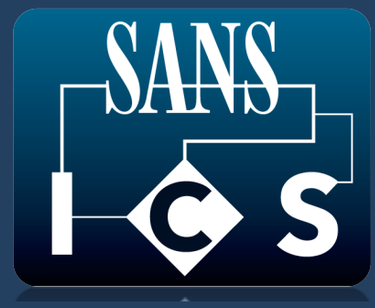
Terms: N (continued) - S

- NSE - Nmap Scripting Engine
- NSM - Network Security Monitoring
- NST - Network Stress Testing
- NSTB - National SCADA Test Bed Program
- NTP - Network Time Protocol
- NVD - National Vulnerability Database
- ODVA - Open DeviceNet Vendors Association
- OLE - Object Linking and Embedding
- OOB - Out-of-Band
- OPC - OLE for Process Control
- OS - Operating Systems
- OSHA - Occupational Safety and Health Administration
- OSI - Open Systems Interconnect
- OT - Operational Technology
- OTA - Over-The-Air
- OUI - Organizationally Unique Identifier
- P-NET - Process NETwork
- PAW - Privileged Access Workstations
- PCS - Process Control System
- PEAP - Protected Extensible Authentication Protocol
- PERA - Purdue Enterprise Reference Architecture
- PHA - Process Hazards Analysis
- PICREL - Preparation, Identification, Containment, Recovery, Eradication, Lessons Learned
- PID - Proportional Integral Derivative Algorithm
- PIN - Personal Identification Number
- PLC - Programmable Logic Controller
- PMU - Phasor Measurement Unit
- PNNL - Pacific Northwest National Laboratory
- PoC - Proof-of-Concept
- PPE - Personal Protective Equipment
- PTP - Precision Time Protocol
- PV - Process Value/Variable
- QoS - Quality-of-Service
- QRA - Quantitative Risk Analysis
- RADIUS - Remote Authentication Dial-In User Service
- RARP - Reverse Address Resolution Protocol
- RAT - Remote Access Trojans
- RDP - Remote Desktop Protocol
- RF - Radio Frequency
- RFC - Request for Comment
- RFI - Remote File Inclusions
- RPC - Remote Procedure Call
- RPI - Requested Packet Interval Rate
- RT - Real-Time
- RTOS - Real-Time Operating Systems
- RTU - Remote Terminal (Telemetry) Unit
- SAT - Site Acceptance Test
- SCADA - Supervisory Control and Data Acquisition
- SCCM - System Center Configuration Manager
- SCM - Security Compliance Manager
- SCT - Security Compliance Toolkit
- SDA-S - Security Development Artifacts for Embedded Devices
- SDLA - Security Development Lifecycle Assurance
- SDR - Software-Defined Radios
- SFC - Sequential Function Chart

Terms: S (continued) - Z

- SGIP - Smart Grid Interoperability Panel
- SHA - Secure Hash Algorithm
- SHE - Safety, Health, and Environmental
- SHS - Secure Hash Standard
- SIEM - Security Information Event Management
- SIF - Safety Instrumented Functions
- SIL - Safety Integrity Level
- SIS - Safety Instrumented System
- SLE - Single Loss Expectancy
- SMB - Service Message Bus
- SME - Subject-Matter Expert
- SNL - Sandia National Laboratories
- SOC - Security Operations Center
- SoC - System on a Chip
- SP - Setpoint
- SPAN - Switched Port Analyzer
- SQL - Structured Query Language
- SQLi - SQL Injection
- SRP - Software Restriction Policies
- SSA - System Security Assurance
- SSL - Secure Sockets Layer
- SSO - Single-Sign-On
- SSP - Secure Simple Pairing
- ST - Structured Text
- STIX - Structured Threat Information eXpression
- TAXII - Trusted Automated eXchange of Indicator Information
- TCP - Transmission Control Protocol
- TDMA - Time Division Multiple Access
- TEM - Threat and Environment Manipulation
- TKIP - Temporal Key Integrity Protocol
- TLS - Transport Layer Security
- TTL - Time-To-Live
- TTP - Tactics, Techniques, and Procedures
- TTX - Tabletop Exercise
- UA - Unified Architecture
- UAC - User Account Control
- UDP - User Datagram Protocol
- VCSP - Vehicle Cyber Security Program
- VSAT - Very Small Aperture Terminal
- VIT - Vulnerability Identification Testing
- VLAN - Virtual Local Area Network
- VM - Virtual Machine
- VNC - Virtual Network Computing
- VPN - Virtual Private Network
- WAN - Wide Area Network
- WAP - Wireless Access Point
- WEP - Wired Equivalent Privacy
- WIDS - Wireless Intrusion Detection Systems
- WiTECK - Wireless Industrial Technology Konsortium
- WLAN - Wireless Local Area Network
- WMIC - Windows Management Instrumentation Console
- WPA - Wi-Fi Protected Access
- WSUS - Windows Server Update Services
- XSRF - Cross-Site Request Forgery
- XSS - Cross-Site Scripting



Acronyms
Quick Start Guide v0.1

SANS ICS
ics.sans.org

By Dean Parsons & Don C. Weber
dparsons@sans.org | don@cutawaysecurity.com

This guide covers the basic acronyms used in SANS Industrial Control System Security courses and includes terms from Operational Technology (OT), Information Technology (IT), and Information Security (InfoSec).

Terms: A - B

- ACDC - Active Cyber Defense Cycle
- ACL - Access Control List
- AD - Active Directory
- AES - Advanced Encryption Standard
- AGC - Automatic Generation Control
- AH - Authentication Header Protocol
- ALE - Annualized Loss Expectancy
- AM - Amplitude Modulation
- ANSI - American National Standards Institute
- AP - Access Point
- API - Application Programming Interface
- APT - Advanced Persistent Threat
- ARC - Application Runtime Control
- ARO - Annualized Rate Occurrence
- ARP - Address Resolution Protocol
- ASAP-SG - Advanced Security Acceleration Project for the Smart Grid
- AV - Asset Value
- BACnet - Building Automation and Control Network
- BC - Business Continuity
- BCP - Business Continuity Plan
- BE2 - BlackEnergy2
- BE3 - BlackEnergy3
- BES - Bulk Electric System
- BGAN - Broadband Global Area Network
- BITS - Background Intelligent Transfer Service
- BLE - Bluetooth Low Energy
- BMS - Building Management System
- BP - Business Continuity
- BPF - Berkeley Packet Filter
-

Terms: B (continued) - E

- BTS - Base Transceiver Station
- BYOD - Bring-Your-Own-Device
- C&C - Command-and-Control
- C2 - Command-and-Control
- CANbus - Controlled Area Network Bus
- CART - Complete, Accurate, Relevant, and Timely
- CBC - Cipher Block Chaining
- CCTV - Closed-Circuit Television
- CI - Critical Infrastructure
- CIA - Confidentiality, Integrity, and Availability
- CIKR - Critical Infrastructure Key Resource
- CIP - Common Industrial Protocol
- CIP - Critical Infrastructure Protection
- CNAP - U.S. White House Cybersecurity National Action Plan
- CPU - Central Processing Unit
- CRPA - Cyber Risk Preparedness Assessments
- CRT - Communication Robustness Testing
- CSF - Cyber Security Framework
- CSIRT - Computer Security Incident Response Team
- CSRF - Cross-Site Request Forgery
- CTR - Counter Mode
- CVE - Common Vulnerabilities and Exposures
- CVSS - Common Vulnerability Scoring System
- CWE - Common Weakness Enumeration
- DA - Data Access
- DA - Domain Administrator
- DAS - Data Acquisition System
- DBA - Database Administrator
- DCE - Distributed Computer Environment
- DCS - Distributed Control System
- DDoS - Distributed Denial-of-Service
- DEP - Data Execution Prevention
- DES - Data Encryption Standard
- DFIR - Digital Forensics and Incident Response
- DHCP - Dynamic Host Configuration Protocol
- DHS - U.S. Department of Homeland Security
- DLCI - Data Link Connection Identifier
- DMS - Distribution Management System
- DMZ - Demilitarized Zone
- DNP - Distributed Network Protocol
- DNS - Domain Name Service
- DOE - U.S. Department of Energy
- DoS - Denial-of-Service
- DPI - Deep Packet Inspection
- DPR - Digital Protective Relay
- DR - Disaster Recovery
- DRP - Disaster Recovery Plan
- DUC - Defense Use Case
- ECB - Electronic Code Book
- EDSA - Embedded Device Security Assurance
- EEPROM - Electrically Erasable Programmable Read-Only Memory
- EF - Exposure Factor
- EFS - Encrypted File System
- EMET - Enhanced Mitigation Experience Toolkit
- EMS - Energy Management System

Terms: E (continued) - I

- EMT - Electro Magnetic Transmission
- ENIP - EtherNet/Industrial Protocol
- ENISA - European Union Agency for Network and Information Security
- EoL - End-of-Life
- EOP - Emergency Operations and Preparedness
- EPA - Ethernet for Plant Automation
- EPCIP - European Programme for Critical Infrastructure Protection
- ERO - Electric Reliability Organization
- ERT - Embedded Device Robustness Testing
- ESCSWG - Energy Sector Control Systems Working Group
- ESD - Emergency Shutdown Systems
- ESP - Encapsulating Security Protocol
- EST - Experience Sharing Tool
- EUI - Extended Unique Identifier
- EW - Engineering Workstation
- F&G - Fire and Gas
- FAT - Factory Acceptance Test
- FBD - Function Block Diagram
- FDA - U.S. Food and Drug Administration
- FEP - Front-End Processor
- FIP - Factory Instrumentation Protocol
- FIPS - Federal Information Processing Standards
- FM - Frequency Modulation
- FSA-E - Functional Security Assessment for Embedded Devices
- GCHQ - UK Government Communications Headquarters
- GNSS - Global Navigation Satellite Systems
- GPMC - Group Policy Management Console
- GPO - Group Policy Object
- GPS - Global Positioning System
- HART - Highway Addressable Remote Transducer
- HAZOP - HAZard and OPerability
- HCF - HART Communication Foundation
- HIDS - Host Intrusion Detection System
- HMAC - Hashed Message Authenticity Check
- HMI - Human Machine Interface
- HSE - High-Speed Ethernet
- HVAC - Heating, Ventilation, and Air Conditioning
- HVP - High Voltage Protection
- I/O - Input/Output
- IACS - Industrial Automation and Control Systems
- IAEA - International Atomic Energy Agency
- IANA - Internet Assigned Numbers Authority
- ICMP - Internet Control Message Protocol
- ICS - Industrial Control Systems
- IDEA - International Data Encryption Algorithm
- IDS - Intrusion Detection systems
- IEC - International Electrotechnical Commission
- IED - Intelligent Electronic Device
- IEEE - Institute of Electrical and Electronics Engineers
- IETF - Internet Engineering Task Force
- IIoT - Industrial Internet of Things
- IL - Instruction List
- InfoSec - Information Security
- IoC - Indicators of Compromise

Terms: I (continued) - N

- IPC - Inter Process Communication
- IPFIX - IP Flow Information Export
- IPS - Intrusion Prevention systems
- IPv4 - Internet Protocol Version 4
- IPv6 - Internet Protocol Version 6
- IR - Incident Response
- IRP - Incident Response Plan
- IRT - Isochronous Real-Time
- ISA - International Society of Automation
- ISCI - ISA Security Compliance Institute
- ISAC - Information Sharing and Analysis Center
- ISAO - Information Sharing and Analysis Organization
- ISC - SANS Internet Storm Center
- ISM - Industrial, Scientific, and Medical
- ISMS - Information Security Management System
- ISO - International Standards Organization
- IT - Information Technology
- ITS - Internet Time Service
- IV - Initialization Vectors
- LAN - Local Area Network
- LAPS - Local Administrator Password Solution
- LD - Ladder Diagram (also referred to as Ladder Logic)
- LDAP - Lightweight Directory Access Protocol
- LFI - Local File Inclusions
- LLDP - Link Layer Discovery Protocol
- LOPA - Layers of Protection Analysis
- LoS - Line-of-Sight
- LotL - Living-off-the-Land
- LSASS - Local Security Authority Subsystem Service
- MAC - Media Access Control
- MAC - Message Authentication Code
- MD - Message Digest
- MDM - Mobile Device Management
- MES - Manufacturing Execution System
- MIMO - Multiple-Input Multiple-Output
- MitM - Machine-in-the-Middle
- MMC - Microsoft Management Console
- MTD - Maximum Tolerable Downtime
- MTU - Management Terminal Unit
- MU-MIMO - Multi-User Multiple-Input Multiple-Output
- MV - Manipulated Variable
- NAC - Network Access Control
- NAT - Network Address Translation
- NCCIC - National Cybersecurity and Communications Integration Center
- NERC - North American Electric Reliability Corporation
- NESCOR - National Electric Sector Cybersecurity Organization Resources
- NIC - Network Interface Card
- NIDS - Network Intrusion Detection Systems
- NIPS - Network Intrusion Prevention Systems
- NIST - National Institute of Standards and Technology
- NLB - Network Load Balancing
- NOC - Network Operations Center
- NSA - U.S. National Security Agency