

NUMERICS

21 Steps to Improve Cyber Security of SCADA Networks (PCCIP), 90–96

232 standard (EIA), 10, 12, 47, 48, 50

422 standard (EIA), 47, 48, 50

485 standard (EIA), 10, 63

802.1P standard (IEEE), 58

802.2 standard (IEEE), 50

1779:2005 standard, *Code of Practice for Information Security Management (ISO/IEC)*, 110, 111–112

9506-1:2000 standard (ISO), 53

9506-2:2000 standard (ISO), 53

11898-1 standard (ISO), 54

15408 standard (ISO), 160

60870-5 standard (IEC), 53

60870-6 standard (IEC), 53

61850 standard (IEC), 53–54

61970 standard (IEC), 53

61968 standard (IEC), 53

61158-2 standard (IEC), 63

A

access control

role-based, 19

standards addressing, 112

STOE, 167, 192

accountability, 95

ACL (access control list), 64

active-response IDS, 99–100

Actuator asset, 175

address resolution protocol (ARP), 48, 50

adequacy reliability objective, 20, 21

AGA (American Gas Association)

Cryptographic Protection of SCADA Communications General Recommendations, Draft 3, 143, 144

ALE (Annualized Loss Expectancy), 79

Allen Bradley protocols, 6, 44

ammonia, 25, 38, 146

ammonium nitrate, 26

anomaly-based IDS, 99

API (American Petroleum Institute)

Standard 1164 (Pipeline SCADA Security, First Edition), 142–143

application-based IDS, 99

architecture overview, 7–9

ARO (Annualized Rate of Occurrence), 79

ARP (address resolution protocol), 48, 50

asset

management, 111, 184

STOE asset protection list, 175–176

- attack. *See also* IDS (intrusion detection system)
 - active, 134
 - buffer overflow, 83, 103, 172
 - bypassing security mechanism, 174
 - close-in, 134
 - DDoS, 75, 81, 173, 178
 - distribution, 134
 - file deletion/modification, unauthorized, 174, 176
 - Houston Port attack, 75
 - IDS attack signature database, 99
 - insider, 134
 - Maroochy Shire sewage control system attack, 75
 - passive, 134
 - privilege elevation, unauthorized, 178
 - privilege goal, 83–84
 - route, 82–83
 - Salt River Project attack, 75
 - spoofing authorized user, 173, 177
 - STOE attack type list, 172–174, 176–179
 - traffic analysis, unauthorized, 173, 176
 - war dialing, 92
 - war driving, 82, 92
 - auditing
 - log, 17, 102–105
 - risk associated with, 189
 - security, 77, 92, 113
 - STOE, 167, 193
 - Unix/Linux system, 102
 - authentication
 - STOE, 164, 165, 166, 191
 - two-factor, 18
 - weak, 82
 - awareness of security, fostering, 97, 106–107, 113
- B**
- backup
 - hot stand-by, 7, 20
 - importance of, 95, 141
 - STOE, 167, 191
 - BCIT (British Columbia Institute of Technology), 75, 77, 127
 - Bement, Arden (NIST director), 74–75
 - benzene, 38–39
 - Berinato, Scott
 - “Debunking the Threat to Water Utilities,” 74
 - “The Truth About Cyber Terrorism,” 74
 - biometric security technology, 17
 - boiling water reactor (BWR), 27–28
 - boron trifluoride, 38
 - British Columbia Institute of Technology (BCIT), 75, 77, 127
 - BS (British Standard) for Information Security Management standard 7799-2:2002 (*Specification for Information Security Management Systems*), 110, 112–113
 - buffer overflow attack, 83, 103, 172
 - Bush, George W. (President), 2
 - BWR (boiling water reactor), 27–28
 - bypassing security mechanism, 174
 - Byres, Eric (BCIT faculty member), 75, 77
- C**
- CAN (controller area network)
 - protocols, 54–55
 - carrier sense multiple access with collision detection (CSMA/CD), 54, 58
 - CC (Common Criteria) profile, 129, 130, 158–159
 - Center for SCADA Security, 126
 - central processing unit (CPU) log, 105
 - checksum, applying to audit log, 105
 - chemical plant SCADA system, 38–39, 127, 140, 145
 - Chemical Sector Cybersecurity Program, 127
 - chemicals, dangerous
 - ammonia, 25, 38, 146
 - ammonium nitrate, 26
 - benzene, 38–39

- boron trifluoride, 38
- chlorine, 38, 146
- hydrofluoric acid, 25
- hydrogen, 25, 39
- hydrogen fluoride, 146
- hydrogen sulfide, 25
- methane, 39
- strontium, 27
- sulfuric acid, 25
- toluene, 38–39
- U-235, 27
- xenon, 27
- CI (ControlNet International), 55
- CIA (confidentiality, integrity, availability), 63, 117–119
- CIAG (Cisco Critical Infrastructure Protection Group), 86, 87
- CIAO (Critical Infrastructure Assurance Office), 2
- CIM (Common Information Model), 53
- CIP (Common Industrial Protocol), 55, 56, 57
- CIP (critical infrastructure protection), 2
- CISWG (Communications and Information Sector Working Group), 2
- close-in attack, 134
- Coast Guard, 148
- code, detecting malicious, 18. *See also* virus protection
- Code of Practice for Information Security Management* (ISO/IEC standard 17799:2005), 110, 111–112
- collision detection
 - Ethernet, 54, 58
 - FEB network, 60
 - token-based, 60
- commercial off-the-shelf (COTS) product, 129, 133
- Common Criteria (CC) profile, 129, 130, 158–159
- Common Industrial Protocol (CIP), 55, 56, 57
- Common Information Model (CIM), 53
- Communications and Information Sector Working Group (CISWG), 2
- Computer Oracle and Password System (COPS), 101
- Concurrent Time Domain Multiple Access (CTDMA), 57
- confidentiality, integrity, availability (CIA), 63, 117–119
- configuration management, 94, 97, 172
- continuity management, 112, 166, 168, 191, 193
- contractor, vetting potential, 140
- control system, distributed, 5
- controller area network (CAN) protocols, 54–55
- Controller asset, 175
- ControlNet International (CI), 55
- ControlNet protocol, 6, 44, 57–58
- COPS (Computer Oracle and Password System), 101
- copyright compliance, monitoring, 112
- corporation, implementing SCADA in culture of SCADA, 124–125, 138
- human resources security
 - awareness of security, fostering, 97, 106–107, 113
 - commitment to SCADA, 131
 - privacy considerations, 124
 - responsibility for security, 95, 106
 - risk, 184
 - STOE management procedure
 - component, 166
 - training, 95, 111, 113, 141, 172
 - vetting potential employee/contractor, 140
- integrating SCADA into corporate system, 37–38
- investment needed, justifying, 123–124, 127
- management support, 123–124
- migration strategy, 191
- operation, day-to-day, 132
- operational phase, 129–130
- planning, 112–113, 127–130, 191

- corporation, (*continued*)
 policy, 94–95, 110, 111, 112, 135
 requirement for system security,
 defining, 128
 technology acquisition program,
 131–132
- COTS (commercial off-the-shelf)
 product, 129, 133
- CPU (central processing unit) log, 105
- crane control SCADA system, 36–37
- Critical Infrastructure Assurance
 Office (CIAO), 2
- Critical Infrastructure Protection, Chal-
 lenges in Securing Control Systems*
 (GAO document 04-140T), 115–116
- critical infrastructure protection
 (CIP), 2
- Cryptographic Protection of SCADA
 Communications General Recommen-
 dations*, Draft 3 (AGA), 143, 144
- cryptography key, 19. *See also*
 encryption
- CSMA/CD (carrier sense multiple
 access with collision detection),
 54, 58
- CSX dispatching and signaling
 system, 75
- CTDMA (Concurrent Time Domain
 Multiple Access), 57
- C37.1-1994, *Definition, Specification,
 and Analysis of Systems Used for
 Supervisory Control, Data Acquisi-
 tion, and Automatic Control* (IEEE), 6
- culture of SCADA, 124–125, 138
- D**
- Dacey, Robert F. (GAO director of
 information security), 115–116
- Data Highway protocols, 6, 44
- data loss/interruption risk, 76
- data unit, MODBUS, 51
- data/slave server, 8, 20
- Davis-Besse nuclear power plant
 attack, 75
- DDoS (distributed-denial-of-service)
 attack, 75, 81, 173, 178
- “Debunking the Threat to Water
 Utilities” (Berinato), 74
- DEC (Digital Equipment Corporation)
 PDP 11 computer, 74
- defense-in-depth strategy, 94, 130–134
- definition of SCADA system, 6–7
- Definition, Specification, and Analysis of
 Systems Used for Supervisory Control,
 Data Acquisition, and Automatic Con-
 trol* (IEEE Standard C37.1-1994), 6
- demilitarized zone (DMZ), 65–66,
 67–68, 90, 102
- Department of Agriculture, 3
- Department of Commerce, 3
- Department of Defense. *See* DoD
- Department of Education, 3
- Department of Energy (DOE), 3,
 126, 150
- Department of Homeland Security
 (DHS), 2, 3, 150
- Department of Housing and Urban
 Development, 3
- Department of Justice, 3
- Department of Labor, 3
- Department of State, 3
- Department of the Interior, 3
- Department of the Treasury, 3
- Department of Transportation, 3, 145
- Department of Veterans Affairs, 3
- deterministic time
 communication in deterministic
 time, 43
 defined, 6
 risk involving, 76, 77, 78
- development cycle of system, risk
 associated with, 186
- device. *See* hardware
- DeviceNet standard, 6, 44, 56
- DF1 protocol, 44
- DHS (Department of Homeland
 Security), 2, 3, 150

- Digital Equipment Corporation (DEC)
 - PDP 11 computer, 74
 - digital signature
 - designing signature system, 128
 - IDS, signature-based, 99
 - log file, protecting using, 105
 - Directive 8500.1, *Information Assurance (IA)* (DoD), 130
 - disabling unused service, 91, 171
 - disaster
 - natural, 178, 185
 - recovery, 95, 97, 168
 - discovery scanning, 101
 - disk capacity log, 105
 - distributed control system, 5
 - distributed-denial-of-service (DDoS)
 - attack, 75, 81, 173, 178
 - distribution attack, 134
 - DMZ (demilitarized zone), 65–66, 67–68, 90, 102
 - DNP3 protocol, 52–53
 - DoD (Department of Defense)
 - Directive 8500.1 (*Information Assurance (IA)*), 130
 - Homeland Security Presidential Directive, responsibility delegated to by, 3
 - information system security approach, 127
 - TCP/IP development, involvement in, 48
 - DoE (Department of Energy), 3, 126, 150
 - drive pump oil field SCADA system, 11, 32
- E**
- EAL (Evaluation Assurance Level), 160
 - EF (exposure factor), 79
 - EIA (Electronic Industries Association)
 - standards
 - 485, 10, 63
 - 422, 47, 48, 50
 - 232, 10, 12, 47, 48, 50
 - 802.1P standard (IEEE), 58
 - 802.2 standard (IEEE), 50
 - Electric Power Research Institute (EPRI), 53, 126
 - electricity distribution security, 30, 75
 - electricity generating plant SCADA system
 - conventional plant
 - coal-fired, 31
 - DNP3 protocol, 52
 - HMI, 15
 - IEC standards, 53–54
 - interdependency, 145
 - local control loop, 15
 - MTU, 15
 - overview of generating process, 30–31
 - physical security, 140
 - PLC, 15, 32
 - RTU, 15, 32
 - UCA protocols, 53
 - vulnerability, 75
 - nuclear plant
 - BWR, 27–28
 - Davis-Besse nuclear power plant
 - attack, 75
 - fuel, spent, 30
 - light water reactor, 27
 - moderator, 27
 - overview of generating process, 26–27
 - PWR, 27, 28–29
 - TMI incident, 29–30
 - electricity outage, security involving, 167, 179
 - electromagnetic interference (EMI), 82
 - Electronic Industries Association standards. *See* EIA standards
 - 11898-1 standard (ISO), 54
 - e-mail
 - control network, on, 83
 - disabling unnecessary e-mail service, 91
 - firewall, blocking at, 69

- e-mail (*continued*)
 - IDS alert, sending via, 100
 - SMTP, 47, 49, 69
 - spam, 64
 - embedded system, 40
 - EMI (electromagnetic interference), 82
 - employee, vetting potential, 140. *See also* human resources security
 - encryption
 - cryptology key, 19
 - designing encryption system, 128
 - gas industry SCADA system, 127, 144
 - IDS considerations, 98
 - log file, protecting using, 105
 - password, 140
 - protocol, vulnerability of clear-text, 171
 - risk involving lack of, 77
 - environmental security, 111
 - EPRI (Electric Power Research Institute), 53, 126
 - Ethernet
 - CAN communication over, 54
 - CIP encoding, 57
 - collision detection, 54, 58
 - Fast Ethernet, 58
 - Gigabit Ethernet, 58
 - IP implementation, 57–59
 - radio, 8
 - TCP/IP implementation, 57
 - UDP implementation, 58
 - Evaluation Assurance Level (EAL), 160
 - export restriction compliance, monitoring, 112
 - exposure factor (EF), 79
- F**
- failure, single point of, 172
 - FAS (Fieldbus Access Sublayer), 61
 - Fast Ethernet, 58
 - fault detection failure, 178
 - FBI (Federal Bureau of Investigation), 2
 - Federal Information Processing Standards Publication (FIPS Pub) 199, *Standards for Security Categorization of Federal Information and Information Systems*, 117–119, 120
 - Federal Transit Administration (FTA) Office of Safety and Security, 145
 - FFB (flexible function block), 59–61
 - Fieldbus Access Sublayer (FAS), 61
 - Fieldbus Message Specification (FMS), 61, 62
 - Fieldbus protocols, 6, 59–63
 - file
 - access attempt log, 105
 - deletion/modification, unauthorized, 174, 176
 - log file, protecting, 105
 - file transfer protocol (FTP), 47, 49, 69
 - FIPS Pub (Federal Information Processing Standards Publication) 199, *Standards for Security Categorization of Federal Information and Information Systems*, 117–119, 120
 - firewall
 - ACL implementation, 64
 - application-layer, 65
 - blocking access based on IDS response, 100
 - delay introduced by, 18
 - DMZ, 65–66, 67–68, 90, 102
 - e-mail, blocking at, 69
 - filtering, 63–64, 140
 - FTP rule, 69
 - HTTP rule, 69
 - IAONA rule guideline, 66
 - implementing, 97
 - inspection, stateful, 65
 - log, 103
 - protocol support, 18, 63, 66, 69
 - proxy, 65
 - SCADA-aware, 63, 97
 - SMTP rule, 69
 - SNMP rule, 69
 - Telnet rule, 69

- TFTP rule, 69
 virus protection using, 63
 flexible function block (FFB), 59–61
 FMS (Fieldbus Message Specification), 61, 62
 Foundation Fieldbus protocol, 6
 485 standard (EIA), 10, 63
 422 standard (EIA), 47, 48, 50
 fractionation petroleum refining process, 24
 FTA (Federal Transit Administration) Office of Safety and Security, 145
 FTP (file transfer protocol), 47, 49, 69
- G**
- GAO (Government Accountability Office) document 04-140T (*Critical Infrastructure Protection, Challenges in Securing Control Systems*), 115–116
 gas industry SCADA system, 127, 142–143, 144
 Gas Technology Institute, 127
Generally Accepted Principles and Practices for Securing Information Technology Systems (NIST Special Publication SP 800-14), 134–135
 Gigabit Ethernet, 58
 GPS (Global Positioning System), 151
Guide for Assessing the Security Controls in Federal Information Systems (NIST Special Publication SP 800-53A), 121–122
Guide for the Security Certification and Accreditation of Federal Information Systems (NIST Special Publication SP 800-37), 119–120
- H**
- hardware
 configuration management, 97, 172
 device audit, technical, 92
 disk capacity log, 105
 life cycle of control system, 135, 140
 security, using built-in, 91, 140
 vulnerability, using hardware platform with known, 77, 78
 hash function, 105
 HDN (hydrodenitrogenation), 25
 HDS (hydrodesulfurization), 25
 HMI (human machine interface)
 described, 7
 electricity generating plant SCADA system, 15
 IT system compared, 125
 petroleum wellhead pump control SCADA system, 11
 STOE, 164, 175
 water purification SCADA system, 14
 water reservoir SCADA system, 13
 Homeland Security Advanced Research Projects Agency (HSARPA), 151
 Homeland Security Council, 2
 Homeland Security Presidential Directives (HSPD), 2–3
 Honeyd honeypot, 85
 Honeynet Project, 85–87
 host-based IDS, 18, 98–99, 103
 hot stand-by system, 7, 20
 Houston Port attack, 75
 HSARPA (Homeland Security Advanced Research Projects Agency), 151
 HSPD (Homeland Security Presidential Directives), 2–3
 HTTP (HyperText Transfer Protocol), 47, 69
 human machine interface. *See* HMI
 human resources security
 awareness of security, fostering, 97, 106–107, 113
 commitment to SCADA, 131
 privacy considerations, 124
 responsibility for security, 95, 106
 risk, 184
 STOE, 166, 170

- human resources security (*continued*)
 - training, 95, 111, 113, 141, 172
 - vetting potential employee/
contractor, 140
- hydrodenitrogenation (HDN), 25
- hydrodesulfurization (HDS), 25
- hydrofluoric acid, 25
- hydrogen, 25, 39
- hydrogen fluoride, 146
- hydrogen sulfide, 25
- hydrotreating petroleum refining
process, 25
- HyperText Transfer Protocol (HTTP),
47, 69
- I**
- IA (*Information Assurance*) (DoD
Directive 8500.1), 130
- The IAONA Handbook for Network
Security-Draft/RFC v0.4* (IAONA), 66
- IATFF (Information Assurance Techni-
cal Framework Forum), 127, 130
- ICMP (Internet control message
protocol), 48, 49
- ICS (industrial control system),
160–161
- Idaho National Engineering and
Environmental Laboratory (INEEL)
Test Bed, 41, 126, 150
- identity repudiation, 177
- IDS (intrusion detection system)
 - action taken upon intrusion, 100–101
 - active-response, 99–100
 - alert, sending, 100
 - analyzing data collected by, 100
 - anomaly-based, 99
 - application-based, 99
 - batch-mode processing, 100
 - described, 97–98
 - encryption considerations, 98
 - entry point, at, 90, 91
 - external, 92
 - host-based, 18, 98–99, 103
 - internal, 92
 - interval-based, 100
 - logging, 100
 - monitoring, 92
 - network-based, 18, 98
 - passive-response, 100
 - protocol support, 18
 - signature-based, 99
- IEC (International Electrotechnical
Commission) standards
 - 1779:2005 (*Code of Practice for Informa-
tion Security Management*), 110,
111–112
 - 60870-5, 53
 - 60870-6, 53
 - 61850, 53–54
 - 61970, 53
 - 61968, 53
 - 61158-2, 63
- IEEE (Institute of Electrical & Elec-
tronics Engineers) standards
 - C37.1-1994 (*Definition, Specification,
and Analysis of Systems Used for
Supervisory Control, Data Acquisi-
tion, and Automatic Control*), 6
 - 802.1P, 58
 - 802.2, 50
 - P1547 series, 41
- impact defined, 79
- impersonation of authorized user,
173, 177
- incident reporting, 77, 107, 112
- independent system operator (ISO), 91
- Industrial Automation Open Net-
working Association (*The IAONA
Handbook for Network Security-Draft/
RFC v0.4*), 66
- industrial control system (ICS),
160–161
- INEEL (Idaho National Engineering
and Environmental Laboratory)
Test Bed, 41, 126, 150
- Information Assurance (IA)* (DoD
Directive 8500.1), 130

- Information Assurance Technical Framework Forum (IATFF), 127, 130
- information disclosure, unauthorized, 176, 186
- information security management system (ISMS), 112–113
- information technology. *See* IT
- information-system security engineering (ISSE), 127–130
- Institute of Electrical & Electronics Engineers standards. *See* IEEE standards
- Instrumentation, Systems, and Automation Society. *See* ISA
- Integrating Electronic Security into the Manufacturing and Control System Environment* (ISA report TR99.00.02-2004), 41, 114–115
- International Electrotechnical Commission standards. *See* IEC standards
- International Organization for Standardization standards. *See* ISO standards
- Internet
- connection vulnerability, 139
 - disabling unnecessary Internet access, 91
 - risk associated with Internet access, 187
- Internet control message protocol (ICMP), 48, 49
- interval-based IDS, 100
- intrusion detection system. *See* IDS
- investment needed, justifying, 123–124, 127
- IP (Internet protocol), 48, 49, 57–59, 82. *See also* TCP/IP (transmission control protocol/Internet protocol)
- ISA (Instrumentation, Systems, and Automation Society)
- reports
 - S50.02-1992, 61
 - TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*, 41, 113–114
 - TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control System Environment*, 41, 114–115
 - research done by, 126
- ISMS (information security management system), 112–113
- ISO (independent system operator), 91
- ISO (International Organization for Standardization) standards
- 11898-1, 54
 - 9506-1:2000, 53
 - 9506-2:2000, 53
 - 15408, 160
 - 1779:2005 (*Code of Practice for Information Security Management*), 110, 111–112
- ISSE (information-system security engineering), 127–130
- IT (information technology)
- convergence, 16–17
 - HMI, 125
 - process control security assignment to IT department, 139
 - risk, SCADA versus IT system, 74, 76–77
- J**
- JPEG (Joint Photographic Experts Group) standard, 47
- K**
- key, cryptography, 19
- L**
- LAS (link active scheduler), 61
- life cycle of control system, 135, 140
- Linux/Unix system, auditing, 102
- log
- audit, 17, 102–105
 - checksum, applying to, 105

log (*continued*)

- CPU, 105
- disk capacity, 105
- file access attempt, 105
- firewall, 103
- IDS, 100
- memory consumption, 105
- monitoring, 17
- process initiation, 105
- protecting log file, 105
- resource utilization, 105
- system shutdown, 105

Los Alamos National Laboratory, 126

M

- MAC (media access control), 46
- malicious code detection, 18. *See also* virus protection
- Manchester biphase signal
 - encoding, 61
- Manufacturing Message Specification (MMS), 53
- Maritime Transportation Security Act of 2002 (MTSA 2002), 148
- Maroochy Shire sewage control system attack, 75
- Massachusetts Water Resource Authority (MWRA), 74
- master control station, 52, 83, 84
- master terminal unit. *See* MTU
- media access control (MAC), 46
- memory consumption log, 105
- meter reading, disabling automated, 91
- methane, 39
- MMS (Manufacturing Message Specification), 53
- MODBUS protocols, 6, 44, 50–51, 104
- modem, vulnerability of dial-up, 82, 92
- Modicon protocols, 44, 50–51
- MPEG (Motion Pictures Experts Group) standard, 47
- MTSA 2002 (Maritime Transportation Security Act of 2002), 148

MTU (master terminal unit)

- described, 7
- petroleum wellhead pump control
 - SCADA system, 11
 - water reservoir SCADA system, 13
- MWRA (Massachusetts Water Resource Authority), 74
- Myth of Obscurity, 75

N

- National Infrastructure Advisory Council (NIAC), 2
- National Infrastructure Protection Center (NIPC), 2
- National Infrastructure Simulation and Analysis Center, 126
- National Institute of Standards and Technology. *See* NIST
- National SCADA Test Bed (NSTB), 41, 126, 150
- National Science Foundation (NSF) Workshop on Critical Infrastructure Protection for SCADA & IT, 74–75
- NERC (North American Electric Reliability Council), 20–21
- Nessus software, 102
- network
 - auditing network security, 92
 - configuration management, 94
 - connection vulnerability, 77, 78, 90–91, 92
 - documenting network architecture, 93
 - e-mail on control network, 83
 - IDS, network-based, 18, 98
 - port
 - blocking access based on IDS response, 100
 - scanning, 101, 102
 - protection strategy, developing, 94
 - remote access vulnerability, 171
 - risk associated with network communication, 186–187
 - STOE network connectivity assumption, 169

- network update time (NUT), 57
- NFS (network file system), 47
- NIAC (National Infrastructure Advisory Council), 2
- 9506-1:2000 standard (ISO), 53
- 9506-2:2000 standard (ISO), 53
- NIPC (National Infrastructure Protection Center), 2
- NIST (National Institute of Standards and Technology)
 - PCSRF, 126, 130, 160
 - SP 800-53 (*Recommended Security Controls for Federal Information Systems*), 120–121, 170
 - SP 800-53A (*Guide for Assessing the Security Controls in Federal Information Systems*), 121–122
 - SP 800-14 (*Generally Accepted Principles and Practices for Securing Information Technology Systems*), 134–135
 - SP 800-37 (*Guide for the Security Certification and Accreditation of Federal Information Systems*), 119–120
 - SP 800-26 (*Security Self-Assessment Guide for Information Technology Systems*), 136–137
 - SPP ICS (*System Protection Profile for Industrial Control Systems*)
 - access control, 167, 192
 - asset protection list, 175–176
 - attack type list, 172–174, 176–179
 - auditing, 167, 193
 - authentication, 164, 165, 166, 191
 - availability, 167
 - backup, 167, 191
 - boundary protection, 165, 167, 190
 - CC profile, use of, 129, 130, 158
 - continuity management, 166, 168, 191, 193
 - EAL targeted, 160
 - feature overview, STOE, 166–168
 - formatting convention, 158–159
 - generic ICS, 163
 - HMI, 164, 175
 - human resources security, 166, 170
 - integrity, 166
 - ISO 15408 standard, extends, 160
 - management procedure component, STOE, 166
 - migration strategy, 191
 - monitoring, 167, 193
 - need for, 162
 - network connectivity assumption, 169
 - notation convention, 158–159
 - objective list, 190–193
 - PCSRF, relation to, 160
 - physical security, 165, 167, 169, 179, 190
 - policy, 167–168, 172, 180–181
 - power outage, 167, 179
 - remote access, 167, 169, 171, 175, 192
 - risk list, 181–190
 - scope, 117, 164–165
 - self verification, 167
 - terminology used, 158
 - threat agent characterization, 170
 - training, 172
 - virus protection, STOE, 173, 179
 - vulnerability list, 171–172
- NMap software, 102
- North American Electric Reliability Council (NERC), 20–21
- NRC (Nuclear Regulatory Commission), 29
- NSF (National Science Foundation)
 - Workshop on Critical Infrastructure Protection for SCADA & IT, 74–75
- NSTB (National SCADA Test Bed), 41, 126, 150
- nuclear power plant SCADA system
 - BWR, 27–28
 - Davis-Besse nuclear power plant
 - attack, 75
 - fuel, spent, 30
 - light water reactor, 27

nuclear power plant SCADA system,
(*continued*)
 moderator, 27
 overview of generating process,
 26–27
 PWR, 27, 28–29
 TMI incident, 29–30
Nuclear Regulatory Commission
(NRC), 29
NUT (network update time), 57

O

Obscurity, Myth of, 75
ODVA (Open DeviceNet Vendor
 Association), 55
OECD (Organization for Economic
 Cooperation and Development),
 134
Office of Energy Assurance (DOE),
 126
oil pipeline SCADA system, 142–143
oil refining SCADA system, 23–25,
 142, 144
oil wellhead pump control SCADA
 system, 11, 32
15408 standard (ISO), 160
Open DeviceNet Vendor Association
(ODVA), 55
open systems interconnection (OSI)
 model, 44–48
operator error causing security breach,
 173
Organization for Economic Coopera-
 tion and Development (OECD), 134
organization, implementing
 SCADA in
 culture of SCADA, 124–125, 138
 human resources security
 awareness of security, fostering,
 97, 106–107, 113
 commitment to SCADA, 131
 privacy considerations, 124
 responsibility for security, 95, 106
 risk, 184

 STOE management procedure
 component, 166
 training, 95, 111, 113, 141, 172
 vetting potential employee/
 contractor, 140
integrating SCADA into corporate
 system, 37–38
investment needed, justifying,
 123–124, 127
management support, 123–124
migration strategy, 191
operation, day-to-day, 132
operational phase, 129–130
planning, 112–113, 127–130, 191
policy, 94–95, 110, 111, 112, 135
requirement for system security,
 defining, 128
technology acquisition program,
 131–132
OSI (open systems interconnection)
 model, 44–48
outstation, 52

P

PA (Profibus Process Automation), 61
Partnership for Critical Infrastructure
 Security (PCIS), 2
passive-response IDS, 100
password
 authentication, two-factor, 18
 challenge-response token, 18
 COPS, 101
 encryption, 140
 lockout on incorrect, 18
 master control station, obtaining
 from, 83, 84
 personnel, divulgence by, 95
 sharing, 140
 supervisor-level, 18
Patriot Act, 2
PCCIP (President's Commission on
 Critical Infrastructure Protection)
 Executive Order establishing, 1
 *21 Steps to Improve Cyber Security of
 SCADA Networks*, 90–96

- PCIB (President's Critical Infrastructure Board), 2
- PCIS (Partnership for Critical Infrastructure Security), 2
- PCSRF (Process Control Security Requirements Forum), 126, 130, 160
- PDD (Presidential Decision Directive) 63, 2
- PDP 11 computer, 74
- performance, evaluating, 94–95
- personnel security
- awareness of security, fostering, 97, 106–107, 113
 - commitment to SCADA, 131
 - privacy considerations, 124
 - responsibility for security, 95, 106
 - risk, 184
 - STOE, 166, 170
 - training, 95, 111, 113, 141, 172
 - vetting potential employee/contractor, 140
- petroleum refining SCADA system, 23–25, 142, 144
- P1547 standard series (IEEE), 41
- phone line, vulnerability of using leased, 83
- physical security
- assessing, 92
 - described, 111
 - electricity generating plant, 140
 - risk, 185
 - STOE, 165, 167, 169, 179, 190
 - water purification SCADA system, 140
- PID (proportional, integral, derivative) control, 7
- PING utility, 48, 49
- Pipeline SCADA Security*, First Edition (API Standard 1164), 142–143
- PLAN-DO-CHECK-ACT cycle, 112–113
- planning SCADA system, 112–113, 127–130, 191
- PLC (programmable logic controller)
- attacker privilege goal, 83, 84
 - electricity generating plant SCADA system, 15, 32
 - petroleum wellhead pump control SCADA system, 11
 - relay ladder logic, 5
 - water purification SCADA system, 14
 - water reservoir SCADA system, 13
- point of failure, single, 172
- point-to-point protocol (PPP), 48, 50
- policy
- compliance, monitoring, 112
 - developing, 94–95, 110, 111, 112, 135
 - risk, 183
 - STOE, 167–168, 172, 180–181
- port, network
- blocking access based on IDS response, 100
 - scanning, 101, 102
- port security (shipping), 75, 146–151
- power outage, security involving, 167, 179
- PPP (point-to-point protocol), 48, 50
- Presidential Decision Directive (PDD) 63, 2
- Presidential Executive Orders, 1, 2
- President's Commission on Critical Infrastructure Protection.
See PCCIP
- President's Critical Infrastructure Board (PCIB), 2
- pressurized water reactor (PWR), 27, 28–29
- privacy considerations, 124
- privilege
- attack goal, 83–84
 - elevation, unauthorized, 178
- Process Control Security Requirements Forum (PCSRF), 126, 130, 160
- Profibus Process Automation (PA), 61
- Profibus (Process Fieldbus) protocol, 6, 44, 61–63

programmable logic controller.
 See PLC

proportional, integral, derivative (PID) control, 7

protocol vulnerability
 clear-text, 171
 proprietary, 91

push architecture, 125

PWR (pressurized water reactor), 27, 28–29

R

radio, Ethernet, 8

Radio Frequency Identification (RFID), 151

radio frequency interference (RFI), 82

rail industry SCADA system, 145–146

RAPS (Remote Access Perimeter Scanner), 102

real-time operating system (RTOS), 7

Recommended Security Controls for Federal Information Systems (NIST Special Publication SP 800-53), 120–121, 170

Red Team expert group, 93

redundancy security component, 20

relay ladder logic, 5

reliability, 20–21

remote access
 diagnosis, 175
 risk, 187
 STOE, 167, 169, 171, 175, 192
 vulnerability, 171

Remote Access Perimeter Scanner (RAPS), 102

remote procedure call (RPC), 47

Remote Terminal Unit. *See* RTU

reporting security incident, 77, 107, 112

requirement for system security,
 defining, 128

resource utilization log, 105

responsibility for security, 95, 106

RFI (radio frequency interference), 82

RFID (Radio Frequency Identification), 151

risk. *See also* vulnerability
 ALE calculation, 79
 assessing, 79–80, 93–95, 112, 172, 190
 asset management, associated with, 184
 assumption, 81
 auditing, associated with, 189
 avoidance, 81
 change to system, associated with, 188
 continuity of access, associated with, 189
 data loss/interruption, 76
 defined, 79
 development cycle of system, associated with, 186
 disaster, natural, 185
 encryption, from lack of, 77
 human resources security, 184
 information disclosure, unauthorized, 186
 Internet access, 187
 IT versus SCADA system, 74, 76–77
 managing, 78–80, 93–94, 183
 mitigating, 80–81
 Myth of Obscurity, 75
 network communication, 186–187
 operating environment, to external, 190
 penetration testing, 77, 90
 physical security, 185
 policy, 183
 remote access, 187
 residual, 80
 STOE risk listing, 181–190
 time, risk involving deterministic, 76, 77, 78
 transference, 81
 virus protection, delay caused by, 76

Rockwell Allen Bradley protocols, 6, 44

role-based security, 19, 93

- RPC (remote procedure call), 47
- RTOS (real-time operating system), 7
- RTU (Remote Terminal Unit)
- attacker privilege goal, 83, 84
 - described, 7
 - electricity generating plant SCADA system, 15, 32
 - embedded system, 40
 - petroleum wellhead pump control SCADA system, 11
 - push architecture, 125
 - water purification SCADA system, 14
 - water reservoir SCADA system, 13
- S**
- safeguard defined, 79
- Salt River Project attack, 75
- Sandia National Laboratories, 41, 126
- SATAN (System Administrator Tool for Analyzing Networks), 101
- SC (security category) calculation, 117–119
- seaport security, 75, 146–151
- secure sockets layer (SSL), 69
- Security Self-Assessment Guide for Information Technology Systems* (NIST Special Publication SP 800-26), 136–137
- Security Technologies for Manufacturing and Control Systems* (ISA report TR99.00.01-2004), 41, 113–114
- self assessment
- NIST self-assessment guide, 136–137
 - physical security, 92
 - risk, 79–80, 93–95, 112, 172, 190
 - vulnerability, 80, 90, 93, 100–102
- Sensor asset, 175
- server
- audit log, 103
 - data/slave, 8, 20
 - vulnerability scanning, 101
- service
- disabling unused, 91, 171
 - vulnerability scan, detecting running service during, 101
 - 1779:2005 standard, *Code of Practice for Information Security Management* (ISO/IEC), 110, 111–112
 - sewage control SCADA system
 - vulnerability, 75 - S50.02-1992 report (ISA), 61
 - Siemens protocols, 44
 - signature, digital
 - designing signature system, 128
 - IDS, signature-based, 99
 - log file, protecting using, 105 - Simple Mail Transport Protocol (SMTP), 47, 49, 69
 - Simple Network Management Protocol (SNMP), 47, 49, 69, 82
 - Single Loss Expectancy (SLE), 79
 - single point of failure, 172
 - 60870-5 standard (IEC), 53
 - 60870-6 standard (IEC), 53
 - 61850 standard (IEC), 53–54
 - 61970 standard (IEC), 53
 - 61968 standard (IEC), 53
 - 61158-2 standard (IEC), 63
 - Slammer worm, 75
 - slave/data server, 8, 20
 - SLE (Single Loss Expectancy), 79
 - SMTP (Simple Mail Transport Protocol), 47, 49, 69
 - SNMP (Simple Network Management Protocol), 47, 49, 69, 82
 - Sobig virus, 75
 - social engineering, 95, 173
 - software
 - configuration management, 97, 172
 - detecting unauthorized, 101
 - distribution attack, 134
 - IDS, application-based, 99
 - Nessus, 102
 - NMap, 102
 - patching, 77, 82, 97
 - vulnerability, using software with known, 77, 78 - SP 800-53, *Recommended Security Controls for Federal Information Systems* (NIST), 120–121, 170

- SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (NIST), 121–122
- SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems* (NIST), 134–135
- SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* (NIST), 119–120
- SP 800-26, *Security Self-Assessment Guide for Information Technology Systems* (NIST), 136–137
- spam, 64
- Specification for Information Security Management Systems* (BS for Information Security Management standard 7799-2:2002), 110, 112–113
- spoofing authorized user, 173, 177
- SPP ICS (*System Protection Profile for Industrial Control Systems*) (NIST)
 - CC profile, use of, 129, 130, 158
 - EAL targeted, 160
 - formatting convention, 158–159
 - generic ICS, 163
 - ISO 15408 standard, extends, 160
 - need for, 162
 - notation convention, 158–159
 - PCSRF, relation to, 160
- STOE
 - access control, 167, 192
 - asset protection list, 175–176
 - attack type list, 172–174, 176–179
 - auditing, 167, 193
 - authentication, 164, 165, 166, 191
 - availability, 167
 - backup, 167, 191
 - boundary protection, 165, 167, 190
 - continuity management, 166, 168, 191, 193
 - feature overview, 166–168
 - HMI, 164, 175
 - human resources security, 166, 170
 - integrity, 166
 - management procedure component, 166
 - migration strategy, 191
 - monitoring, 167, 193
 - network connectivity assumption, 169
 - objective list, 190–193
 - physical security, 165, 167, 169, 179, 190
 - policy, 167–168, 172, 180–181
 - power outage, 167, 179
 - remote access, 167, 169, 171, 175, 192
 - risk list, 181–190
 - scope, 117, 164–165
 - self verification, 167
 - threat agent characterization, 170
 - training, 172
 - virus protection, 173, 179
 - vulnerability list, 171–172
- terminology used, 158
- SSL (secure sockets layer), 69
- Standards for Security Categorization of Federal Information and Information Systems* (FIPS Pub 199), 117–119, 120
- stand-by system, hot, 7, 20
- STOE (System Target of Evaluation)
 - access control, 167, 192
 - asset protection list, 175–176
 - attack type list, 172–174, 176–179
 - auditing, 167, 193
 - authentication, 164, 165, 166, 191
 - availability, 167
 - backup, 167, 191
 - boundary protection, 165, 167, 190
 - continuity management, 166, 168, 191, 193
 - feature overview, 166–168
 - HMI, 164, 175
 - human resources security, 166, 170
 - integrity, 166
 - management procedure component, 166
 - migration strategy, 191
 - monitoring, 167, 193
 - network connectivity assumption, 169
 - objective list, 190–193

physical security, 165, 167, 169, 179, 190
 policy, 167–168, 172, 180–181
 power outage, 167, 179
 remote access, 167, 169, 171, 175, 192
 risk list, 181–190
 scope, 164–165
 self verification, 167
 threat agent characterization, 170
 training, 172
 vulnerability list, 171–172
 strontium, 27
 sulfuric acid, 25
 System Administrator Tool for Analyzing Networks (SATAN), 101
 system architecture overview, 7–9
 system, embedded, 40
System Protection Profile for Industrial Control Systems (NIST). *See* SPP ICS (NIST)
 system shutdown log, 105
 System Target of Evaluation. *See* STOE

T

TCP/IP (transmission control protocol/Internet protocol)
 DoD, role in developing, 48
 Ethernet TCP/IP implementation, 57
 Honeyd TCP/IP simulation, 86, 87
 OSI model, 48–49
 protocols, associated, 49–50
 Tcpview software, 102
 technology acquisition program, 131–132
 telephone line, vulnerability of using leased, 83
 testing, 77, 90, 129–130, 172
 Texas City refinery explosions, 26
 TFTP (Trivial File Transfer Protocol), 69
 threat
 defined, 79
 overview of common threats, 81–82
 Three Mile Island (TMI) incident, 29–30

time, deterministic
 communication in deterministic time, 43
 defined, 6
 risk involving, 76, 77, 78
 timeline of critical infrastructure protection activity, 4
 TMI (Three Mile Island) incident, 29–30
 toluene, 38–39
 traffic analysis, unauthorized, 173, 176
 training, 95, 111, 113, 141, 172
 Transmission Control Protocol (TCP), 47, 49, 57, 82
 transmission control protocol/Internet protocol. *See* TCP/IP
 Trivial File Transfer Protocol (TFTP), 69
 TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems* (ISA), 41, 113–114
 TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control System Environment* (ISA), 41, 114–115
 “The Truth About Cyber Terrorism” (Berinato), 74
 tunnel, VPN, 69
 21 *Steps to Improve Cyber Security of SCADA Networks* (PCCIP), 90–96
 232 standard (EIA), 10, 12, 47, 48, 50

U

UCA (Utility Communications Architecture) protocols, 53
 UDP (user datagram protocol), 47, 49, 57, 58, 82
 Unix/Linux system, auditing, 102
 Uranium 235 (U-235), 27

V

virus protection
 delay caused by, 76
 firewall, using, 63
 IT versus SCADA system, 76
 Sobig virus, 75
 STOE, 173, 179
 updating virus database, 18

VPN (virtual private network),
69–70, 82

vulnerability. *See also* risk
analyzing data concerning, 100–102
assessing, 80, 90, 93, 100–102
defined, 79
electricity distribution, 75
electricity generating plant SCADA
system, 75
hardware platform with known
vulnerability, using, 77, 78
Internet connection, 139
IP, 82
IT versus SCADA system, 74, 76–77
modem, dial-up, 82, 92
Myth of Obscurity, 75
network connection, 77, 78, 90–91, 92
protocol
clear-text, 171
proprietary, 91
remote access, 171
scanning, 100–102
sewage control SCADA system, 75
SNMP, 82
software with known vulnerability,
using, 77, 78
STOE vulnerability listing, 171–172
TCP port, 82

telephone line, leased, 83
UDP port, 82
water purification SCADA system,
36, 74

W

war dialing, 92
war driving, 82, 92
water purification SCADA system
DNP3 protocol, 52
functions controlled by, 34
HMI, 14
interdependency, 145
maintenance, deferred, 140
MTU, 14
MWRA, 74
physical security, 140
PLC, 14
RTU, 14
vulnerability, 36, 74
water reservoir SCADA system, 13
Workshop on Critical Infrastructure
Protection for SCADA & IT, 74–75
workstation vulnerability scanning,
101

X

xenon, 27

