Interactive session on

“Smart Grid for Smart Cities”

30th October 2018

India Habitat Centre, New Delhi

Presentation Title: **Cyber Security for Smart Grid Solutions**

By: **Mahendiran Gunasekaran, ERL - India**

Jointly Organized by

National Smart Grid Mission
Ministry of Power
Government of India

ieema
your link to electricity

Introduction

- Technological misuse and/or abuse has become a serious concern in all areas where computers are used and networked.
    - **Around 47% of the People in the Globe are utilizing the Network Communications**
- Computer security has now become the focus of national consideration
- Power System is classified as one of Most Critical Infrastructure
    - **Electrical Grid enables and supports the other Infrastructures such as**
        - **Oil and Natural gas**
        - **Water**
        - **Food & Health Care**
        - **Transportation**
        - **Telecommunications and**
        - **Financial sectors**

Need of Cyber Security

Conventional SAS Systems	Modern SAS Systems
Highly Sophisticated System (Touch Me not)	Every utility feels the necessity (No more a Luxury)
No Remote Operations	Possibilities for Remote operations
Closed network well within the SS premises	Remote Monitoring, including corporate and external networks
Minimal / No external integrations	Increasing integration between various systems within and outside the organization
Communications based on Serial Interfaces	IP based communications including the field sub-devices
Hierarchical communication between control center, field devices	Data / Information exchanges at different levels
	Hierarchical Grid Connectivity to Inter Connected Grid

Cyber Security in Power Systems

- **Definition of Cyber Security**
  - Techniques and Practices defined to PROTECT Data
    - Applies to Digital Data
    - Stored, Transmitted, In Use etc.,
- **Power Substation Threats are primarily in Remotely Accessed Protection, Control, Automation & SCADA**
  - *Suspects*
    - Internal Attackers
    - Suppliers with a malicious intent
    - Hackers
    - Criminals
    - Terrorists

Threats Experienced by Utilities World-Wide

- **Physical Attack**
  - Most common in rural substations is **copper theft**.
  - In April 2013, a physical attack occurred at **Pacific Gas and Electric's (PG&E's) Metcalf transmission substation**. Two fiber-optic lines running underground near the substation were cut, and more than 100 rifle shots were fired at the substation's transformers.
- **Cyber Attack**
  - **Stuxnet** was the first sophisticated cyber attack reported on critical infrastructure. Stuxnet is a malicious computer worm, first identified in 2010, that targeted Iran's nuclear program
  - Then in both 2015 and 2016 December, Ukraine electric grid experienced power outages caused by remote cyber intrusions.

Communications Used in Indian Utilities

- Optical Fibre Composite Ground Wire (OPGW)
- Power Line Carrier Communication (PLCC)
- Micro-Wave Communication
- Very Small Aperture Terminal (VSAT)
- Leased Line (LL)
- Asymmetric digital subscriber line (ASDL) / Symmetric digital subscriber line (SDSL)

Vulnerabilities in Substation Automation

- **Real Time Operating System (RTOS)**
  - All IED's System software is designed to operate in an environment focusing to events; security is lower priority
- **Communication Media or Network**
  - All IED's are working on IP based communication; they can communicate with any computer having internet
- **Open Protocols**
  - All IED's are working in Open protocols, well documented and available in general public. (When the protocols were defined, security was not a key issue)
- **Lack of Authentication & Administration**
- **Large Number of Remote Users**
  - Remote Servers diversified in geographically different Locations.

Security Requirements

- **Basic Requirements:**
  - Secure system architecture such as different security zones
  - Protect the Electronic Security Perimeter (ESP)
  - Improve the robustness and hardening
  - Authentication and authorization (User Account Management)
  - Auditability and logging (User Activity Logging)
  - Antivirus Protection

Security Requirements

- **Enhanced Requirements:**
  - Patch Management
  - Application White Listing
  - Secure communication from outside the system using https, VPN, etc…
- **Security in protocols / Comply with upcoming standards (Ex: IEC 62351):**
  - DNP 3.0 / IEC 60870-5-104 Secure authentication based on IEC 62351
  - Central user Account Management
  - Certificate Handling

Security Requirements

➢ **How to Protect Data**

- **Access** - ***Confidentiality***
- **Modification** - ***Integrity***
- **Deletion** - ***Availability***

- Device or Computer
- Files or Directory
- Software Application

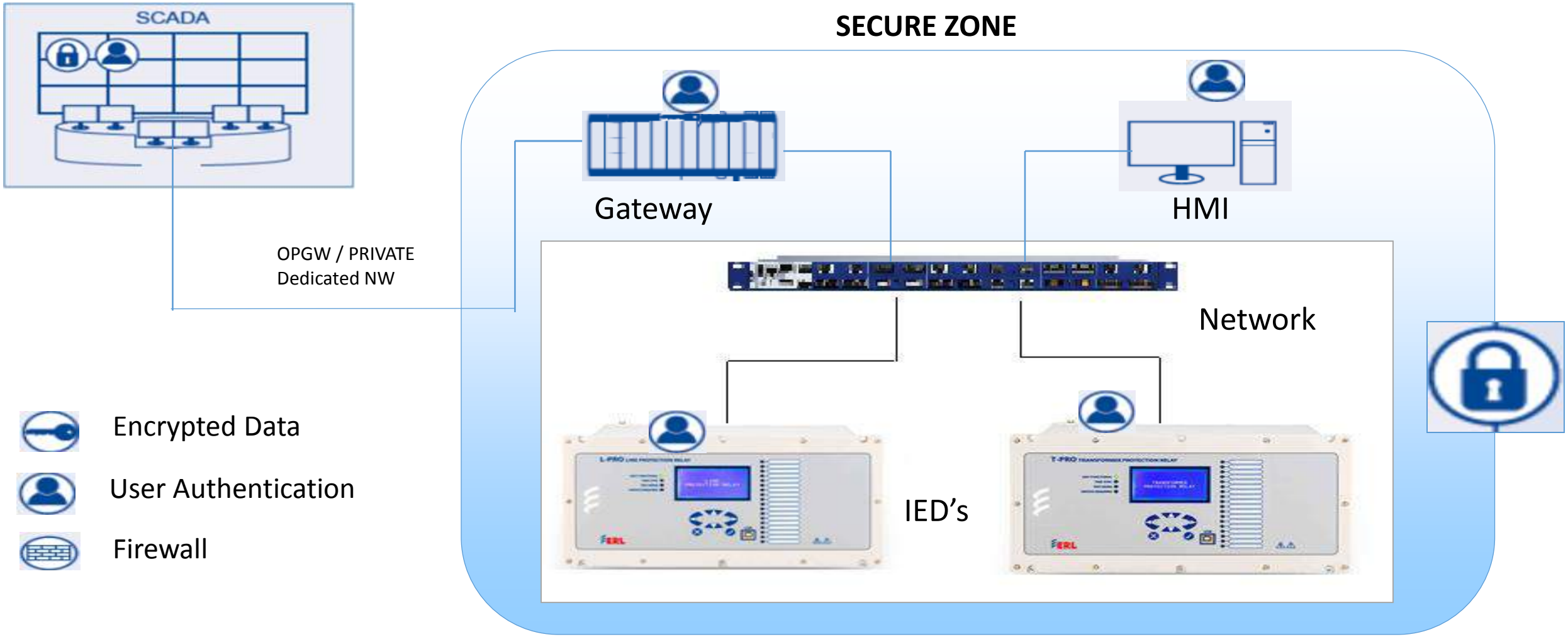
Cyber Security in IED's / Gateway's / HMI's

- IED's default password to be removed and New Password to be set
- User Password should not be simple
  - **Password Complexity Rules**
    - ✓ Password Length (from 4 to 23 characters)
    - ✓ At least one upper case character (On/Off)
    - ✓ At least one lower case character (On/Off)
    - ✓ At least one number (On/Off)
    - ✓ At least one special character (On/Off)
  - **Password change period**
    - ✓ Enabled attribute
    - ✓ Password change period Value; range: 1 - 3650 days (10years), default 450 (15 months)

Cyber Security in IED's / Gateway's / HMI's

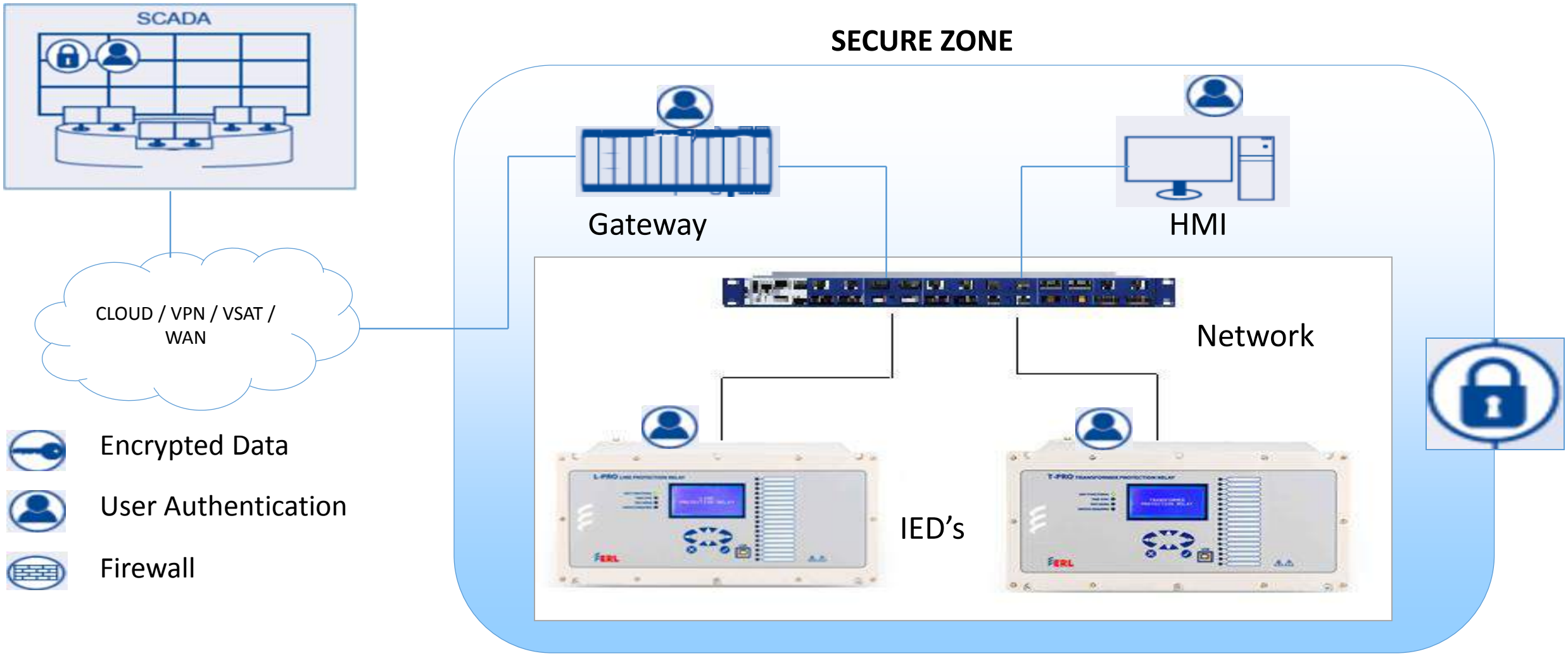
- Different level of Access Privileges shall be provided to the users
  - **Access Policies include**
    - ➢ Login timeout (initial 5 minutes, increases to 10 minutes after one attempt)
    - ➢ Session Inactivity Timeout; range: 1 - 120 minutes; default is 60 min
    - ➢ Session Duration Timeout; range: 1 – 8760hrs (1 year), default is 16hr
    - ➢ Account Lockout rules
      - ✓Failed re-tries counter; range: 0 (unlimited) – 20 , default is 7
      - ✓Lockout timeout value; range: 3 – 60 minutes, default is 5
- Encrypting Communications
- Detecting the Trespasser
  - By creating the Log for the User
  - By deploying IDS (Intrusion Detection Systems)

Present Substation Architecture 1



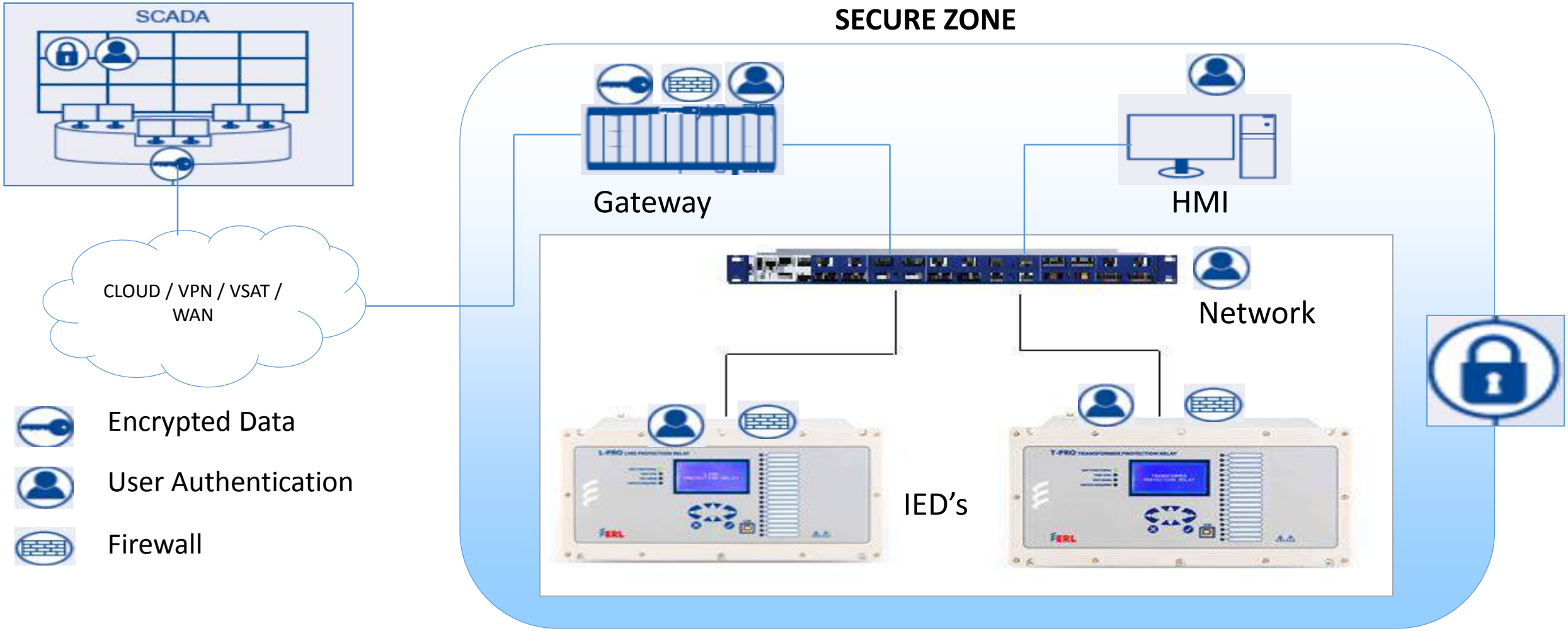
LOW POTENTIAL THREAT

Present Substation Architecture 2

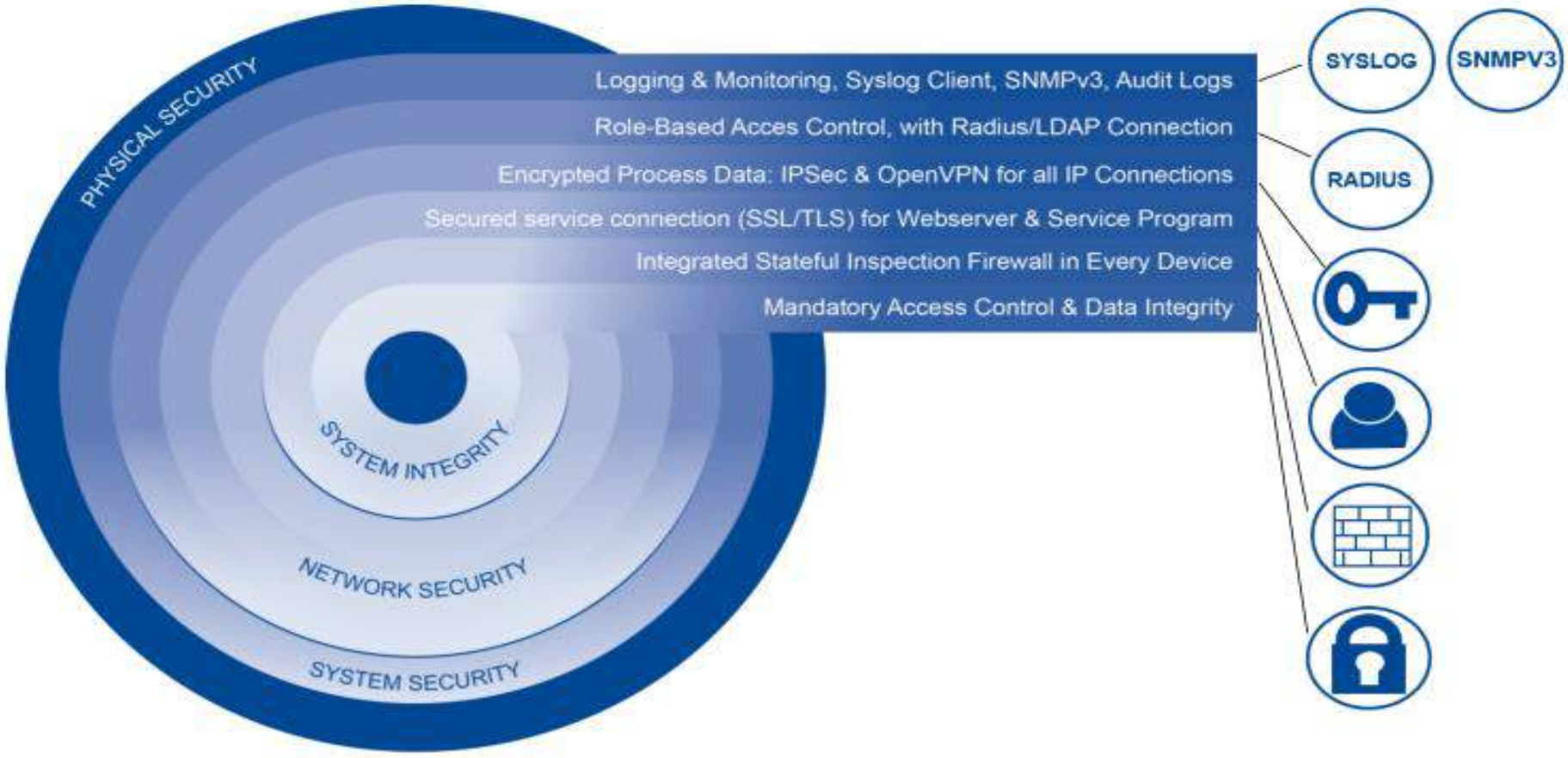


HIGH POTENTIAL THREAT

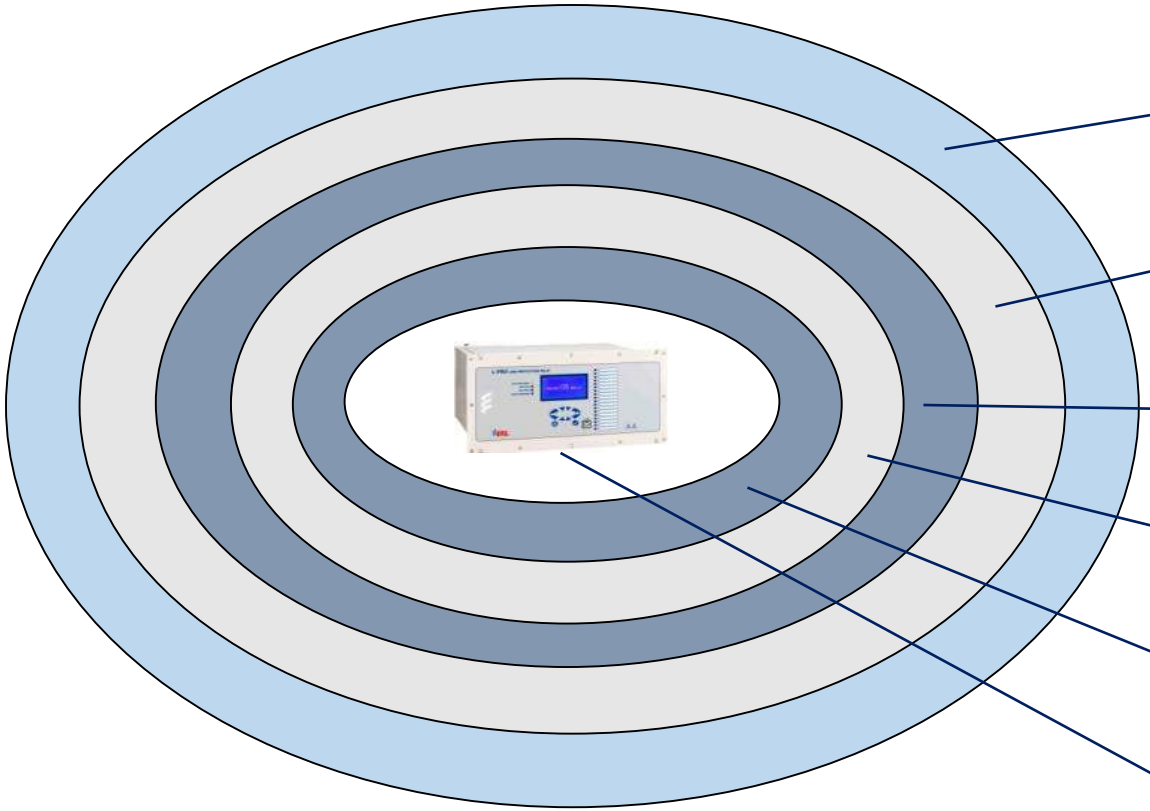
Expected Security



Cyber Security



The ONION Approach to Security



Security Monitoring

Encryption

Firewall

Authentication

System hardening

Protection & Control

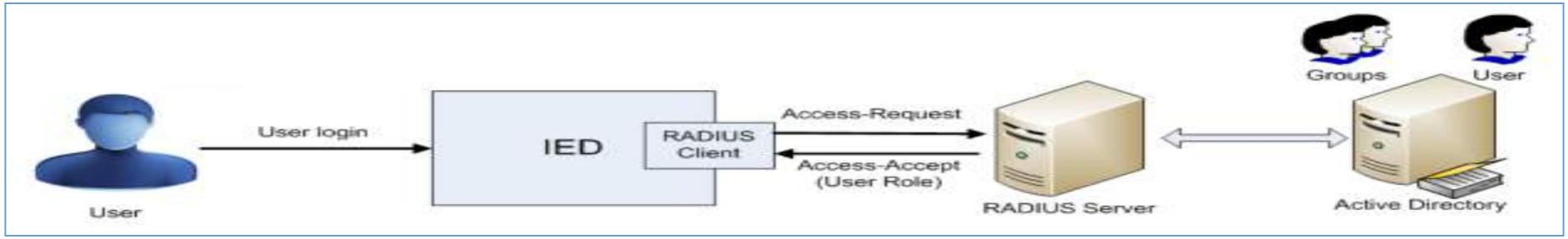
SYSLOG

SNMPV3

RADIUS

Network Level Security

- Port based network access control
- SSH/SSL encryption
- RADIUS (Remote Authentication Dial-In User Service) password management



- SNMPv3 authentication
- Access security
  - to complement its existing set of security features, such as multi-level passwords, MAC based port security, and VLANs.

Cyber Security Standards

- **NERC CIP**
- **IEEE 1686-2013 -** Standard for Intelligent Electronic Devices Cyber Security Capabilities
- **IEC/TS 62351-8** - Power systems management and associated exchange – Data and communications security – Part 8: Role-based access control **(RBAC)**
- **IEEE C37.231-2006** – Recommended Practice for Microprocessor Based Protection Equipment Firmware Control
- **RFC 5424** The Syslog Protocol
- **ISA-99/IEC-62443** - Procedures for implementing electronically secure Industrial Automation and Control Systems (IACS)

NERC CIP Standard Overview

- Defines the requirement of Cyber Security for the Bulk Energy Supply (BES) / Utilities and not to IED Vendors

➢ *"The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliable operation of the BES" - CIP-002-5.1*

- Specific Requirements will be defined in Regional Level

➢ *"The Regional Entity shall serve as the Compliance Enforcement Authority ("CEA") unless the applicable entity is owned, operated, or controlled by the Regional Entity. In such cases the ERO or a Regional Entity approved by FERC or other applicable governmental authority shall serve as the CEA" - CIP-002-5.1*

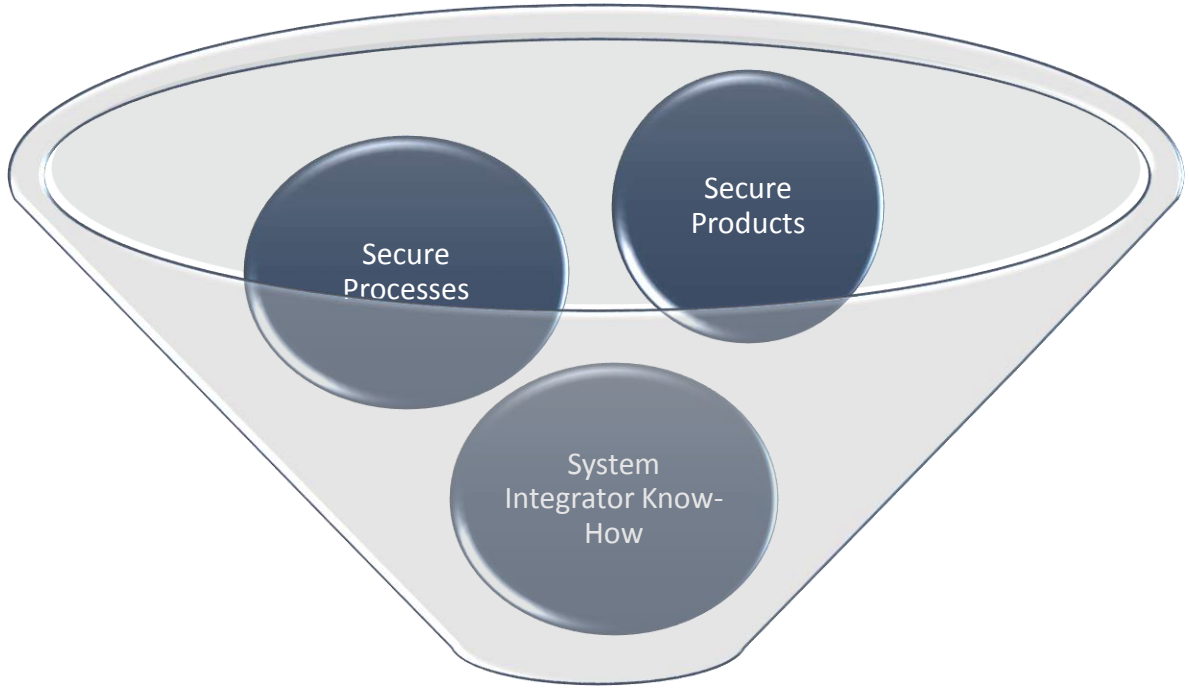
NERC CIP Standard Overview

- **Categories of BES systems:**
  - High Impact (>= 3000 MW)
  - Medium Impact (>= 1500 MW)
  - Low Impact
- **Security Management Controls (Cyber Security Policies)**
  - Personnel & training
  - Electronic Security Perimeters including Interactive Remote Access
  - Physical security of BES Cyber Systems
  - System security management
  - Recovery plans for BES Cyber Systems
  - Configuration change management and vulnerability assessments
  - Information protection

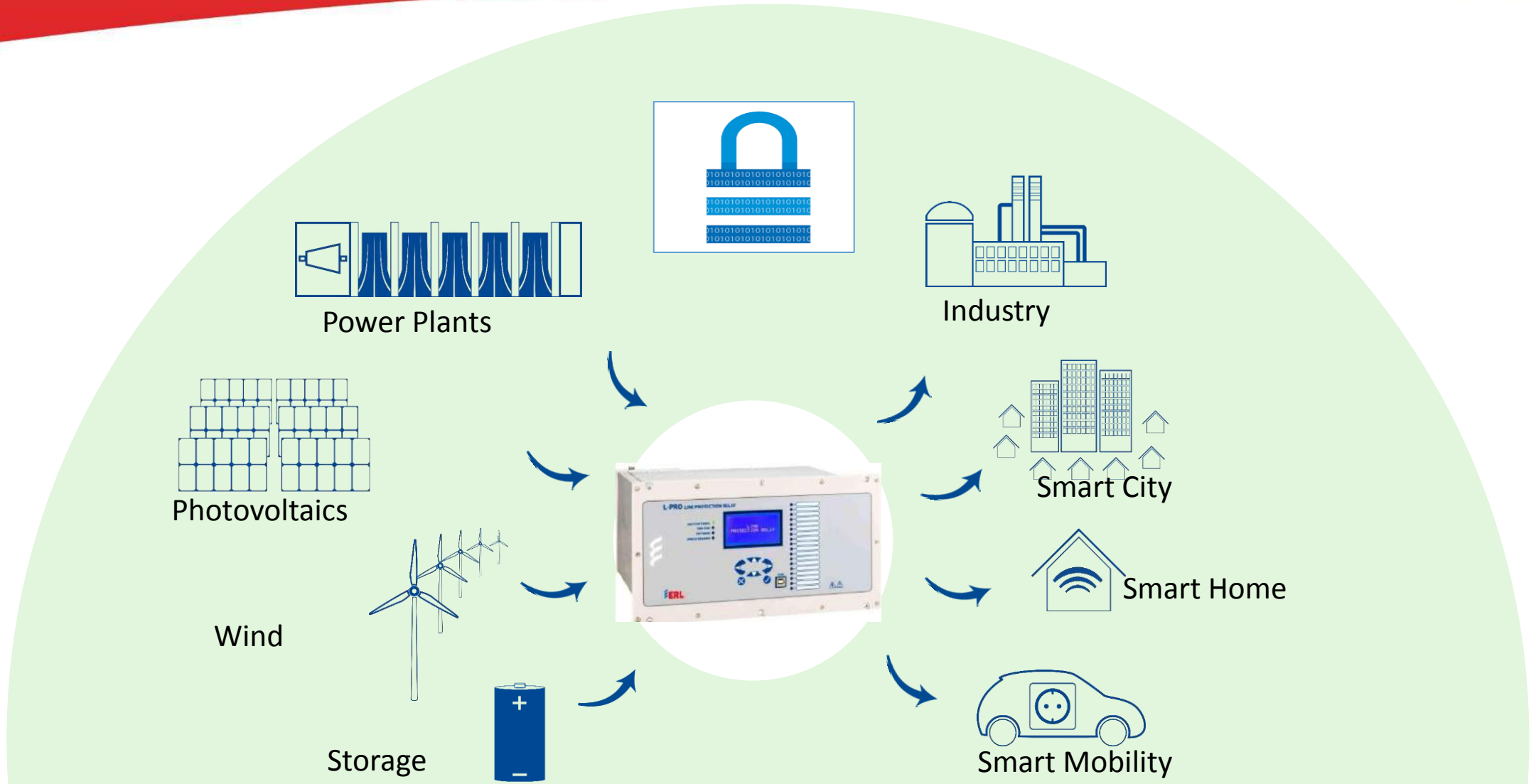
3 R's in Cyber Security

- **Recognize**
  - Identifying the source of the incident is paramount to minimizing the resulting damage.
  - Internal controls play a significant role in identifying a hacker's point of entry.
- **React**
  - An incident response plan to unauthorized access should be able to cut off the access point, slow down the intruder, preserve the environment that has been compromised.
  - This can be accomplished through proactive monitoring, user training and a layered security approach.
- **Recovery**
  - The environment that had the compromised / crashed data may require the implementation of long-term corrections; First priority goes to fixing the problems that led to the breach

Conclusion



SECURED AUTOMATION



For Secure Energy Systems

THANKS !!!