CYBERSECURITY OF ELECTRICAL POWER SYSTEMS

Dr. Murty Yalla

Distribution Protection and Control Track
Thursday, August 7, 2025
Day 4 – Session 3

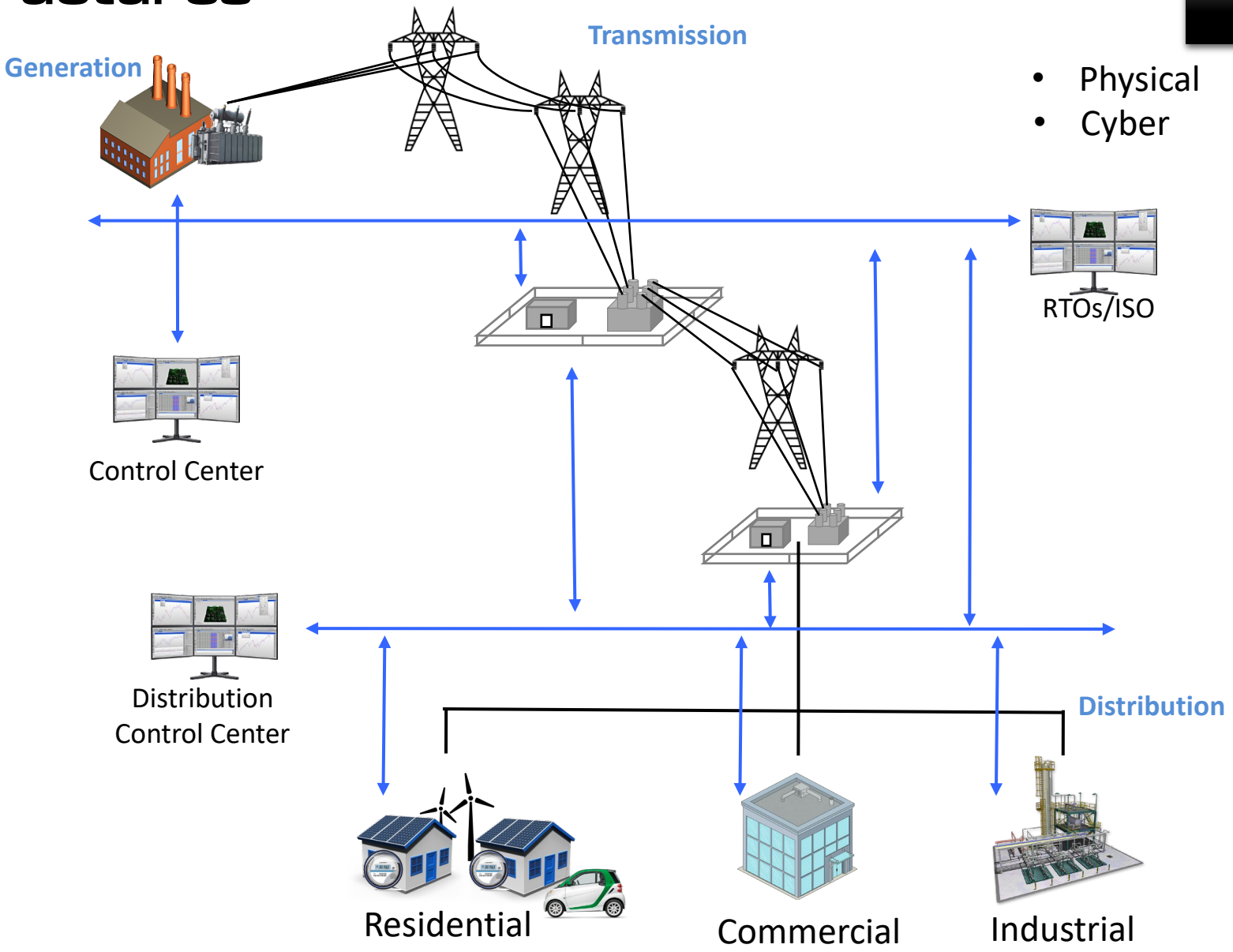
Outline

- Cybersecurity Definitions
  - Physical and Cyber Infrastructures
  - RISKS (Viruses, Worms, Trojan, Key loggers, Denial of Service)
  - Assets
  - Management
- Industry Standards on Cybersecurity
  - IEEE, IEC, NIST, NERC
- Cybersecurity of Distribution Protection and Control IEDs
  - Ukraine Attack
  - Cyber Attack on Distribution Volt-Var Control IEDs
  - How to Secure Electric Power Distribution Protection and Control Devices
    - IEEE 1686
    - RADIUS and LDAP for Password Management
    - Role Based Authentication
    - IPSec VPN Tunneling
- Conclusions

Two Infrastructures

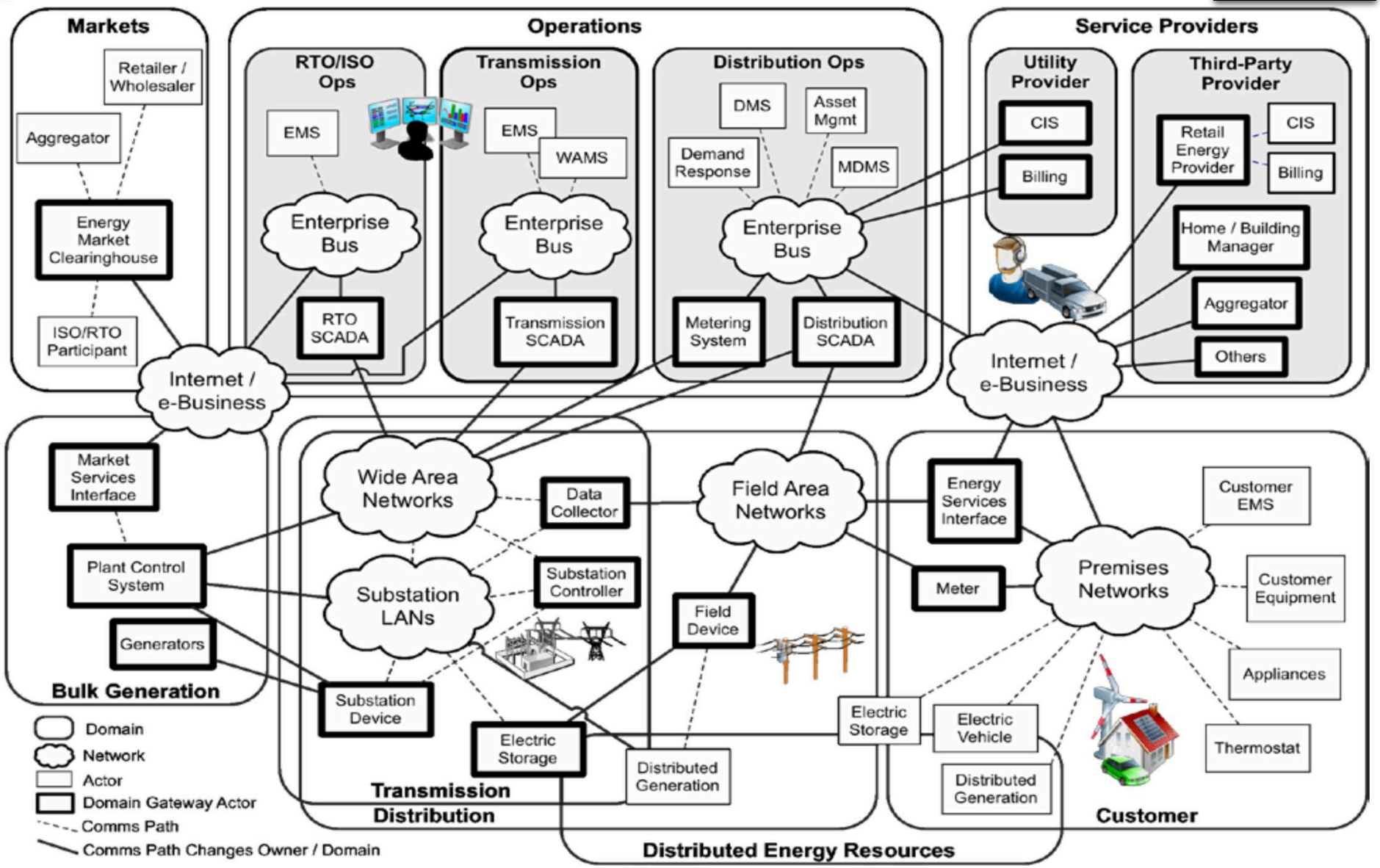
RISK

- Physical
- Cyber



NIST Smart Grid Infrastructure

RISK

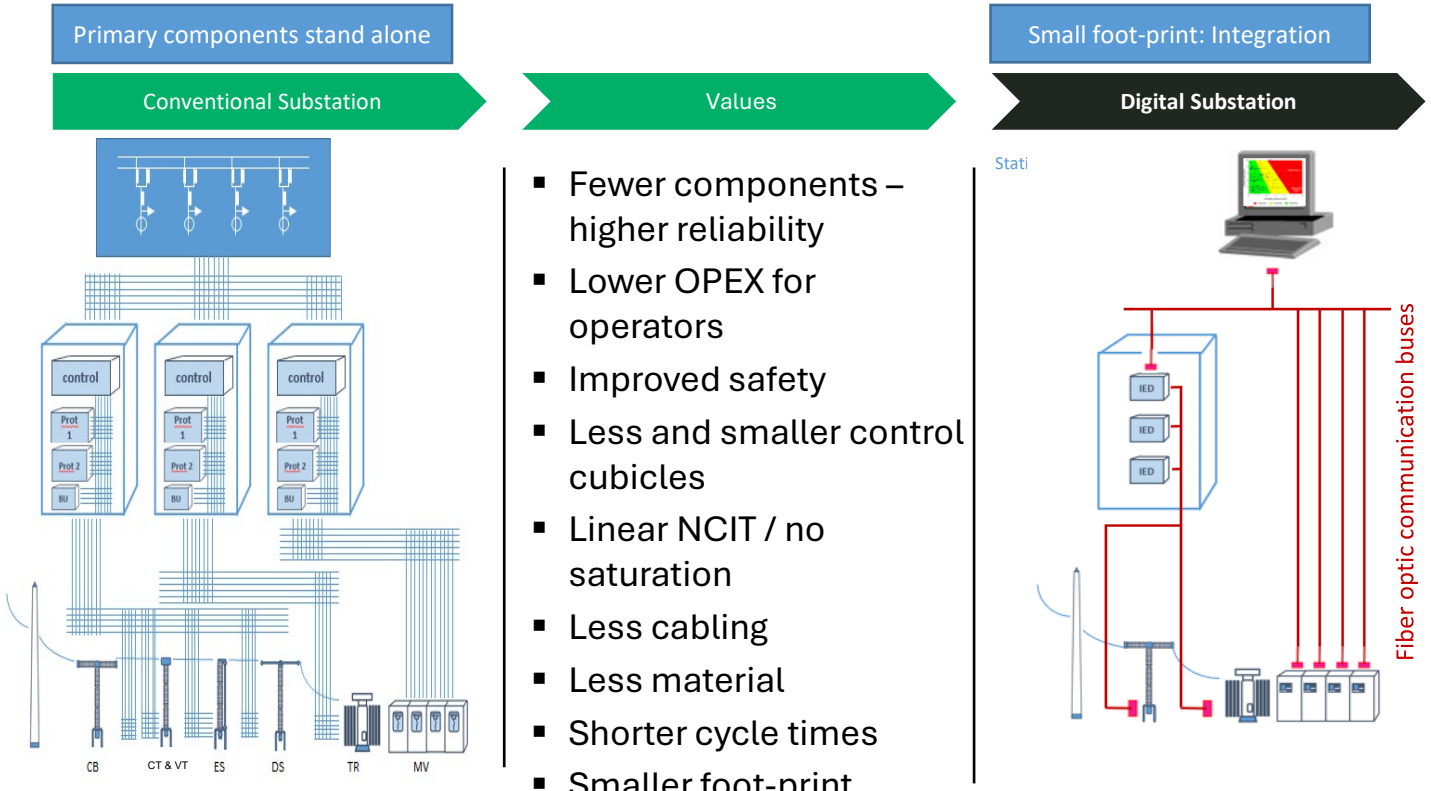


Source: NIST Smart Grid Framework

Trends on Digital Substation

RISK

Shift from a conventional to a digital substation



- Fewer components – higher reliability
- Lower OPEX for operators
- Improved safety
- Less and smaller control cubicles
- Linear NCIT / no saturation
- Less cabling
- Less material
- Shorter cycle times
- Smaller foot-print

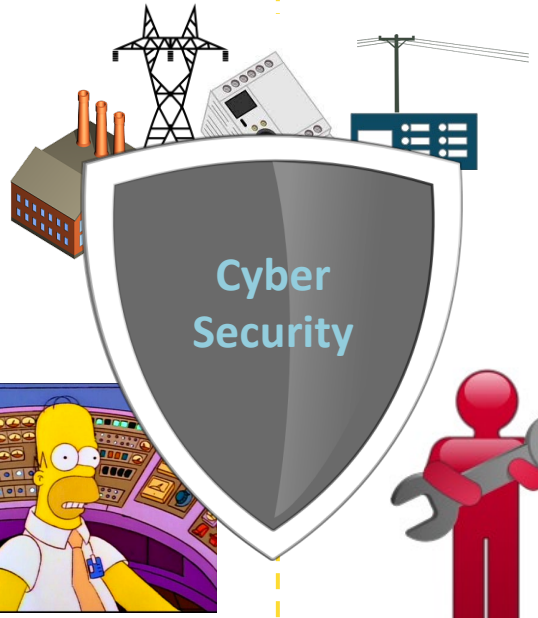
ETHERNET ARCHITECTURES AND OPEN PROTOCOLS REQUIRED – BRINGS CYBERSECURITY RISKS

RISK

Security: "The facet of reliability that relates to the degree of certainty that a **cyber device or** system will not operate incorrectly."

Cybersecurity = Physical + EMI + Digital[Computing & Communications]

Misconfiguration

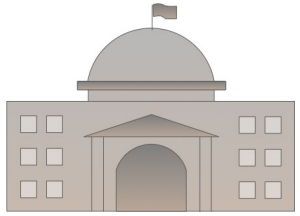


Hackers

Vendors

Accident
Insider

Intentional
Insider



Nation States

Malware: Virus | Worm | Trojan | Keylogger

RISK

Piece of software that infects a legitimate program, replicates and spreads to other computers when activated by a user

Computer Virus Hits U.S. Drone Fleet

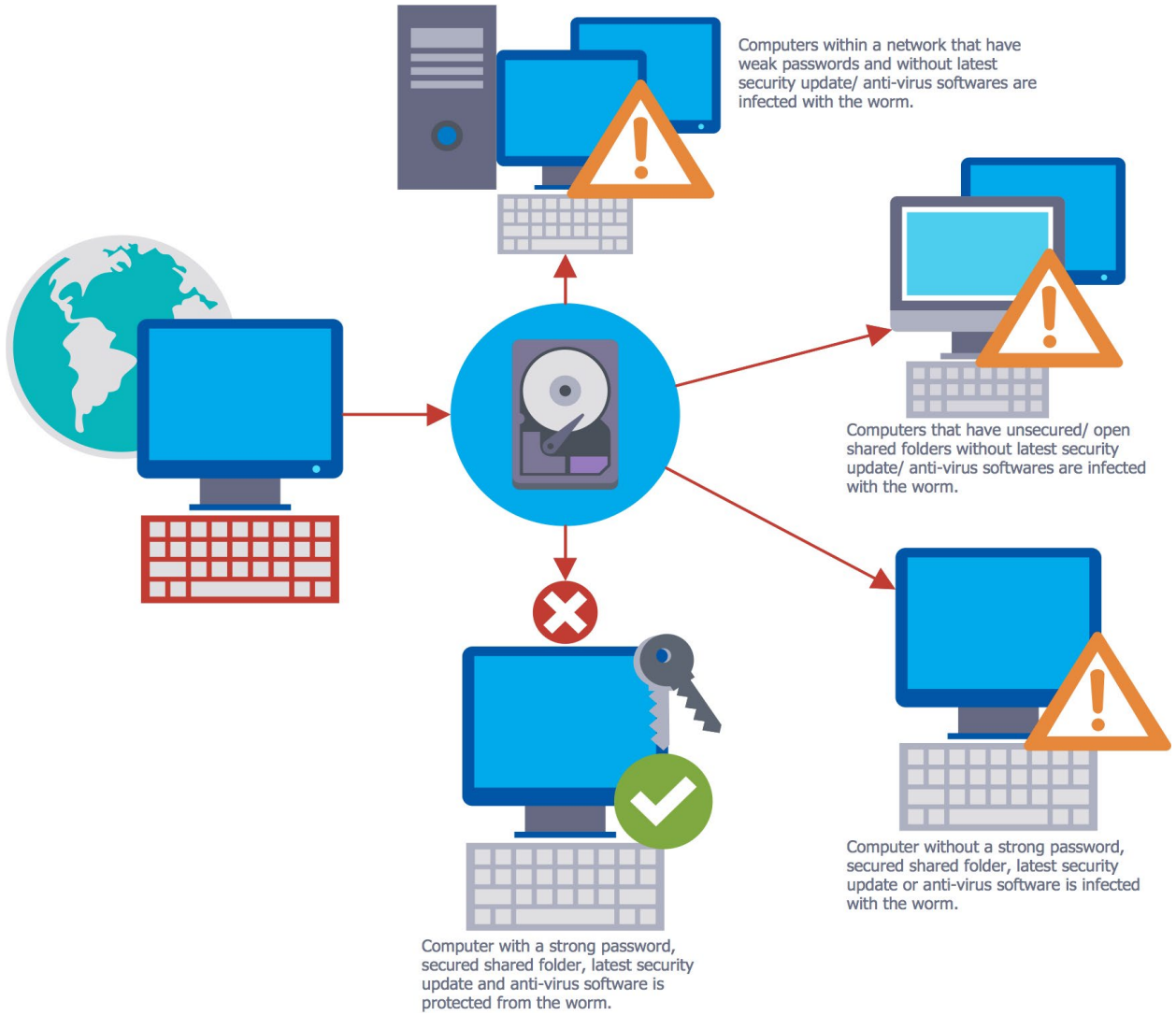
Src: https://www.wired.com/2011/10/virus-hits-drone-fleet/

"A COMPUTER VIRUS has infected the cockpits of America's Predator and Reaper drones, logging pilots' every keystroke as they remotely fly missions over Afghanistan and other warzones."

Recently GPS spoofing crashed drones.

Malware: Virus | Worm | Trojan | Keylogger

RISK



Worms are similar to a viruses but are self-replicating and will spread to other computers automatically.

Examples:

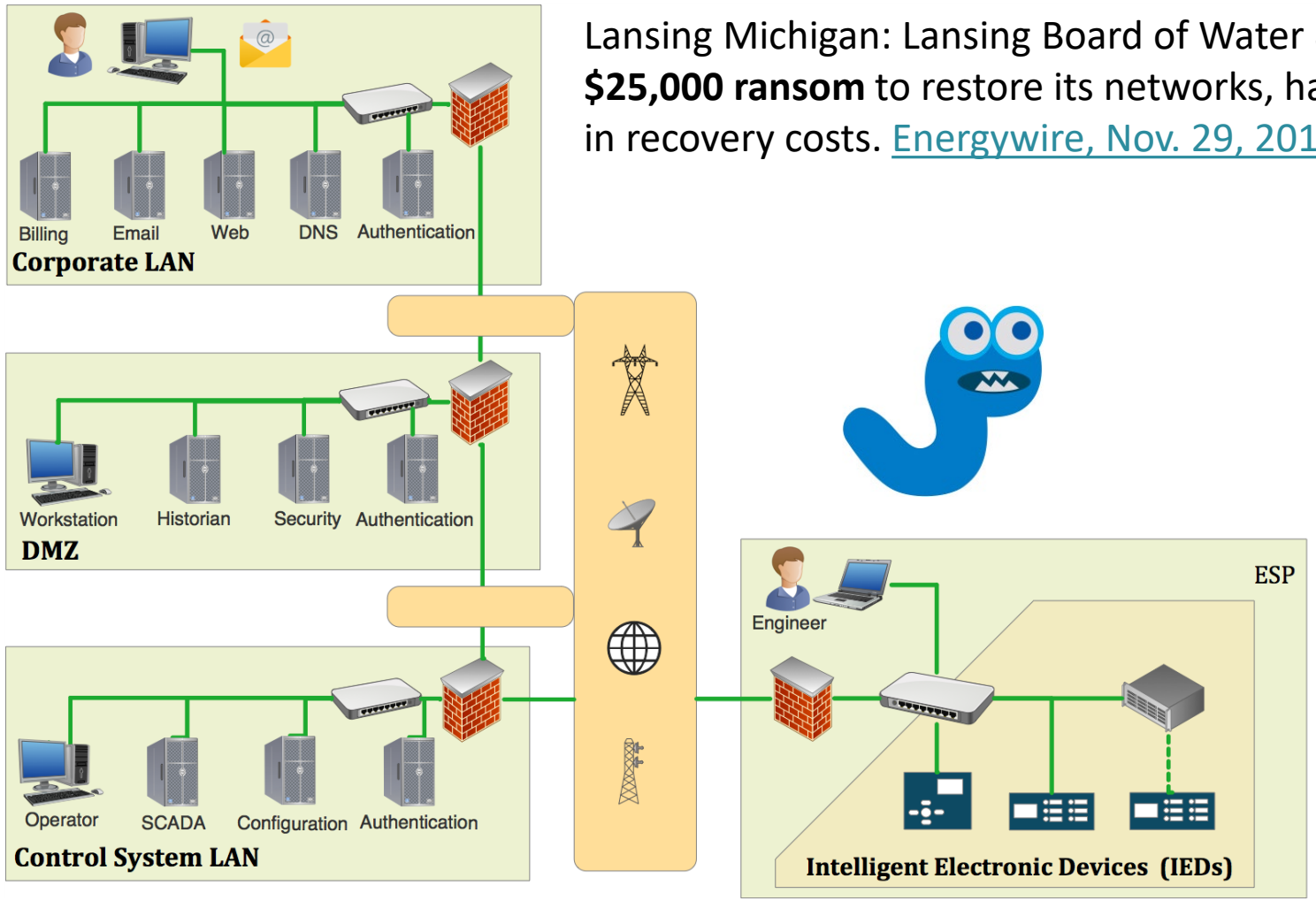
Variants of Ransomware

Stuxnet (attacks SCADA systems and PLCs)

Malware: Virus | Worm | Trojan | Keylogger

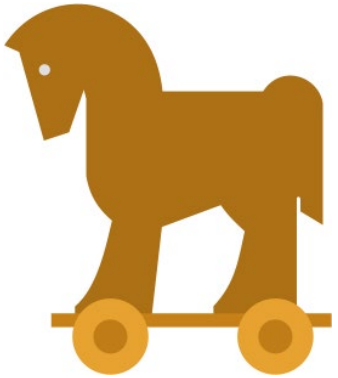
RISK

Lansing Michigan: Lansing Board of Water & Light paid a **$25,000 ransom** to restore its networks, had nearly **$2.4 million** in recovery costs. Energywire, Nov. 29, 2016.



Malware: Virus | Worm | Trojan | Keylogger

RISK



A trojan horse:

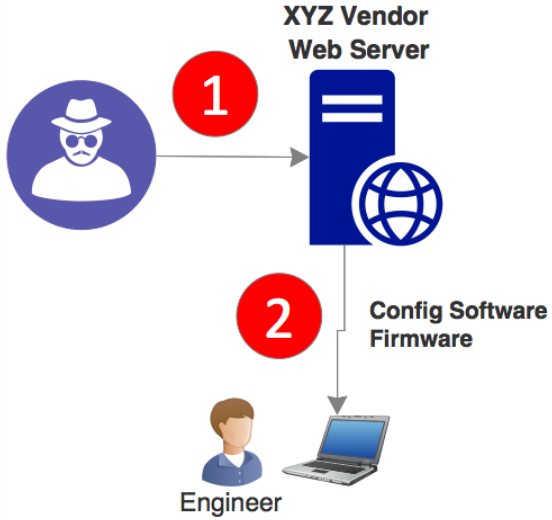
- Is an attack vector or mechanism to get malicious software installed on victim's machine.
- They appear to have a useful function but have a malicious function that evades security mechanisms.

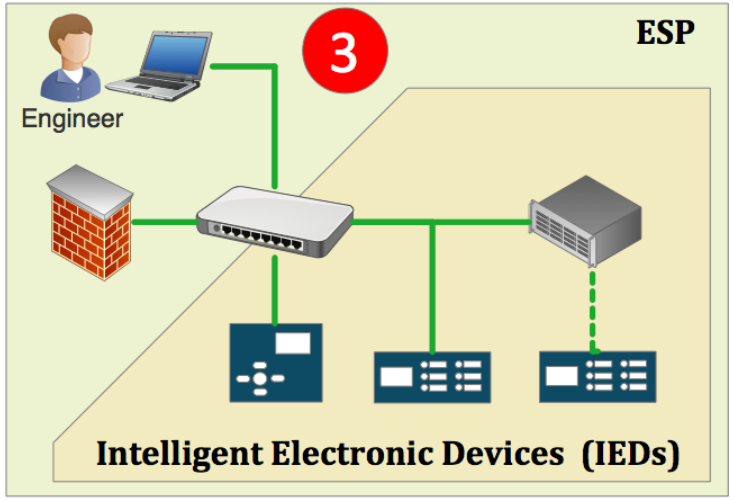
Example: Watering hole attack to install Remote Access Trojan (RAT)

(1) Infiltrate vendor's server

(2) User downloads software

(3) User infects critical LAN



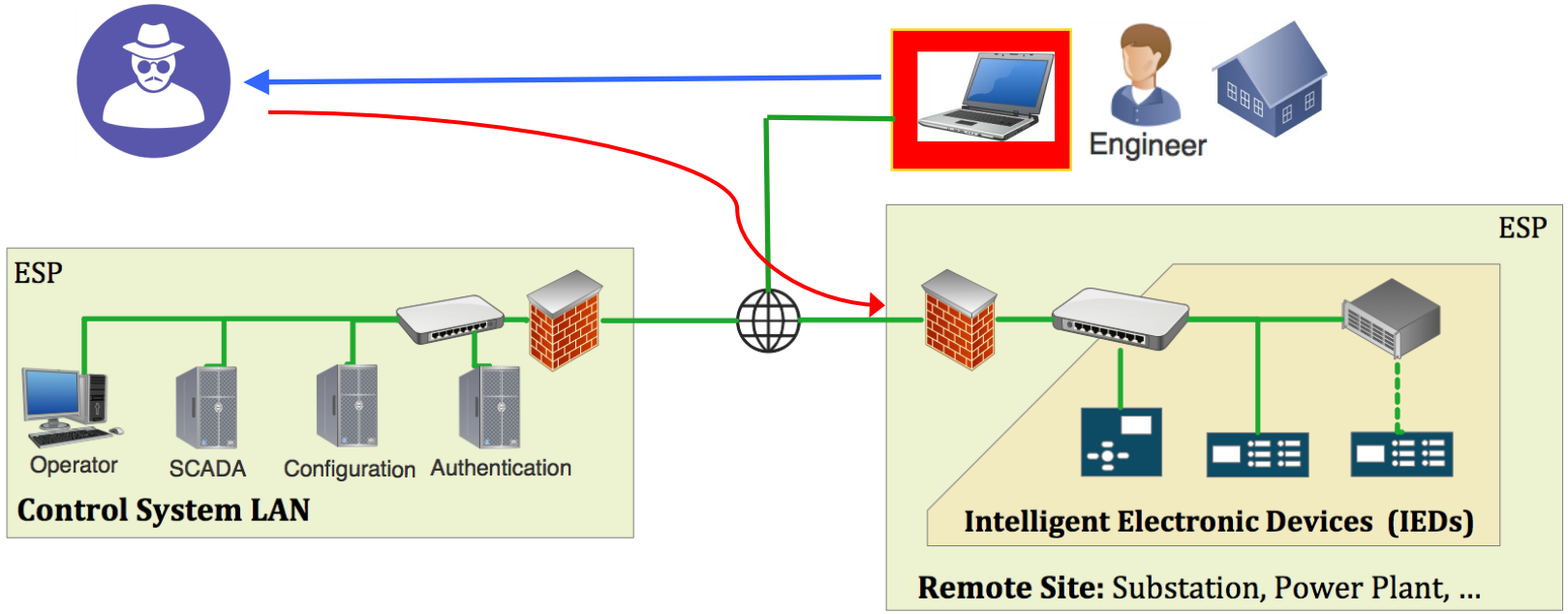


Recommended Reading: https://www.f-secure.com/weblog/archives/00002718.html

Malware: Virus | Worm | Trojan | Keylogger

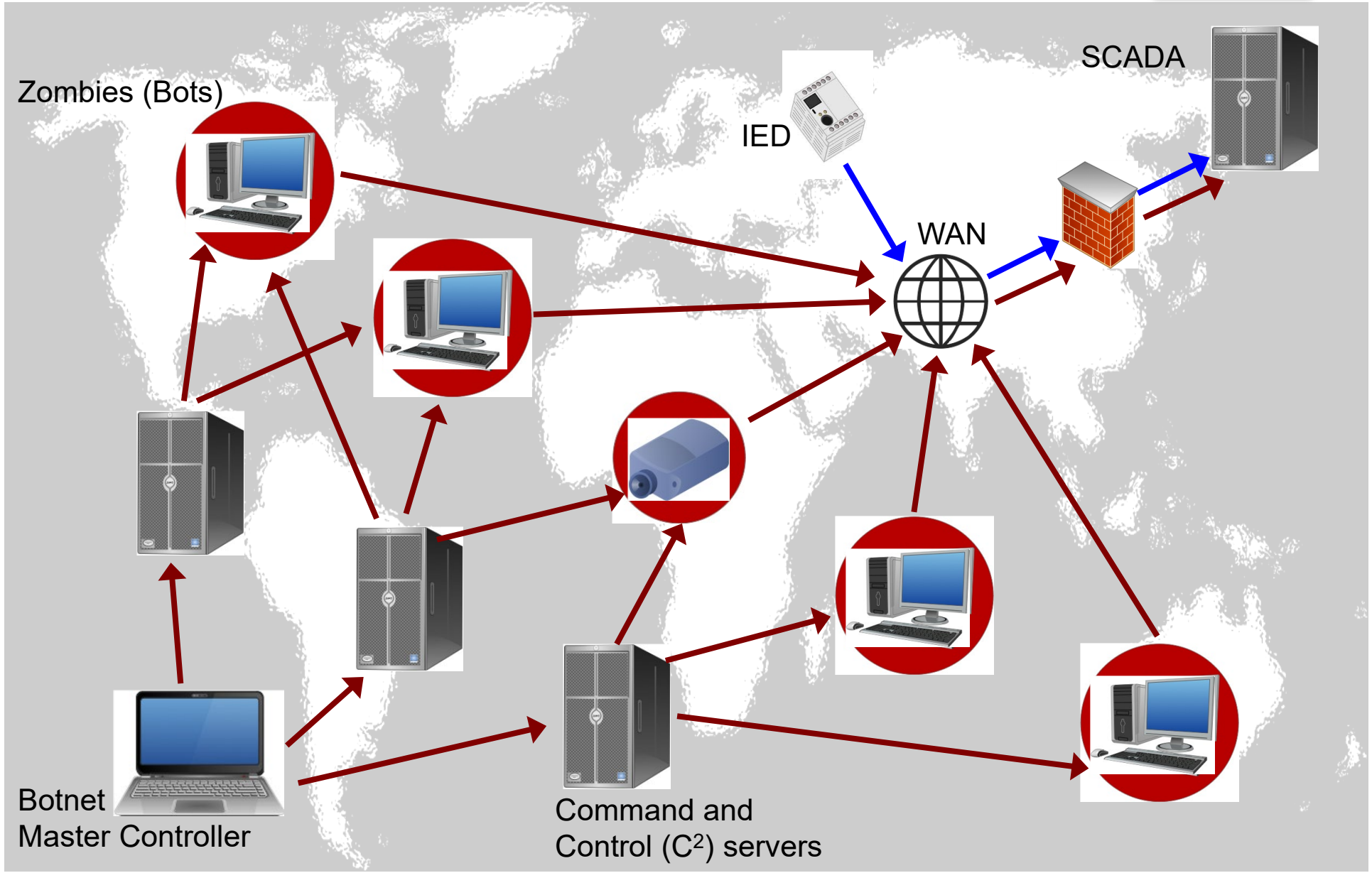
RISK

Keyloggers are specialized malware that monitor the computer and record anything that is typed onto the keyboard, transmitting that data out to the attacker.



Denial of Service (DoS)

RISK



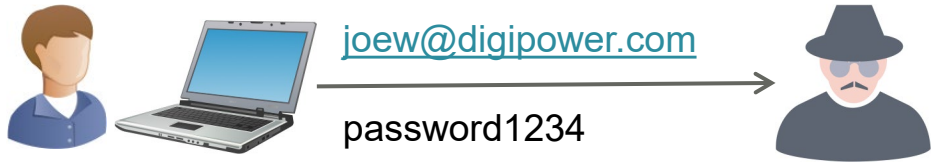
Malware: Virus | Worm | Trojan | Spyware | Keylogger

Engineer, Operator, Technician

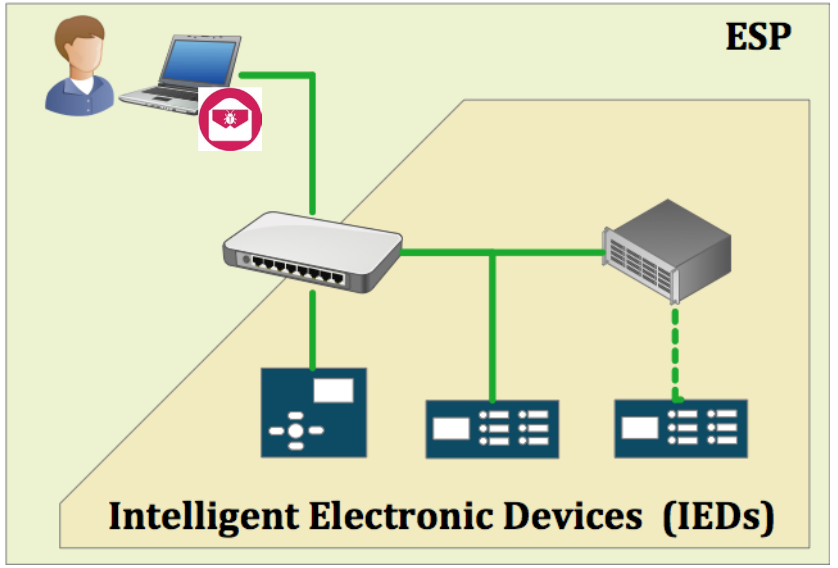
Phishing

RISK

Scenario I: Victim sends user credentials



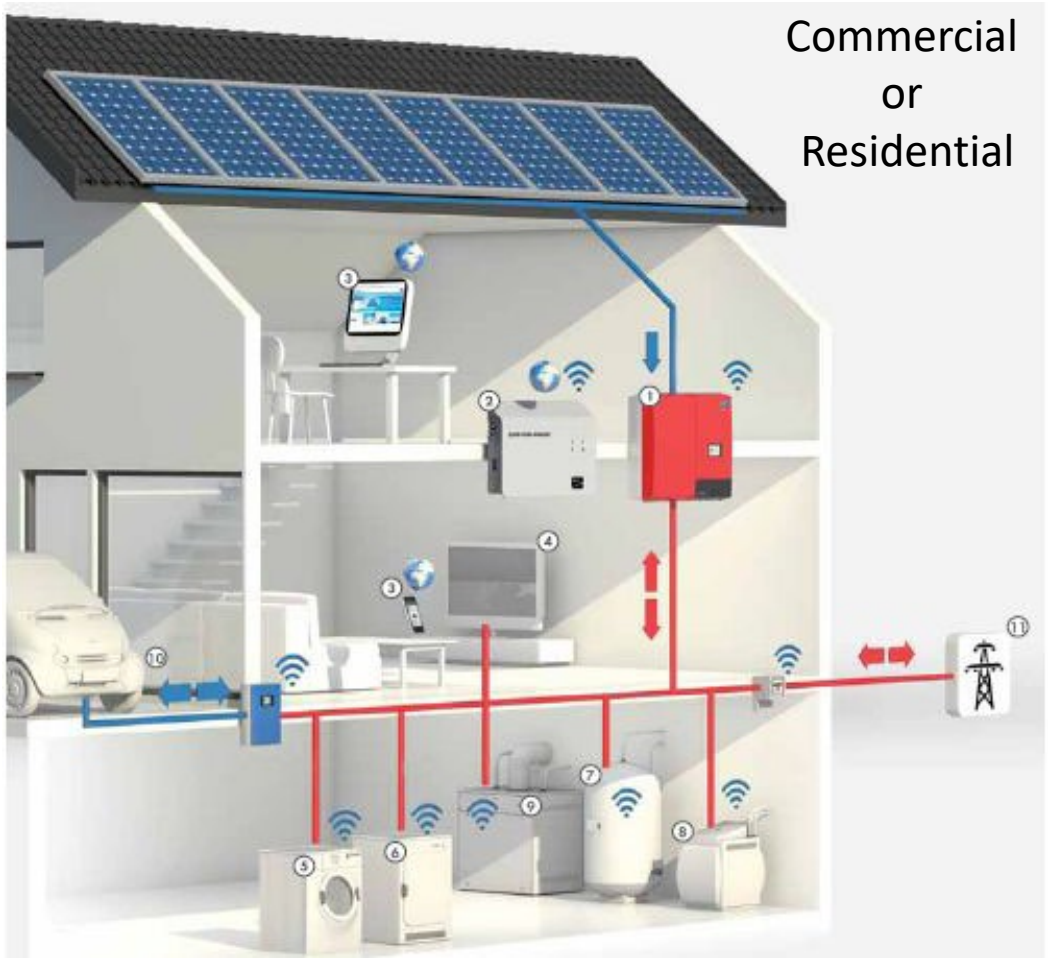
Scenario II: Malicious software jumps air-gap



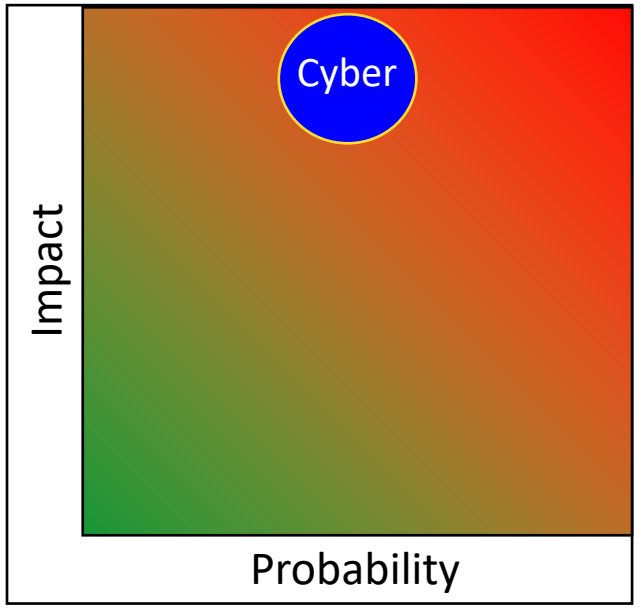
RISK = (Threat x Vulnerability) x (Impact) (Probability)

RISK

Example: Alter software on Smart Inverter



Source: http://acesolar.co.uk/services/solar-pv-panels/

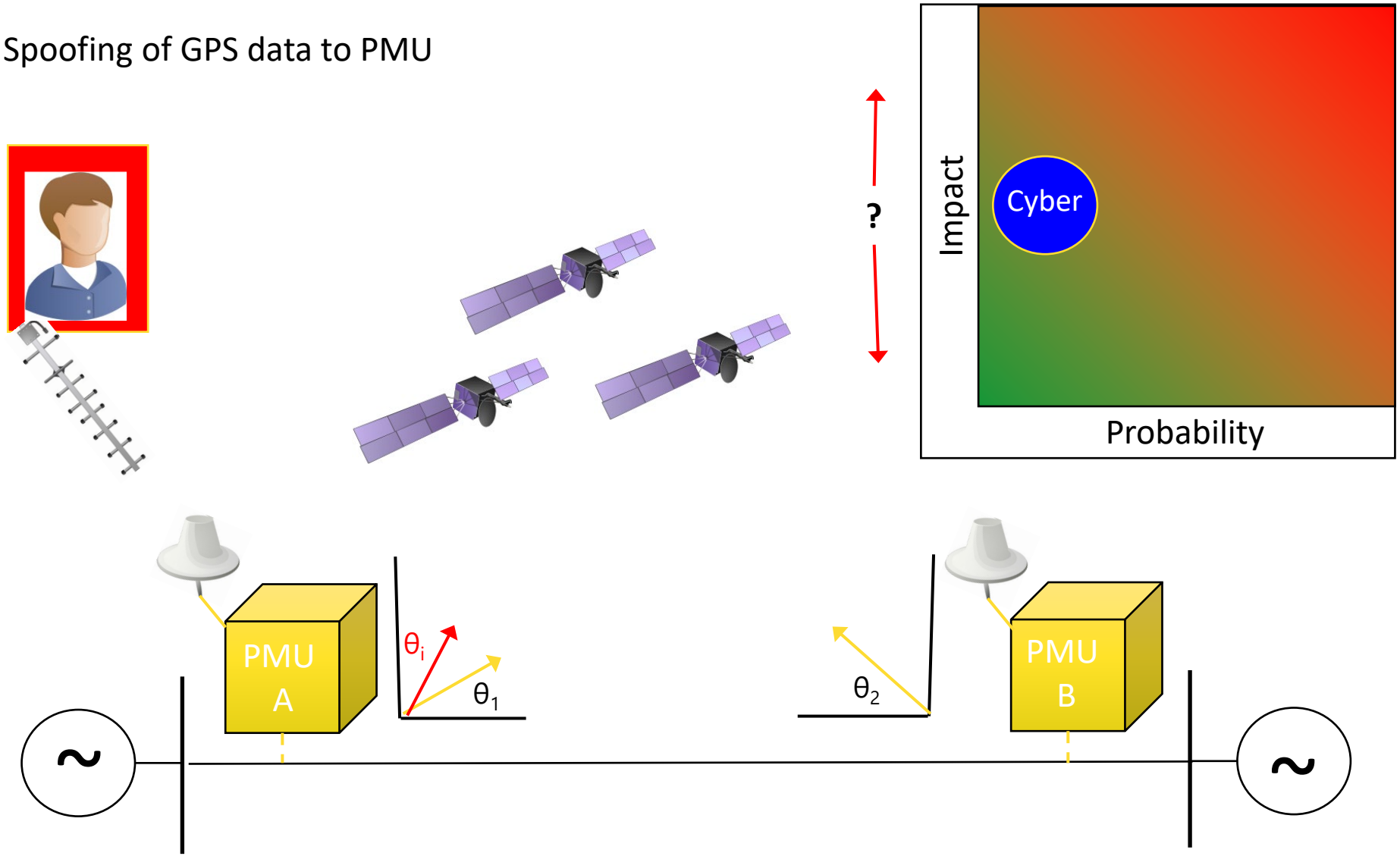


- Cloud based management
- Code on device to detect faults
- Remote V and f control
- Regulates energy flows
- Dispatchable

RISK = (Threat x Vulnerability) x (Impact) (Probability)

RISK

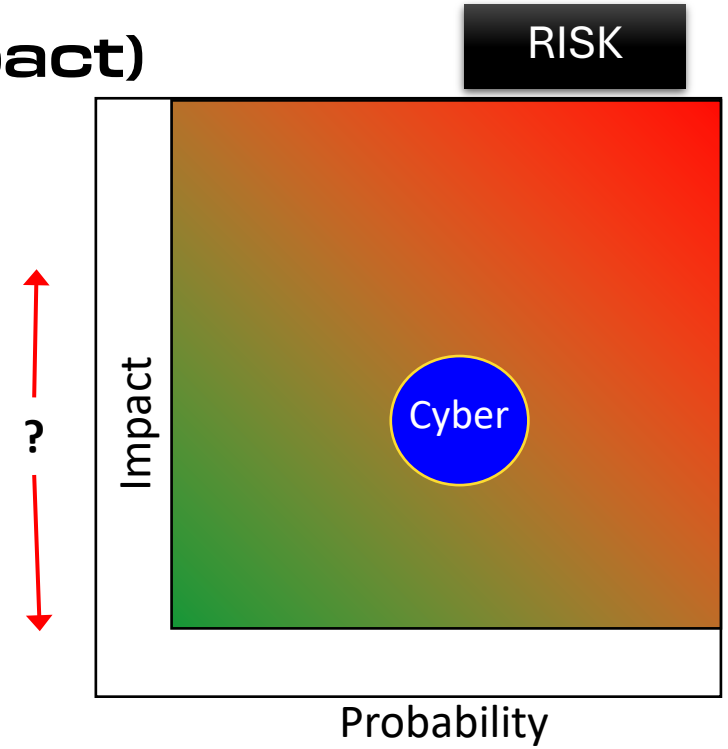
Example: Spoofing of GPS data to PMU



RISK = (Threat x Vulnerability) x (Impact) (Probability)

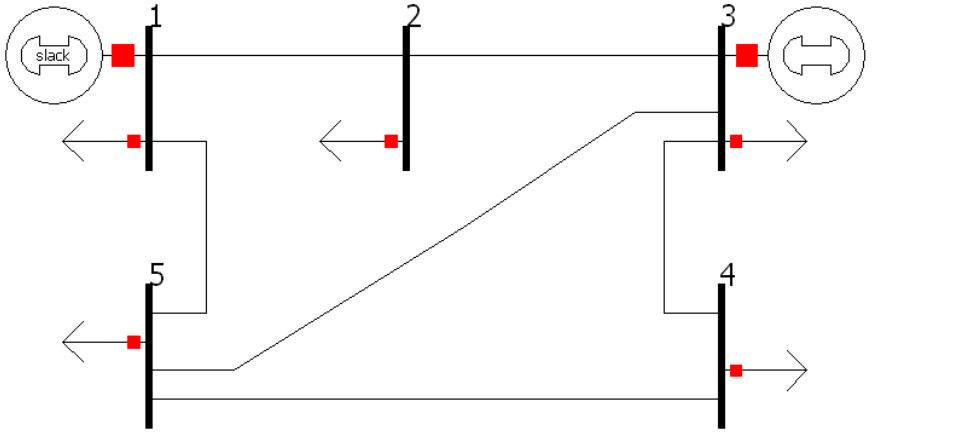
Example: State Estimation Attack, Spoofing State Variables

Remote SCADA or Local Automation



Injected Readings

Line Flows			
Bus	To Bus	MW	MVAR
1	2	73.98	33.78
	5	95.69	40.23
2	1	-71.4	-23.5
	3	-43.5	-33.1
3	2	44.59	37.28
	4	40.47	22.3
	5	24.94	19.23
4	3	-38.7	-15.4
	5	-31.2	-8.4
5	1	-92.6	-27.6
	3	-24.4	-17.2
	4	32.04	11.6



Malware: Virus | Worm | Trojan | Spyware | Keylogger

RISK

Social Engineering

Scenario I: Attacker conveniences IT Dept. to reset password for user: joew and gains remote access to ESP.

Scenario II: Attacker poses as network admin and gains access to PSP.

Video of Pen-Testing team hacking and social engineering their way into a small power company: https://youtu.be/pL9q2lOZ1Fw

Cyber Assets

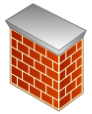
ASSETS

Laptop 

Computer 

Switch 

Media Converter 

Firewall 

Radio 

RTU 

Relay 

Meter 

PLC 

Programmable electronic **devices**, including the

hardware,

I/O cards
Network cards
CPU, RAM, Physical Ports

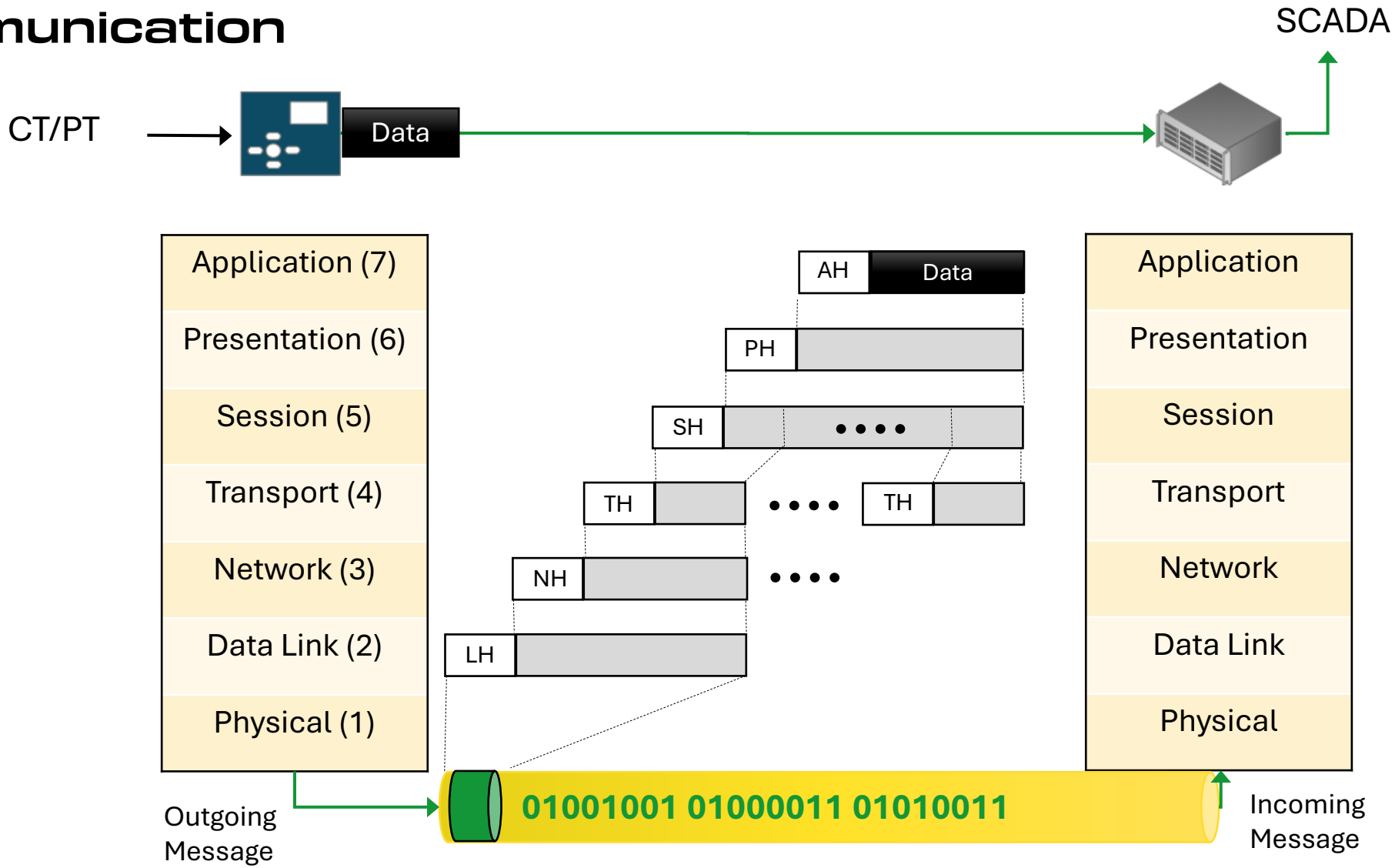
software, and

User Applications (EMS, HMI, FTP, Apache, etc.)
Device Applications (Protocol Parsers/Converters)
Application Programming Interface (API)
Software Libraries and Tools

data, in those devices.

Settings and Configuration Files
Stored Binary and Analog Values
Sequence of Events & DFR Logs
Usernames, Password Hashes, IP Tables

Communication



Open Systems Interconnection (OSI) Model

Protection and Control of the Digital Grid

Management

Event Monitoring

Functions	Physical Infrastructure (Flow of Power)	Cyber Infrastructure (Computation & Communication)
Identify	-Loads, transformers, breakers, cap banks	-Cyber Assets
Protect	-Controls, Relays, RTUs, EMS, IED settings configuration	-Controls, Firewalls, data-diodes, IED setting configuration
Detect	-Relay Protection Logic, Primary & Back-up, SCADA	-IEDs, Relays, RTUs, SCADA Firewalls, IDS
Respond	-Isolate Fault, reclose, lockout, open, close, SOE	-Remove access, SOE Digital forensics, drop packets
Recover	-open, close, +/- Vars, Watts	-Backups, Replace

NIST. *Framework for Improving Critical Infrastructure Cybersecurity*, V1, 2014

Vulnerability Handling and Incident Response

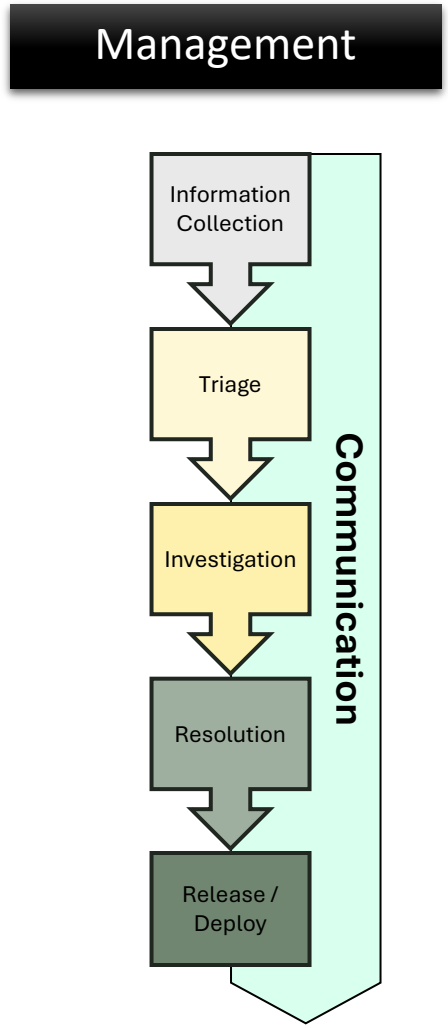
Minimize risk

Vendor Responsibility

- Cultural change: Accept that vulnerabilities exist
  (having a vulnerability is acceptable, improperly handling them is not!)
- Formal processes and policies
- Proper communication at the right time

Utility Responsibility

- Awareness: continuous monitoring of product updates to ensure software versions are assessed and implemented
- Cultural change: Accept that vulnerabilities will require patches and firmware upgrades



Industry Standards on Cybersecurity

Standards

- NISTIR 7628 Guidelines for Smart Grid Cybersecurity

- IEEE standards and Guides
  - IEEE Std 1686-2022 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities (under revision)
  - IEEE 1711.1 Standard for Serial SCADA Protection Protocol (SSPP)
  - IEEE 1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP)
  - IEEE C37.240-2014 Cyber Security Requirements for Substation Automation, Protection and Control Systems (presently under revision)
  - IEEE 1815 (DNP3) Secure Authentication
  - IEEE 1547.3 “Guide for Cybersecurity of DERs Interface with Electric Power Systems”) under revision at present.

- IEC 62351: Power systems management and associated information exchange – Data and communications security

- NERC - CIP standards

IEEE PES Power Systems Communications and Cybersecurity (PSCC) Committee

Standards

WG S1: 1686 IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities

Chair: Marc Lacroix **Vice-chair:** Éric Thibodeau

Scope: The standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Confidentiality, integrity and availability of external interfaces of the IED is also addressed.

WG S2: P1711.1 Standard for Serial SCADA Protection Protocol (SSPP)

Chair: Ed Cenzon

Scope: This standard defines the Substation Serial Protection Protocol (SSPP), a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol.

WG S3: P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems

Chair: Jim Bougie **Vice-chair:** Marc Lacroix **Secretary:** James Formea

Scope: This standard specifies requirements for interoperability of devices utilized within utility control systems which implement the Internet Protocol Security (IPsec) protocol suite within an IPv4 environment.

WG S4: P1711.2 Standard for Secure SCADA Communications Protocol (SSCP)

Chair: Scott Mix **Vice-chair:** Mark Hadley **Secretary:** James Formea

Scope: This trial use standard defines a cryptographic protocol to provide integrity with optional confidentiality for cyber security of substation serial links. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol.

IEEE PES Power Systems Communications and Cybersecurity (PSCC) Committee

Standards

TF S9: Task Force on Utility IT-OT Cybersecurity challenges in roles and terminology

Chair: Theo Laughner **Vice-chair:** Brian Smith

A core theme from the IEEE Cybersecurity workshop was the utility need for IT and OT collaboration to address cybersecurity differences (culture, application, perspective and terminology)
Scope: Assess the IT-OT challenge in Utility Cybersecurity roles and create a report to assist in building organizational understanding and collaboration

TF S10: Task Force on Utility & municipality challenges on understanding cybersecurity standards

Chair: Jeff Pack **Vice-chair:** Steve Mark

Scope: Assess the challenge in utilities & municipalities with limited resources on the applicability and relevance of the cybersecurity standards and create a report to assist summarizing the relevant cybersecurity standards

WG S13: Review 1547.3 Guide for Cybersecurity of DERs Interface with Electric Power Systems

Chair: Anthony Johnson **Vice-chair:** Benjamin Kazimier
Scope: Review the proposed SCC21 PAR for IEEE 1547.3 and make recommendations on how to proceed.

Status: The Study Group met to discuss the SCC21 proposed PAR for IEEE 1547.3 and make a recommendation on how to coordinate. The recommendation was for the PSCC to form a Work Group to jointly develop 1547.3 with SCC21. WG formation received PSCC Main Committee approval.

NERC CIP Standards

Standards

(CIP) Critical Infrastructure Protection (91)

Subject to Future Enforcement (5)

CIP-005-6	Cyber Security — Electronic Security Perimeter(s)
CIP-008-6	Cyber Security — Incident Reporting and Response Planning
CIP-010-3	Cyber Security — Configuration Change Management and Vulnerability Assessments
CIP-012-1	Cyber Security – Communications between Control Centers
CIP-013-1	Cyber Security - Supply Chain Risk Management

Subject to Enforcement (11)

CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-8	Cyber Security — Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security

TASK FORCE ON
Security Integration into BPS Engineering Practices

Task Force Chairs
Ryan Quint, NERC
Larry Collier, NERC
Dan Goodlett, NERC
John Stewart, EPRI

Sub-Group Leads
Richard Alcalde, Con Edison
Sam Chanoski, INL
Johnny Gest, RF
Jessica Harris, NERC
Mohammad Reza Khalghani, FPU
Roger Hales, Contractor (NERC)
David Sopata, RF
John Stewart, EPRI

IEEE PES-NERC Liaison
Murty Yalla, Hubbell (Beckwith Electric BU)

Members

Aaron Shaw	David Wallach	Jodi Jensen	Reynaldo Ramos
Alekhya Vaddiraj	Deepak Maragal	John Anasis	Scott Mix
Alex Benoliel	Dennis Holstein	John Skeath	Scott Morris
Anthony Johnson	Dmitry Kosterev	Manuel Avendaño	Shaun Murphy
Bo Chen	Eric Howell	Joseph Januszewski	Song Wang
Carter Manucy	Eric Ruskamp	Kevin Grant	Stephen Trachian
Charles Abell	Eriks Surmanis	Lingyu Ren	Steven Briggs
Chip Wenz	Evan Paull	Marie Whyatt	Steven Kunsman
Chris Holmquest	Hamody Hindi	Mario Roberto Jardim	Theo Laughner
Christopher Reali	Herb Falk	Marjorie Parsons	Tom Hofstetter
Craig Preuss	Hongyu Wu	Michael Legatt	Tony Eddleman
Curtis Dorcheus	Jalal Gohari	Michael Sanders	Warren Wu
Darrell Klimitchek	James Formea	Olushola Lutalo	Wei Sun
Darren Hulskotter	Jay Anderson	Phil Clark	Will Edwards
David Revill	Jay Cribb	Philip Huff	Xin Fang

IEEE Power & Energy Society

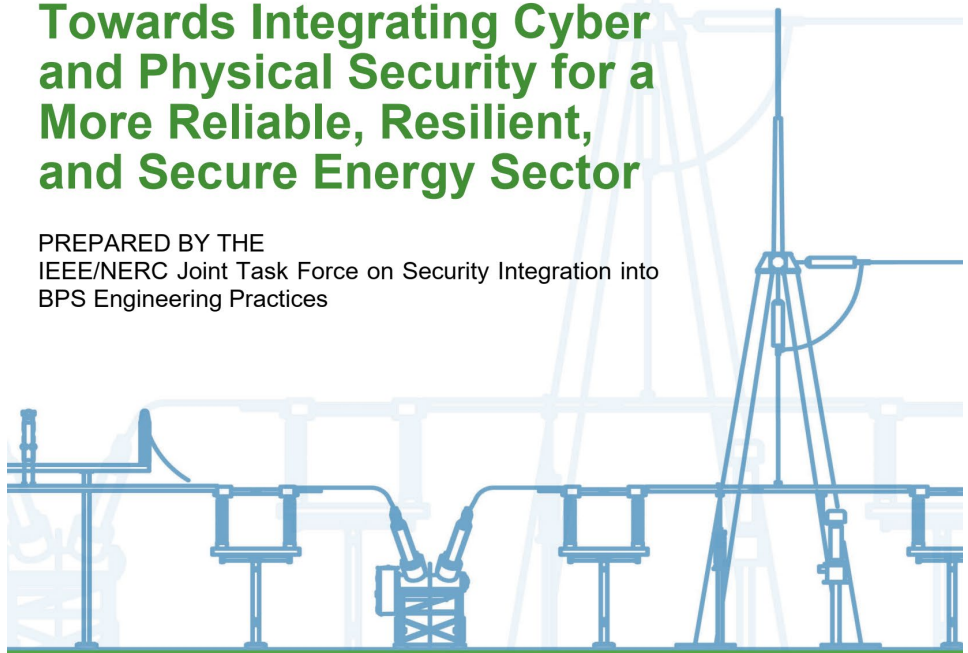
December 2022

TECHNICAL REPORT

PES-TR105

Towards Integrating Cyber and Physical Security for a More Reliable, Resilient, and Secure Energy Sector

PREPARED BY THE
IEEE/NERC Joint Task Force on Security Integration into BPS Engineering Practices



© IEEE (2022) The Institute of Electrical and Electronics Engineers, Inc.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Cybersecurity of Protection and Control IEDs Concerns

- Modern Distribution systems incorporate IEDs which communicate with Distribution Management Systems (DMS).
- The protection/control IEDs and DMS typically send commands to open/close breakers, Reclosers and switches.
- The DMS also sends commands to raise/lower a tap position of a LTC transformer and Voltage Regulator, open/close capacitor banks etc
- All these actions use communications and a cyber attack on the communications system can create serious issues.

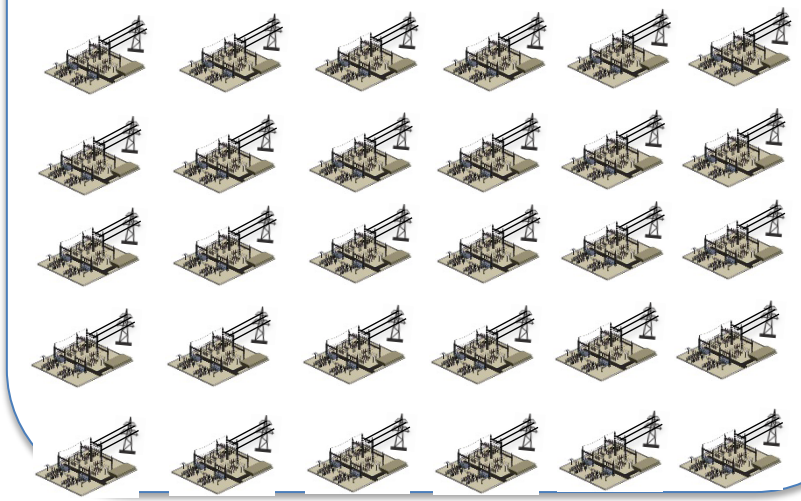
Cyber Attack on Distribution Protection and Control IEDs

- Compared to Generation plants and Transmission Substations the distribution system IEDs are not physically protected.
- Majority of these IEDs are outside the fence of a substation mounted on a pole near residential neighborhoods and highways and have no physical barrier to protect them.
- Unless end to end security is maintained it is not difficult to hack into any of these IEDs and send commands mimicking DMS system commands.

Ukraine Attack

Dec 23, 2015

30 Stations De-energized



- Spear phishing email with malware (*approx. 9 months prior to attack*)
- Hackers accessed critical systems (*SCADA, HMI, operator PCs, etc.*)
- Telephone denial of service (*Prevented calls going in/out)*
- Control Center's UPS shutdown
- Altered firmware at substations
- Implemented Kill-disk virus
- 7 - 110kV & 23 - 35kV dead stations
- 225,000+ customers affected ~6hrs
- **First known cyber attack to cause power outages**

"We were blinded"

"What hit us?"

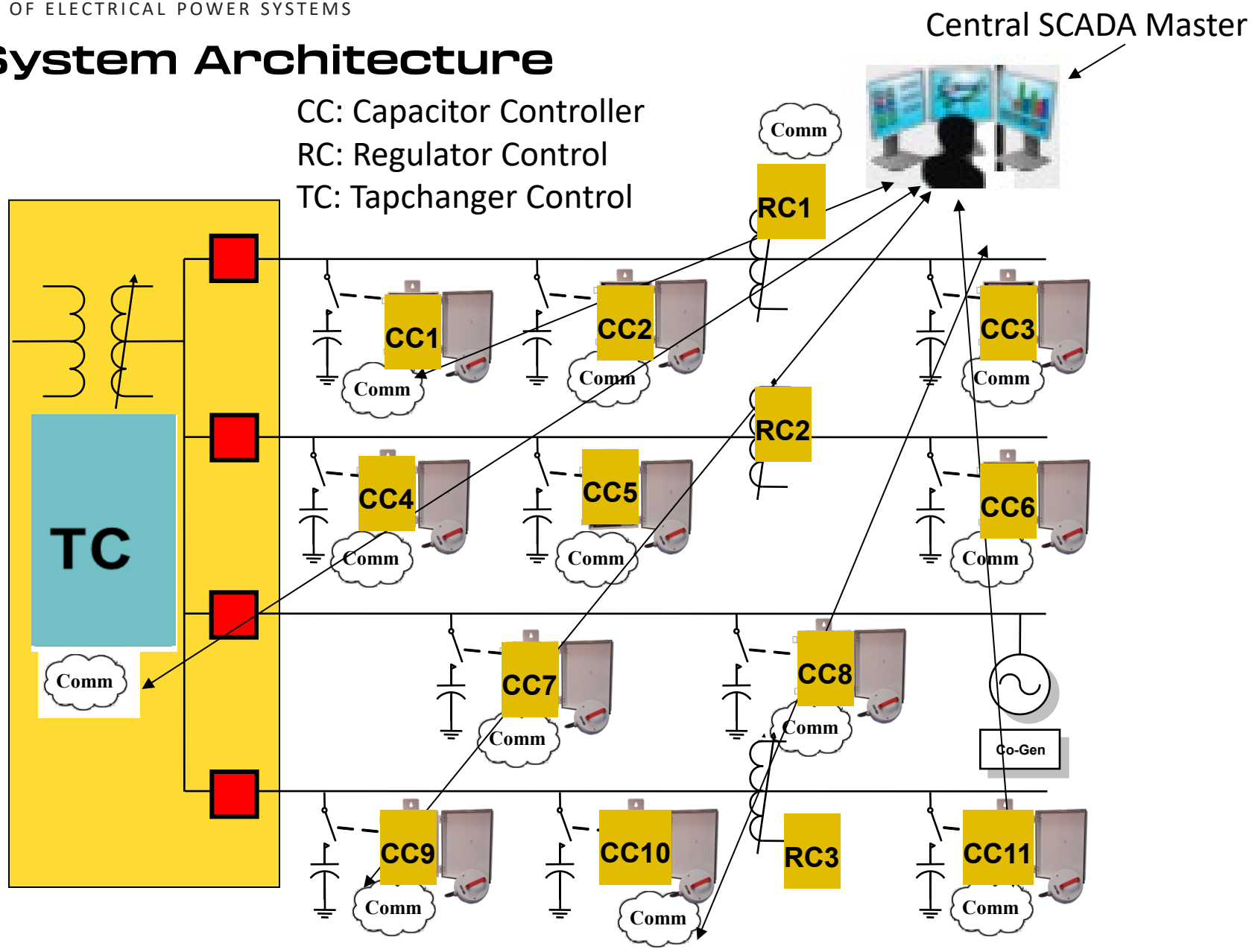
Control Center Operator

Source: E-ISAC. Analysis of the Cyber Attack on the Ukrainian Power Grid. March 18, 2016

Cyber Attack on Distribution Volt-Var Control IEDs

IVVC System Architecture

CC: Capacitor Controller
RC: Regulator Control
TC: Tapchanger Control



Cyber Attack on Distribution Volt-Var Control IEDs

Attack during a night when the load is light and the tap positions are on the lower end will be most severe.

Hypothetical Example: Conditions before the attack

Substation Transformer (TC) shows a tap position of 8L

Voltage Regulators (RC#1, RC#2 and RC#3) show a tap position of 4L

Capacitor banks (CC#1 to CC#11) all are OFF

Conditions after the attack: the hacker drives TC and RC#1 to #3 to 16R. Switches all Capacitor banks to ON.

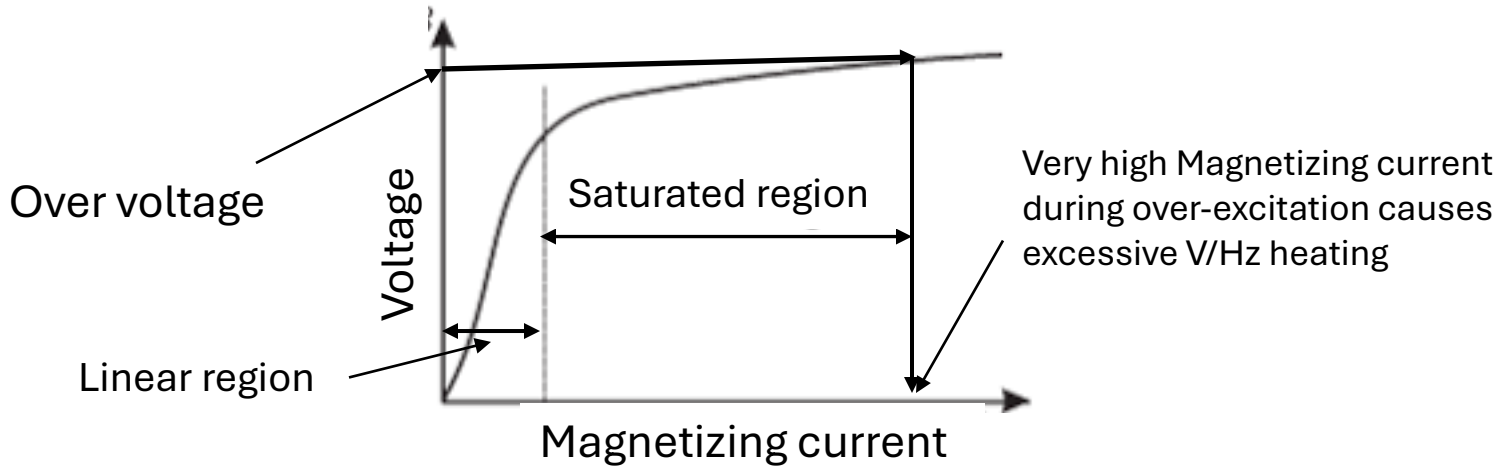
Now looking at the voltage on the feeder:

- *LTC transformer going from 8L to 16R will increase voltage by 15%*
- *Voltage regulator changing from 4L to 16R will increase the voltage by 12.5%*
- *Capacitor banks changing from OFF to ON position will increase the voltage by 5 to 10%*

The cumulative effect of these actions can have as much as 30 to 35% Overvoltage on the feeder causing sever damage to pole-top distribution transformers and customer equipment.

Overvoltage on the Distribution System

- Overvoltage on distribution system can have serious damage to the pole top distribution transformers which feed residential loads.
- Generally, there is no protection relays on these transformers except fuses.
- Fuses will not blow as the current will be below the full load current.
- The overvoltage results in severe overheating due to over-fluxing of the transformer core and the damage will be in few minutes.



Overvoltage on the Distribution System

- The consumer loads will also get damaged due to overvoltage. The power companies are regulated by the Public Utility Commissions to supply consumer loads with rated voltage ± 5%.

- The impact of a Cyberattack on the electric power distribution Volt-var control system can have serious consequences including damage to utility as well as consumer equipment.

- If a coordinated attack on several distribution substations takes place the damage can run into millions of dollars.

- The restoration of power can take a long time due to equipment damage.

How to Secure Electric Power Distribution Protection and Control Devices

Cybersecurity Implementation Example

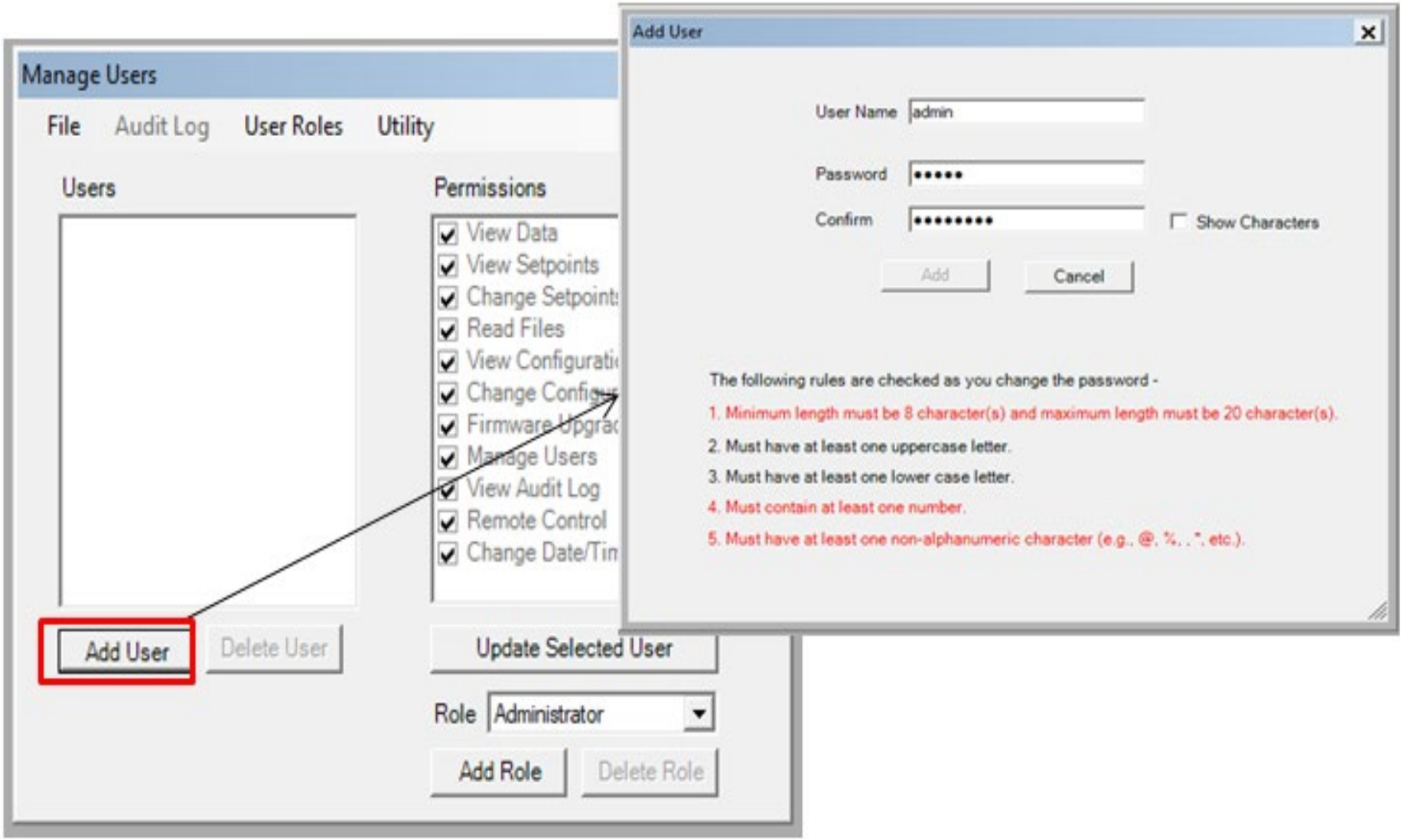
Capacitor Bank Controller

- Follows IEEE 1686 for local **authentication**
- DNP **Secure Authentication**
- **Intrusion Detection** via a micro-switch mounted on cabinet door
- Centralized **Authentication**, Authorization & Accounting:
  - RADIUS.
  - LDAP.
- IPsec/IKE provides **encryption** of data

IEEE 1686 “IEEE Standard for Intelligent Electronic Devices (IEDs) Cybersecurity Capabilities”

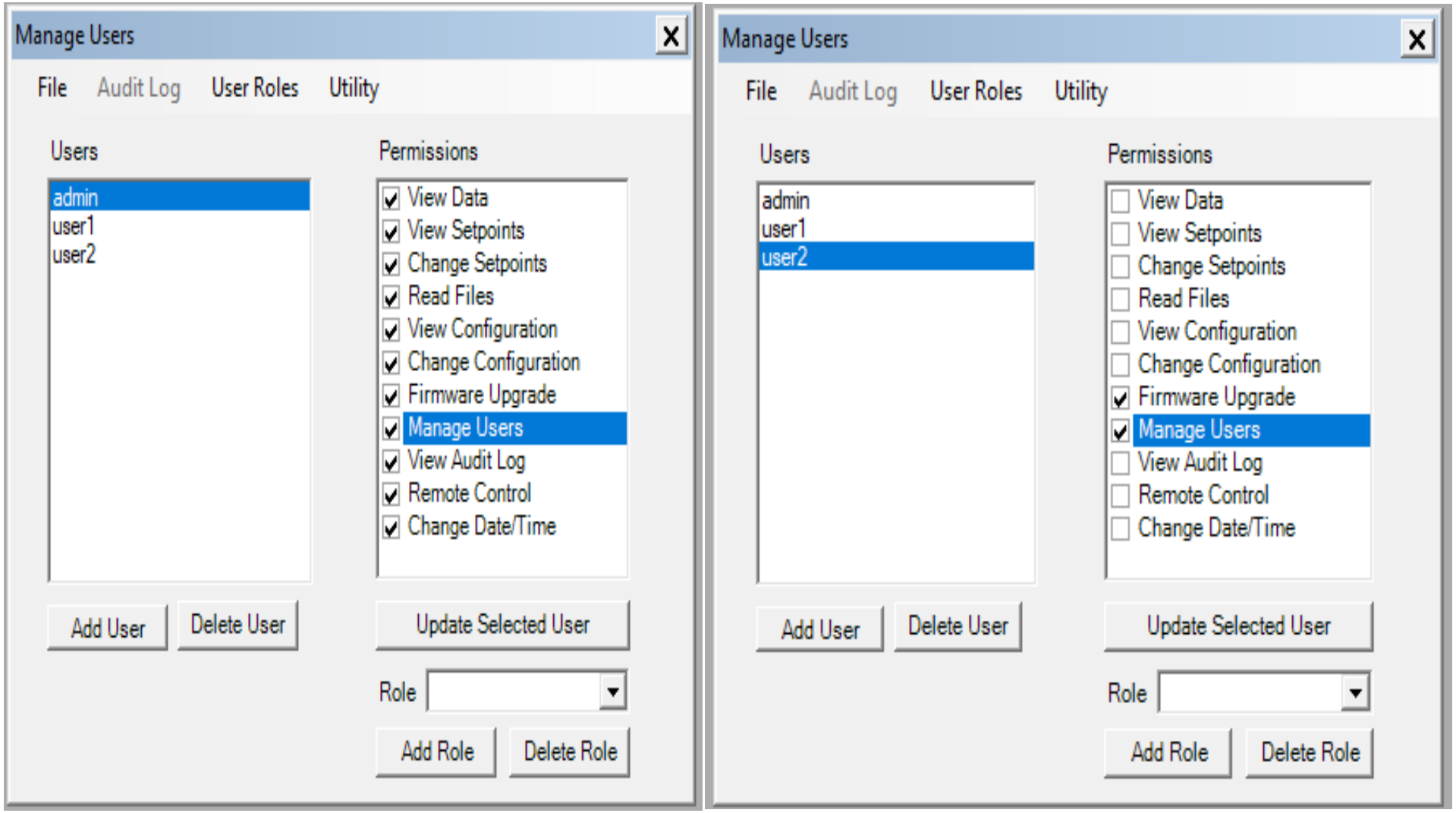
- Strong password construction
- No undisclosed bypass or “back door”
- Multiple access levels
- Non-modifiable audit trail
- Alarm Generation

Local password management (IEEE 1686)

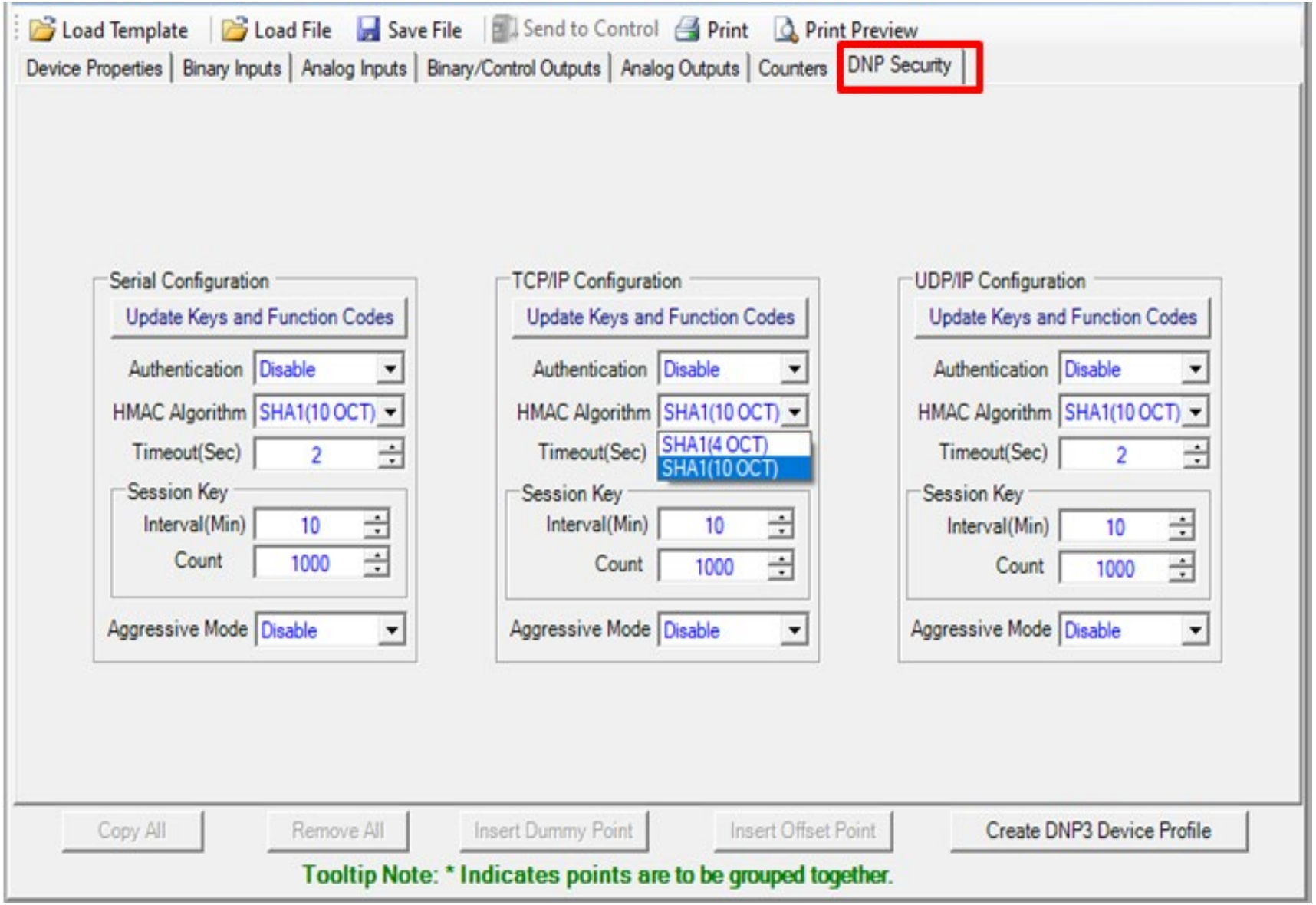


Ability to create User ID/password combination for each user

Role Based Permissions (IEEE 1686)



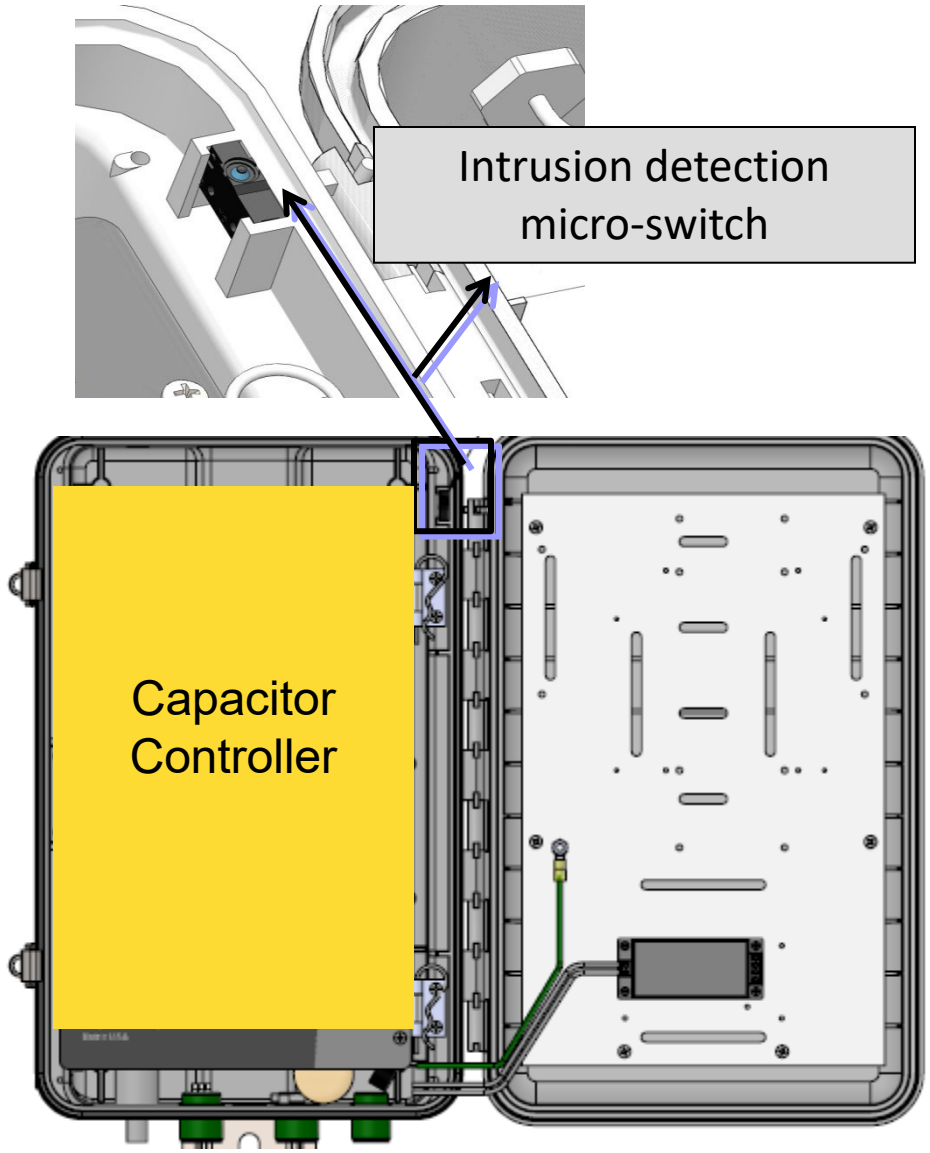
DNP Secure Authentication



Intrusion Detection

- Intrusion detection via a micro switch which detects opening of the enclosure door.

- When the control enclosure door is opened by an intruder a Report By Exception (RBE) message is sent to SCADA to alert the maintenance personnel



Centralized Authentication, Authorization and Accounting

Centralized Authentication, Authorization and Accounting

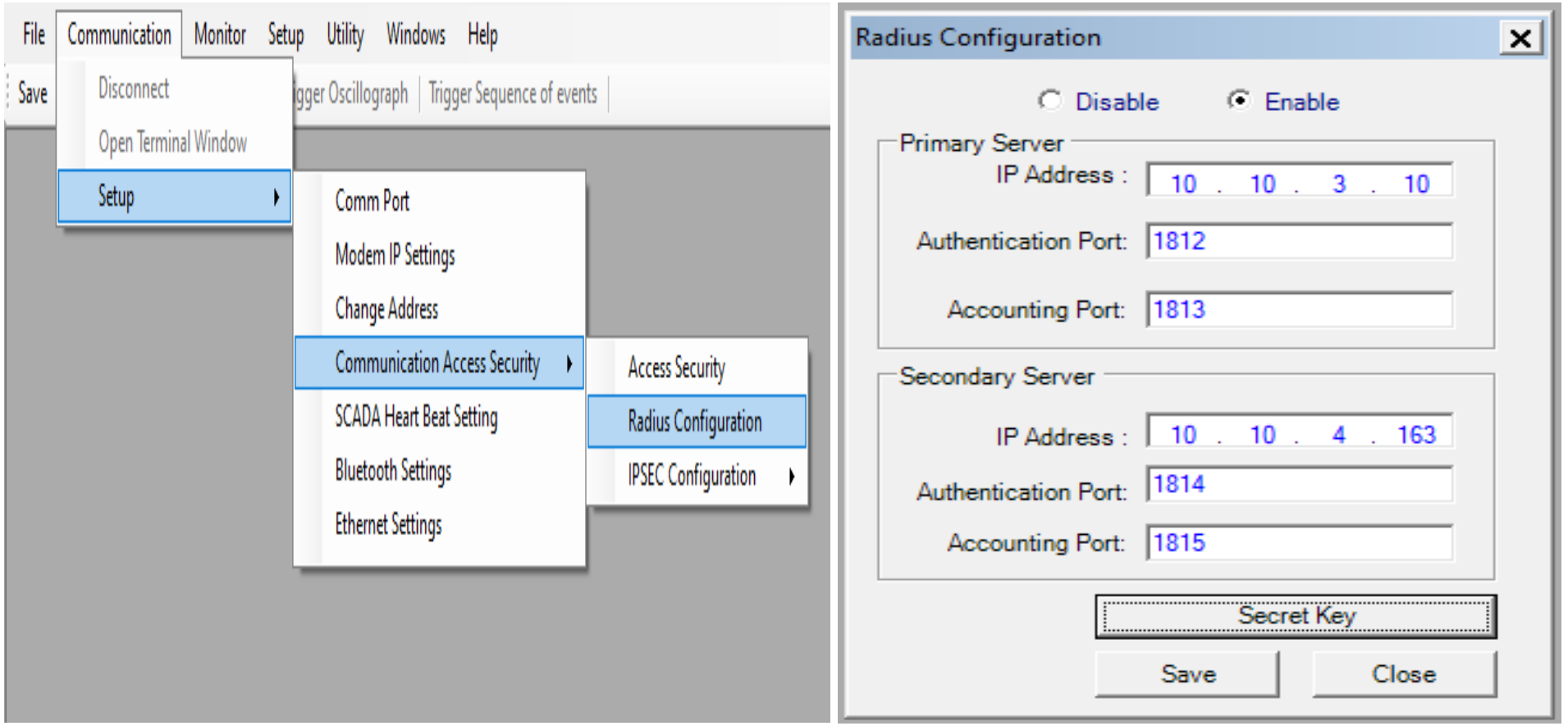
- Centralized User ID/Password management
  - Stored in server, not in individual IEDs
  - Reduced maintenance effort required
- Only one location needs change rather than changing them at thousands of IEDs
- Remote Authentication Dial-In User Service (RADIUS)
  - Networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use network services

RADIUS Functions

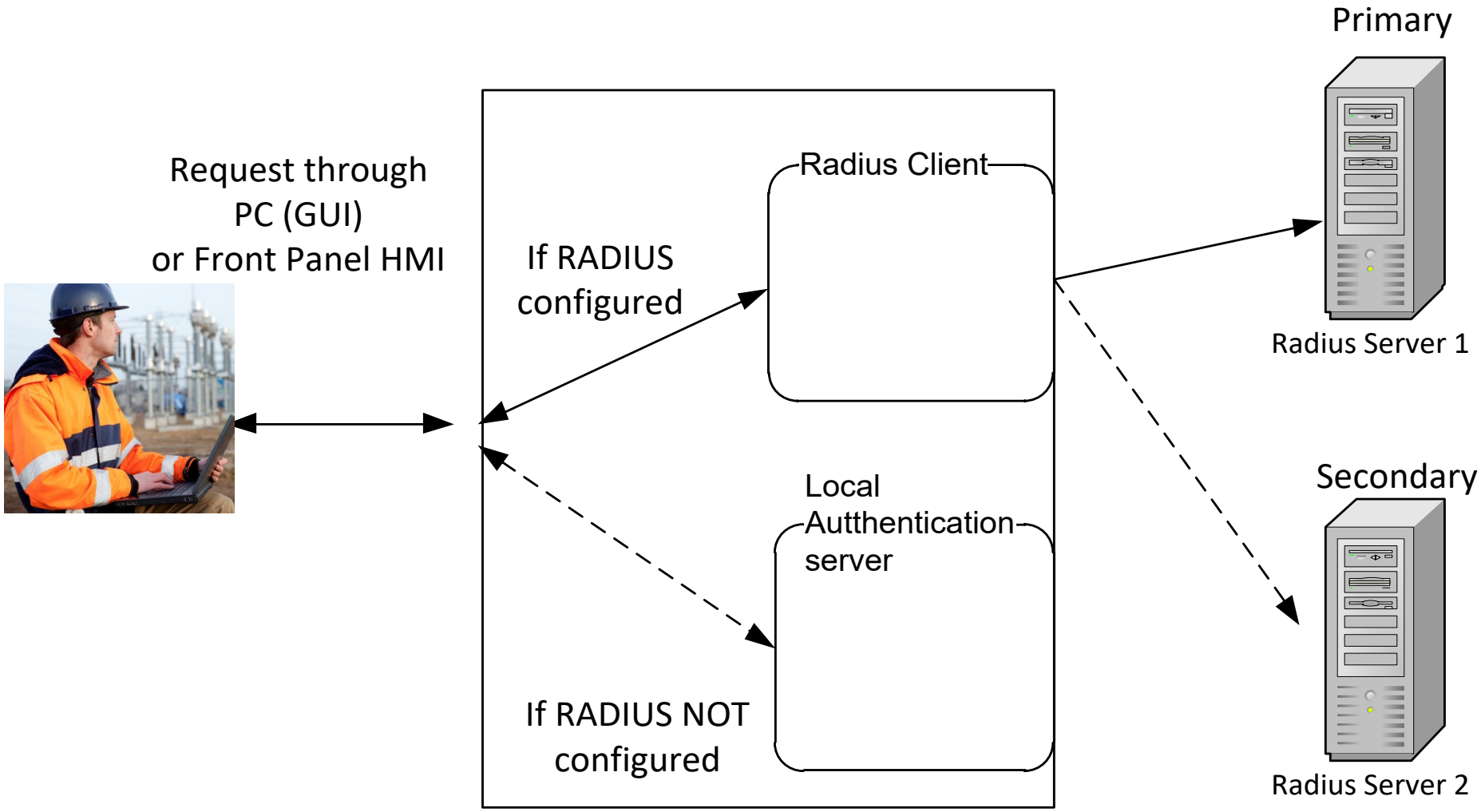
RADIUS serves three functions:

- **Authenticate users or devices before granting them access to a network**
- **Authorize those users or devices for certain network services**
- **Account for usage of those services**

RADIUS Server Configuration

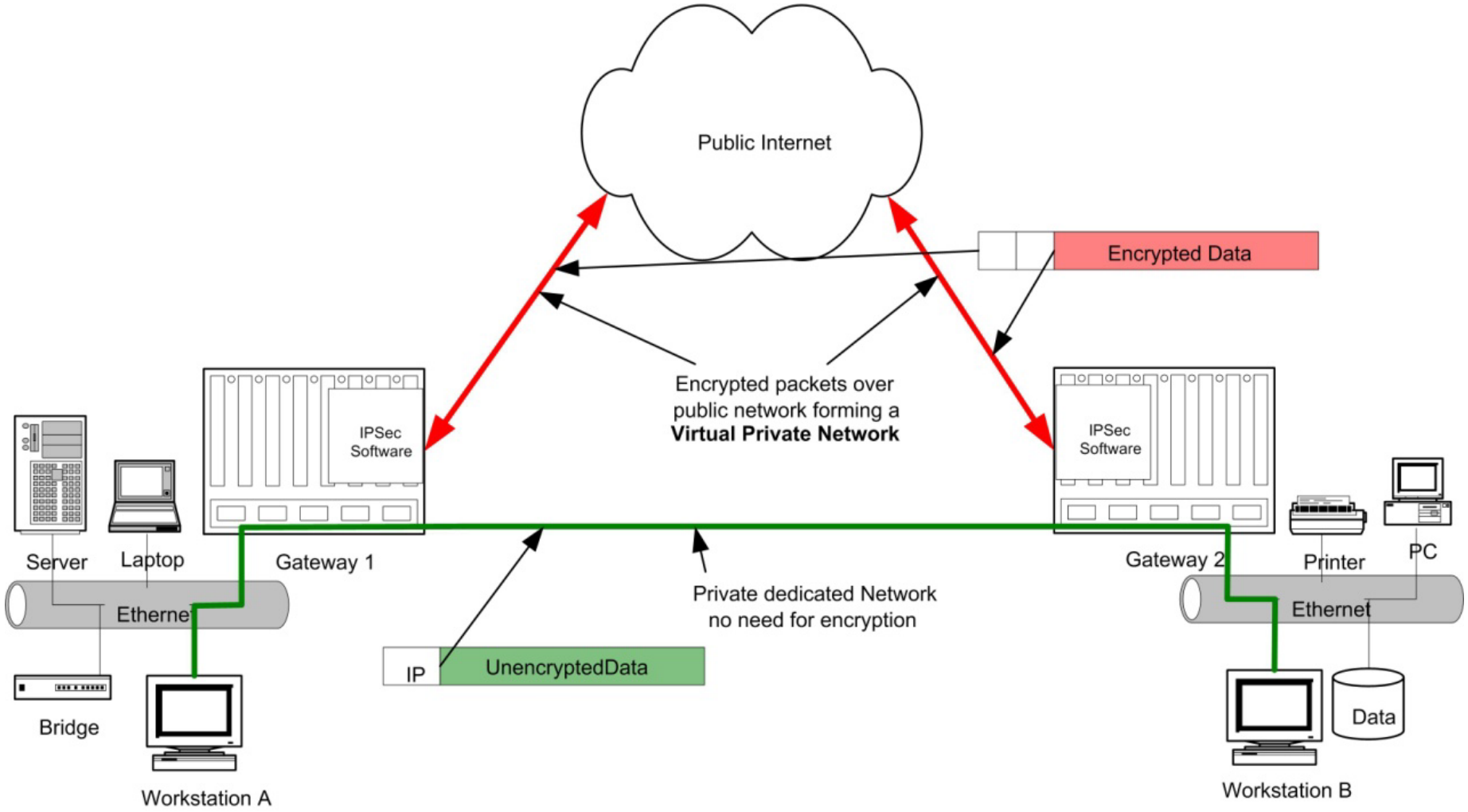


RADIUS - Authentication Mechanism



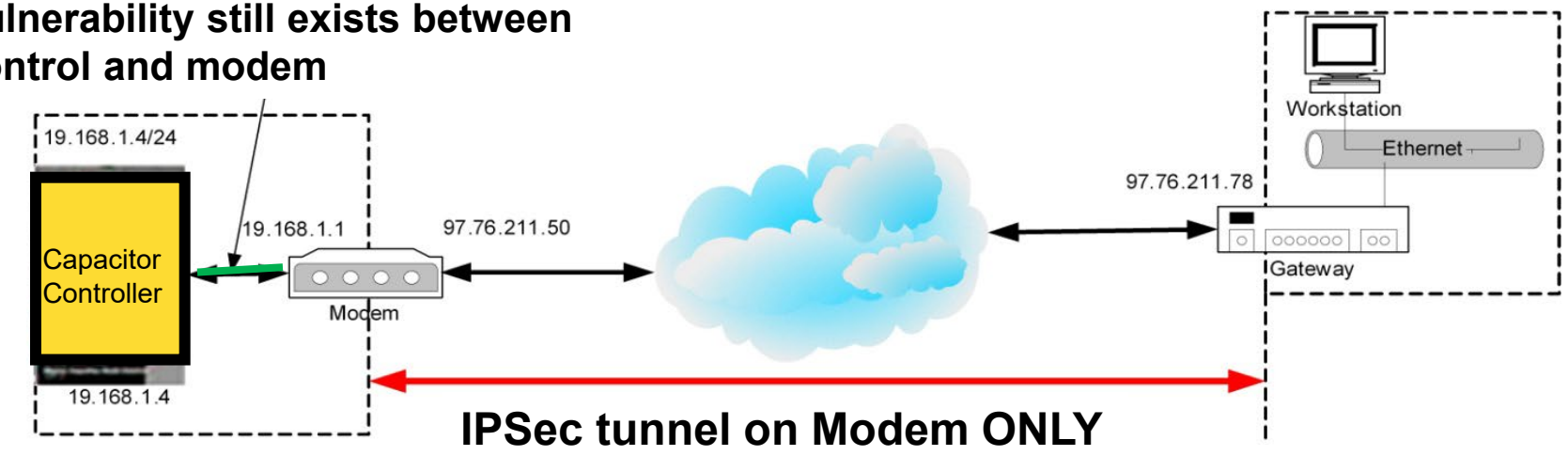
Internet Protocol Security (IPSec)

IPSec VPN

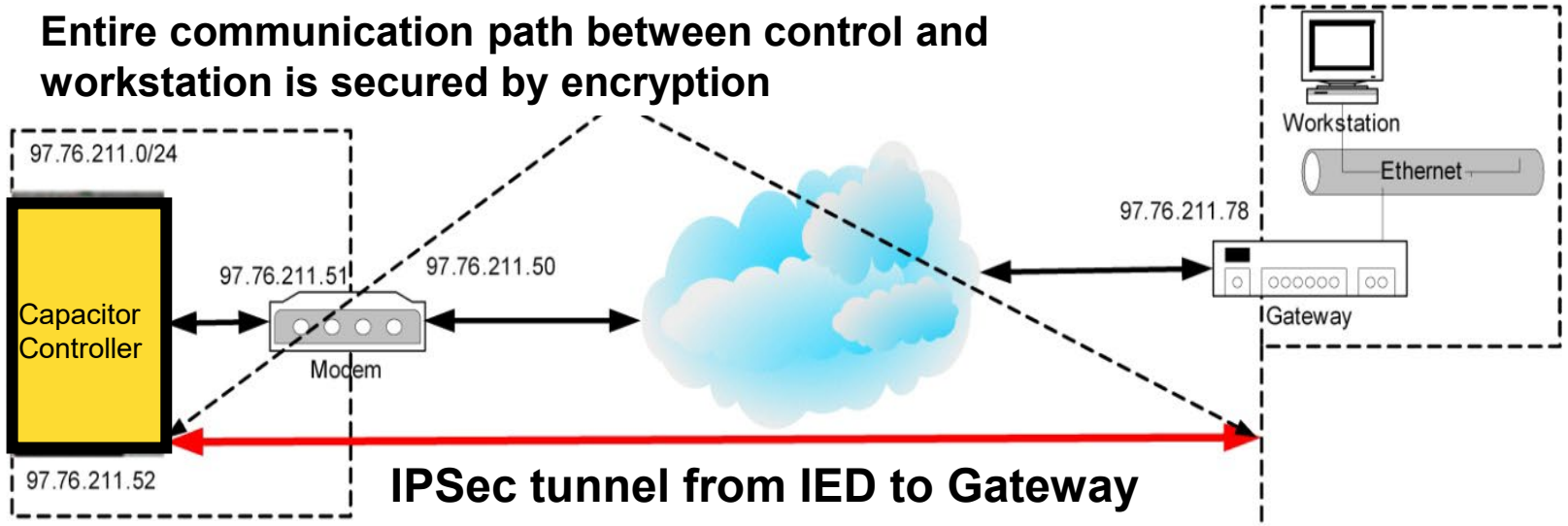

Public Internet
Encrypted Data
Encrypted packets over
public network forming a
Virtual Private Network
IPSec
Software
IPSec
Software
Server
Laptop
Gateway 1
Gateway 2
Printer
PC
Ethernet
Ethernet
Private dedicated Network
no need for encryption
IP
UnencryptedData
Bridge
Data
Workstation A
Workstation B

IPSec Using Wireless Modem

Vulnerability still exists between control and modem



Entire communication path between control and workstation is secured by encryption



Internet Protocol Security (IPSec)

Benefits of IPSec

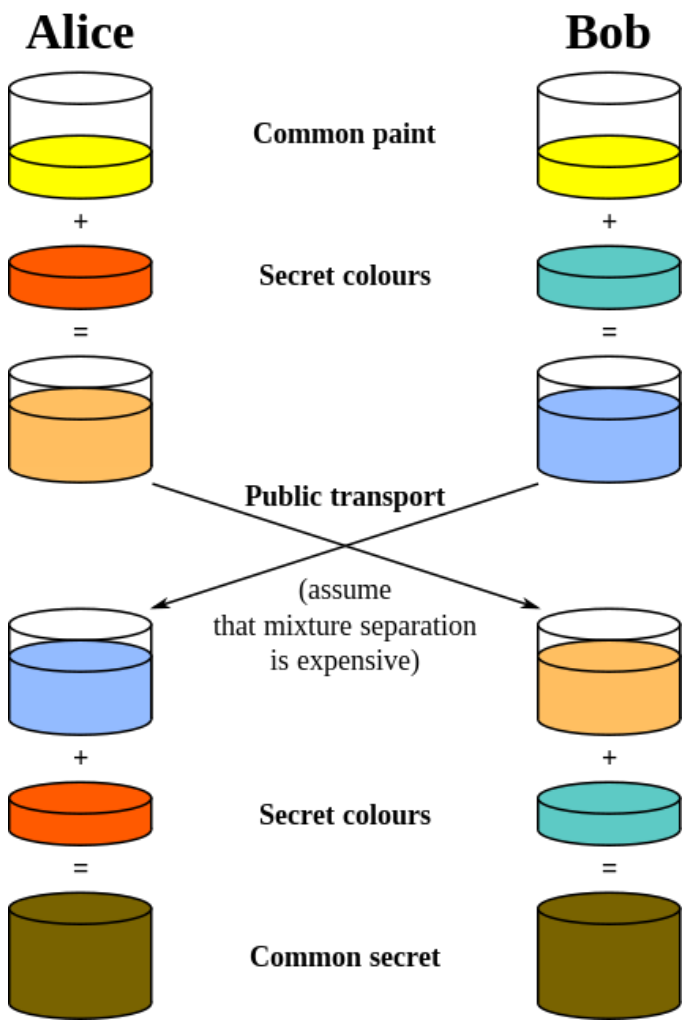
- Confidentiality - by encrypting data
- Integrity - routers at each end of a tunnel calculates the checksum or hash value of the data
- Authentication - signatures and certificates
- IPSec is designed to provide interoperable, high quality, cryptographically- based security for IPv4 and IPv6 - (RFC 2401)

All these while still maintaining the ability to route through existing IP networks

Internet Key Exchange

- Given enough time, ANY encryption can be defeated
- For effective protection, IPsec must be deployed with some type of key exchange protocol
- Changing Encryption Key at a regular interval minimizes risk of hacking

Diffie-Hellman Key Exchange Illustration

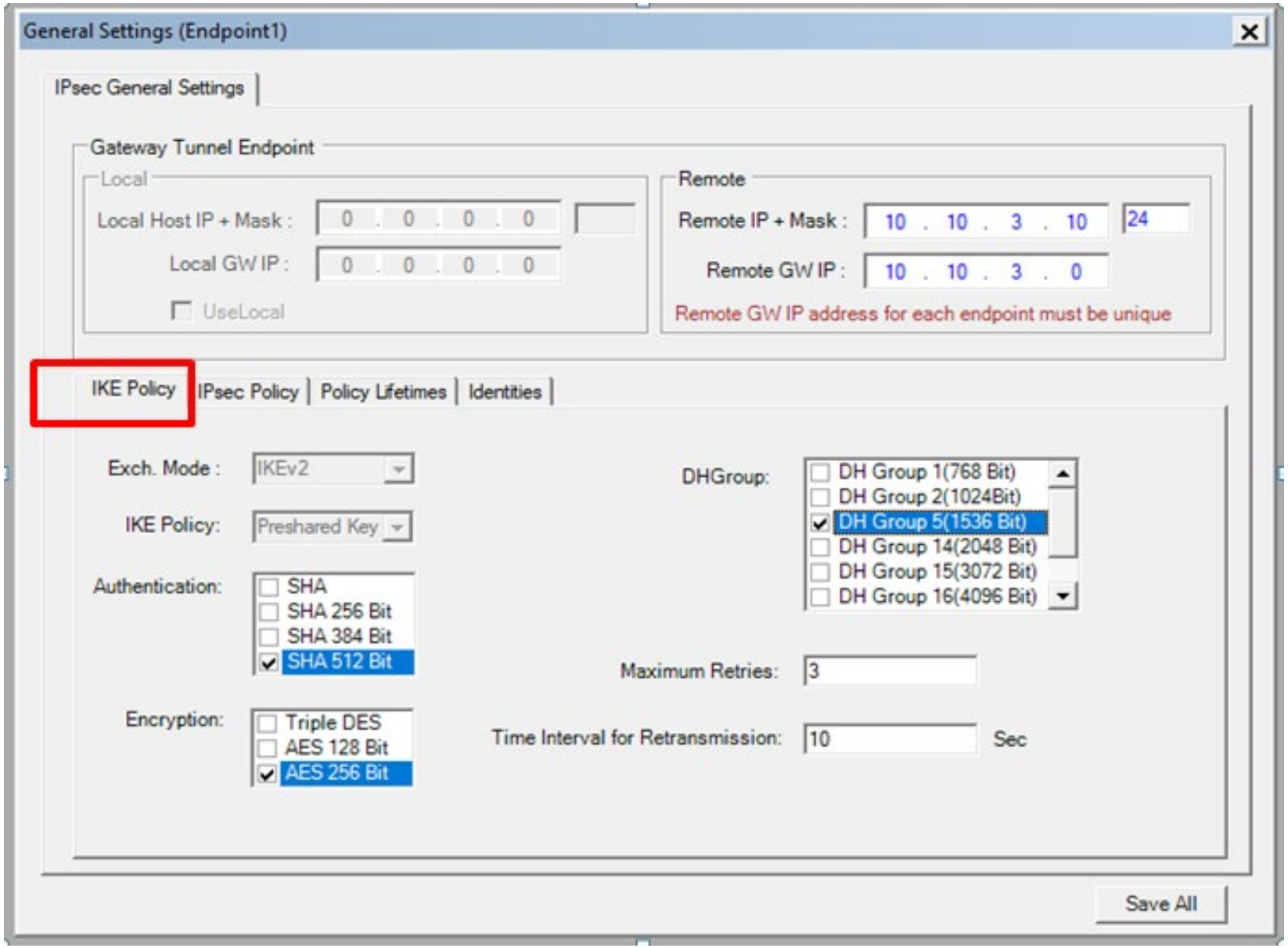


Courtesy of Wikipedia

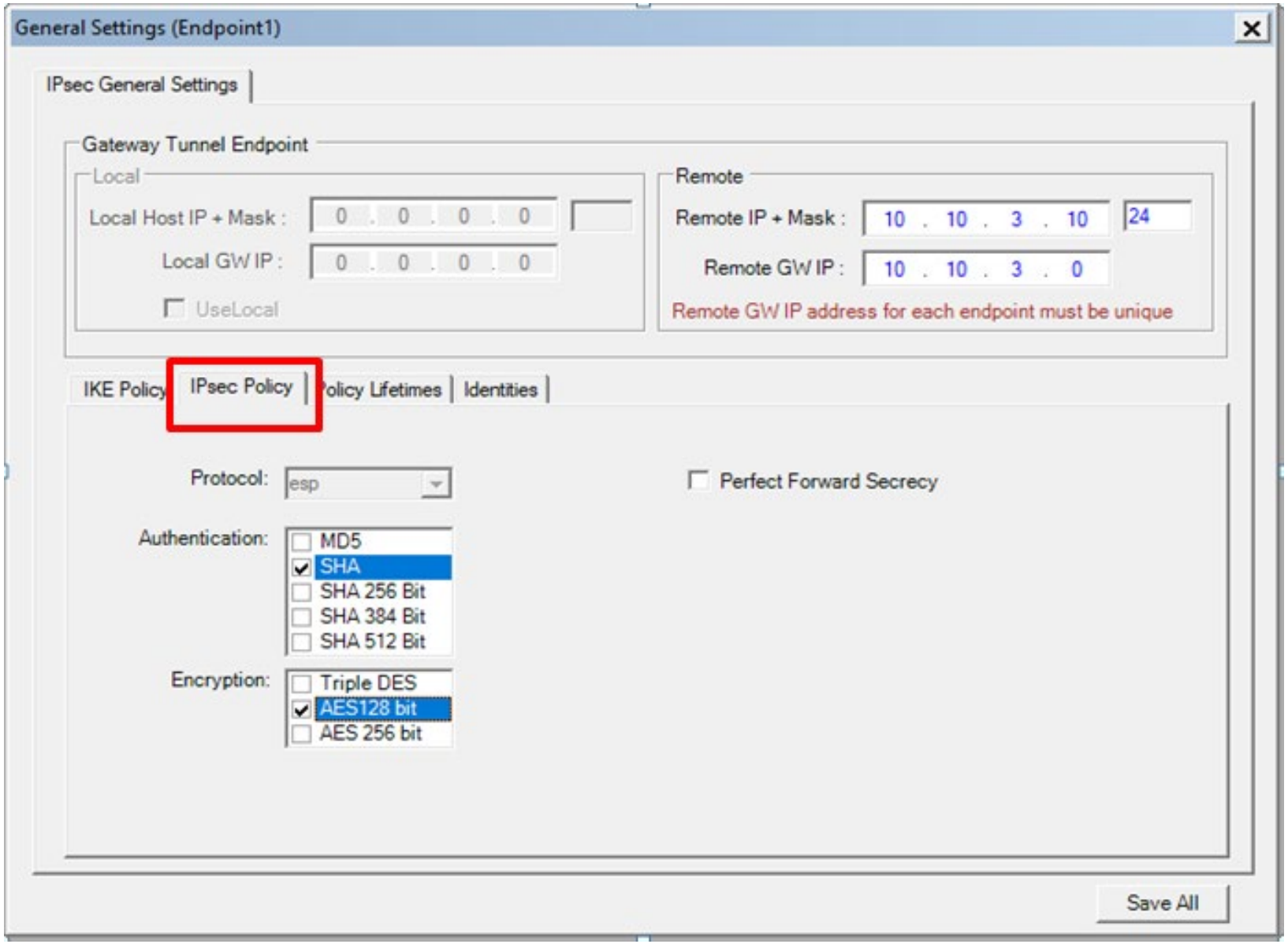
Alice				Bob		
Secret	Public	Calculates	Sends	Calculates	Public	Secret
a	p, g		$p, g \rightarrow$			b
a	p, g, A	$g^a \bmod p = A$	$A \rightarrow$		p, g	b
a	p, g, A		$\leftarrow B$	$g^b \bmod p = B$	p, g, A, B	b
a, s	p, g, A, B	$B^a \bmod p = s$		$A^b \bmod p = s$	p, g, A, B	b, s

1. Alice and Bob agree to use a prime number $p = 23$ and base $g = 5$.
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23 = 2$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret (the number 2).

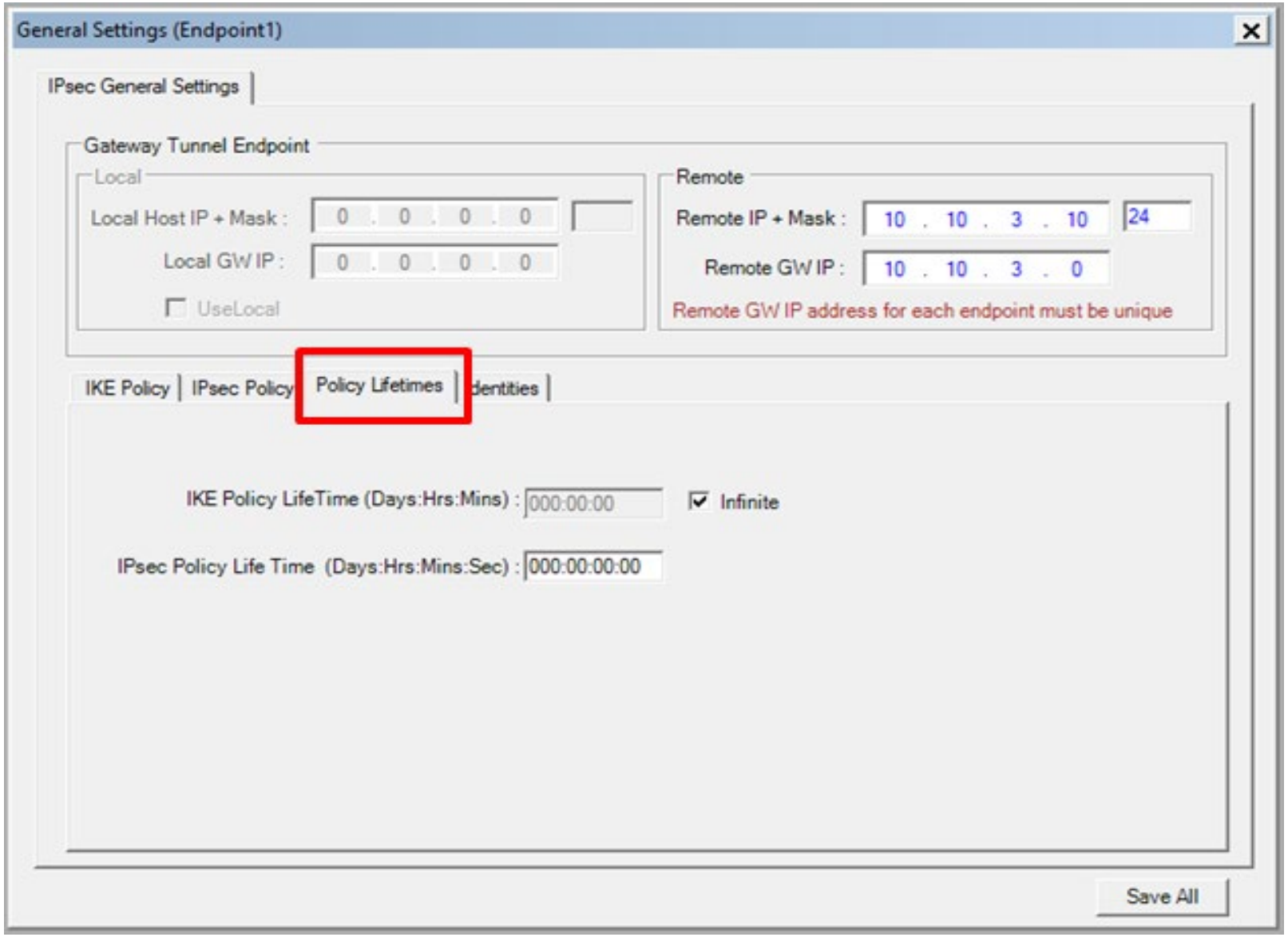
IKE Policy Settings



IPSec Policy Settings

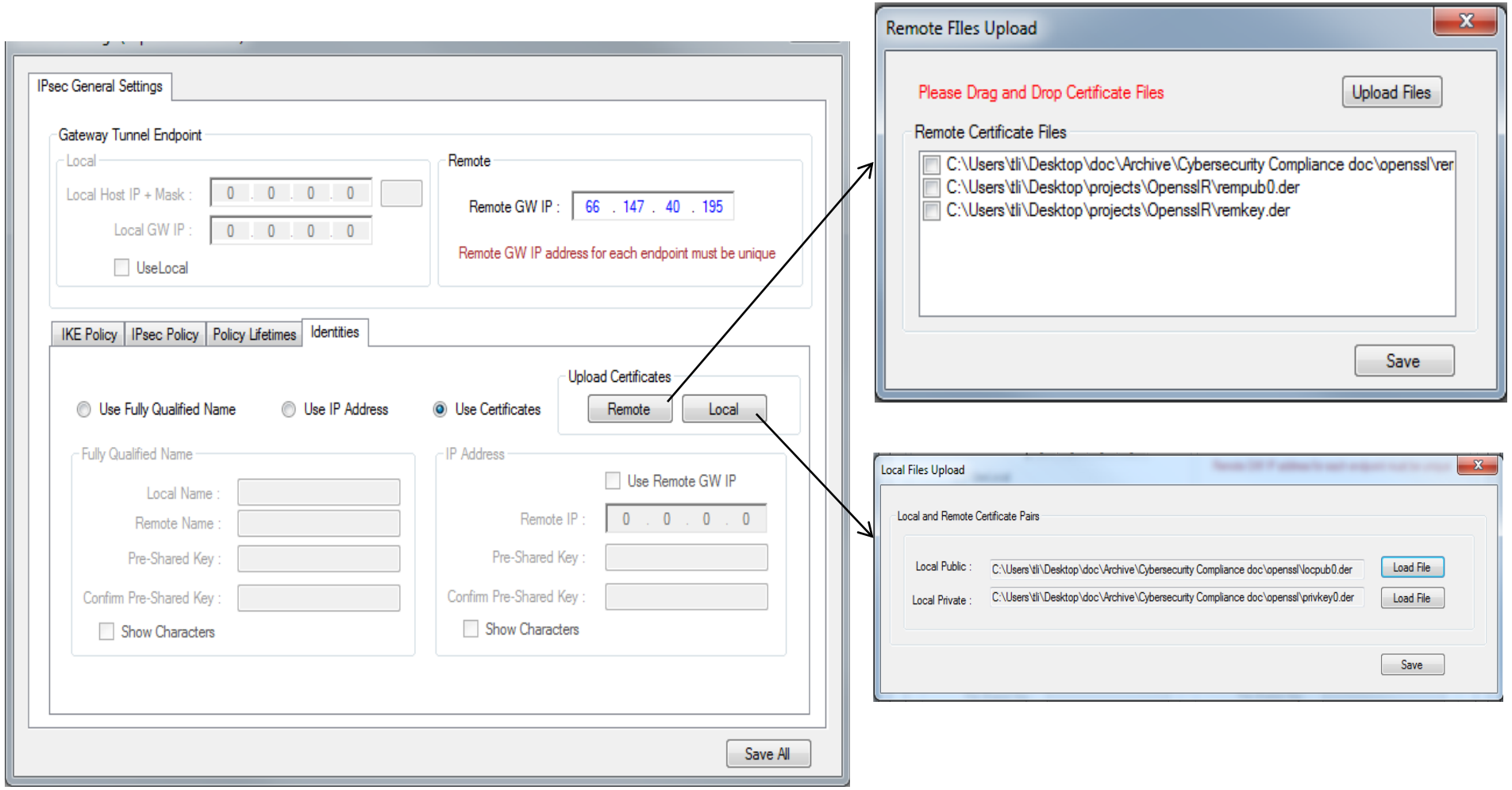


Policy Lifetimes

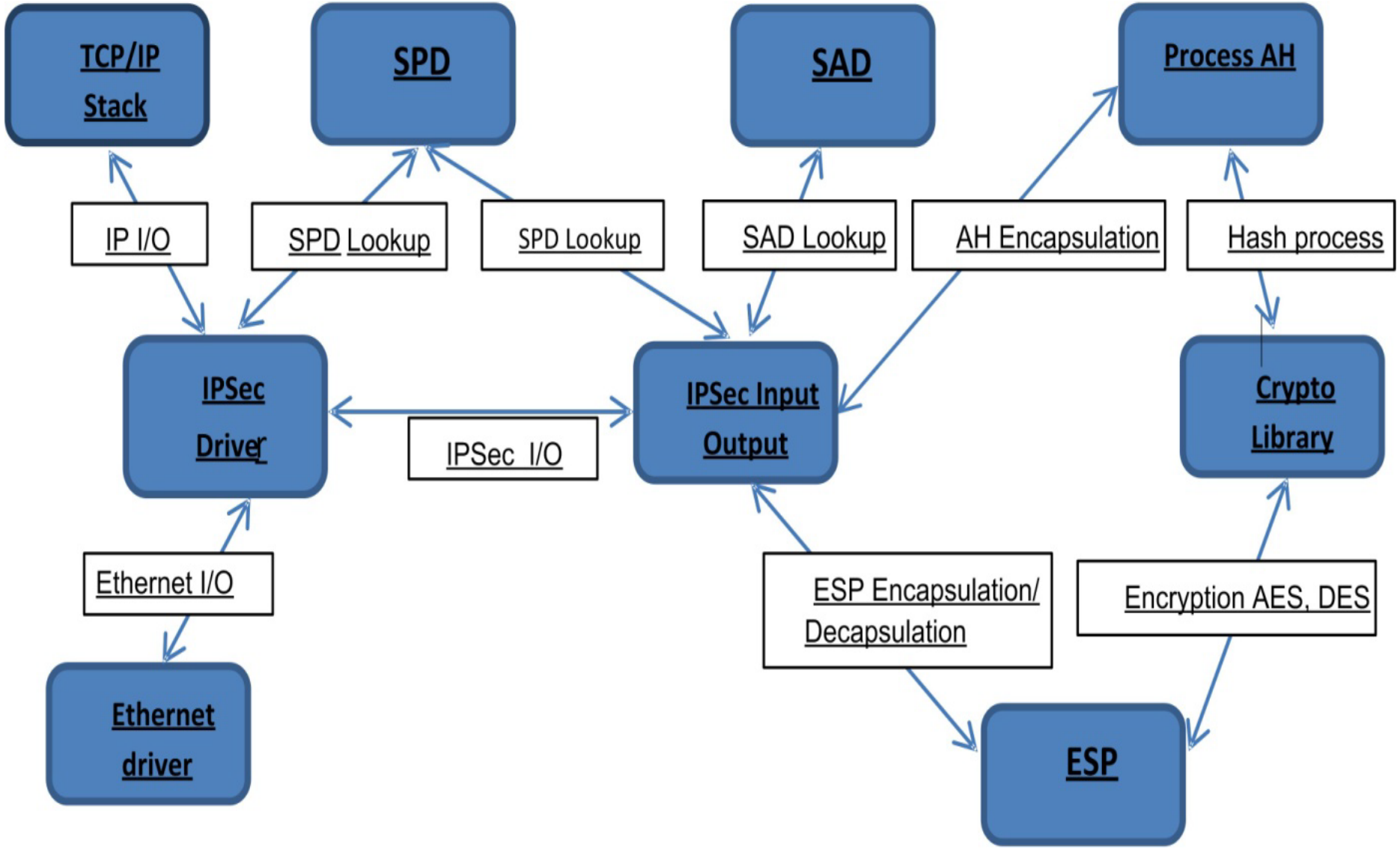


Certificates

Loading the Certificates



Software Implementation



Throughput Performance

IPSec mode	64 bytes	128 + 64 bytes	256 + 64 bytes	512 + 64 bytes	768 + 64 bytes	1024 + 64 bytes	1280 + 64 bytes
no IPSec	min 0.6 ms avg 2 ms	min 0.5 ms avg 1.7 ms	min 0.8 ms avg 2 ms	min 0.7 ms avg 2 ms	min 0.9 ms avg 2.2 ms	min 0.8 ms avg 2.3 ms	min 1 ms avg 2.3 ms
ESP 3DES HMAC SHA-256	min 2.2 ms avg 3.6 ms	min 2.6 ms avg 4 ms	min 3.2ms avg 4.9 ms	min 4.8 ms avg 6.3 ms	min 6.4 ms avg 7.9 ms	min 7.7 ms avg 10.9 ms	min 9.2 ms avg 12.6 ms
ESP AES 128 HMAC SHA-256	min 2.7 ms avg 4.1 ms	min 3.5 ms avg 5 ms	min 4.9 ms avg 6.7 ms	min 8.3 ms avg 11.5 ms	min 11.8 ms avg 15.3 ms	min 15 ms avg 20 ms	min 18 ms avg 24 ms
ESP AES 256 HMAC SHA-256	min 3 ms avg 4.3 ms	min 4 ms avg 5.9 ms	min 6.2 ms avg 8.3 ms	min 10.8 ms avg 14.3 ms	min 15.3 ms avg 21.2 ms	min 19.8 ms avg 27.1 ms	min 25 ms avg 33 ms

Conclusions

- Modern protection, monitoring and controls in electric power systems with advanced communication are vulnerable to cyber attacks,
- IEEE and other standards are available which address Cybersecurity requirements,
- It is important to consider applying these standards to IEDs that are being integrated into substations and feeder equipment to provide secure communications,
- Advanced Cybersecurity features such as RADIUS for Authentication, Authorization and Accounting and IPSec VPN tunneling for secure communications via shared network can be embedded into protection and control IEDs which will provide secure communication inside as well as outside the substation.

Acknowledgements

We would like to acknowledge contributions of some material in this presentation from Dr Nathan Wallace of Cybirical and Steve Kunsman of Hitachi Energy.

www.BeckwithElectric.com

(727) 544-2326