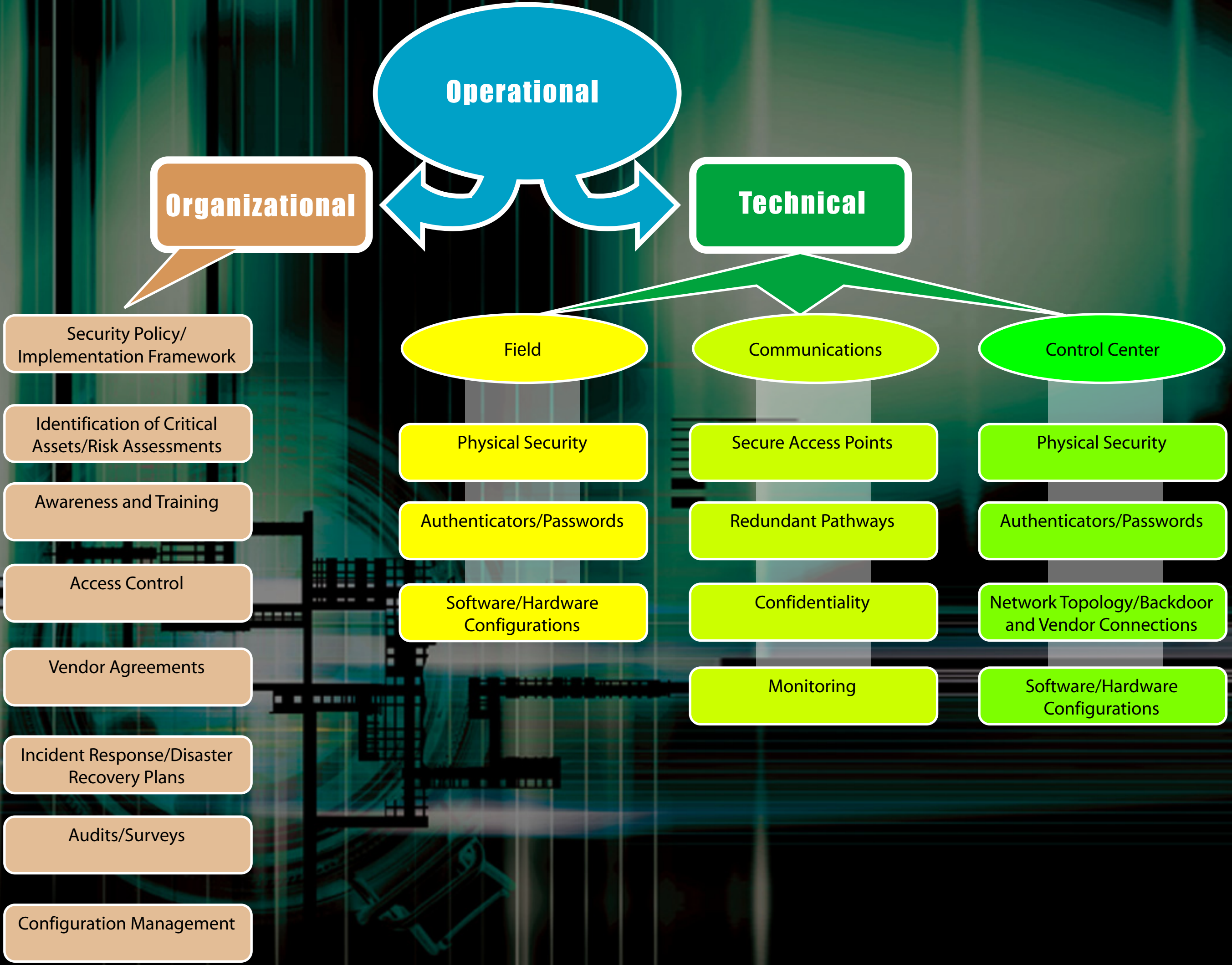
NSTB
National SCADA Test Bed
enhancing control systems security in the energy sector

Metrics Taxonomy



Operational

Organizational

- Security Policy/ Implementation Framework
- Identification of Critical Assets/Risk Assessments
- Awareness and Training
- Access Control
- Vendor Agreements
- Incident Response/Disaster Recovery Plans
- Audits/Surveys
- Configuration Management

Technical

Field

- Physical Security
- Authenticators/Passwords
- Software/Hardware Configurations

Communications

- Secure Access Points
- Redundant Pathways
- Confidentiality
- Monitoring

Control Center

- Physical Security
- Authenticators/Passwords
- Network Topology/Backdoor and Vendor Connections
- Software/Hardware Configurations

Sandia National Laboratories

Security Policy/Implementation Framework

- Is there (i) a formal, documented, control systems security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls? (RRCSS 2.1, CIP-003)

- Is there a management framework to initiate and control the implementation of an overall security program? Is there a framework with management leadership to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization? (RRCSS 2.2)

Identification of Critical Assets/ Risk Assessments

- Is there a risk management plan that includes (i) the identification of risks for all assets in the control system; (ii) the classification of each risk depending upon its impact on the system; (iii) the mitigation of risks and necessary controls over risks; and (iv) the resolution of administrative controls necessary when technical controls are not possible? (RRCSS 2.18.1, CIP-002)

- Are risk assessments of the control system and facilities performed to identify and document the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of the control systems and/or control system information and processes? (RRCSS 2.18.7)

METRICS TAXONOMY

Awareness and Training

- Are risk designations assigned to all positions? Are there screening criteria for individuals filling those positions? Are position risk designations reviewed and revised periodically or as deemed necessary based on organizational changes in policy? (RRCSS 2.3.1, CIP-004)

- Are employees and contractors provided with complete job descriptions and details of conduct, duties, terms and conditions of employment, legal rights, and responsibilities? (RRCSS 2.3.8)

- Are all users (including managers, senior executives, and third party business partner users) familiar to basic physical, information, and control systems security awareness materials before being granted authorized access to a control system? (RRCSS 2.11.1)

- Are personnel with significant control system security roles and responsibilities appropriately trained before being granted authorized access to the system, with periodic training thereafter? (RRCSS 2.11.2)

- Are personnel tested on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the control system? (RRCSS 2.11.5)

Metrics Taxonomy

Access Control

- Are there lists of personnel with authorized access to facilities containing control systems, except for those areas within the facilities officially designated as publicly accessible, and are appropriate authorization credentials (e.g., badges, identification cards, smart cards) issued? (RRCSS 2.4.2, CIP-004)

- Is access to the control system based on (i) a valid need-to-know basis that is determined by assigned official duties and that satisfies all personnel security criteria and (ii) intended system use? (RRCSS 2.15.1)

- Are user identifiers managed by (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user identifier from an appropriate organization official, (iv) ensuring that the user identifier is issued to the intended party, (v) disabling user identifier after a pre-determined defined time period of inactivity, and (vi) archiving user identifiers? (RRCSS 2.15.2)

- Are access authorizations terminated/reviewed when an employee is terminated, resigns, or is transferred? (RRCSS 2.3.3--2.3.4)

- Are appropriate access agreements completed for individuals (including third parties and contractors) before authorizing access? (RRCSS 2.3.5)

Vendor Agreements

- Have security requirements for third-party providers been established and is service provider compliance monitored to ensure adequate security? (RRCSS 2.3.6, 2.5.8)

- Are security requirements and/or security specifications, either explicitly or by reference, in control system acquisition contracts? (RRCSS 2.5.3)

Incident Response/Disaster Recovery Plans

- Are there security plans that define the roles and responsibilities of various employees and contractors in the event of a significant incident? (RRCSS 2.7.4, CIP-008, CIP-009)

- Is there an incident recovery and business continuity plan dealing with the overall issue of maintaining or reestablishing production in the event of an undesirable interruption for a control system? (RRCSS 2.12.1)

- Are personnel trained in their incident response and business continuity plan roles and responsibilities with respect to the control system? (RRCSS 2.12.3)

- Are the plans tested to determine the effectiveness and are results documented? (RRCSS 2.12.4)

Metrics Taxonomy

Audits/Surveys

- Are audits conducted at planned intervals to determine whether the control objectives, controls, processes, and procedures (i) conform to the requirements and relevant legislation or regulations, (ii) conform to the identified information security requirements, (iii) are effectively implemented and maintained, (iv) perform as expected, and (v) identify inappropriate activities? (RRCSS 2.16.10, CIP-005)

- Is there a robust audit mechanism in the control system to capture sufficient and detailed information in audit records to establish what events occurred, the sources of the events, and their outcomes? (RRCSS 2.16.2)

Configuration Management

- Is there a formal, documented Configuration Management policy that addresses purpose, scope, roles, responsibilities, and compliance? Are there formal, documented procedures to facilitate the implementation of the physical security policy? Is it clear who is allowed to make changes, under what conditions are changes allowed, and what approvals are required for changes?
(RRCSS 2.6.1, CIP-003)

- Is there a current, baseline configuration of the control system and an inventory of the system's constituent components? (RRCSS 2.6.2)

- Are security impact analyses performed to determine the effects of changes to the control system? (RRCSS 2.6.4)

METRICS TAXONOMY

Physical Security

- Are all physical access points (including designated entry/exit points) to facilities containing control system devices (except those areas within the facilities officially designated as publicly accessible) controlled? Are individual access authorizations verified before access is granted? Are publicly accessible areas controlled, as appropriate, in accordance with an assessment of risk? (RRCSS 2.4.3, CIP-006)

- Are physical access logs (including visitor logs) to control system facilities monitored and reviewed? (RRCSS 2.4.6, 2.4.8)

Metrics Taxonomy

Authenticators/Passwords

- Are system authenticators managed by (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution for lost, compromised, or damaged authenticators and for revoking authenticators; and (iii) changing default authenticators upon information system installation?

- For password-based authentication, does the information system (i) protect passwords from unauthorized disclosure and modification when stored and transmitted; (ii) prohibit passwords from being displayed when entered; (iii) enforce password minimum and maximum lifetime restrictions; and (iv) prohibits password reuse for a specified number of generations? For PKI-based authentication, does the information system (i) validate certificates by constructing a certification path to an accepted trust anchor; (ii) establish user control of the corresponding private key; and (iii) map the authenticated identity to the user account? (RRCSS 2.15.3, CIP-007)

- Are users authenticated prior to control system access? (RRCSS 2.15.8)

- Are there policies and procedures concerning the generation and use of passwords? Do they stipulate rules of complexity, based on the criticality level of the systems to be accessed? (RRCSS 2.15.14)

Software/Hardware Configurations

1 of 2

- Is the control system configured to provide only essential capabilities and specifically to prohibit and/or restrict the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list? (RRCSS 2.6.7, CIP-007, NIST 6.2.6)

- Is there a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all electronic assets within the electronic security perimeter(s)? Are patches and updates for devices and hosts validated by technically competent control system operations personnel and tested on a production-like test system before being applied to the production system? Is guidance for patch installation provided with assurance that no new flaws are introduced as a result of the corrections? (RRCSS 2.6.10—2.6.12)

- Are all factory default authentication credentials changed after installation? (RRCSS 2.6.14)

METRICS TAXONOMY

Software/Hardware Configurations

2 of 2

- Are malicious code protection mechanisms employed at critical control system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network? (RRCSS 2.14.2)

- Are integrity verification applications employed on the control system to provide monitoring, detection, and protection against unauthorized changes to software and information? (RRCSS 2.14.6)

Secure Access Points

- Is there a prohibition against the use of unapproved networks and portable media use and/or integration with the control system? Are measures in place to ensure that devices cannot be connected to external unrestricted networks via physical connections or wireless access points? (RRCSS 2.4.19, CIP-005)

- Are there (i) use restrictions and implementation guidance for wireless technologies (microwave, satellite, packet radio [UHF/VHF], 802.11x, Bluetooth, and other forms of wireless communications) and (ii) documentation, monitoring, logging, and control of wireless access to the control system? (RRCSS 2.15.24)

METRICS TAXONOMY

Redundant Pathways

- Are there alternate telecommunications services to support the control system? Are there agreements to permit the resumption of system operations for critical mission/business functions when the primary telecommunications capabilities are unavailable? (RRCSS 2.12.14)

Metrics Taxonomy

Confidentiality

- Is physical access controlled to system communication media carrying unencrypted or plain text information to prevent eavesdropping, in-transit modification, disruption, or physical tampering? (RRCSS 2.4.4)

- Does the control system detect modification, deletion, insertion, and/or replay errors of the user data in transit between trusted systems?

- Is communication of private information over the Internet encrypted with a secure socket layer or (if non-web) with encryption of equivalent or better strength?

- Are network connections terminated at the end of a session or after a period of inactivity per policy and procedures?

- Is there a policy on the use of cryptographic controls for protection of information? When cryptography is employed within the control system, does the system perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation? (RRCSS 2.8.8—2.8.13, CIP-007)

Monitoring

- Are tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools) employed to monitor security events and system activities on the control system, detect attacks, and provide identification of unauthorized use of the system? (RRCSS 2.14.3, CIP-007)

Metrics Taxonomy

Network Topology

- Is the operational system boundary, the strength required for the boundary, and the respective barriers to unauthorized access and control of system assets and components defined? Does the control system monitor and control communications at the operational system boundary and at key internal boundaries within the system? (RRCSS 2.8.7, CIP-005, NIST 5.1–5.11)
- Are all external control system and communication connections identified and adequately protected from tampering or damage? (RRCSS 2.8.25)
- Is there a mechanism in the control system network to identify and authenticate specific devices before establishing a connection? (RRCSS 2.15.10)
- Are there security measures to address and protect against the risks of remote access to the control system, field devices, and communication facilities? (RRCSS 2.15.21—2.15.22)
- Are security functions isolated from non-security functions by means of partitions, domains, etc., including control of access to and integrity of the hardware, software, and firmware that perform those functions? (RRCSS 2.8.3)
- Is the integrity of the control system protected by preventing integration, whether intentional or unintentional, of the control system with the enterprise network and/or business systems? (RRCSS 2.14.7)