Platform IT (PIT) Control Systems Cybersecurity Glossary

ACRONYMS

A	Assess
AA	Assess and Authorize
AO	Authorizing Official
APMS	Army Portfolio Management Solution
APS	Airfield & Pier Systems
ATFP	Anti-Terrorism Force Protection
ATO	Authority to Operate
BACNet	Building Automation and Control Network
BCS	Building Control System
BOS	Base Operation and Support
CCTV	Closed Circuit Television
CENet	Civil Engineer Network
C-I-A	Confidentiality-Integrity-Availability
CMMS	Computerized Maintenance Management System
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CP	Contingency Planning (controls)
CPS	Cyber-Physical System
CSET	Cyber Security Evaluation Tool
DADMS	DON Application and Database Management System
DCS	Distributed Control System
DHP SIRT	Defense Health Program Systems Inventory Reporting Tool
DHS	Department of Homeland Security
DIACAP	DoD Information Assurance Certification and Accreditation Process
DITPR	DoD Information Technology Portfolio Repository
DLA	Defense Logistics Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
EI&E	Energy, Installations & Environment
EITDR	Enterprise Information Technology Data Repository
eMASS	Electronic Mission Assurance Support Service
FAS	Fire Alert System
FAT	Facility Acceptance Test
FISMA	Federal Information Security Act

HIPAA	Health Information Privacy Assurance Act
HMI	Human-Machine Interface
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication (controls)
IATT	Interim Authority to Test
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IRP	Incident Response Plan
IS	Information System
ISC	Interagency Security Committee
ISO	Information System Owner
ISO	International Standards Organization
LSSS	Life Safety & Security Systems
MHPCS	Materials Handling & Process Control Systems
MILCON	Military Construction
NA	Not Applicable
NIPRNet	Nonsecure Internet Protocol Router Network
NIST	National Institute for Standards and Technology
OI	Other Infrastructure
OSD	Office of the Secretary of Defense
OT	Operational Technology
PACS	Physical Access Control System
PCI	Peripheral Component Interconnect
PCII	Protected Critical Infrastructure Information
PE	Physical and Environmental (controls)
PE	Platform Enclave
PIDS	Physical Intrusion Detection System
PII	Personally Identifiable Information
PIT	Platform Information Technology
PL	Planning (controls)
PLC	Programmable Logic Controller
POA&M	Plan of Action and Milestones
POC	Point of Contact
POL	Petroleum, Oils and Lubricants
PSNet	Public Safety Network
RMF	Risk Management Framework
SAR	Security Assessment Report
SAT	System Acceptance Testing
SC	System and Communication (controls)
SCADA	Supervisory Control and Data Acquisition

SI	System and Information Integrity
SP	Special Publication
SRM	Sustainment, Restoration and Modernization
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TBB	Transport Backbone
TFS	Transportation Fueling System
UCS	Utility Control System
UFC	Unified Facilities Criteria
UMCS	Utility Monitoring and Control Systems
WG	Working Group
WHS	Washington Headquarters Service

DEFINITIONS

Term — **Definition**

Building Automation System (BAS) — A system which provides automatic centralized control of a building's heating, ventilation and air conditioning, lighting and other systems. The objectives of building automation are improved occupant comfort, efficient operation of building systems, and reduced energy consumption and operating costs.

Term

Definition

Building Control System (BCS)

A system that controls building electrical and mechanical systems such as HVAC (including central plants), lighting, vertical transport systems, and irrigation systems. Building Control Systems generally do not have a full-featured user interface; they may have “local display panels” but typically rely on the UMCS front end for full user interface functionality.

Closed Circuit Television System (CCTV)

An ESS that allows video assessment of alarm conditions via remote monitoring and recording of video events. Video monitoring may also be incorporated into other systems which are not CCTV.

Control System

A system of digital controllers, communication architecture, and user interfaces that monitor and control infrastructure and equipment.

Controller

An electronic device – usually having internal programming logic and digital and analog input/output capability – which performs control functions. Two primary types of controller are equipment controller and supervisory controller.

Cyber Physical Systems

Cyber-Physical Systems or "smart" systems are co-engineered interacting networks of physical and computational components. These systems are at the heart of our critical infrastructure and form the basis of our future smart services. These promise increased efficiency and interaction between computer networks and the physical world enabling advances that improve the quality of life, including advances such as in personalized health care, emergency response, traffic flow management, and the electric power generation and delivery. (NIST CPS http://www.nist.gov/cps/)

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will far exceed the simple embedded systems of today. CPS technology will transform the way people interact with engineered systems -- just as the Internet has transformed the way people interact with information. New smart CPS will drive innovation and competition in sectors such as agriculture, energy, transportation, building design and automation, healthcare, and manufacturing. (NSF CPS http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286&org=NSF&sel_org=NSF&from=fund)

Defense Business System (DBS)

An information system, other than a national security system, operated by, for, or on behalf of the Department of Defense, including financial systems, information technology, and information assurance infrastructure used to support business activities such as acquisition, logistics, planning and budgeting.

Distributed Control System

This term is being phased out in preference of BAS, BCS, UCS, and/or UMCS.

Electronic Security System (ESS)

The integrated electronic system that encompasses interior and exterior intrusion detection systems (IDS), CCTV systems for assessment of alarm conditions, access control systems, data transmission media, and alarm reporting systems for monitoring, control, and display.

Term **Definition**

Energy Monitoring Control Systems

This term is being phased out in favor of BAS, BCS, UCS, and/or UMCS.

Equipment Controller (EC)

A controller implementing control logic to control a piece of equipment. Note: a controller is defined by use, and many ECs also have the capability to act as supervisory controllers (SC). Some examples of equipment controllers are air handler controller, protective relay, and pump controller.

Field Control System (FCS)

A Building Control System, Utility Control System, Process Control System, Access Control System, etc. within the Facility and "downstream" of the FPOC.

Field Control Network (FCN)

The network used by the Building Control System, Utility Control System, Process Control System, etc., within a facility "downstream" of the FPOC. This includes IP, ethernet, and other network infrastructure that support control system(s) in a given facility.

Field Point of Connection (FPOC)

The FPOC is the point of connection between the ICS IP network and the field control network (an IP network, a non-IP network, or both). The hardware which provides the connection at this location is generally a control protocol router, a control protocol gateway, or an IT device such as a switch, IP router, or firewall; it may include a supervisory controller.

Front End [UMCS, PCS, ESS, etc.]

The portion of the control system consisting primarily of IT equipment, such as computers and related equipment, intended to perform operational functions and run monitoring and control/engineering tool application software. The front end does not directly control physical systems; it interacts with them only through field control systems (FCS). The front end is a component of the [UMCS, ESS, etc.] infrastructure (see definition).

Hybrid/Converged Systems

The Department of Homeland Security's (DHS) Interagency Security Committee (ISC) has issued guidance titled "Securing Government Assets through Combined Traditional Security and Information Technology". The ISC guidance is specific to Homeland Security Presidential Directives (HSPD)-12 and Presidential Decision Directive (PDD)-21, and applies to Physical Access Control Systems (PACS), closed-circuit television, and physical intrusion detection systems.

Proposed DoD ICS PIT - A Hybrid/Converged System (H/CS) consists of an Information System (IS) front end that uses credentials to authenticate a user, combined with a Platform Information Technology (PIT) back end that operates a physical device. A H/CS credential can include PII, HIPAA, PCI, biometric, or other personally identifiable data that requires a higher level of data protection. The H/CS physical devices use the H/CS credential and embedded software/firmware to execute physical commands."

Industrial Control System (ICS)

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures. An ICS consists of combinations of control components (e.g., electrical, mechanical, hydraulic, pneumatic) that act together to achieve

Term	**Definition**
	an industrial objective (e.g., manufacturing, transportation of matter or energy).
Information Technology (IT)	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.
Infrastructure [UMCS, ESS, ...]	The portion of a control system (such as a UMCS or ESS) which includes all components that are not part of a field control system. These components include the FPOC, the platform enclave, and the front end.
Internet of Things	The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a Smart Grid. Things, in the IoT, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, or field operation devices that assist fire-fighters in search and rescue. Current market examples include smart thermostat systems and washer/dryers that utilize wifi for remote monitoring http://en.wikipedia.org/wiki/Internet_of_Things
Industrial Internet of Things	The industrial internet is a term coined by General Electric and refers to the integration of complex physical machinery with networked sensors and software. The industrial Internet draws together fields such as machine learning, big data, the Internet of things and machine-to-machine communication to ingest data from machines, analyze it (often in real-time), and use it to adjust operations. http://en.wikipedia.org/wiki/Industrial_Internet, Industrial Internet 101 http://www.industrialinternet.us/revive/ Industrial Internet Consortium http://iiconsortium.org/
Intrusion Detection System [Physical/ESS]	A system consisting of interior and exterior sensors, surveillance devices, and associated communication subsystems that collectively detect an intrusion of a specified site, facility, or perimeter and annunciate an alarm.
Intrusion Detection System [Cyber]	A device or software application that monitors network or system activities for malicious activities or policy violations, and produces reports to management.
Operational Technology	Operational technology (OT) is hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Gartner OT http://www.gartner.com/it-glossary/operational-technology-ot/)
Platform Enclave [UMCS, ESS, ...]	An enclave is a collection of computing environments connected by one or more internal network(s) under the control of a single approval and security policy, including personnel and physical security. Examples include a local area network (including smart terminals), an agency-wide backbone, a

Term **Definition**

communications network, a departmental data processing center (including its operating system and utilities), a tactical radio network, or a shared information processing service. Enclaves provide standard cybersecurity controls such as boundary defense, incident detection and response, and key management. Enclaves may be specific to an organization or a mission, and the computing environments may be organized by physical proximity or by function.

Platform IT (PIT)
IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

PIT System
A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

PIT Interconnect
For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Examples of platform IT interconnections that impose security considerations include remote administration, remote upgrade or reconfiguration, and interfaces for data exchanges with enclaves for mission planning or execution.

Security Content Automation Protocol (SCAP)
A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation (e.g., FISMA compliance). The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP.

Supervisory Controller
A controller that implements a combination of supervisory logic (global control or optimization strategies), scheduling, alarming, event management, trending, web services or network management. A supervisory controller may be located between the platform enclave and the FCS serving as the data aggregation conduit between the FCS and the front end. Note that this arrangement is defined by use; many supervisory controllers have the capability to also directly control equipment, and serve the role of both supervisory controller and equipment controller.

Utility Control System (UCS)
A type of field control system used for control of utility systems such as electrical distribution & generation, sanitary sewer collection and treatment, water generation and pumping, etc. Building controls are excluded from a UCS, however it is possible to have a Utility Control System and a Building Control System in the same facility, and for those systems to share components such as the FPOC.

Utility Monitoring and Control System (UMCS)
The system consisting of one or more building control systems or utility control systems and the associated UMCS Infrastructure. In other words, it is the complete utility monitoring system – from the front end to equipment controllers. At the highest level the UMCS is composed of a UMCS platform enclave and a common architecture.