:fdFreeScanPd | ao |
| booster | iocbbpm1 | iocbbpm1:fdScanPd | ao |
| booster | iocbbpm1 | iocbbpm1:fdTotScanPd | ao |

Find Examine

Installed Components

IOC's Network Components Racks

Component Types

Search Spares

Cables / Connections

*Implemented in PHP, Java, JavaScript, XML, ...*

# *Web-based Controls Applications - Security Issues*

- User authentication and roles
  - Web site access
  - Relational database access

- Web site session fixation
  - Force the creation of a known valid session

- Web site session hijacking
  - Cross-site scripting
  - SQL injection
  - Network eavesdropping
  - Unwitting exposure
  - Forwarding, Proxies, and Phishing
  - Reverse proxy attack

- Real-time auditing of users' activities

# *Web-based Controls Applications - Security Strategies*

- Web Server
  - Secure Web server, HTTPS
    - *Deter session hijacking*
    - *HTTPS uses Secure Sockets Layer (SSL) to encrypt the request and response*
- User Authentication
  - LDAP, Lightweight Directory Access Protocol
    - *Standard for communicating record-based, directory-like data between programs*
  - SSO, Single Sign-On service
    - *Sun Java System Access Manager (also provides for real-time auditing)*
- PHP
  - Message-Digest algorithm 5 (MD5) cryptographic hash PHP function
    - *Transfer user authenticated phrase*
  - PHP session feature (PHP-created cookie)
    - *Deter session fixation*
    - *Customize with PHP functions*
      - session_set_save_handler( )
      - session_set_cookie_params( )
  - PHP htmlentities( ) function
    - *Prevent cross-site scripting attacks*
  - PHP mysql_real_escape_string( )
    - *Prevent SQL injection*

# *Web-based Controls Applications - Security Strategies, Continued...*

- JavaScript
  - JavaScript code runs under the security privileges of its parent HTML file
  - By default, JavaScript code loaded from an HTML page will be allowed to make requests only to that server
  - Handling of “potential enemy” depends on browser:  Internet Explorer, Firefox, and Mozilla-based
- XML
  - Ensure message integrity
    - *Digital signature*
      - Hash algorithm such as SHA1 or MD5
    - *Data encryption*
      - PHP function mycrypt_create_iv( )
    - *W3C specifications for encrypting and digitally signing XML*
      - http://www.w3.org/TR/xmldsig-core/
- MySQL
  - Database access credentials stored in Apache Web server environment variables
  - MySQL encryption functions
    - *PASSWORD( ) for password encryption*
  - Users’ roles defined in database table

# *Web-based Controls Applications - Security Strategies, Continued...*

- Web Services

*A Web service is a software system designed to support interoperable machine-to-machine interaction over a network. It has an interface described in a machine-processable format (specifically WSDL). Other systems interact with the Web service in a manner prescribed by its description using SOAP messages, typically conveyed using HTTP with an XML serialization in conjunction with other Web-related standards.*

*W3C Web Services Architecture Working Group*

- – SSL, XML Signature, and XML Encryption (already discussed)
- – SAML, Security Assertion Markup Language
  - *Protocol whereby clients make assertions and Web services can authenticate these claims*
  - *Adds above SSL a SOAP-based messaging protocol and XML-based data structures for communicating assertions*
  - *Organization for the Advancement of Structured Information Standards (OASIS) approved version 1.0 of SAML, www.oasis-open.org*

# APS Cyber Security Measures

- LDAP for user authentication
- Firewalls for scanning email for viruses, URL filtering, and anti-spam
  - virus infected email 50 to 200 per day
  - 20% to 30% of all email is spam
- Intrusion detection hardware
  - worms, denial-of-service, and application attacks
  - provides automated network blocks (100-400 network blocks per day)
- Portal Servers v 6.3
  - provide secure access to select applications such as email, Intranet Web, and file access
  - Secure Sockets Layer (SSL) - RS4 128 bit encryption
- Cyber Security Process Toolkit
  - perform divisional risk assessment

# Future APS Cyber Security Initiatives

- Next generation devices to improve performance*
  - 10 Gb/s backbone network
  - 10 Gb/s firewalls (Tier 1 and Tier 2)
  - 10 Gb/s Intrusion Detection System (IDS)
  - 802.1x authentication for wireless access to internal network
  - Distributed iperf servers to measure network performance
  - SSL VPN – Clientless or automatically downloaded client.  Web-based “Anywhere” access.  Support for Windows Vista, Mac OS X, Linux
- Reviewing Web Services as an option for implementing APS Single-Sign On (SSO) user authentication

* More and more of the beamline users are using the Internet to securely transfer data to their home institutions.

# *Summary*

- *Cyber security attacks are prevalent in national research laboratories*
- *Tools are available for security assessment*
- *Good cyber security strategy is multifaceted and includes both network and software design*
- *As computer technology changes, cyber security practices are required to change as well*

# *Acknowledgements*

- Ken Sidorowicz, APS IT Group Leader
- Ned Arnold, APS Controls Group Leader