ICCC-7

“Systematic Application of the Common Criteria Methodology to Evaluation of IT Products and Systems Used in Automated Physical Protection Systems”

Alexander Piskarev (AtomZaschitaInform)
Vladimir Lykov, Anatoly Shein (AtomInform),
Lynne Ambuel, Ronald B. Melton (Decisive Analytics Corp.)
David M. DeVaney, Cristen L. Duncan (Pacific Northwest National Laboratory),
Daniel R. Miller (Gregg Protection Services)

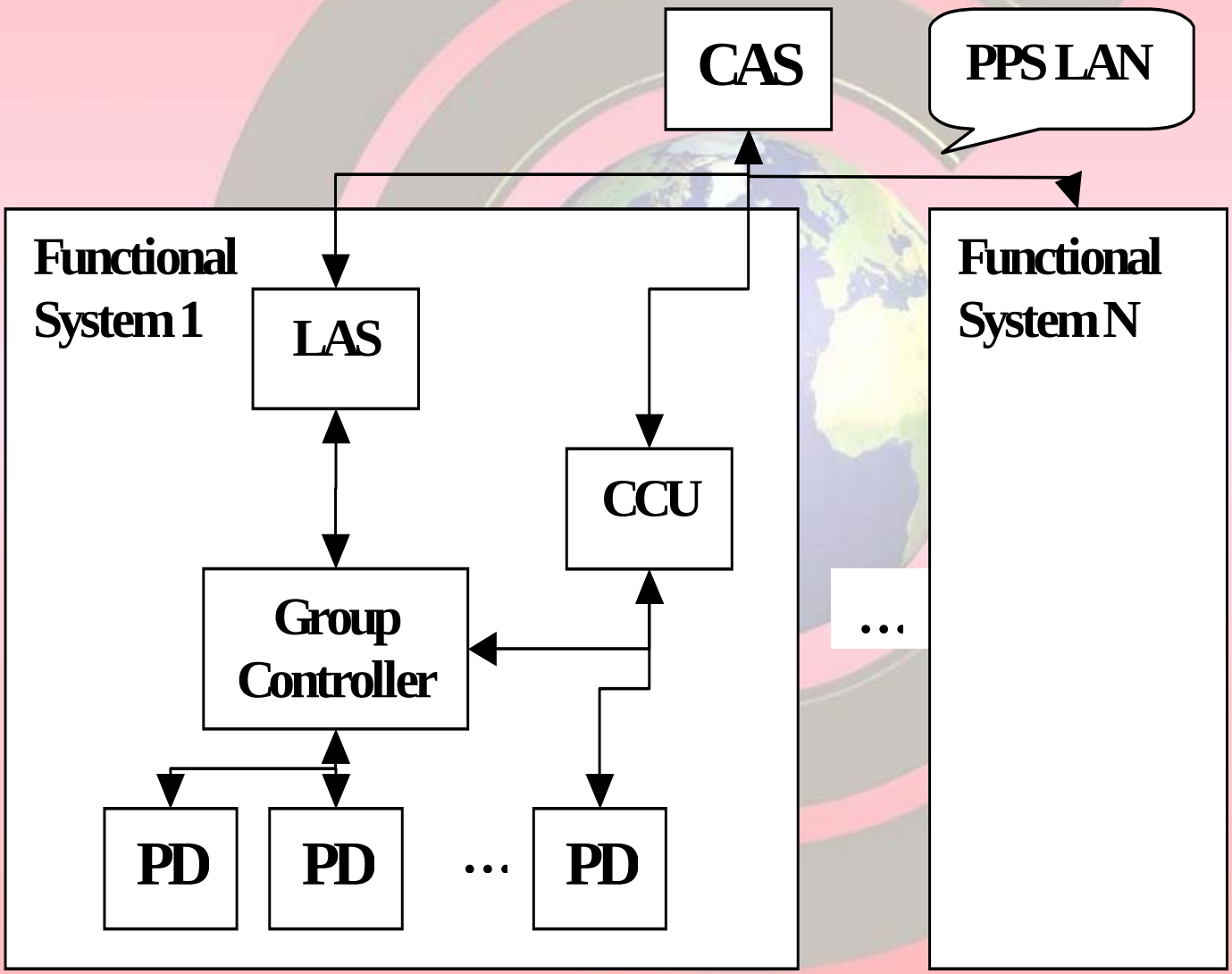
Content of the presentation

- Physical protection system (PPS) background
- IT security problems for Automated Physical Protection Systems (APPS)
- Technical regulations and certification of IT products
- Advantages of the Common Criteria methodology
- Development of protection profiles for APPS
- Current status and future plans

Physical Protection System Background

- Integrated sets of physical protection equipment are the basis for a PPS
- Hardware, software and firmware form a special class of IT products that may be used in an APPS
- Most Commonly Used Functional Subsystems:
  - Alarm Systems (AS)
  - Access Control Systems (ACS)
  - Video Surveillance Systems (VSS)
- Systems combining the requirements set for two or more subsystems = integrated systems (IS)
- Central alarm stations (CAS) and local/ secondary alarm stations (LAS/SAS)

Structure of an Integrated APPS System



Access Control System

- **An ACS structure in particular includes:**
  - **Access blocking equipment (booths, turnstiles, etc.) installed at the access control points**
  - **Equipment for input of identification attributes (readers, keypads, biometric scanners, etc.)**
  - **Peripheral devices (PD)**
  - **Controllers and Group Controllers**
  - **Central control units (CCU)**
  - **Workstations of operators and administrators**
  - **Database servers**
  - **Badge printing workstations**

Personnel having contact with ACS

- **The following personnel may be considered as having contact with ACS:**
  - **Nuclear site personnel, physical protection personnel or visiting specialists (ACS users)**
  - **ACS operators**
  - **ACS administrators**
  - **ACS security administrator**
- **Various categories of personnel have different authorization for access to secure areas and information**
- **ACS users do not have contact with workstations, servers and group controllers**
- **ACS operators, administrators and security administrator have access to sensitive information and systems**

The IT Security Problem for an APPS

- Primary factors related to APPS information security:
  - Information assets of the APPS
  - List of assumed threats to the information assets
  - Potential threat agent model
  - Location, condition of use and potential accessibility of the APPS information assets
- Protected, Internal, Vital and Limited Access Areas of PPS for a nuclear site
- Security problems for APPS and the extent of APPS integration
- Unauthorized disclosure or modification of information and denial of access

Technical Regulations

- Development of technical regulations must consider:
  - Up-to-date technical requirements
  - APPS development lifecycle
- Current Russian regulatory documents are incomplete and based on an out-of-date methodology
- Late 90's APPS information security requirements did not take into account categorization or new approaches of the CC
- Categorization of Access Control Systems
  - Autonomous
  - Centralized (networked)
  - Universal

Certification of IT products

- IT products used in APPS must be certified to meet IT security requirements
- Software of some ACS has been certified within the framework of the Russian certification system
  - Zirconi-M, Eleron enterprise, Russia
  - ASSaD-32 Software, Algont Ltd, Russia
  - Advantage Suite for Networks (ASN), “Advantor” Corp.
- Globalization of IT based products results in need to develop new regulatory documents based on international standards

Advantages of the Common Criteria

- Advantages of the CC Approach:
  - Requirements are defined for specific products or systems
  - Rationale for requirements explicitly identified
  - Justification of requirements in PP's and ST's support their selection
  - Requirements do not require additional interpretation
  - Mandatory independent evaluation of PP's and ST's increases their level of correctness
- Flexibility of the CC structure gives opportunity to replace the current IT requirements with PP's
- Use of PP's for APPS in different countries will facilitate better understanding of consumer's needs by developers

Development of PP's for APPS

- **Factors for characterizing the family of PP's include:**
  - **Functionality of the Physical Protection subsystems**
  - **Architecture of APPS (*Autonomous, Centralized, Universal*)**
  - **Zoning of PPS (*Protected, Internal, Vital Areas*)**
  - **Security level, and**
  - **Level of integration**

Conceptual Approach

- Systematic, top-down analysis
- Identification of:
  - Information assets
  - Threats (agent, method & attack Path) directed toward the Information assets
  - Vulnerabilities of assets to threats
  - Countermeasures to counter threats
- Hierarchical decomposition
  - System protection profile
  - Subsystem protection profiles
  - Component protection profiles

Initial Protection Profile Development

- ACS is first PP subsystem selected for protection profile development
  - Most common subsystem
  - Relatively more complex
  - Functionality can be expanded
- Scope of this protection profile includes logical IT security functions for software of LAN nodes and other devices
- Security functions of general purpose SW (OS, DBMS, etc.) may be used to implement security functions in application programs and firmware
- Security target must map between the statement of security function requirements in the protection profile and implementation of those functions in the product

Summary

- IT security requirements should be based on application of Common Criteria
- Family of PP's are defined based on:
  - Analysis of APPS Functional Subsystems
  - APPS IT products
  - Conditions of use and
  - Level of integration
- Initial efforts are focused on developing the ACS protection profile

Future Plans

- Future Plans include:
  - Complete development of PP's, evaluate and certify it and develop the list of additional PP's for use in APPS
  - Develop a system protection profile of an APPS as a whole
  - Evaluate and certify IT products and systems for APPS
- By using CC methodology, these PP's can be recognized and used by interested parties all over the world