Webinar Sponsor

Michael McClellan, Jr.
Levine Lectronics and Lectric, Inc.
200 Powers Ferry Road
Marietta, GA. 30067
Phone: 770 565-1556 FAX: 770 973-9264
Cell: 770-500-9216
E-mail: McClellan@L-3.com
Web: http://www.L-3.com/

CONTROLINFOTECH

Cyber Security Analytics for Power & Control Operations

Tony Leszczynski
Business Development Manager
Control Infotech, Inc.
106, Kitty Hawk Drive
Morrisville NC 27560,
USA
O: (919) 544-3131
C: (984) 227-4121

CONTROLINFOTECH
www.control-infotech.com

Cyber Security Subject Matter Expert

SAM ANALYTIC SOLUTIONS

Balakrishna Subramoney

Lead Analyst - Cybersecurity
SAM Analytic Solutions
p: 919.800.0044, m: 919.525.8559
f: 919.297.8742
a: 2511 E NC Highway 54, Durham NC 27713
w: www.samanalyticsolutions.com e: balu@samanalytic.com

What is the role of a systems integrator?

https://www.control-infotech.com/index.html

- Case 1 - Cybersecurity and NERC-CIP Compliance Testing

We help organizations identify points of departure from standards and develop strategies to address the gaps in meeting the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.

- **Consider our IT Infrastructure Services**
  - Control Infotech provides Networking (wired and wireless) and server setup and virtualization services.
  - We have developed, delivered and managed on-premise and cloud-based systems and security services.
  - We feature Siemens' world-leading networking gear, switches, routers, industrial PCs and Power Supplies
  - We collaboratively work with users to tailor our systems to the users and EPC's cyber specifications

- **Work with our subject matter experts to specify Cyber Security Services over the life of your operations.**
  - We offer customized solutions for securing OT (Operations Technology) infrastructure.
    - Security Awareness Workshops
    - Cyber Asset Data collection and Analyses,
    - Security Information and Event Management (SIEM) solutions
    - Cyber Security Threat Vulnerability and Risk Assessment
  - Not only do we
    - Develop APIs for specific customer requirements and;.
    - Install and commission computer operating systems and runtime applications
  - We also manage the Security Operations Center (SOC) at the facility
    - We provide the sensor(s) and services to supervise your network traffic
    - Our Cyber SOC platform helps bring state-of-the-art security operations to your organization

The role of Cyber Security Analyst is to assist organizations at all levels in the development and testing of Cybersecurity prevention, protection, mitigation, and response capabilities

Cyber Security – Solutions & Services

The goal of the Cybersecurity Practice at Sam Analytic is to assist organizations at all levels in the development and testing of Cybersecurity prevention, protection, mitigation, and response capabilities* (*Adapted from https://www.cisa.gov/cybersecurity-training-exercises)

- **Developing Information Security standards and guidelines for Operations**
- **Implementing Cybersecurity Event and Incident management solutions**
- **Compliance Management Services**
- **Vulnerability Assessment**
- **Penetration Testing**
- **Security Awareness and Training**
- **Cybersecurity Threat Assessment Program**
- **Automating daily Cybersecurity Tasks**
  - **– data collection and analyses**
  - **– timely reporting of events and incidents**
  - **– ETL of log data, etc.**

Please refer to the handout detailing solutions provided.

Services Catalogue

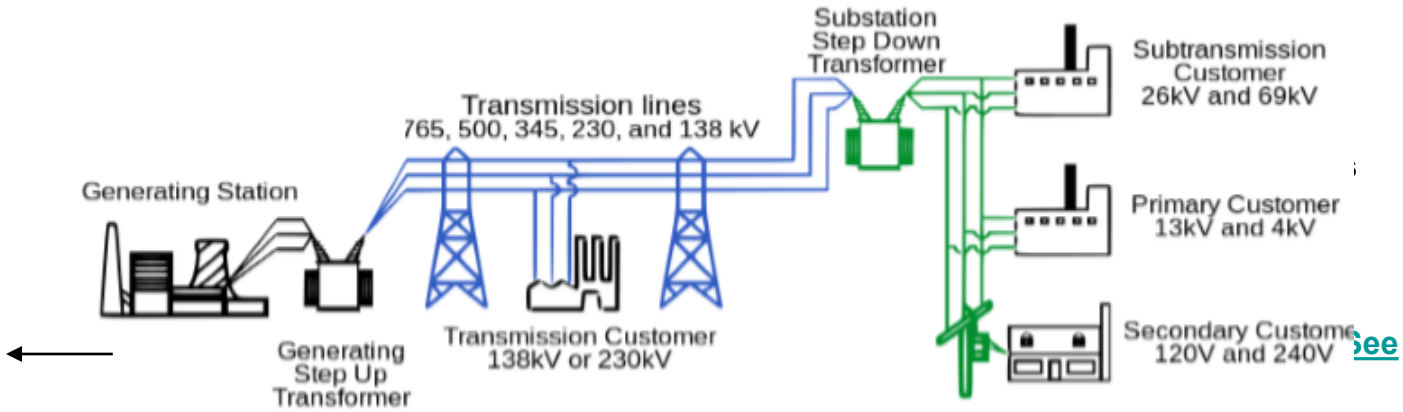
Note: The list of activities against each service are indicative and not complete or comprehensive.

Developing Information Security standards and guidelines for operational environments	• Enumeration of Cyber Assets • Security Categorization • Threat and Vulnerability analyses (open source intelligence) • Security Control Selection • Determine baseline/profile.
• Scope Requirement (E.g. MDR, HIDS or NIDS) • Identify SIEM Solution (Open source?) • Establish data collection processes/policies • Install SIEM (includes testing and reporting) • SIEM Administration and upkeep • Multi-tenant SOC (Security Operations Center). • Identify active and dormant threats lurking in your environment.	Implementing Cybersecurity Event and Incident management solutions
Compliance Management Services (Compliance Testing/Security Assessments) (PCI, HIPAA, GDPR, NIST, etc.)	• Preparation of Compliance requirements checklist (based on Security Policy, regulatory requirements, project needs E.g. HIPAA, NERC CIP) • Cybersecurity Testing strategies/tactics (development and execution) • Evidence collection and documentation • Findings and recommendations report • Change management processes and implementation assistance.
• Prepare Rules of Engagement Document • Identify Assessment objects • Define Testing viewpoints • Identify and install required tools (Scanning tools or Pen testing tools) (may include • Execute Scans/Tests (may include passive and active Tests) • Collect Test results & Prepare reports.	Vulnerability Assessment
Penetration Testing	• Application Pen Testing (Web Applications and Mobile Applications) based on Rules of Engagement Document – includes application enumeration and inputs from OWASP top 10, CVE and other vulnerability databases • SCADA Pen testing (E.g. PLC) – includes inputs from public databases and vendor datasheets and Rules of Engagement Document

Case 1 - CI Capabilities overview – Generating Station

NERC Cyber Security Compliance Proposal Quote for Switchgear OEM

- CI NERC compliance testing services proposals was packaged by Switchgear OEM with the E Houses for Generating Stations and Balance of Plant



Please refer to NERC CIP Standards – available .

CONTROLINFOTECH

CI Capabilities overview

NERC Cyber Security Compliance

EPC - Specification Example

SECTION I3

CYBERSECURITY REQUIREMENTS

1. GENERAL:

1.1 [redacted] will comply with the latest North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards (CIP-002-5.1; CIP-003-6; CIP-004-6; CIP-005-5; CIP-006-6; CIP-007-6; CIP-008-5; CIP-009-6; CIP-010-2; CIP-011-2) for the 2018 (CIP-002-5.1; CIP-003-6; CIP-004-6; CIP-005-5; CIP-006-6; CIP-007-6; CIP-008-5; CIP-009-6; CIP-010-2; CIP-011-2) for the impact facility. This docume... requirement of the latest NE... associated with physical and ... comply with all physical a... procedures as outlined herein.

1.2 NERC Requir... Subcontractors involved with... equipment and products must ... technically feasible. Security ... signed, and include Owner ... practices including requirem... Commission (FERC), the N... applicable commissions, US ... Energy (DOE).

1.3 Acronyms:

BES
CIP
DHS
DOE
ESP
EAP
FAT
FERC
NERC
PSP
SAT
SIEM
TFE

1.4 CIP-005 Pertin...

1.4.1 Cyber Asset: ... and data in those devices.

1.4.2 BES Cyber Asset: A Cyber Asset that if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. Redundancy of affected Facilities, systems, and equipment shall not be considered when determining adverse impact.

1.4.3 Cyber Security System: ... that will be installed to protect all the c... the latest NERC CIP standards.

1.4.4 Electronic Security Peri... which BES (Bulk Electric System) Cy...

1.4.5 Electronic Access Poin... routable communications between Cy...

1.4.6 Electronic Access Cont... perform electronic access control or e... Systems, including Intermediate Syste...

1.4.7 Intermediate System (IS... access control to restrict Interactive R... System must not be located inside the ...

1.4.8 External Routable Conn... from a Cyber Asset that is outside of ... connection.

1.4.9 Interactive Remote Acc... remote access client or other remote ac... originates from a Cyber Asset that is n... Responsible Entity's ESP(s) or at a def...

a. Cyber Assets us...
b. Cyber Assets us...
c. Cyber Assets us...

Note: Interactive remote access does n...

1.4.10 Physical Security Perim... which Cyber Assets, BES Cyber Syste... reside, and for which access is controll...

1.4.11 Physical Access Control System (PACS): Cyber Assets that control, alert, or log access to the Physical Security Perimeter(s), exclusive of locally mounted hardware or devices at the Physical Security Perimeter. Exclusion examples include motion sensors, electronic lock control mechanisms, and badge readers.

1.4.12 Other relevant CIP specific definitions can be found here: http://www.nerc.com/fil...

2. SECURI... all physical and cyber rel... herein.

2.1 Per the I... submit a TFE if vendor ... required if the desired ... switches.

2.2 Seller's p... to requirements describ... comply with the latest ... Requirements include O... or industry practices inc... applicable commissions, ... framework for the identi... of the BES. Seller shall ... to comply with the NER... CIP standards.

2.3 Seller's s... Homeland Security's (D... cert.gov/advisories-by-v... not be present on the ind...

a. R... eq...
b. R...
c. R... m...

Seller will certify the NERC CIP compliance and presence or absence of any DHS ICS advisories (https://ics-cert.us-cert.gov/advisories-by-vendor) for their systems and any of their components at the time of equipment shipment.

3. GENERAL REQUIREMENTS:

3.1 The system shall be capable of ... described in the latest NERC CIP standards for ... Standards and Technology (NIST) Special Publica... The referenced NIST documents are available for ...

3.2 The Seller shall provide all informa... for Buyer approval of all equipment/assets ... equipment/asset to a classification identified by ... Cyber System, Associated Protected Cyber Asse... Systems, or Physical Access Control and Monitori...

3.3 Seller shall provide and apply scree... Project Cyber Assets listed in the Cyber Assets ... model, and serial number with minimum charact... Cyber Assets Log in accordance with the followin...

Company
Cyber Asset ID: <Contra...
Product: <Supplie...
Model: <Supplie...
Serial: <Supplie...

Figure 2: Example o...

3.4 The referenced NERC CIP specific... http://www.nerc.com/pa/Stand/Pages/CIPStandard...

3.5 The Seller shall provide and/or en... updates for Seller's Cyber Assets.

3.6 The Seller shall provide patch man... Associated Protected Cyber Assets, and Electroni...

3.7 The Seller shall provide detailed O... on the Cyber Security System hardware, softwa... configuration of the system. See Section GR-B for...

I3-...

4. PERSONNEL AND TRAINING:

4.1 Personnel Risk Assessment Program: Personnel shall receive security awareness training in accordance with Owner requirements before being granted unescorted access to the customer site and operational equipment and/or ... except during CIP Exceptional Circumstances

5. SOFTWARE AND SERVICES: T... devices. Devices include, but are not limited to ... PLCs, and other microcontrollers.

5.1 Where technically feasible, sy... maintenance functions with no risk to system ope... patch and malware updates, minor applicatio... modification/addition/removal of user accounts, ... restore full operation. Maintenance functions req... for Buyer review and approval prior to purchase.

5.2 The Seller shall provide standard ... source in the procured product. DCS Provider pr...

5.3 The Seller shall provide the Bu... components provided. This will consist of filling ... Section. Delivery of the completed Cyber Assets ... impede the primary function of the procured pro... removed or disabled, the Seller shall document a ... recommendations and/or specific technical justif... on what is removed and/or disabled. The software ... not be limited to:

a. Games
b. Device drivers for product ...
c. Messaging services (e.g., e... sharing)
d. Source code
e. Software compilers in user...
f. Software compilers for pro... energy delivery system
g. Unused networking and co...

h. Unused administrative utilities, diagnostics, network management, and system management functions
i. Backups of files, databases, and programs used only during system development
j. All unused data and configuration files

6. MAINTENANCE:

6.1 Interchangeable Parts - Seller shall commit to maintaining spares and making interchangeable repair parts available for each component supplied, including third party equipment and software, for a minimum of three (3) years from the date of the Purchase Order, with an option for a period of additional 10 years. An interchangeable repair part is defined as an exact replacement for an existing part (same form factor, same electrical characteristics, etc.). However, an interchangeable repair part may have new or advanced features not present in the original part but must be compatible with the existing system. This list will conform to the formatting requirements of spare parts lists as defined in Section GR-B.

7. SECURE HARDWARE AND SOFTWARE DELIVERY: System information types classified as sensitive shall be communicated in advance to the Seller.

7.1 No system sensitive information shall be contained in system documentation required for routine system operation and maintenance. Where technically feasible, the system shall be risk evaluated such that all components necessary for system operation have operational, communication and power supply redundancy.

7.2 All security features/components shall be installed and configured prior to and during FAT and SAT. FAT and SAT test plans shall be provided by the Seller and include security feature testing.

7.3 Upon completion of FAT and commissioning, a system security assessment, including configuration baselines for each device shall be performed and documented by the Seller.

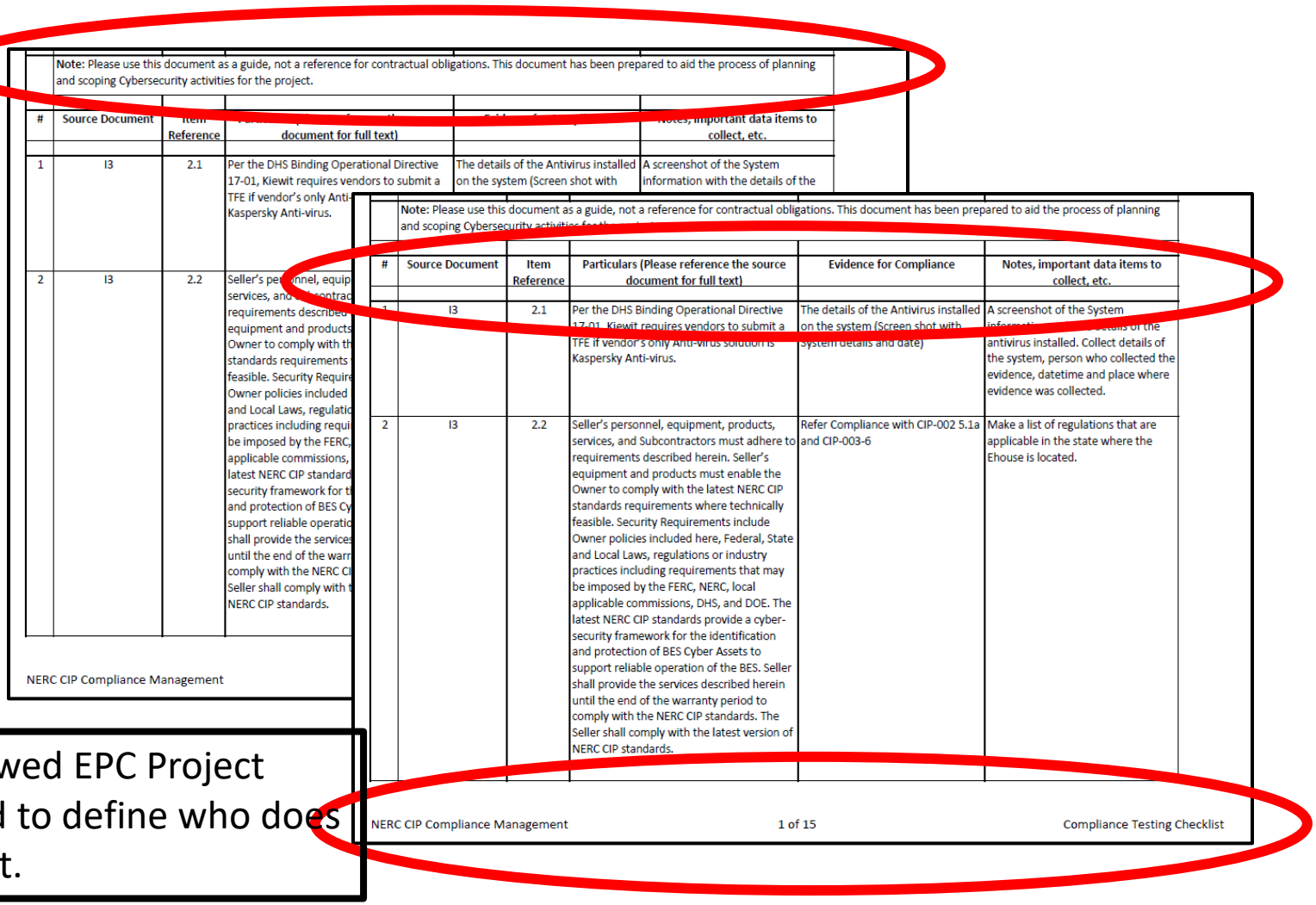
7.4 The Seller shall provide drawings and documentation to fully describe system configurations, interconnections, data flow and layout prior to FAT, with updated revisions upon completion of FAT and SAT.

7.5 The Seller shall provide a system description, a narrative describing the system overview, and detailed function of each component provided prior to FAT, with updated revisions upon completion of FAT and SAT. Following SAT, the Seller shall provide electronic and hard copies of an as-built set of all documentation deliverables, including but not limited to the

I3-6

Refer to the EPC sample specification for examples of what to look for?

SI delivers spec review – a checklist of deliverables



Note: Please use this document as a guide, not a reference for contractual obligations. This document has been prepared to aid the process of planning and scoping Cybersecurity activities for the project.

#	Source Document	Item Reference	Particulars (Please reference the source document for full text)	Evidence for Compliance	Notes, important data items to collect, etc.
1	I3	2.1	Per the DHS Binding Operational Directive 17-01, Kiewit requires vendors to submit a TFE if vendor's only Anti-virus solution is Kaspersky Anti-virus.	The details of the Antivirus installed on the system (Screen shot with System details and date)	A screenshot of the System information with the details of the antivirus installed. Collect details of the system, person who collected the evidence, datetime and place where evidence was collected.
2	I3	2.2	Seller's personnel, equipment, products, services, and Subcontractors must adhere to requirements described herein. Seller's equipment and products must enable the Owner to comply with the latest NERC CIP standards requirements where technically feasible. Security Requirements include Owner policies included here, Federal, State and Local Laws, regulations or industry practices including requirements that may be imposed by the FERC, NERC, local applicable commissions, DHS, and DOE. The latest NERC CIP standards provide a cyber-security framework for the identification and protection of BES Cyber Assets to support reliable operation of the BES. Seller shall provide the services described herein until the end of the warranty period to comply with the NERC CIP standards. The Seller shall comply with the latest version of NERC CIP standards.	Refer Compliance with CIP-002 5.1a and CIP-003-6	Make a list of regulations that are applicable in the state where the Ehouse is located.

NERC CIP Compliance Management 1 of 15 Compliance Testing Checklist

Allowed EPC Project Lead to define who does what.

CI Capabilities overview

NERC Cyber Security Compliance

CI Delivered Scope

E HOUSE xxxx

- CIP-002-5.1a Cyber Security – BES Cyber System Categorization
- CIP-003-6 Cyber Security – Security Management Controls

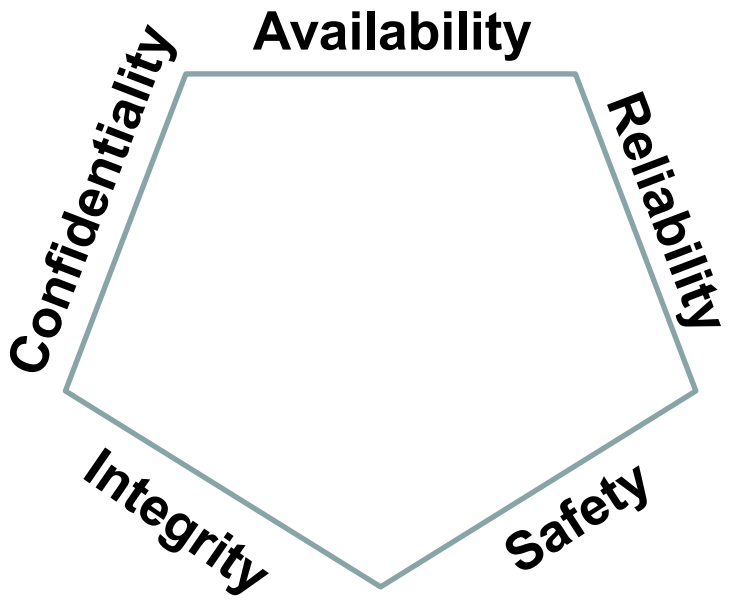
Question:
Why was it necessary to assist the EPC in defining the scope of services:

- Shouldn't the user just provide the scope?

5 Dimensions of ICS Security

Operations Technology is characterized by
- **Safety**
- **Reliability**

Information Technology is characterized by
- **Confidentiality**
- **Integrity**
- **Availability**



Security Objectives & Controls

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- **Integrity:** Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
- **Availability:** Ensuring timely and reliable access to and use of information.
- **Security Control:** A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

SAM ANALYTIC SOLUTIONS

CONTROLINFOTECH

Security Assessments

- An information security assessment is the process of determining how effectively an entity being assessed (e.g., host, system, network, procedure, person—known as the assessment object) meets specific security objectives. [NIST SP.800-115]
- Self Assessments and Third-Party Assessments

SAM ANALYTIC SOLUTIONS

CONTROLINFOTECH

Infrastructure Protection & Compliance

- Critical Infrastructure Protection (CIP) standards

https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- NIST (National Institute of Standards & Technology)

https://www.nist.gov/

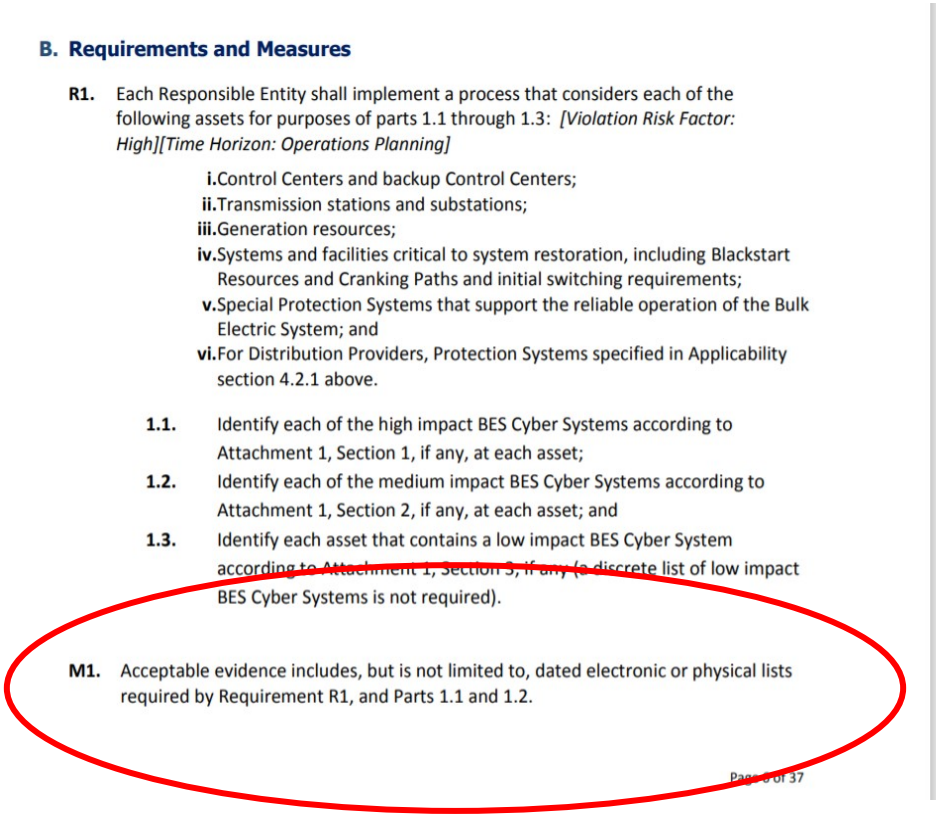
- Cybersecurity & Infrastructure Security Agency (CISA)

https://us-cert.cisa.gov/ics

SAM ANALYTIC SOLUTIONS

CONTROLINFOTECH

NERC CIP* 002-5-1a



B. Requirements and Measures

R1. Each Responsible Entity shall implement a process that considers each of the following assets for purposes of parts 1.1 through 1.3: *[Violation Risk Factor: High][Time Horizon: Operations Planning]*

- **i.** Control Centers and backup Control Centers;
- **ii.** Transmission stations and substations;
- **iii.** Generation resources;
- **iv.** Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements;
- **v.** Special Protection Systems that support the reliable operation of the Bulk Electric System; and
- **vi.** For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above.

1.1. Identify each of the high impact BES Cyber Systems according to Attachment 1, Section 1, if any, at each asset;

1.2. Identify each of the medium impact BES Cyber Systems according to Attachment 1, Section 2, if any, at each asset; and

1.3. Identify each asset that contains a low impact BES Cyber System according to Attachment 1, Section 3, if any (a discrete list of low impact BES Cyber Systems is not required).

M1. Acceptable evidence includes, but is not limited to, dated electronic or physical lists required by Requirement R1, and Parts 1.1 and 1.2.

Page 5 of 37

*** North American Electric Reliability Corporation Critical Infrastructure Protection**

https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

SAM ANALYTIC SOLUTIONS

CONTROLINFOTECH

NERC CIP* 003-6

R1. Each Responsible Entity shall review and obtain CIP Senior Manager approval at least once every 15 calendar months for one or more documented cyber security policies that collectively address the following topics: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1 For its high impact and medium impact BES Cyber Systems, if any:

1.1.1. Personnel and training (CIP-004);

1.1.2. Electronic Security Perimeters (CIP-005) including Interactive Remote Access;

1.1.3. Physical security of BES Cyber Systems (CIP-006);

1.1.4. System security management (CIP-007);

1.1.5. Incident reporting and response planning (CIP-008);

1.1.6. Recovery plans for BES Cyber Systems (CIP-009);

1.1.7. Configuration change management and vulnerability assessments (CIP-010);

1.1.8. Information protection (CIP-011); and

1.1.9. Declaring and responding to CIP Exceptional Circumstances.

1.2 For its assets identified in CIP-002 containing low impact BES Cyber Systems, if any:

1.2.1. Cyber security awareness;

1.2.2. Physical security controls;

1.2.3. Electronic access controls for Low Impact External Routable Connectivity (LERC) and Dial-up Connectivity; and

1.2.4. Cyber Security Incident response

M1. Examples of evidence may include, but are not limited to, policy documents, revision history, records of review, or workflow evidence from a document management system that indicate review of each cyber security policy at least once every 15 calendar months; and documented approval by the CIP Senior Manager for each cyber

*** North American Electric Reliability Corporation Critical Infrastructure Protection**

https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

Poll Questions

- Question 1
  - Which of the following are not primary tasks required to generate cyber asset log.
    a) Organizing and Collecting Data
    b) Checking designated assets for known threats
    c) Reporting findings and mitigation
    d) Tracking down known hackers

Cyber Security Analyst – Solutions & Services - continued

The goal of the Cybersecurity Practice at Sam Analytic is to assist organizations at all levels in the development and testing of Cybersecurity prevention, protection, mitigation, and response capabilities* (*Adapted from https://www.cisa.gov/cybersecurity-training-exercises)

- Developing Information Security standards and guidelines for Operations
- Implementing Cybersecurity Event and Incident management solutions
- Compliance Management Services – (Case 1)
- Vulnerability Assessment
- Penetration Testing (Case 2)
- Security Awareness and Training
- Cybersecurity Threat Assessment Program
- Automating daily Cybersecurity Tasks
  - – data collection and analyses
  - – timely reporting of events and incidents
  - – ETL of log data, etc.

Please refer to the handout detailing solutions provided.

Services Catalogue

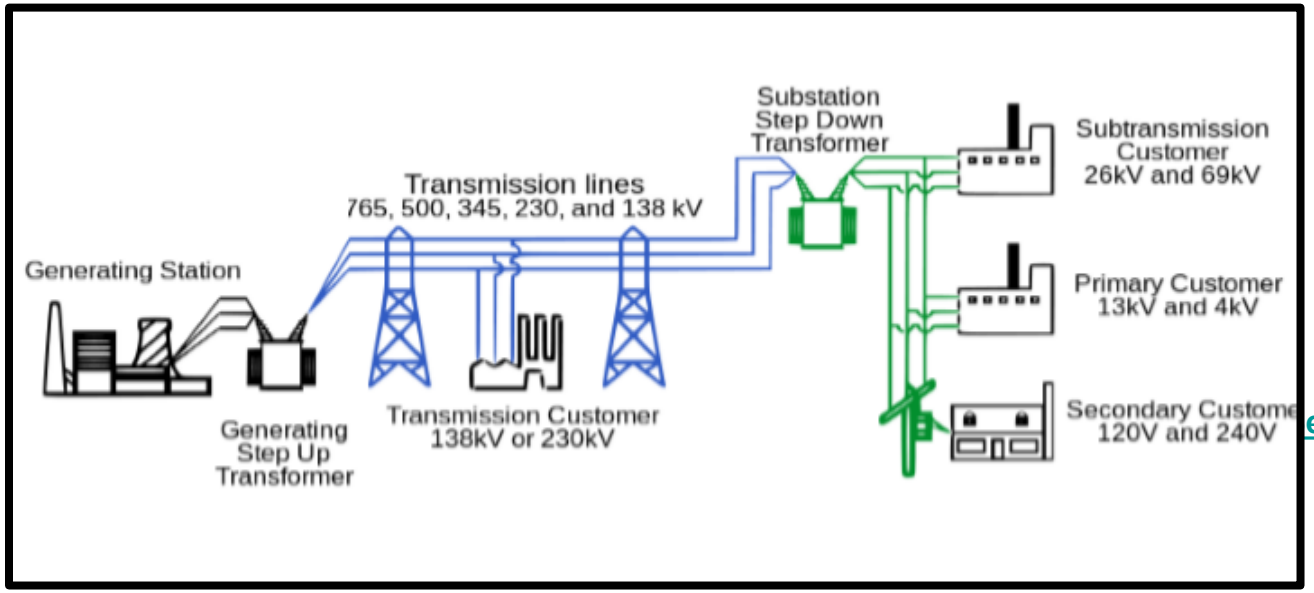
Note: The list of activities against each service are indicative and not complete or comprehensive.

Developing Information Security standards and guidelines for operational environments	• Enumeration of Cyber Assets • Security Categorization • Threat and Vulnerability analyses (open source intelligence) • Security Control Selection • Determine baseline/profile.
• Scope Requirement (E.g. MDR, HIDS or NIDS) • Identify SIEM Solution (Open source?) • Establish data collection processes/policies • Install SIEM (includes testing and reporting) • SIEM Administration and upkeep • Multi-tenant SOC (Security Operations Center). • Identify active and dormant threats lurking in your environment.	Implementing Cybersecurity Event and Incident management solutions
Compliance Management Services (Compliance Testing/Security Assessments) (PCI, HIPAA, GDPR, NIST, etc.)	• Preparation of Compliance requirements checklist (based on Security Policy, regulatory requirements, project needs E.g. HIPAA, NERC CIP) • Cybersecurity Testing strategies/tactics (development and execution) • Evidence collection and documentation • Findings and recommendations report • Change management processes and implementation assistance.
• Prepare Rules of Engagement Document • Identify Assessment objects • Define Testing viewpoints • Identify and install required tools (Scanning tools or Pen testing tools) (may include • Execute Scans/Tests (may include passive and active Tests) • Collect Test results & Prepare reports.	Vulnerability Assessment
Penetration Testing	• Application Pen Testing (Web Applications and Mobile Applications) based on Rules of Engagement Document – includes application enumeration and inputs from OWASP top 10, CVE and other vulnerability databases • SCADA Pen testing (E.g. PLC) – includes inputs from public databases and vendor datasheets and Rules of Engagement Document

- Case 2 - CI Capabilities overview – Traction Power Substation

Commercial Cyber Security - Penetration Testing Proposal Quote for TPSS Switchgear OEM

- Primary Customer: Municipal Area Transportation System specifies penetration testing for Traction Power substation SCADA



CI Capabilities overview

Cyber Security Threat Testing

Transportation Authority specification example

- CI delivers real time analytics – SCADA for Traction power station with Cyber Security Penetration Testing

1.5 QUAILITY ASSURANCE

A. Standards Compatibility. Contractor's materials, design, installation, and testing shall comply with all applicable References and Standards.

B. The SCADA system and all related interfaces, software, hardware and related network infrastructure/components shall meet modern cyber security standards and follow recommendations as outlined by the most recent APTA Control and Communications Cyber Security standards, as well as applicable standards referenced by the Department of Homeland Security and its Industrial Systems Cyber Response Team. All SCADA traffic must be encrypted throughout the entire network, from field devices to the office end (NOC/CCH) and back; any design modifications, hardware, software and/or network elements required to accommodate this are solely the responsibility of the vendor at no additional cost to CATS.

C. Applications, hardware, hardware/software interfaces and network connections/components shall be thoroughly tested by a third party Licensed Penetration Tester (LPT) or similarly qualified tester/firm as approved by the City of Charlotte. Vulnerabilities that are discovered must be eliminated or sufficiently mitigated, then retested as necessary to demonstrate security improvements, prior to system acceptance. The general types of vulnerabilities may include (but are not limited to), any addressed in the cyber security references noted in these specifications, network sniffing (switch to switch and end- device to switch), spoofing, replay, reflection, injection, denial of service, and memory corruption. It will be the Contractor's responsibility to provide this testing.

D. The penetration test shall incorporate thorough code reviews of all applicable source code, but the vendor need only provide certification that this has taken place and the general types of vulnerabilities found/addressed rather than releasing proprietary code or specifics that may compromise any of their existing releases at other locations.

E. Design modifications, additional hardware, software and/or network elements required to address these vulnerabilities are solely the responsibility of the vendor at no additional cost to CATS.

CI Capabilities overview

Vulnerability Assessment & Penetration Testing

CI Delivered Scope

- We handle and perform simple-to-complex Application Penetration Tests on any software or applications that sit on premise, on the web or via cloud-based systems
- Not only do we cover the standard set of threats defined in the “Open Web Application Security Project (OWASP) Top 10 Dangerous Vulnerabilities” but we can also go one step further with complex testing, depending on each customer’s needs.

* OWASP is an organization that provides unbiased and practical, cost-effective information about computer and Internet applications. This organization defines the following most dangerous vulnerabilities

- Injection
- Broken Authentication
- Sensitive data exposure
- XML External Entities (XXE)
- Broken Access control
- Security misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with known vulnerabilities
- Insufficient logging and monitoring

CI Capabilities overview

Commercial/Industrial Penetration Testing

CI Delivered Scope

Why would commercial users require 3rd Party testing - What are the main services these users want ?

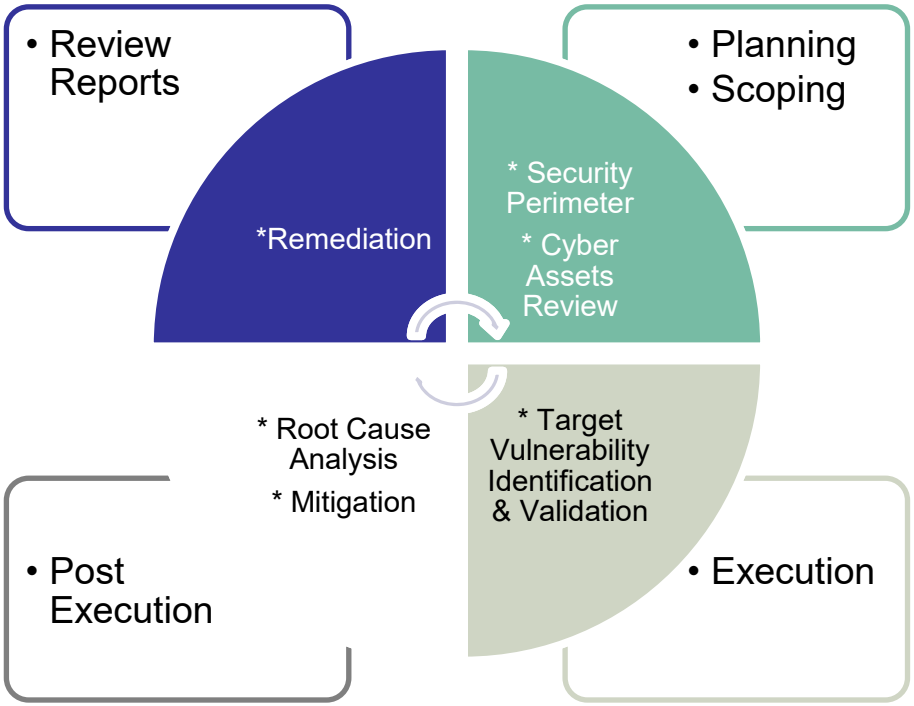
- Fuzzing of PLCs/Modbus devices
  - Link Layer
  - Transport Functions
  - Application Object Headers
- HMI
  - SQL Injection
  - Cross-Site Scripting
- Denial of Service on PLC and HMI
- PLC Holding Register Address Value Injection
- Switch assessment

Security Assessment Methods

- **Testing** is the process of exercising one or more assessment objects under specified conditions to compare actual and expected behaviors.
- **Examination** is the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence.
- **Interviewing** is the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or identify the location of evidence.

Penetration Testing

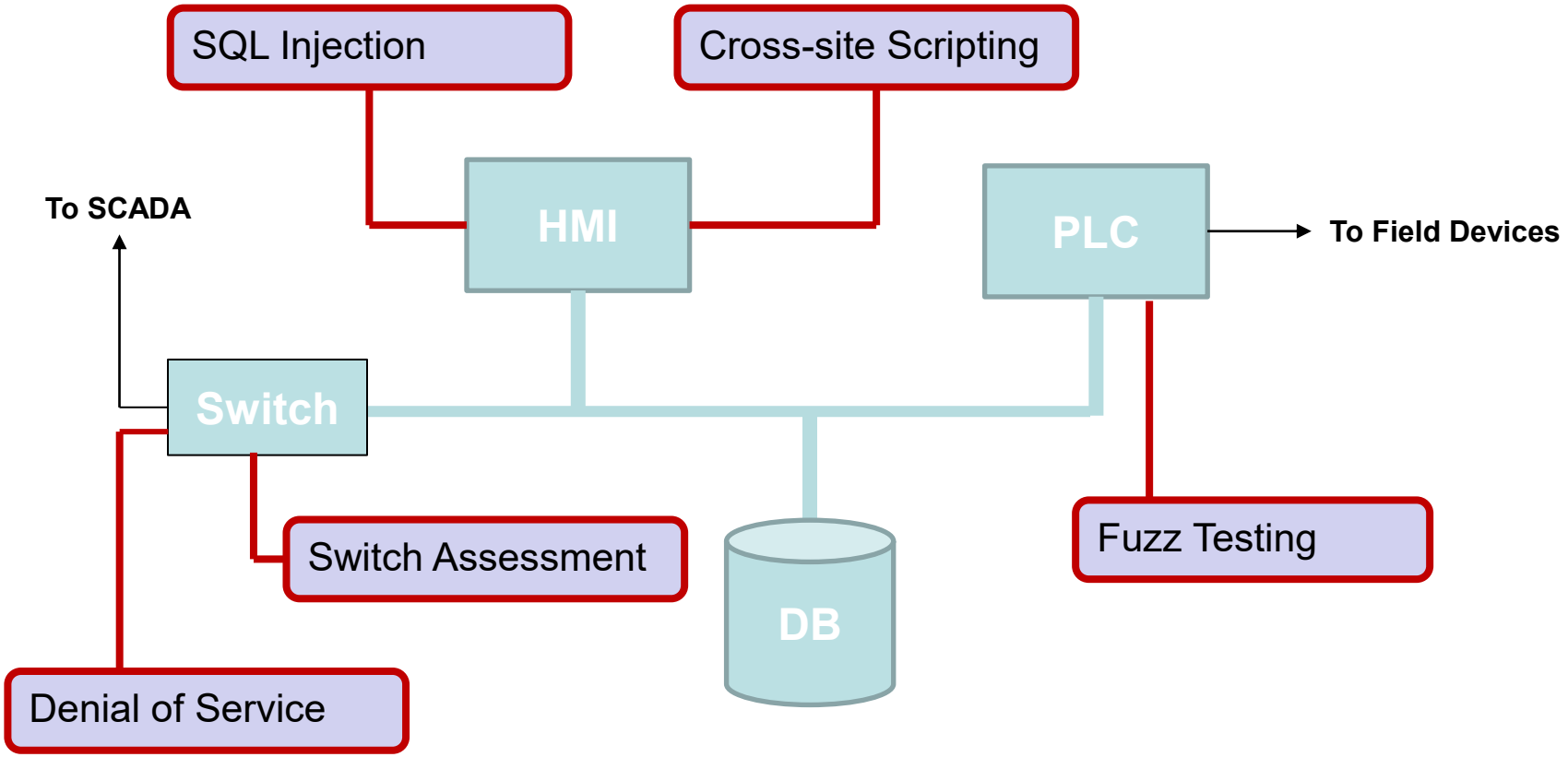
- A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.



SAM ANALYTIC SOLUTIONS

CONTROLINFOTECH

Schematic to Illustrate Concepts



* Contains Animation

Poll Questions

- Question 2
  - What systems and devices are tested?
    - » Networks
    - » Switches
    - » Controller HMIs
    - » HMI
    - » TSA restricted items

CONTROLINFOTECH

Cyber Security Analytics for Power & Control Operations

Tony Leszczynski
Business Development Manager
Control Infotech, Inc.
106, Kitty Hawk Drive
Morrisville NC 27560,
USA
O: (919) 544-3131
C: (984) 227-4121

CONTROLINFOTECH
www.control-infotech.com

Cyber Security – Solutions & Services

SAM ANALYTIC SOLUTIONS

Balakrishna Subramoney

Lead Analyst - Cybersecurity
SAM Analytic Solutions
p: 919.800.0044, m: 919.525.8559
f: 919.297.8742
a: 2511 E NC Highway 54, Durham NC 27713
w: www.samanalyticsolutions.com e: balu@samanalytic.com

Cyber Security Analytics for Power & Control Operations