Maintenance of Cybersecurity of Electrical Networks

SC B5 CIGRE Seminar

Iony Patriota de Siqueira, D.Sc.
iony@tecnix.com.br
www.tecnix.com.br
Scope

- To discuss the **concepts and principles of Maintenance** applied to **Cybersecurity**
- To discuss a **methodology** for cybersecurity maintenance
- To exemplify its **application** to Electrical Power Networks
Cigre Brochures about Cybersecurity

- **TB 427** - The Impact of Implementing Cyber Security Requirements using IEC 61850
- **TB 317** - Security for Information Systems and Intranets in Electric Power Systems
- **TB 419** - Treatment of Information Security for Electric Power Utilities (EPUs)
- **TB 603** - Application and Management of Cybersecurity Measures for Protection and Control
- **WG D2.38** – Framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure (Final draft)
Cybersecurity Risk to Electrical Networks

**Societal Sectors**
- Economical, Legal, Operational
- Social, Environmental, Technical
- Safety, Political

**Many Attacks**
- Internal
- External
- Contractors
- Concurrent Partners
- Enemies

**Wide-area exposure**
- Unmanned far sites
- Huge number of IED
- Multi-drop nets
- Noise fields
- Narrowband channels
- Low processing IED
- Difficult to test
- Ignorance
- Forbidden DOS

**Risk**

**Impact**

**Vulnerability**

**Threats**
Different Attitudes about Security (IT vs OT)

**Understanding Security Tools and How They Work**
- Understand security tools and how they work
- What do you do about Security?
  - Understand the automation systems and how they behave

**Lock it down. Minimum password length, change it**
- Lock it down. Minimum password length, change it
- What do you do about Access?
  - Keep it open. Need for quick access / emergency

**Must patch everything. Latest update**
- Must patch everything. Latest update
- What do you do about Versions?
  - OEM specific, difficult to install. If it works, keep it

**Regular & scheduled. Document everything! Trust administrators**
- Regular & scheduled. Document everything! Trust administrators
- What do you do about Changes?
  - Rare & unscheduled. As simple as possible. Let me do my job

**Compliance?**
- Regulated. Incident response & forensics
- Unregulated. No incident / forensics

**Information Technology**
- IT

**Operation Technology**
- OT
Cybersecurity Fundamental Questions

1. What facilities to protect?
2. What systems are there?
3. What functions to preserve?
4. What assets to protect?
5. What incidents can happen?
6. What threats are there?
7. What impacts can result?
8. What risks are incurred?
9. What countermeasures to apply?
10. What policies to adopt?
Cybersecurity Implementation Framework

1 - What facilities to protect?
2 - What systems are there?
3 - What functions to preserve?
4 - What assets to protect?
5 - What incidents can happen?
6 - What threats are there?
7 - What impacts can result?
8 - What risks are incurred?
9 - What countermeasures to apply?
10 – What policies to adopt?
Maintenance of Cybersecurity

RCM
- Plant Selection
- System Identification
- Asset Identification
- Failure Mode Identification
- Function Identification
- Functional Failure Identification
- FMEA
- Activity Selection
- Maintenance Policy

Physical Assets

CYBERSECURITY
- Facility Selection
- System Identification
- Cyber Asset Identification
- Cyber Function Identification
- Cyber Threat Identification
- Cyber Incident Identification
- Risk Analysis
- Countermeasure Selection
- Cybersecurity Policy

Cyber Assets
UML Class Diagram for RCM
UML Class Diagram for Cybersecurity

Assets are part of systems, which are part of facilities. Systems consist of functions. Threats can exploit vulnerabilities, which increase the risk of incidents. Hacker types can cause attacks, which lead to vulnerabilities. The failure of tasks can result in incidents, which can cause impacts. Countermeasures can mitigate risks, and policies can be deployed to ensure security.
Maintenance of Cybersecurity of Electrical Networks

Scope Definition

Iony Patriota de Siqueira, D.Sc.
iony@tecnix.com.br
www.tecnix.com.br
Step 1 – Scope Definition

Scope Definition

Facility Selection

System Identification

Function Identification

Asset Identification

Incident Identification

Threat Identification

Impact Risk Analysis

Countermeasure Analysis

Security Policy
### Layered Security Scope

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Installation</strong></td>
<td>Logical <strong>group of systems</strong> gathered to generate one or more products</td>
</tr>
<tr>
<td><strong>System</strong></td>
<td>Logical <strong>group of functions or subsystems</strong> that interact to attain system objectives</td>
</tr>
<tr>
<td><strong>Function</strong></td>
<td><strong>Group of assets</strong> that attain an <strong>objective</strong> with a given performance level</td>
</tr>
<tr>
<td><strong>Asset</strong></td>
<td><strong>Smallest part</strong> that a system is divided for functional purpose</td>
</tr>
</tbody>
</table>
Physical Assets for Transformer Bay

- Switch Controller
- Breaker Controller
- Merging Unit
- Breaker Controller
- Bay Controller
- Differential Protection
- Operator Console
- Bay Controller

Station & Process Bus Network
Cyber Assets for Transformer Bay

CU1 <<control unit>> D1Q2SB1
XCBR1
IP 10.0.0.11 Breaker Controller

MU1 <<merging unit>> D1Q2SB3
TCTR1 TCTR2
IP 10.0.0.13 Merging Unit

CU2 <<control unit>> E1Q3SB1
XCBR2
IP 10.0.0.15 Breaker Controller

CU3 <<control unit>> E1Q3SB3
XSWI
IP 10.0.0.17 Switch Controller

IED1 <<logical device>> D1Q2SB2
CSWI1
IP 10.0.0.12 Bay Controller

IED2 <<logical device>> A1KA1
IHMI
IP 10.0.0.18 Operator Controller

IED3 <<logical device>> D1Q2BP1
PDIF
IP 10.0.0.14 Differential Protection

IED4 <<logical device>> E1Q3SB2
CSWI2
IP 10.0.0.16 Bay Controller
Protection Systems and Functions

**Protection**

- Trip the protected equipment after the inception of an internal fault in no more than 100ms
- Do not trip the equipment for an external fault

**Differential Protection**

**Monitoring**

- Notify the operator about protection status in no more than 200ms

**Control**

- Switch breakers under operator control in no more than 200ms
# Cybersecurity System Description

<table>
<thead>
<tr>
<th>No</th>
<th>Subsystem</th>
<th>No</th>
<th>Function</th>
<th>No</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Protection</td>
<td>1</td>
<td>Trip the protected equipment after the inception of an internal fault in no more than 100ms</td>
<td>1</td>
<td>Logical Node: PDIF, XCBR1, XCBR2, TCTR1, TCTR2, CSWI1, CSWI2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Control Unit: CU1, CU2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Merging Unit: MU1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>Logical Device: IED1, IED3, IED4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>Network: Switches &amp; Cables</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Monitoring</td>
<td>2</td>
<td>Do not trip the equipment for an external fault</td>
<td>1</td>
<td>Logical Node: PDIF, TCTR1, TCTR2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Merging Unit: MU1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Control</td>
<td>3</td>
<td>Notify the operator about protection status in no more than 200ms</td>
<td>1</td>
<td>Logical Node: IHMI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Logical Device: IED2, IED3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Network: Switches &amp; Cables</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Control</td>
<td>4</td>
<td>Switch breakers under operator control in no more than 200ms</td>
<td>1</td>
<td>Logical Node: IHMI, XCBR1, XCBR2, CSWI1, CSWI2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Control Unit: CU1, CU2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Logical Device: IED1, IED2, IED4</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>Network: Switches &amp; Cables</td>
</tr>
</tbody>
</table>
Maintenance of Cybersecurity of Electrical Networks

Risk Analysis

Iony Patriota de Siqueira, D.Sc.
iony@tecnix.com.br
www.tecnix.com.br
Step 2 – Risk Analysis

- Facility Selection
- System Identification
  - Function Identification
  - Incident Identification
  - Impact Risk Analysis
  - Countermeasure Analysis
  - Security Policy
- Asset Identification
  - Threat Identification

Risk Analysis
Structured procedure to identify:

- **Function**: Objective + performance level
- **Incident**: Loss or deviation of function
- **Threat**: What can fail
- **Attack**: Why it fails (hackers = causes)
- **Impact**: Resultant effects
- **Risk**: Severity of the impact
Potential Incident
Measurable and identifiable condition that signals a pending functional incident or in process of occurring

Functional Incident
Inability of a system to perform a specific function between desired performance limits

ATTACK TIMELINE
NORMAL CYBER CAPACITY
Probing stage
Penetration stage
Perpetuation stage

PF Interval

Cyber Incident (RCM Failure) Timeline
RCM and Cybersecurity Failure Curve

RCM

- Normal stage
- Defect stage
- Failure stage

ASSET TIMELINE

Cybersecurity

- Probing stage
- Penetration stage
- Perpetuation stage

ATTACK TIMELINE

Physical Assets

Cyber Assets

Maintenance of Grid Cybersecurity
**Functional Incidents of a Differential Protection**

**Function 1**
Trip the protected equipment after the inception of an internal fault in no more than 100ms

- **Incident 1**
  Do not trip the protected equipment after the inception of an internal fault

- **Incident 2**
  Trip the protected equipment in more than 100ms

**Function 2**
Do not trip the equipment for an external fault

- **Incident 1**
  Trip the equipment for an external fault
1. Threats describe how functional incidents may happen due to cyber attacks.

2. Threats define how to combat a functional incident due to cyber attacks.

**Cyber Threat**

An event or logical condition, in a cyber asset, that may result in a functional incident.
Types of Cyber Attacks (RCM Causes)

1. Sniff - Unauthorized traffic analysis
2. Replay - Unauthorized replay of captured traffic
3. Spoof - Impersonating an authorized user
4. Dos - Deny service or overload network
5. Error - Operator error
6. Social - Social engineering of authorized users
7. Virus - Virus infection of system components
8. Destroy - Destruction of control/business/configuration data
9. Modify - Modification of control/business/configuration data
10. Bypass - Bypass of system security functions and mechanisms
11. Physical - Compromise of physical security mechanisms
Types of **Hackers** (RCM Root Cause)

**White Hats**
- **Good guys**, computer security experts, attest that information systems are secure

**Black Hats**
- **Bad guys**, just plain hackers, break into networks or computers, or create computer viruses

**Script Kiddies**
- **Black hat** hackers who use borrowed programs to attack networks and deface websites in an attempt to make names for themselves.

**Hacktivists**
- Motivated by politics or religion, or to expose wrongdoing, or revenge, or harass their target

**State Sponsored**
- **Governments** with limitless time and funding to target civilians, corporations, and governments.

**Spies**
- **Corporate** hired hackers to infiltrate the competition and steal trade secrets

**Cyber Terrorists**
- Motivated by religious or politics, try to create fear and chaos by disrupting critical infrastructures
Typical Cybersecurity Vulnerabilities

1. **Plaintext** - Use of clear text protocols
2. **Services** - Unnecessary services enabled
3. **Remote** - Uncontrolled remote access
4. **Architecture** - Poor system architecture
5. **Development** - Poor system implementation
6. **Nopolicies** - Inadequate security policies
7. **Spof** - Single Points of Failure
8. **Notraining** - Inadequate user training
9. **3rdparty** - Unauthorized 3rd party access
10. **Norisk** - Lack of risk assessment
Maintenance of Grid Cybersecurity

OSI Stack Communication Threats

- **Physically disrupt cables or signals**
  Protocols 100BaseT & 1000 Base-X

- **Logically disrupt frames, flood MAC**, Protocols 802.X, GOOSE, SV, GSSE

- **Logically disrupt segments and TCP/IP**
  DoS SYN attack, UDP flood, SNTP

- **Logically disrupt packets and addresses**
  Protocol IP, ICMP, ARP, & RIP

- **Logically disrupt connections**
  Protocol Telnet, RPC

- **Logically disrupt presentation contents**
  Protocols XML, EBCDIC

- **Logically disrupt applications & protocols**
  FTP, HTTP, POP3, MMS & ACSI
Physically disrupt cables or signals
Protocols 100BaseT & 1000 Base-X

Logically disrupt frames, flood MAC,
Protocols 802.X, GOOSE, SV, GSSE

Logically disrupt packets and addresses
Protocol IP, ICMP, ARP, & RIP

Logically disrupt segments and TCP/IP
DoS SYN attack, UDP flood, SNTP

Logically disrupt connections
Protocol Telnet, RPC

Logically disrupt presentation contents
Protocols XML, EBCDIC

Physically disrupt cables or signals
Protocols 100BaseT & 1000 Base-X

Logically disrupt applications & protocols
FTP, HTTP, POP3, MMS & ACSI

Logically disrupt segments and TCP/IP
DoS SYN attack, UDP flood, SNTP

Logically disrupt connections
Protocol Telnet, RPC

Logically disrupt presentation contents
Protocols XML, EBCDIC

Logically disrupt applications & protocols
FTP, HTTP, POP3, MMS & ACSI

VE 61850 Communication Vulnerabilities

User

OSI

Application

Presentation

Session

Transport

Network

Data Link

Physical

Network

Physical

Ethernet

IP

TCP

UDP

MMS (ISO 9506)

ASN.1

Session

ACSI

TimeSync
(SNTP)

GSSE

GOOSE

SV
Cyber Threats of a Differential Protection

Function 1
Trip the protected equipment after the inception of an internal fault in no more than 100ms

Incident 1
Do not trip the protected equipment after the inception of an internal fault

Incident 2
Trip the protected equipment in more than 100ms

Function 2
Do not trip the equipment for an external fault

Incident 1
Trip the equipment for an external fault

Incident 2
Trip the equipment for an external fault

Threats
- Misconfigured Logical Node (PDIF, XCBR1, XCBR2, TCTR1, TCTR2, CSWI1, CSWI2)
- Blocked Control Unit (CU1, CU2)
- Blocked Merging Unit (MU1)
- Blocked Logical Device (IED1, IED3, IED4)
- Network Deny-of-Service

Threats
- Delayed Logical Node (PDIF, XCBR1, XCBR2, TCTR1, TCTR2, CSWI1, CSWI2)
- Delayed Control Unit (CU1, CU2)
- Delayed Merging Unit (MU1)
- Delayed Logical Device (IED1, IED3, IED4)
- Overloaded Network

Threats
- Misconfigured Logical Node (PDIF, TCTR1, TCTR2)
1. Impacts describe the *effects* of cyber threats on the functions of the system
2. Impacts determine the *consequences* of cyber incidents

**Definition of Impacts**

- What happens when a cyber threat occurs

**IMPACT**
**Impacts of a Differential Protection Incident**

**Function 1**
Trip the protected equipment after the inception of an internal fault in no more than 100ms

Incident 1
Do not trip the protected equipment after the inception of an internal fault

Incident 2
Trip the protected equipment in more than 100ms

**Function 2**
Do not trip the equipment for an external fault

Incident 1
Trip the equipment for an external fault

**Impact**
- Severe Damage
- Increased Damage
- Low Damage
### Risk Matrix

<table>
<thead>
<tr>
<th>Severity Frequency</th>
<th>Insignificant</th>
<th>Minimal</th>
<th>Marginal</th>
<th>Critical</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent</td>
<td>Undesirable</td>
<td>Undesirable</td>
<td>Intolerable</td>
<td>Intolerable</td>
<td>Intolerable</td>
</tr>
<tr>
<td>Probable</td>
<td>Tolerable</td>
<td>Undesirable</td>
<td>Undesirable</td>
<td>Intolerable</td>
<td>Intolerable</td>
</tr>
<tr>
<td>Occasional</td>
<td>Tolerable</td>
<td>Tolerable</td>
<td>Undesirable</td>
<td>Undesirable</td>
<td>Intolerable</td>
</tr>
<tr>
<td>Remote</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Tolerable</td>
<td>Undesirable</td>
<td>Undesirable</td>
</tr>
<tr>
<td>Improbable</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Tolerable</td>
<td>Tolerable</td>
</tr>
<tr>
<td>Incredible</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Insignificant</td>
<td>Insignificant</td>
</tr>
</tbody>
</table>
### Failure Mode and Effect Analysis

<table>
<thead>
<tr>
<th>Plant</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recife II</td>
<td>RCD</td>
<td>Ivan</td>
<td>15/03</td>
<td>1</td>
</tr>
<tr>
<td>Transformer</td>
<td>T1</td>
<td>Iony</td>
<td>15/03</td>
<td>Of 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FU</th>
<th>FUNCTION</th>
<th>FA</th>
<th>FAILURE</th>
<th>MO</th>
<th>MODE</th>
<th>CAUSE</th>
<th>EFFECT</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**RCM FMEA - Failure Mode and Effects Analysis**

**Maintenance of Grid Cybersecurity**
## Cybersecurity Threats and Impact Analysis

<table>
<thead>
<tr>
<th>FU</th>
<th>FUNCTION</th>
<th>IN</th>
<th>INCIDENT</th>
<th>TH</th>
<th>THREAT</th>
<th>ATTACK</th>
<th>IMPACT</th>
<th>RISK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Trip the protected equipment after the inception of an internal fault in no more than 100ms</td>
<td>1</td>
<td>Do not trip the protected equipment after the inception of an internal fault</td>
<td>1</td>
<td>Misconfigured Logical Node (PDIF, XCBR1, XCBR2, TCTR1, TCTR2, CSWI1, CSWI2)</td>
<td>Internal</td>
<td>Severe damage</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Blocked Control Unit (CU1, CU2)</td>
<td>Internal</td>
<td>Severe damage</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Blocked Merging Unit (MU1)</td>
<td>Internal</td>
<td>Severe damage</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>Blocked Logical Device (IED1, IED3, IED4)</td>
<td>Internal</td>
<td>Severe damage</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>Network deny-of-service</td>
<td>Internal</td>
<td>Severe damage</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>Trip the protected equipment in more than 100ms</td>
<td>1</td>
<td></td>
<td>1</td>
<td>Delayed Logical Node (PDIF, XCBR1, XCBR2, TCTR1, TCTR2, CSWI1, CSWI2)</td>
<td>External</td>
<td>Increased damage</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>Delayed Control Unit (CU1, CU2)</td>
<td>External</td>
<td>Increased damage</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>Delayed Merging Unit (MU1)</td>
<td>External</td>
<td>Increased damage</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
<td>Delayed Logical Device (IED1, IED3, IED4)</td>
<td>External</td>
<td>Increased damage</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
<td>Overloaded Network</td>
<td>External</td>
<td>Increased damage</td>
<td>2</td>
</tr>
</tbody>
</table>
Maintenance of Cybersecurity of Electrical Networks

Countermeasures

Iony Patriota de Siqueira, D.Sc.
iony@tecnix.com.br
www.tecnix.com.br
Step 3 – Countermeasure Analysis

1. Facility Selection
2. System Identification
   - Function Identification
   - Incident Identification
3. Asset Identification
   - Threat Identification
4. Impact Risk Analysis
5. Countermeasure Analysis
6. Security Policy
**Cybersecurity Countermeasure (RCM Tasks)**

- **Deception** – misleading functionality/information
- **Discretion** – obscuring sensitive information
- **Separation** – enforced access policy restrictions
- **Collection** – automated gathering of information
- **Diversity** – intentional use of different technologies
- **Correlation** – analysis of collected information
- **Commonality** – adoption of security best practices
- **Awareness** – understanding of abnormal status
- **Depth** – enforcing multiple security functional layers
- **Response** – planned reaction to abnormal status

(*) Amoroso, E., *Cyber Attacks: Protecting National Infrastructure*
Deception Methods

- Deceptive **honeypot** and **honeynet** functionality attractive and locally/externally accessible to malicious insiders and outsiders
- Honeypot/honeynet management systems to detect exploit attempts for initiating response
Separation Methods

- Redirect or filter live attack traffic before it reaches local network ingress points
- Enforce network access controls (firewalls, DMZ, VPN) between groups of insiders, organizational resources and any untrusted external network
Commonality Methods

- Written security policies, with supporting training for decision-makers, and mechanisms for enforcement and violation consequences
- Organization compliance to a recognized information security standard attested by an external auditor
Diversity Methods

- **No single vendor** incident can produce a cascading effect in a critical application, computing, or networking functionality.
- At least one live, **alternative back-up vendor** for mission-critical assets.
• **No direct access** to any essential asset without at least two authentication challenges

• **Throttling, diverting, or stopping** attack traffic before it reaches a critical asset

• Failure of any one protection system cannot compromise any critical asset (**N-1 criteria**)
**Collection Methods**

- **Criteria** for which types of information in which contexts will be **collected and stored**
- **Collection systems** to gather information in real-time and store in a secure manner from applications, systems, and networks
Correlation Methods

- **Algorithms** to correlate relevant information in real-time toward actionable results
- **Correlative output** is connected to organizational awareness & response function
Awareness Methods

- Regular **collection of cyber security intelligence information and dissemination** to decision makers on a timely basis
- Real-time security operations function to coordinate any **preventive or response** actions
Response Methods

- Reaction to indicators and warning signals in advance of an attack on any critical asset
- Documentation and metrics on the root cause of past security problems and effectiveness of response activities for security incidents
Discretion Methods

- Organizational information is **properly marked** and such markings are suitably enforced.
- Organizational staff is **fully trained** in local policies for how information is handled and shared externally.

![Diagram showing First, Second, and Third Obscurity Layers with Asset, Data Markings, Sharing Policy, Leakage Policy connections]
**IT OSI Stack Threats and Countermeasures**

**Threats**

- Physically disrupt cables or signals
  - Protocols 100BaseT & 1000 Base-X

- Logically disrupt frames, flood MAC,
  - Protocols 802.X, GOOSE, SV. GSSE

- Logically disrupt packets and addresses
  - Protocol IP, ICMP, ARP, & RIP

- Logically disrupt segments and TCP/IP
  - DoS SYN attack, UDP flood, SNTP

- Logically disrupt connections
  - Protocol Telnet, RPC

- Logically disrupt presentation contents
  - Protocols XML, EBCDIC

- Logically disrupt applications & protocols
  - FTP, HTTP, POP3, MMS & ACSI

**Countermeasures**

- Intrusion Detection (IDS) & Prevention (IPS) Systems, firewall, education, policy

- Intrusion Detection (IDS) & Prevention (IPS) Systems, firewall, education, policy

- Intrustion Detection (IDS) & Prevention (IPS) Systems, firewall, education, policy

- Authentication, encryption by secure protocols: SSL, TLS or SSH

- Password, encrypted connections, Ipsec, IP firewalls with access control list, VPN

- VLAN + close unused ports of switches

- WPA2 or WPA protocols for wireless

- Control & monitor physical access to cables, panels, switches and routers

- **Control & monitor physical access to cables, panels, switches and routers**
Application of IEC 62351 (*) to IEC 61850

62351-6
Device Authentication
No Encryption

SV
GOOSE
GSSE

62351-3
Encryption Certification

TimeSync (SNTP)

62351-4
User & Station Authentication

ACSI

MMS (ISO 9506)

OSI

User

Application
Presentation
Session
Transport
Network
Data Link
Physical

Ethernet

Physical

Network

(*) Power systems management and associated information exchange - Data and communications security
Step 6 – Policy Decision

1. Facility Selection
2. System Identification
   - Function Identification
   - Incident Identification
   - Impact Risk Analysis
   - Countermeasure Analysis
   - Security Policy
3. Asset Identification
4. Threat Identification
5. Security Policy

Maintenance of Grid Cybersecurity
Maintenance of Grid Cybersecurity

IT Cybersecurity Frameworks

- The Committee of Sponsoring Organizations
- Control Objectives for Information Technology
- Information Technology Infrastructure Library
- International Organization for Standardization
- Enterprise Risk Management
- IT Governance
- IT Service Management
- IT Security Management
International Electrotechnical Commission
• IEC 62351 - Power systems management and associated information exchange - Data and communications security
• IEC 62443 - Industrial communication networks - Network and system security (Former ISA 99)

National Institute of Standards and Technology
• SP800 - Framework for Improving Critical Infrastructure Cybersecurity (CSF – Cyber-security Framework)

North American Electric Reliability Corporation
• CIP - Critical Infrastructure Protection

The International Society of Automation
• ISA99 - Network and system security for industrial-process measurement and control

US Department of Energy
US Department of Homeland Security
• ES-C2M2 - Electricity Subsector Cybersecurity Capability Maturity Model
• Energy Sector Cybersecurity Framework Implementation Guidance
**OT Cybersecurity Policy Requirements**

---

### Applicability

1. **Access Control** – of devices and information
2. **Use Control** – of devices and information
3. **Data Integrity** – against unauthorized changes
4. **Data Confidentiality** – against eavesdropping
5. **Restrict Data Flow** – of unauthorized publication
6. **Timely Response to Event** – notify, report & correct
7. **Network Resource Availability** – no denial of service

### Effectiveness

1. **Performance** - latency impacting functions
2. **Interoperability** – capacity to interact
3. **IED H/W & S/W impact** – on security
4. **Client-Server mixed mode** - migration to process bus
5. **Cost effective security management** – of security
6. **End-point security** - against insider threats
7. **Security certification** – availability of a process/entity
8. **RBAC** – Role-Based Access Control

---

(*) CIGRE Technical Brochure 427 - The Impact of Implementing Cyber Security Requirements using IEC 61850
**IEC 62351 Applicability for IEC 61850 Systems**

<table>
<thead>
<tr>
<th>Security Area</th>
<th>Access Control</th>
<th>Use Control</th>
<th>Data Integrity</th>
<th>Confidentiality</th>
<th>Data Flow</th>
<th>Timely Response</th>
<th>Resource Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security for profiles including TCP/IP</td>
<td>![Substantial Security]</td>
<td>![Weak or Unknown]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
</tr>
<tr>
<td>Security for profiles including MMS</td>
<td>![Substantial Security]</td>
<td>![Weak or Unknown]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td>![Substantial Security]</td>
<td>![Weak or Unknown]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
<td>![Not Addressed]</td>
</tr>
</tbody>
</table>

(*) CIGRE Technical Brochure 427 - The Impact of Implementing Cyber Security Requirements using IEC 61850
**IEC 62351 Effectiveness for 61850 Station Bus**

<table>
<thead>
<tr>
<th></th>
<th>Access Control</th>
<th>Use Control</th>
<th>Data Integrity</th>
<th>Data Confidentiality</th>
<th>Restrict Data Flow</th>
<th>Timely Response</th>
<th>Resource Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance (Latency)</td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
</tr>
<tr>
<td>IED H/W Impact</td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
</tr>
<tr>
<td>IED S/W Impact</td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
</tr>
<tr>
<td>Interoperability</td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
<td><img src="#" alt="Yellow" /></td>
</tr>
<tr>
<td>Client-Server Mixed Mode</td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
</tr>
<tr>
<td>Cost Effective Security Management</td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
</tr>
<tr>
<td>End-Point Security</td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
</tr>
<tr>
<td>Security Certification</td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
<td><img src="#" alt="Red" /></td>
</tr>
</tbody>
</table>

(*) CIGRE Technical Brochure 427 - The Impact of Implementing Cyber Security Requirements using IEC 61850
<table>
<thead>
<tr>
<th>Feature</th>
<th>Access Control</th>
<th>Use Control</th>
<th>Data Integrity</th>
<th>Data Confidentiality</th>
<th>Data Flow</th>
<th>Timely Response</th>
<th>Resource Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performance (Latency)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IED H/W Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IED S/W Impact</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role-Based Access Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interoperability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client-Server Mixed Mode</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost Effective Security Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-Point Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Certification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(*) CIGRE Technical Brochure 427 - The Impact of Implementing Cyber Security Requirements using IEC 61850
Cybersecurity Maintenance Policies

<table>
<thead>
<tr>
<th>Asset Vulnerability</th>
<th>Action</th>
<th>Cybersecurity Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unreliable</td>
<td>Avoid</td>
<td>Avoidance</td>
</tr>
<tr>
<td>Measurable</td>
<td>Detect</td>
<td>Detection</td>
</tr>
<tr>
<td>Predictable</td>
<td>Anticipate</td>
<td>Recovery</td>
</tr>
<tr>
<td>Controllable</td>
<td>Control</td>
<td>Limitation</td>
</tr>
<tr>
<td>Hidden</td>
<td>Discover</td>
<td>Assurance</td>
</tr>
<tr>
<td>Uncontrollable</td>
<td>Repair</td>
<td>Assumption</td>
</tr>
</tbody>
</table>
RCM Failure and Policy Timeline

- Design-Change
- Failure-Finding
- Condition-Based
- Operational
- Time-Based
- Run-to-Failure

Functional Capacity:
- Normal
- Defect
- Failed

Asset Timeline:
- Normal stage
- Defect stage
- Failure stage

PF Interval

0 %
100 %
Cybersecurity Threat and Policy Timeline

**Probing stage**
- **Avoidance**
- **Assurance**

**Penetration stage**
- **Detection**
- **Limitation**
- **Recovery**
- **Assumption**

**Perpetuation stage**
## RCM Tasks per Policy

<table>
<thead>
<tr>
<th>TASKS</th>
<th>Design-Change</th>
<th>Failure-Finding</th>
<th>Condition-Based</th>
<th>Operational</th>
<th>Time-Based</th>
<th>Run-To-Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Refurbishing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replacing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Measuring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inspecting</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redesigning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lubricating</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cleaning</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Recording</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Countermeasure</td>
<td>Avoidance</td>
<td>Assurance</td>
<td>Detection</td>
<td>Limitation</td>
<td>Recovery</td>
<td>Assumption</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>------------</td>
<td>----------</td>
<td>------------</td>
</tr>
<tr>
<td>Deception</td>
<td>misleading functionality / information</td>
<td>scan available ports and resources</td>
<td>check honey pot deception traps</td>
<td>periodic updating of honey pots</td>
<td>clean honeypot traps and data base</td>
<td>no misleading functionality / information</td>
</tr>
<tr>
<td>Discretion</td>
<td>obscuring sensitive information</td>
<td>try disclosing sensitive information</td>
<td>check the disclosure of sensitive data</td>
<td>periodic updating of passwords</td>
<td>replace broken passwords / sensitive data</td>
<td>allow disclosing public information</td>
</tr>
<tr>
<td>Separation</td>
<td>enforced access policy restrictions</td>
<td>try unauthorized access</td>
<td>check unauthorized access tentative</td>
<td>periodic review of security domains</td>
<td>rework broken firewall rules</td>
<td>unrestricted open access policy</td>
</tr>
<tr>
<td>Collection</td>
<td>automated gathering of information</td>
<td>simulate incident to gather information</td>
<td>check collected log information</td>
<td>periodic emptying of logs</td>
<td>restore overloaded data base</td>
<td>no information gathering</td>
</tr>
<tr>
<td>Diversity</td>
<td>intentional use of different technologies</td>
<td>try to substitute a supplier</td>
<td>check diversity of suppliers</td>
<td>periodic renewing of suppliers</td>
<td>change disrupted technologies</td>
<td>use identical technologies</td>
</tr>
<tr>
<td>Correlation</td>
<td>analysis of collected information</td>
<td>try injecting correlated information</td>
<td>check correlation of logged information</td>
<td>periodic analysis of collected data</td>
<td>identify &amp; block source of attacks</td>
<td>no analysis of incidents or information</td>
</tr>
<tr>
<td>Commonality</td>
<td>adoption of security best practices</td>
<td>try non-standard practices</td>
<td>check conformance audit records</td>
<td>periodic updating of security policies</td>
<td>reinforce broken security best rules</td>
<td>non-standardized practices</td>
</tr>
<tr>
<td>Awareness</td>
<td>understanding of abnormal status</td>
<td>simulate perception of abnormal status</td>
<td>check perception of incidents</td>
<td>periodic renewing of operator training</td>
<td>retrain after undetected incidents</td>
<td>no understanding of abnormal status</td>
</tr>
<tr>
<td>Depth</td>
<td>enforcing multiple security functional layers</td>
<td>try unauthorized cross of security layers</td>
<td>check logs for partial security layer breaking</td>
<td>periodic review of firewall rules</td>
<td>reinforce broken depth defenses</td>
<td>none or single security functional layer</td>
</tr>
<tr>
<td>Response</td>
<td>misleading functionality / information</td>
<td>simulate reaction to abnormal status</td>
<td>check response to simulated failures</td>
<td>periodic review of disaster / recovery plan</td>
<td>run disaster recovery plans</td>
<td>unplanned reaction to abnormal status</td>
</tr>
</tbody>
</table>
## Cybersecurity Planning Documentation

### Cybersecurity System Documentation

<table>
<thead>
<tr>
<th>Installation</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

### Cybersecurity System Description

<table>
<thead>
<tr>
<th>TYPE:</th>
<th>Installation</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

### Cybersecurity Threats and Impact Analysis

<table>
<thead>
<tr>
<th>No.</th>
<th>Installation</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

### Cybersecurity Impact Analysis

<table>
<thead>
<tr>
<th>FU</th>
<th>Installation</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

### Cybersecurity Decision Analysis

<table>
<thead>
<tr>
<th>FU</th>
<th>INSTALLATION</th>
<th>Code</th>
<th>Leader</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

### Cybersecurity Plan

<table>
<thead>
<tr>
<th>System</th>
<th>Code</th>
<th>Auditor</th>
<th>Date</th>
<th>Sheet</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CODE</th>
<th>ANALYSIS</th>
<th>POLICY COUNTERMEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>FUNCTION</td>
<td>INCIDENT</td>
<td>ASSET</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>-------</td>
</tr>
</tbody>
</table>
Integrated Cybersecurity Maintenance Software
Wide-Area Cybersecurity (WACS)

1. Power Network (Field)
   - MU
   - IED

2. Station Network (Station)
   - IED

3. Corporate Network (Operation)
   - Station Network
   - Corporate Network

4. External Network (Enterprise)
   - External Network

Process:
- Generation
- Transmission
- Distribution
- Consumer

Networks:
- IED
- Station Network
- Corporate Network
- External Network

Security Components:
- Physical Security
- Authentication
- National Security
- Corporate Cybersecurity
- Station Security
- RBAC
- IDS
- Login
- Physical Security

Authentication:
- DMZ
- RBAC
- IDS
- Login
- RBAC
- RBAC

Cybersecurity Zones:
- Corporate
- Station
- External
- National

Cybersecurity Systems:
- Wide-Area Cybersecurity (WACS)
- IED
- Process Network
- Power Network
- Generation
- Transmission
- Distribution
- Consumer
Спасибо

Iony Patriota de Siqueira
iony@tecnix.com.br
www.tecnix.com.br