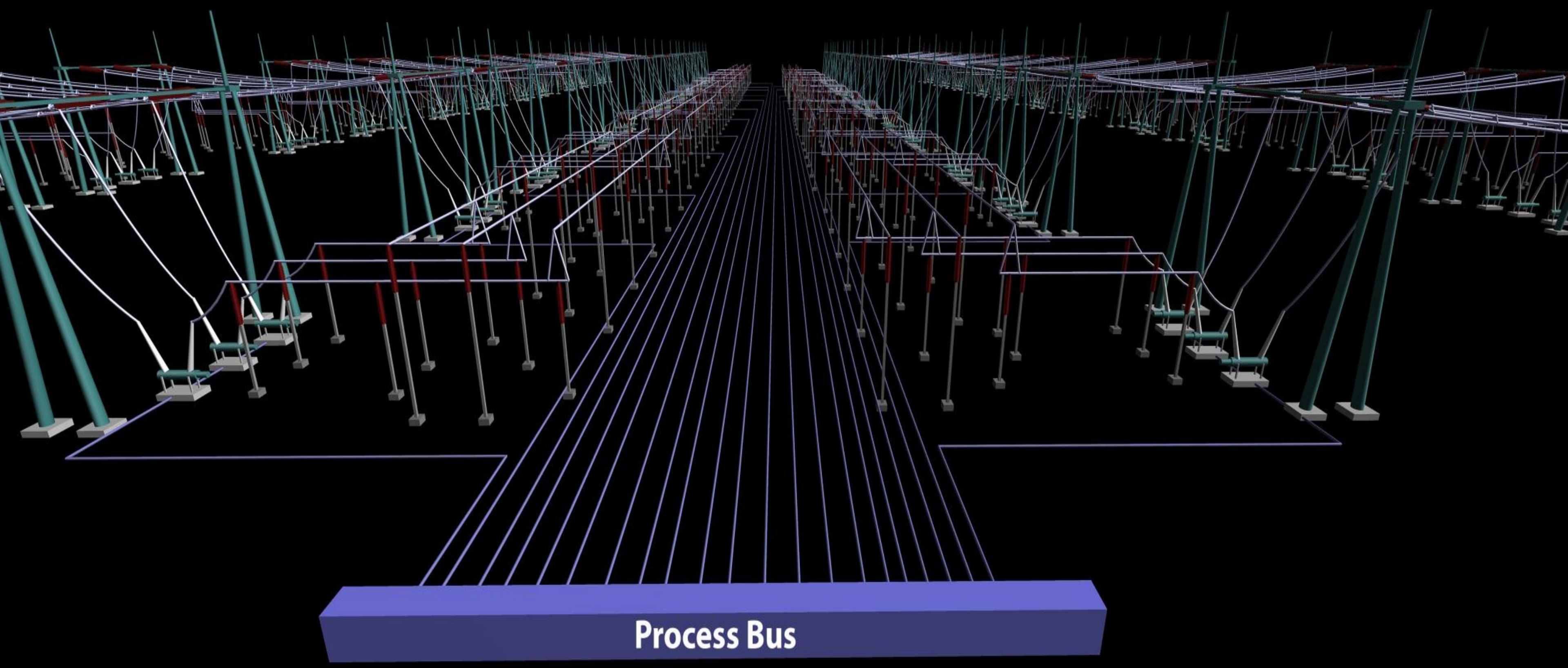
Electric Energy System Cybersecurity: An Overview

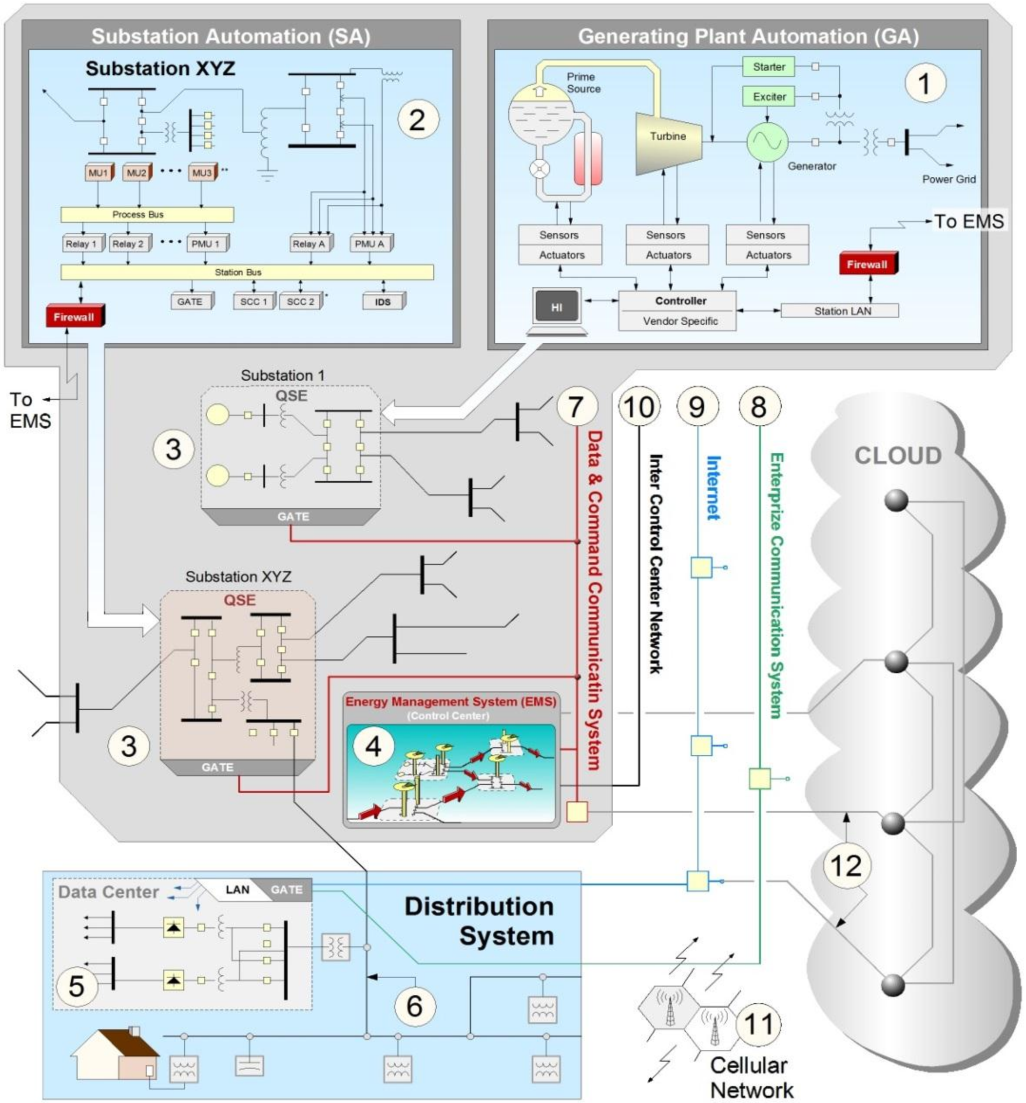
Sakis Meliopoulos
Georgia Power Distinguished Professor
ECE, Georgia Tech



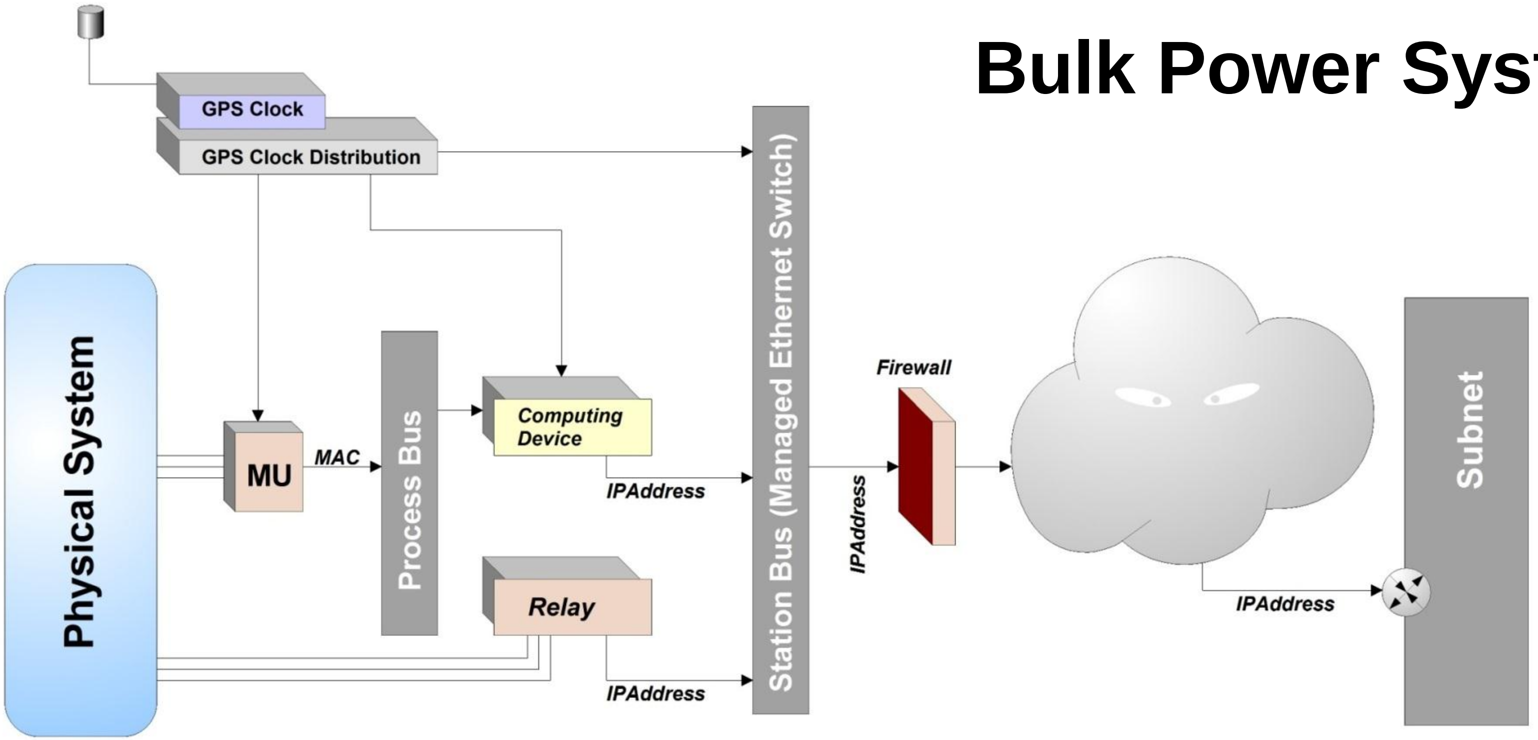
Contents

- Background
- Electric Energy Systems – Cyber Infrastructure
- Vulnerabilities
- Cybersecurity Standards – present practice
- Advanced Cybersecurity Systems
  - State and Model Based Detection Systems
  - Context Based Authentication
- Demonstrations
- Concluding Remarks

The Ever Increasing Attack Surface of the electric Energy Grid



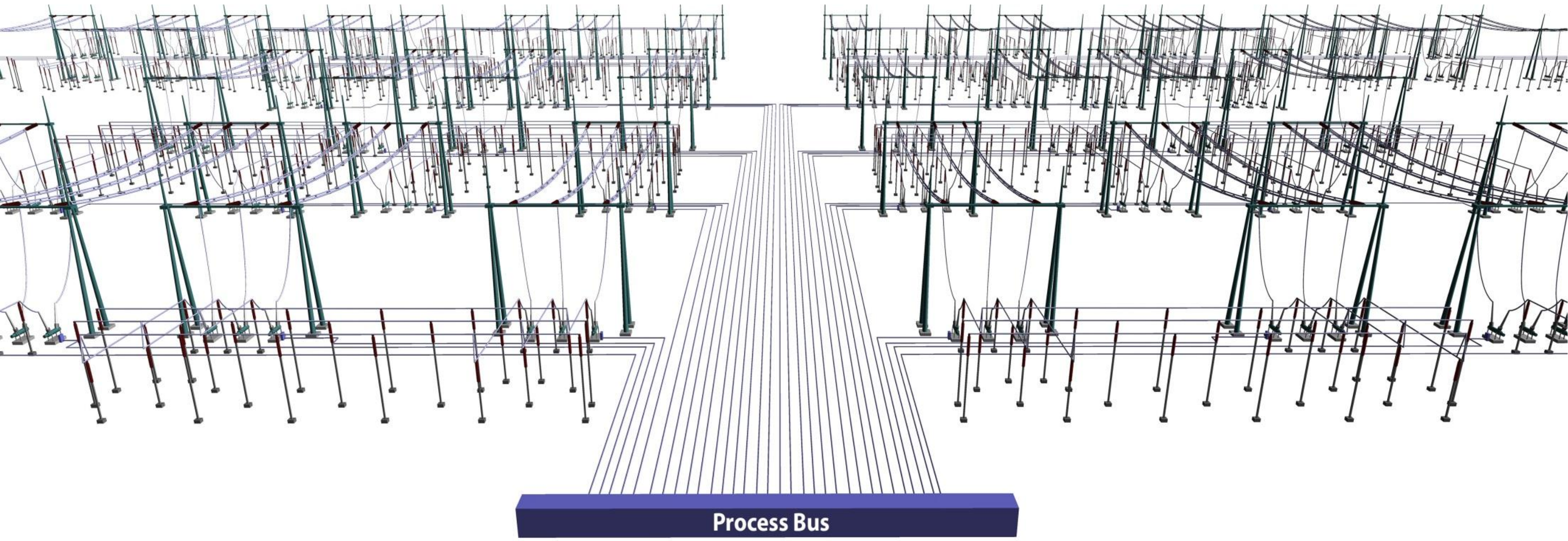
Basic Components of the Electric Energy Grid Cyberspace



Distribution/Customer Level

Need to utilize customer flexibility drives to the concept of IoTE

Vulnerabilities



Hackers can:

Cause severe disruptions to electric grid
Cause severe damage to major electric grid components
Manipulate voltages at customers causing failures

Example 1: GPS Spoofing

Electric energy systems depend on GPS synchronized measurements. Spoofing GPS receivers can lead to relay mis-operations and compromised operational security

Example 2: AURORA Attack/Controller Attack

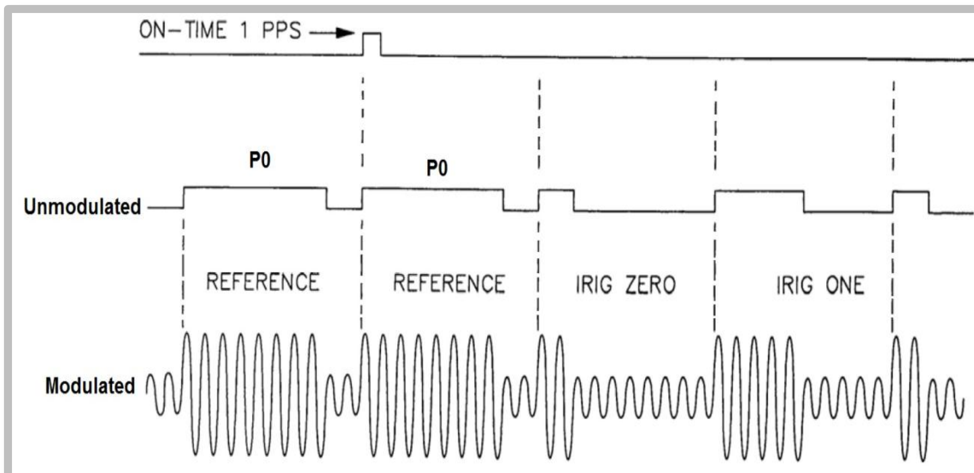
Closing of generator breaker while generator is at standstill

Example 3: Distribution System Controller Attack

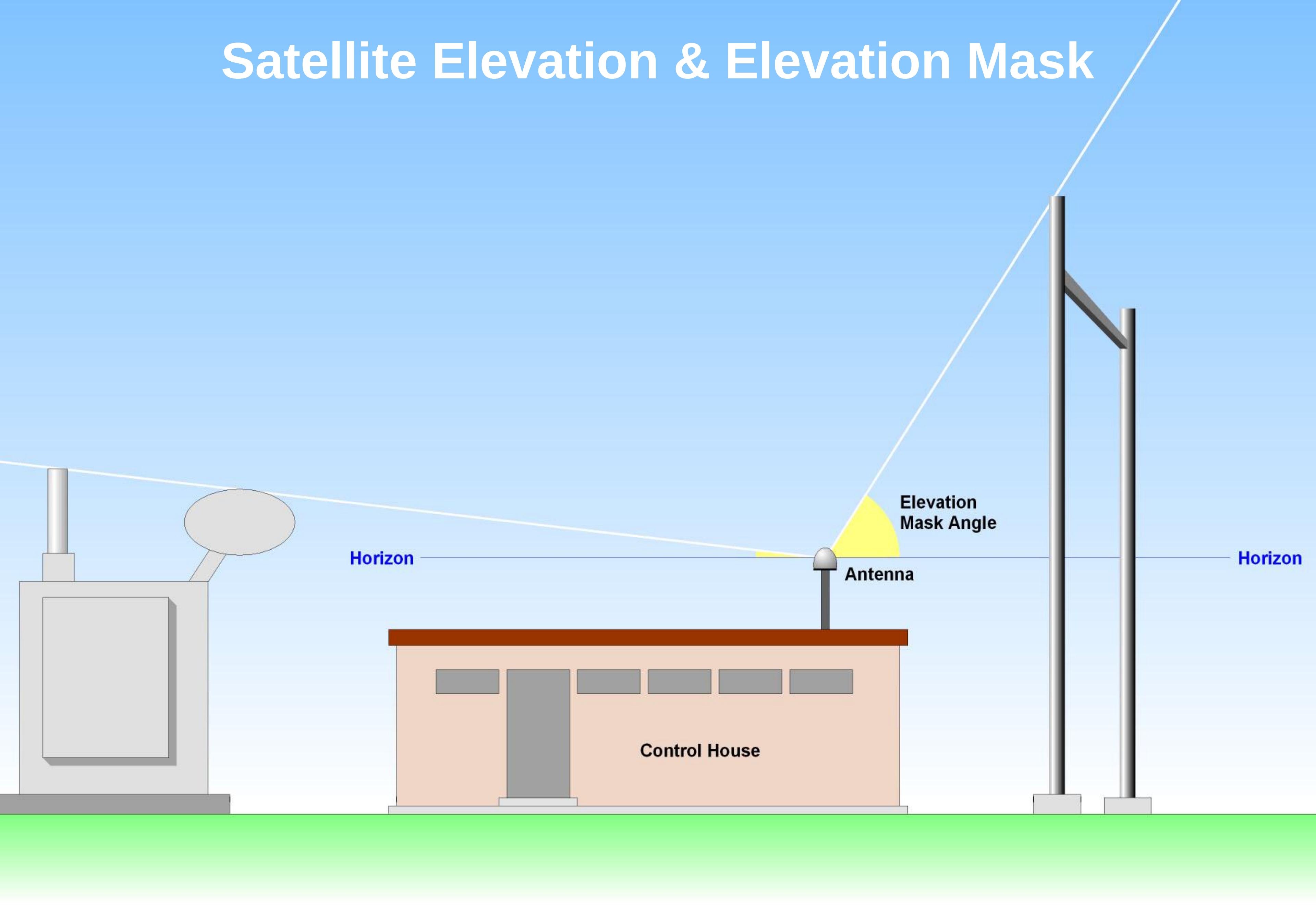
Access controllers of transformers, reclosers, cap banks, and manipulate voltages at customers causing massive appliance failures

IRIG-B Frame Information Encoding

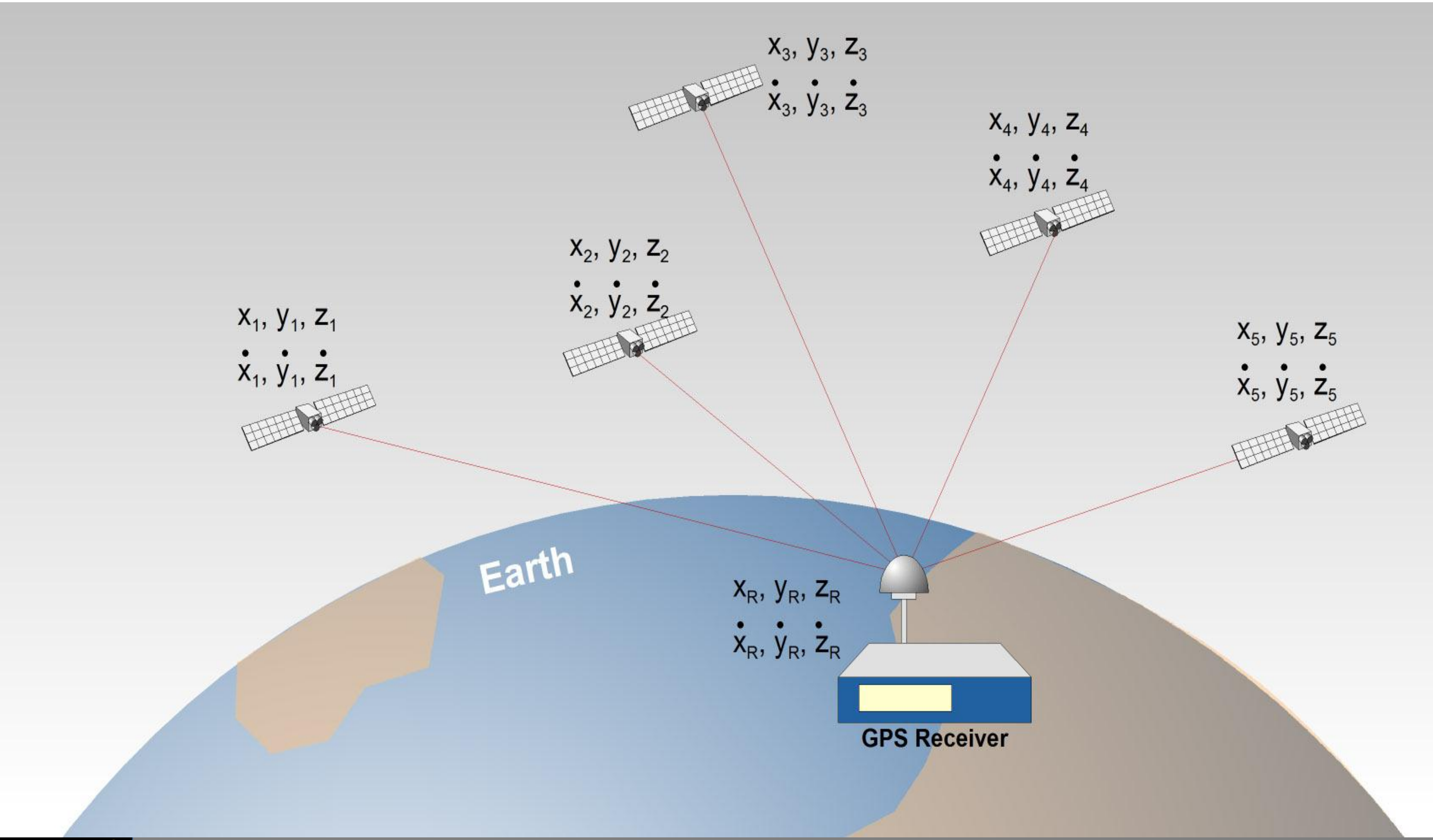
Number of Bits	Encoding	Information
7	BCD	Seconds of Minute (0-59)
7	BCD	Minutes of Hour (0-59)
6	BCD	Hours of Day (0-24)
10	BCD	Days of Year (0-366)
9	BCD	Year (last two digits)
18	Binary	Control Bits
17	Binary	Seconds of Day (0-86399)



Satellite Elevation & Elevation Mask



Satellite Position/Speed and Receiver Position/Speed

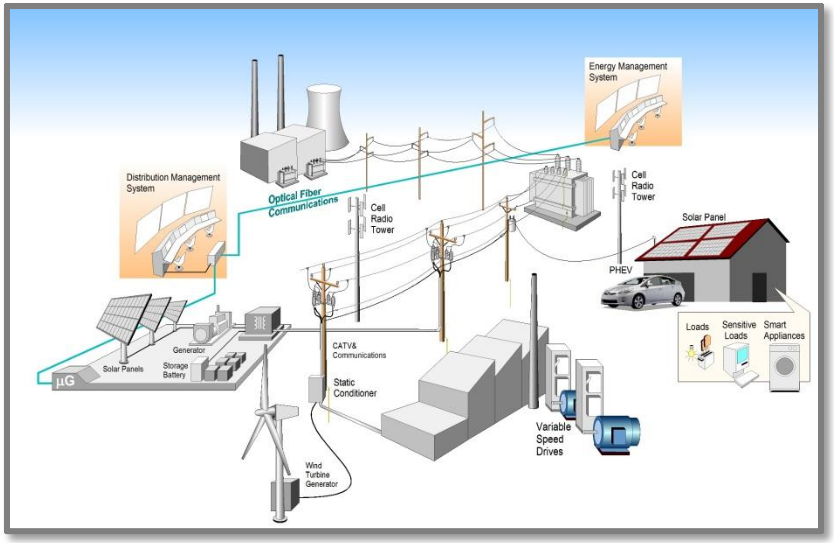


Example 2: Controller Attack

Hacker gains access to distribution system communications

Distribution voltage control uses IEDs to control:

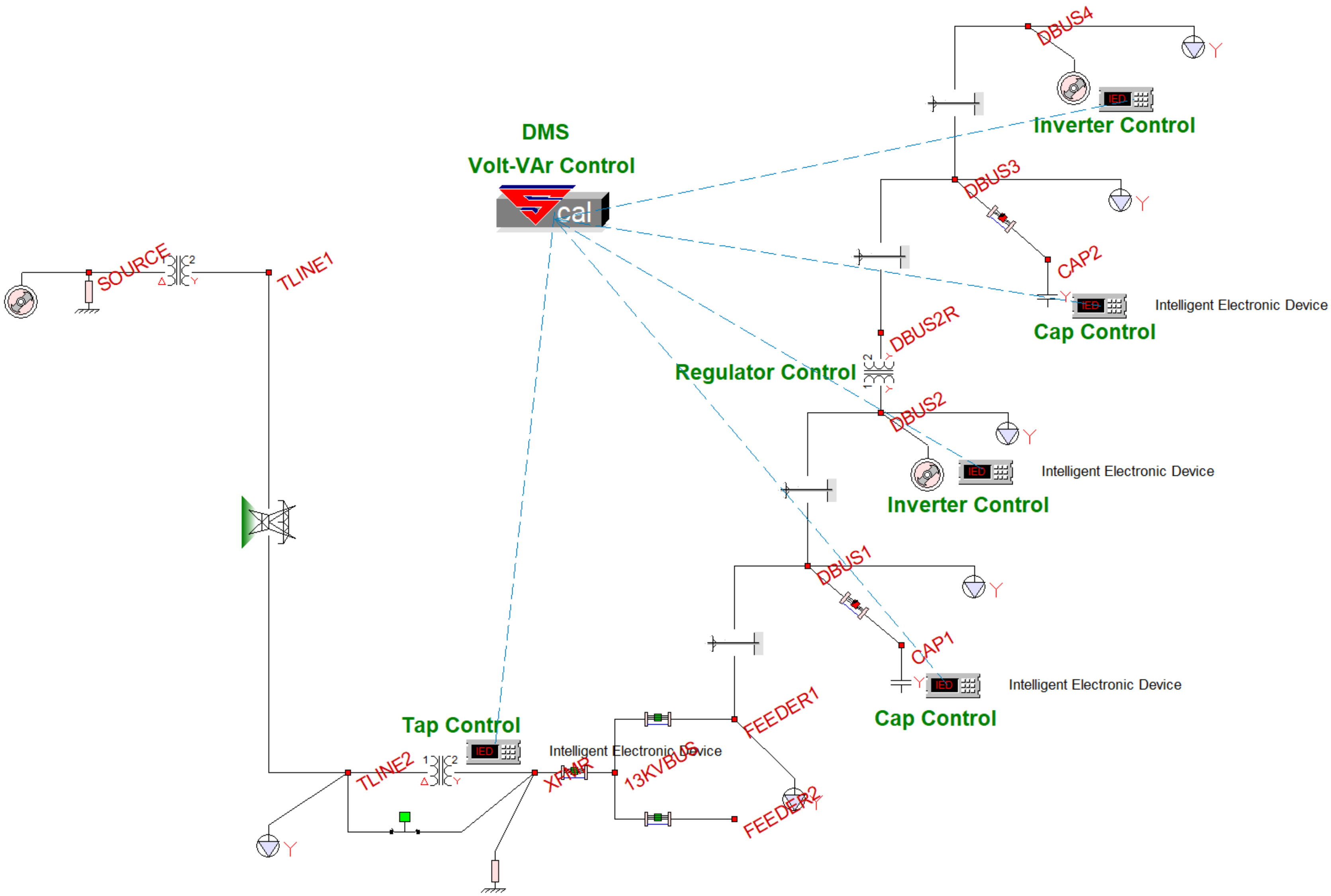
- Load Tap Changer transformers
- Voltage Regulators
- Pole-top capacitor banks



A Successful Hacker can enter the communications network and drive all controls to maximum. In a typical system this may lead to 30% overvoltage causing widespread transformer failures and customer equipment failures (air-conditioners, stereos, refrigerators, etc.)

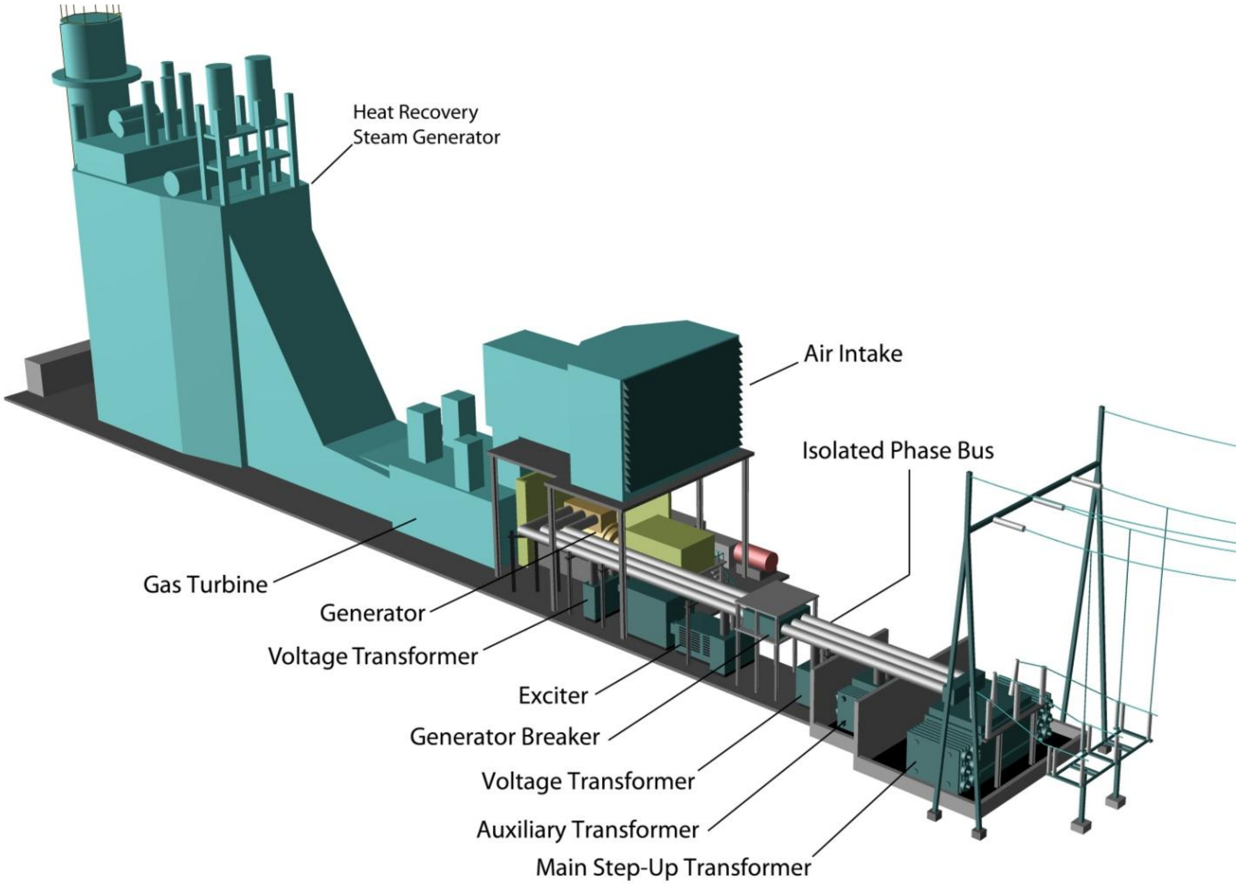
QUESTION: How secure are distribution system communications networks?

Example Controller Attack

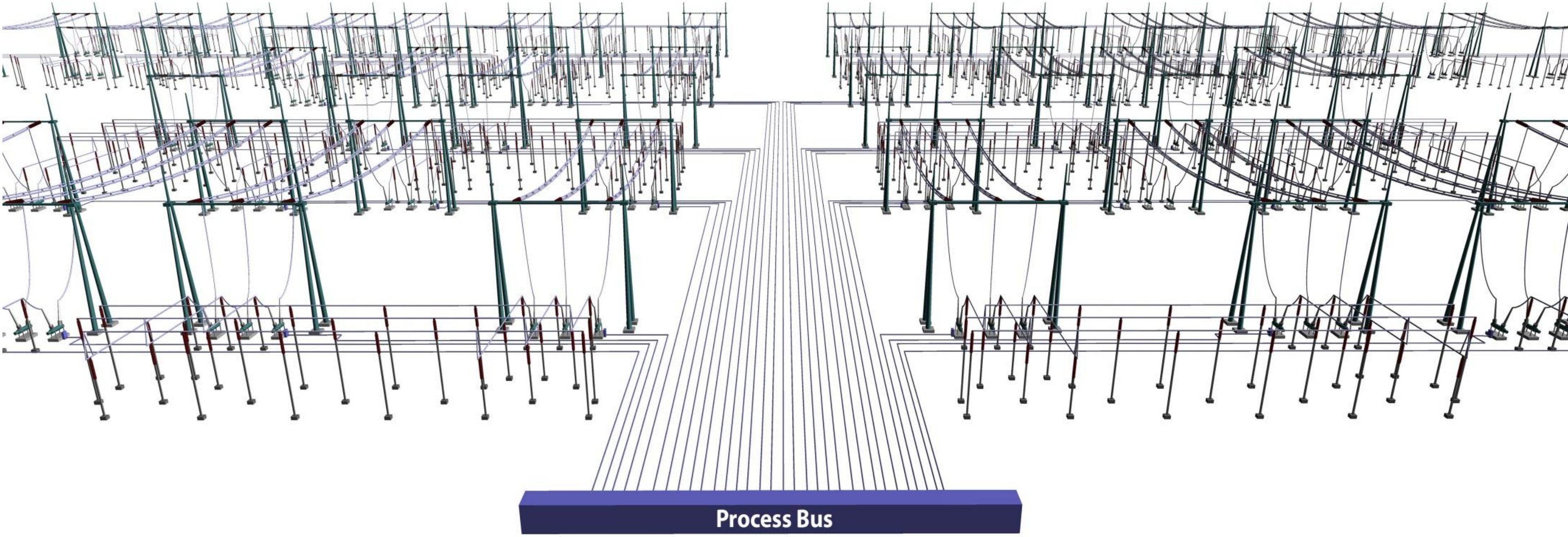


Example 1: AURORA Attack

Closing of generator breaker while generator is at standstill



Standards



- IEEE, CIGRE, NIST, NERC, FERC all are involved in developing cyber security standards

- NIST Cyber Security Framework
(v 1.0 in Feb 2014)

- NERC Critical Infrastructure Protection (CIP) Standards

Example Cyber Security Standards

IEEE Standards

IEEE Std 1686 “IEEE Standard for Intelligent Electronic Devices (IEDs) Cyber Security Capabilities”

IEEE C37.240 “Standard for Cyber Security Requirements for Substation Automation, Protection and Control Systems” (under development)

IEEE Std 1402 “Guide for Electric Power Substation Physical and Electronic Security”

IEEE Std 1711 “IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links”

IEC Standards

IEC 62351

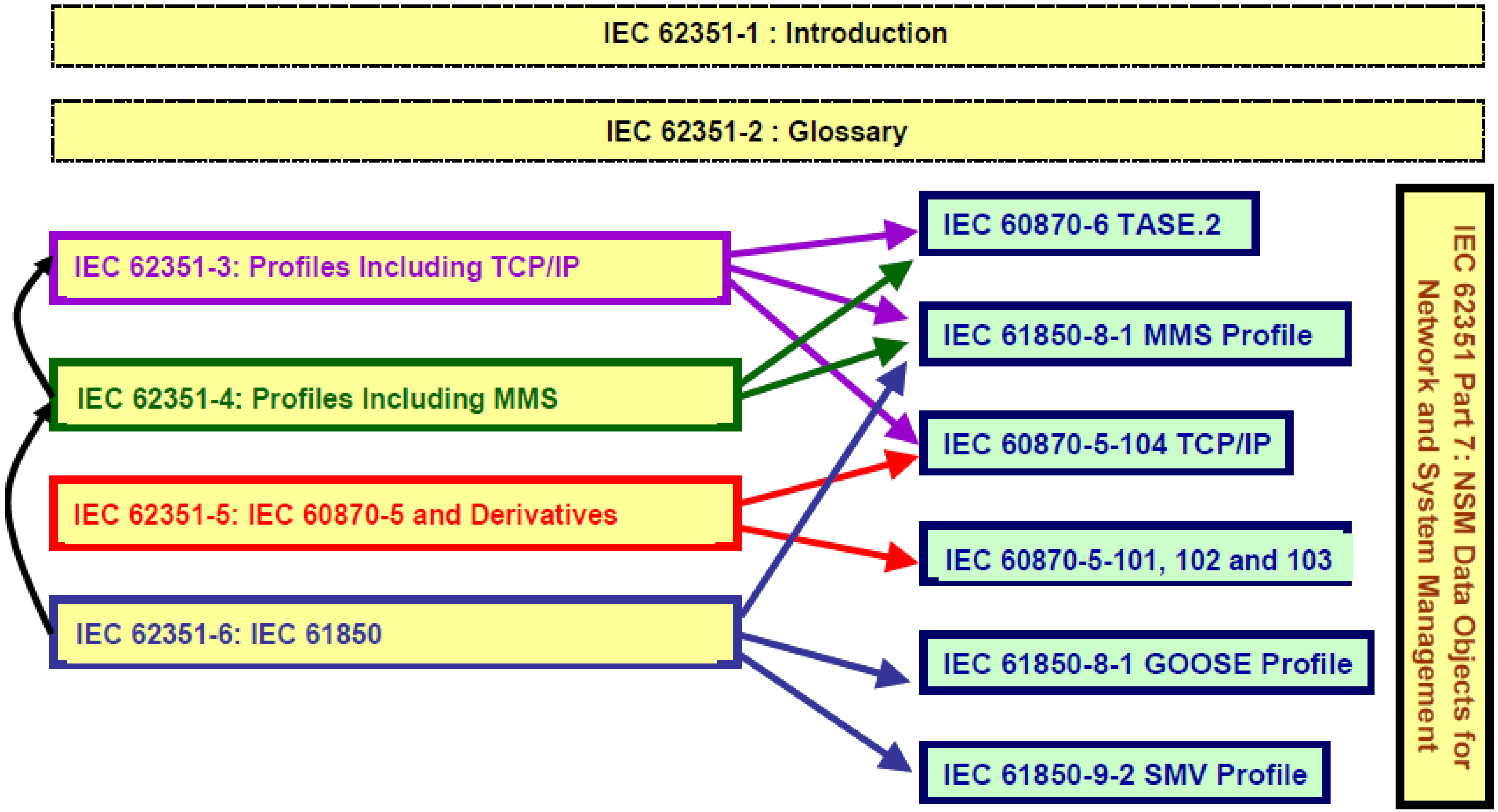
NERC Standards

NERC Critical Infrastructure Protection (CIP) CIP-002 to CIP-009

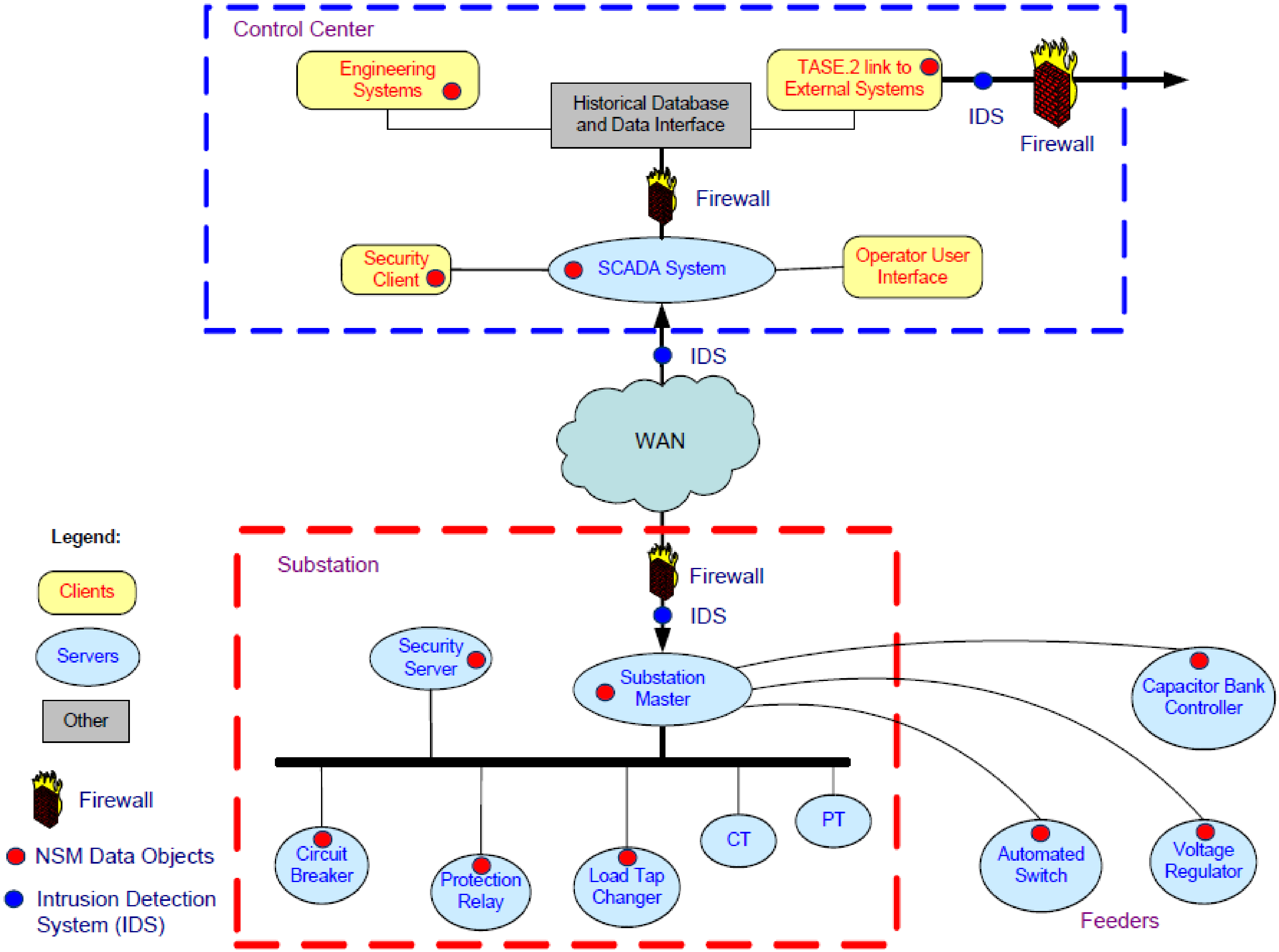
NIST

NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements

IEC Series of Standards



Security Monitoring Architecture, Using NSM Data Objects



IEEE Std C37-240

IEEE Standard

Cybersecurity Requirements for Substation Automation, Protection, and Control Systems.

Effectively maps NISTIR 7628 into the substation system.

Table 2—Substation cybersecurity requirements mapped to NISTIR 7628*

		C	I	A
1a	Interface between control systems and equipment with high availability and with computing and/or bandwidth constraints, for example: - between transmission SCADA and substation equipment - between distribution SCADA and high priority substation and pole-top equipment - between SCADA and DCS within a power plant Serial protocol interface between substation and the National Control Center (NCC) for critical measurements and control, e.g., SCADA Generic object-oriented substation event (GOOSE) communications (compute constraints), e.g., bay to bay or substation to substation	L	H	H
1b	Interface between control systems and equipment without high availability but with compute and/or bandwidth constraints, for example: - Between distribution SCADA and lower priority pole-top equipment - Between pole-top IEDs and other pole-top IEDs Serial protocol interface between substation and NCC for non-critical measurements and monitoring, e.g., asset monitoring	L	H	M
1c	Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: between transmission SCADA and substation automation systems High-bandwith protocol interface between - Substation and NCC for critical measurements and control, e.g., SCADA - WAMS - SIPS - Teleprotection (high availability, time critical)	L	H	H
1d	Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, e.g., between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs Asset monitoring using Ethernet network, local HMI, maintenance, engineering (e.g., DR uploads)	L	H	M
8	Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: between a temperature sensor on a transformer and its receiver	L	M	M
9	Interface between sensor networks and control systems, for example: between a sensor receiver and the substation master, e.g., asset monitoring and SCS or RTU/e.g., MU and bay device (IED)	L	M	M
13	Interface between systems and mobile field crew laptops/equipment, for example: - Between field crews and gas-insulated substations (GISs) - Between field crews and substation equipment	L	H	M
16	Interface between engineering/maintenance systems and control equipment, for example: - Between engineering and substation relaying equipment for relay settings - Between engineering and pole-top equipment for maintenance - Within power plants	L	H	M
17	Interface between control systems and their vendors for standard maintenance and service, for example: between a SCADA system and its vendor	L	H	L
18	Interface between security/network/system management consoles and all networks and systems, for example: between a security console and network routers, firewalls, computer systems, and network nodes	H	H	H

*L = Low, M = Medium, and H = High. The pink cells indicate most critical. The yellow cells indicate intermediate.

IEEE Standard 1686

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

Table A.1—Table of compliance

Clause number	Clause/subclause title	Status	Comment
5	IED cyber security features	Acknowledge	
5.1	Electronic access control	Comply	
5.1.2	Password defeat mechanisms	Comply	
5.1.3	Number of individual users	Exceed	Product provides for 25 individual ID/password combinations
5.1.4	Password construction	Exception	Upper and lower case letters are interchangeable. Non-alphanumeric characters cannot be used in password
5.1.5	IED access control	Acknowledge	
5.1.5.1	Authorization levels by password	Comply	
5.1.5.2	Authorization using role-based access control (RBAC)	Exceed	Product provides six user-defined roles
5.1.6	IED main security functions	Acknowledge	
5.1.6 a)	View data	Comply	
5.1.6 b)	View configuration settings	Comply	
5.1.6 c)	Force values	Exception	Feature not supported on this product
5.1.6 d)	Configuration change	Comply	
5.1.6 e)	Firmware change	Comply	
5.1.6 f)	ID/password or RBAC management	Comply	
5.1.6 g)	Audit trail	Comply	
5.1.7	Password display	Comply	
5.1.8	Access timeout	Exception	Timeout period is set by a jumper on the main board. Possible selections are 1 min, 5 min, 10 min, 30 min, and 60 min
5.2	Audit trail	Comply	
5.2.2	Storage capability	Exceed	Audit trail supports 4096 events before overwrite
5.2.3	Storage record	Comply	
5.2.3 a)	Event record number	Comply	
5.2.3 b)	Time and date	Exceed	User can define the format of the date
5.2.3 c)	User identification	Comply	
5.2.3 d)	Event type	Comply	
5.2.4	Audit trail event types	Comply	
5.2.4 a)	Log in	Comply	
5.2.4 b)	Manual log out	Comply	
5.2.4 c)	Timed log out	Comply	
5.2.4 d)	Value forcing	Comply	
5.2.4 e)	Configuration access	Comply	
5.2.4 f)	Configuration change	Comply	
5.2.4 g)	Firmware change	Exception	Firmware changes are not captured in the audit trail record
5.2.4 h)	ID/password creation or modification	Comply	

IEEE Standard 1686

IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

Table A.1—Table of compliance *(continued)*

Clause number	Clause/Subclause Title	Status	Comment
5.2.4 i)	Password deletion	Comply	
5.2.4 j)	Audit log access	Comply	
5.2.4 k)	Time/date change	Comply	
5.2.4 l)	Alarm incident	Comply	
5.3	Supervisory monitoring and control	Comply	
5.3.2	Events	Comply	
5.3.3	Alarms	Comply	
5.3.3 a)	Unsuccessful login attempt	Exception	Alarm is set after six unsuccessful attempts within a 5-min period
5.3.3 b)	Reboot	Exception	A specific alarm for a reboot is not available. However, user can deduce that a reboot has taken place by examining the DNP3.0 initialization bit being set followed by a DNP3.0 request for time.
5.3.3 c)	Attempted use of unauthorized configuration software	Comply	
5.3.3 d)	Invalid configuration or firmware download	Comply	
5.3.3 e)	Unauthorized configuration or firmware file	Comply	
5.3.3 f)	Time signal out of tolerance	Comply	
5.3.3 g)	Invalid field hardware changes	Comply	
5.3.4	Alarm point change detect	Comply	
5.3.5	Event and alarm grouping	Exceed	Three groups are provided: "Critical Alarms," "Alarms," and "Events"
5.3.6	Supervisory permissive control	Comply	
5.4	IED cyber security features	Acknowledge	
5.4.1	IED functionality compromise	Comply	Download of configuration will disable all other operations during the period of download
5.4.2	Specific crytographic features	Acknowledge	
5.4.2 a)	Webserver functionality	Comply	Feature not offered in this product
5.4.2 b)	File transfer functionality	Comply	
5.4.2 c)	Text-oriented terminal connections	Comply	
5.4.2 d)	SNMP network management	Exception	SNMPv2 implemented in this product
5.4.2 e)	Network time synchronization	Exception	IEEE Std C37.238 implemented in this product
5.4.2 f)	Secure tunnel functionality	Comply	
5.4.3	Cryptographic techniques	Comply	
5.4.4	Encrypting serial communications	Comply	
5.4.5	Protocol-specific security features	Comply	
5.5	IED configuration software	Acknowledge	
5.5.1	Authentication	Exception	Feature not supported
5.5.2	Digital signature	Comply	
5.5.3	ID/password control	Exception	Passwords can be viewed in the configuration by someone with Supervisor Level Authority
5.5.4	ID/password controlled features	Comply	
5.5.4.1	View configuration data	Comply	
5.5.4.2	Change configuration data	Comply	
5.5.4.2 a)	Full access	Comply	
5.5.4.2 b)	Change tracking	Comply	
5.5.4.2 c)	Use monitoring	Comply	
5.5.4.2 d)	Download to IED	Comply	
5.6	Communications port access	Comply	
5.7	Firmware quality control	Comply	

Typical Present Practice

- RADIUS is popular in the electric energy sector.
- RADIUS is a client/server protocol that runs in application layer, using UDP as transport.
- Clients are network access servers—such as wireless access points, 802.1X-capable switches, virtual private network (VPN) servers, and dial-up servers

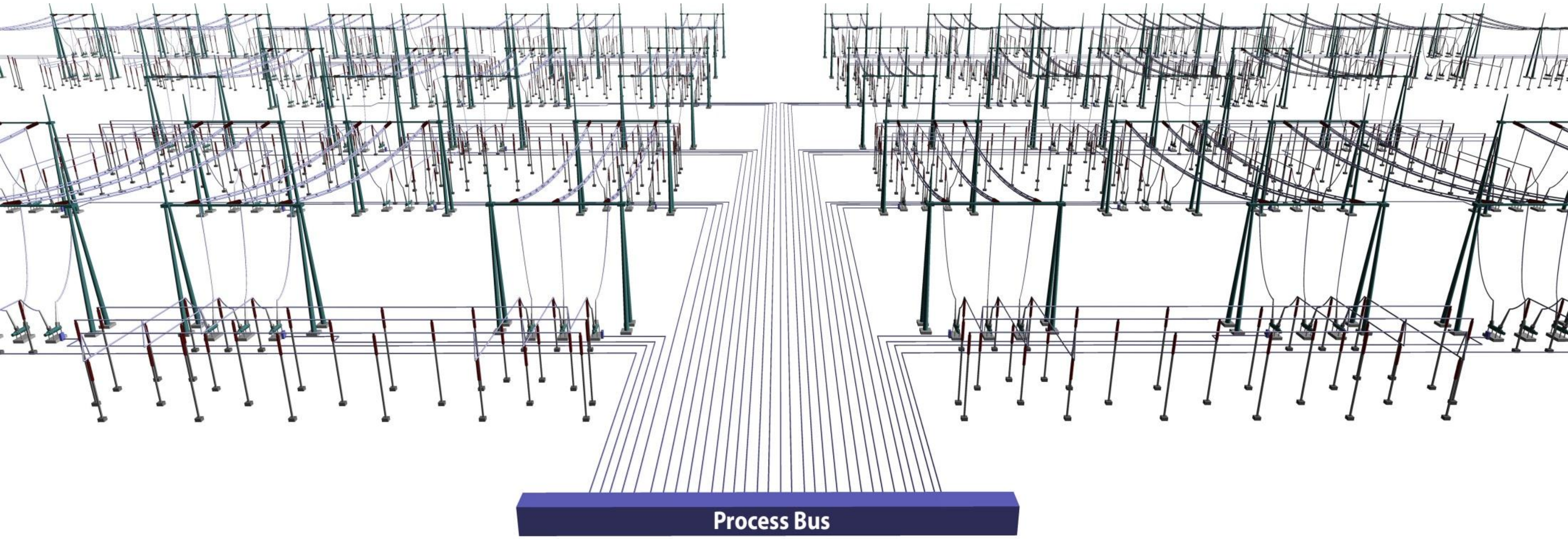
It serves three purposes:

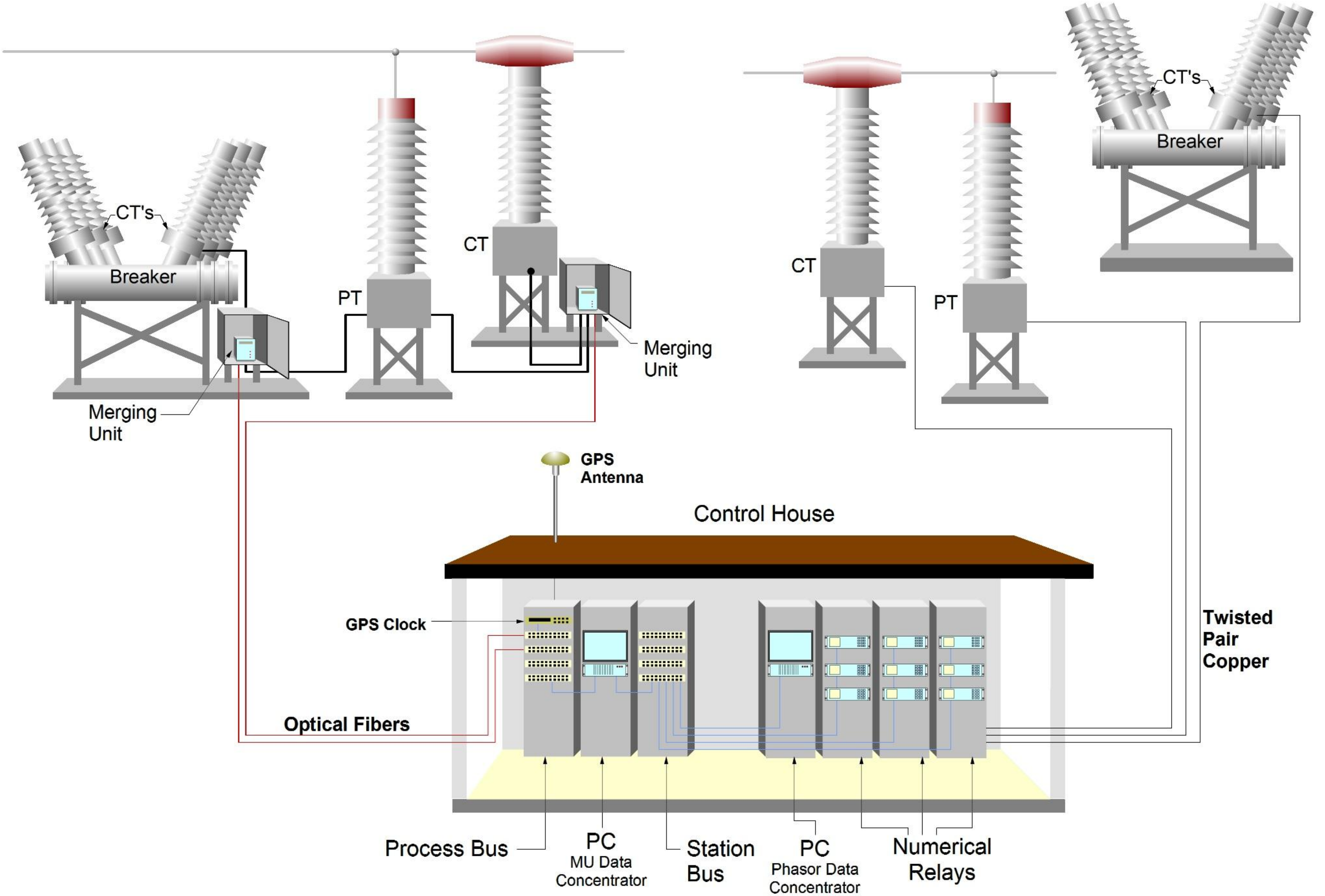
1. Authenticate users or devices before granting access to network and devices
2. Authorize users or devices for specific network services
3. Account for usage of services

Typical Present Practice

- Internet Protocol Security (IPSec)
- Confidentiality – encryption of data exchanges between substations.
- Integrity – routers at each end of communications (checksum or hush value of data)
- Authentication (signatures and certificates)
- Provides interoperable, high quality, cryptographically-based security for IPv4 and IPv6
- Transparent to applications
- Internet Key Exchange (IKE)

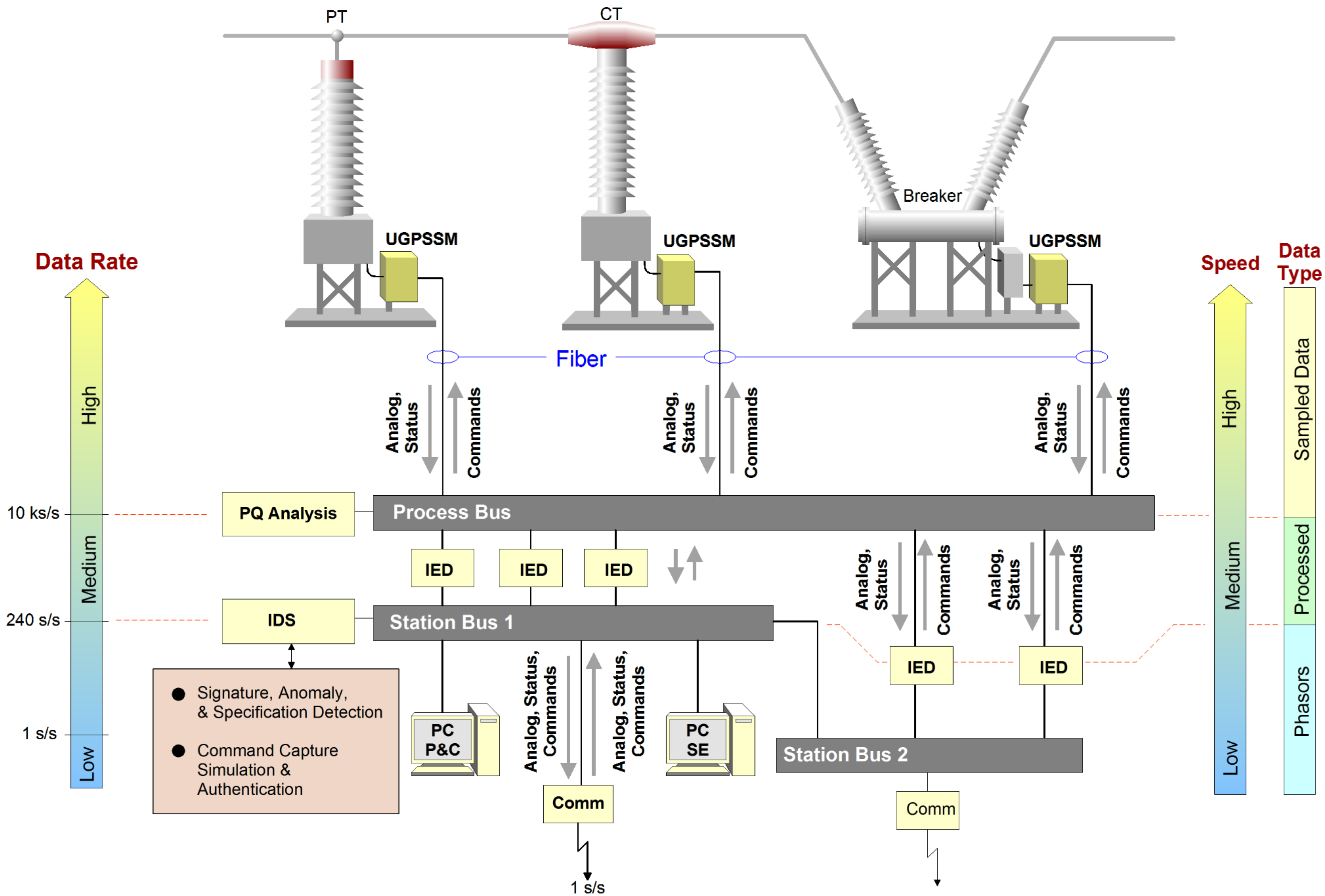
Need More…
New Approaches





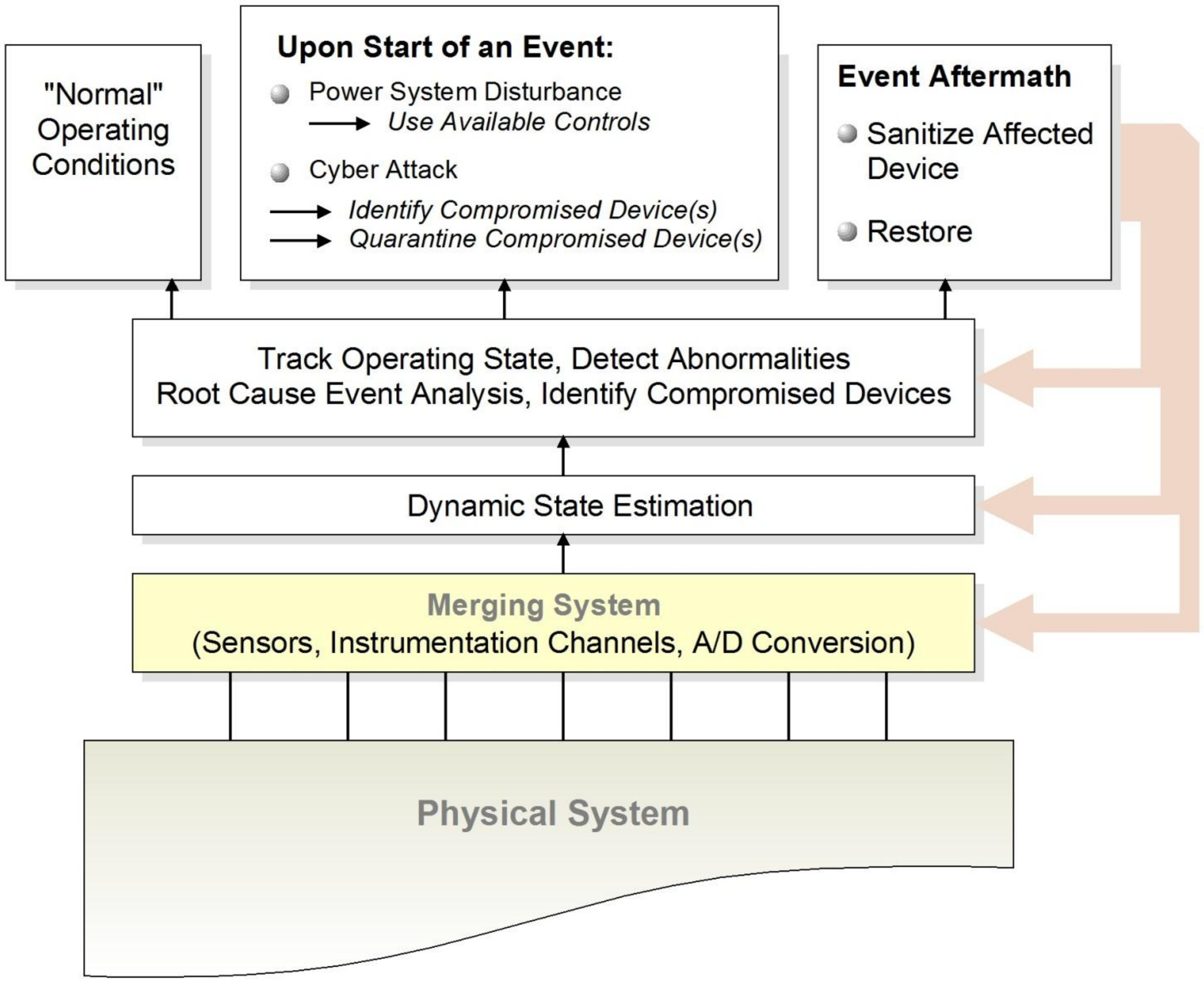
CT's
Breaker
CT
PT
Merging Unit
CT
PT
CT's
Breaker
Merging Unit
GPS Antenna
Control House
GPS Clock
Twisted Pair Copper
Optical Fibers
Process Bus
PC
MU Data Concentrator
Station Bus
PC
Phasor Data Concentrator
Numerical Relays

Data Flow / Applications



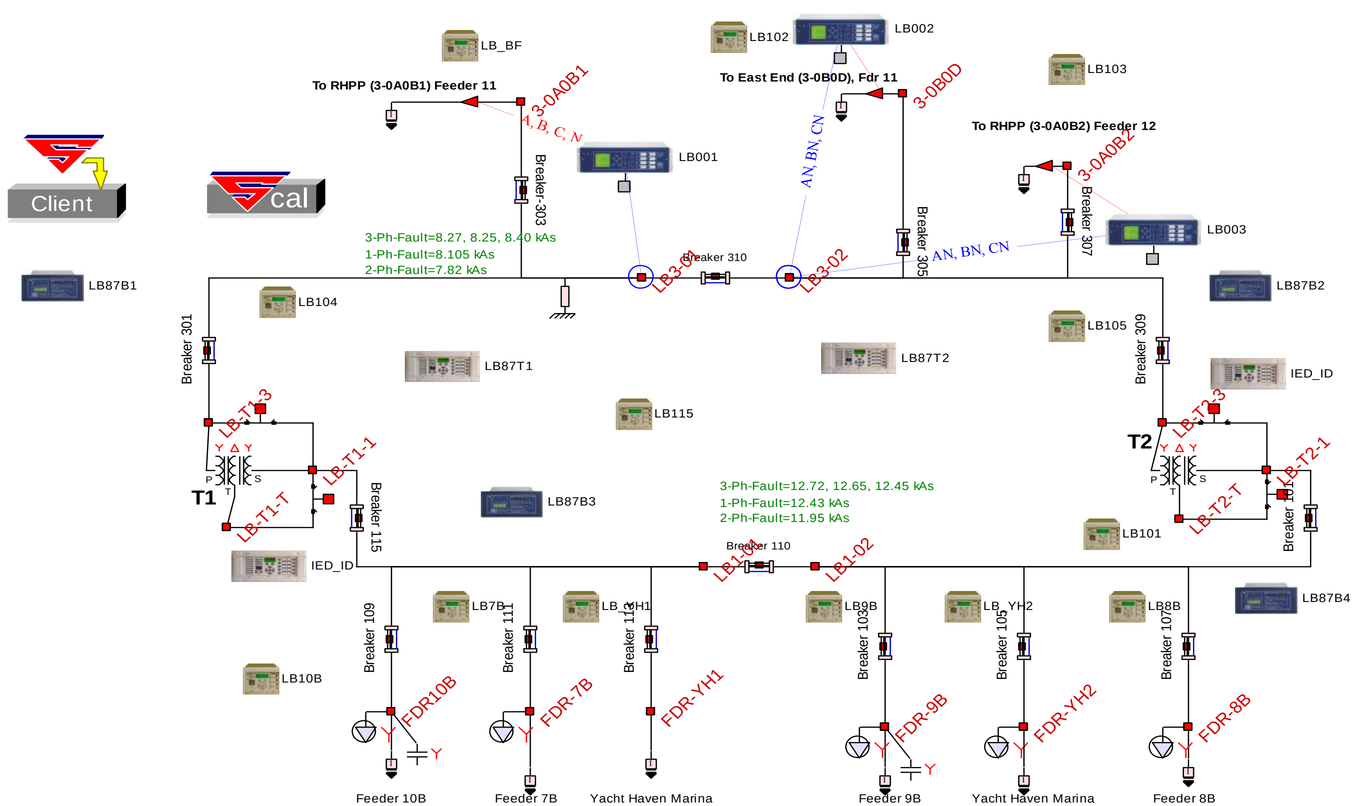
State and Model Tracking Based Approaches

Minimize/Eliminate False Positives



Physically Based Integrated Physical and Cyber System co-Model (PB-PCcoM)

The physical power system (a substation PC co-model is shown) is modeled in terms of its physical construction (3-phase breaker-oriented); the cyber system consisting of relays, instrumentation, communications and human interfaces is integrated with the physical system. Any changes in the physical system propagate to the cyber system and any command at the cyber layer is transmitted to the physical system. This co-modeling approach was introduced 30 years ago before cyber security was a concern.

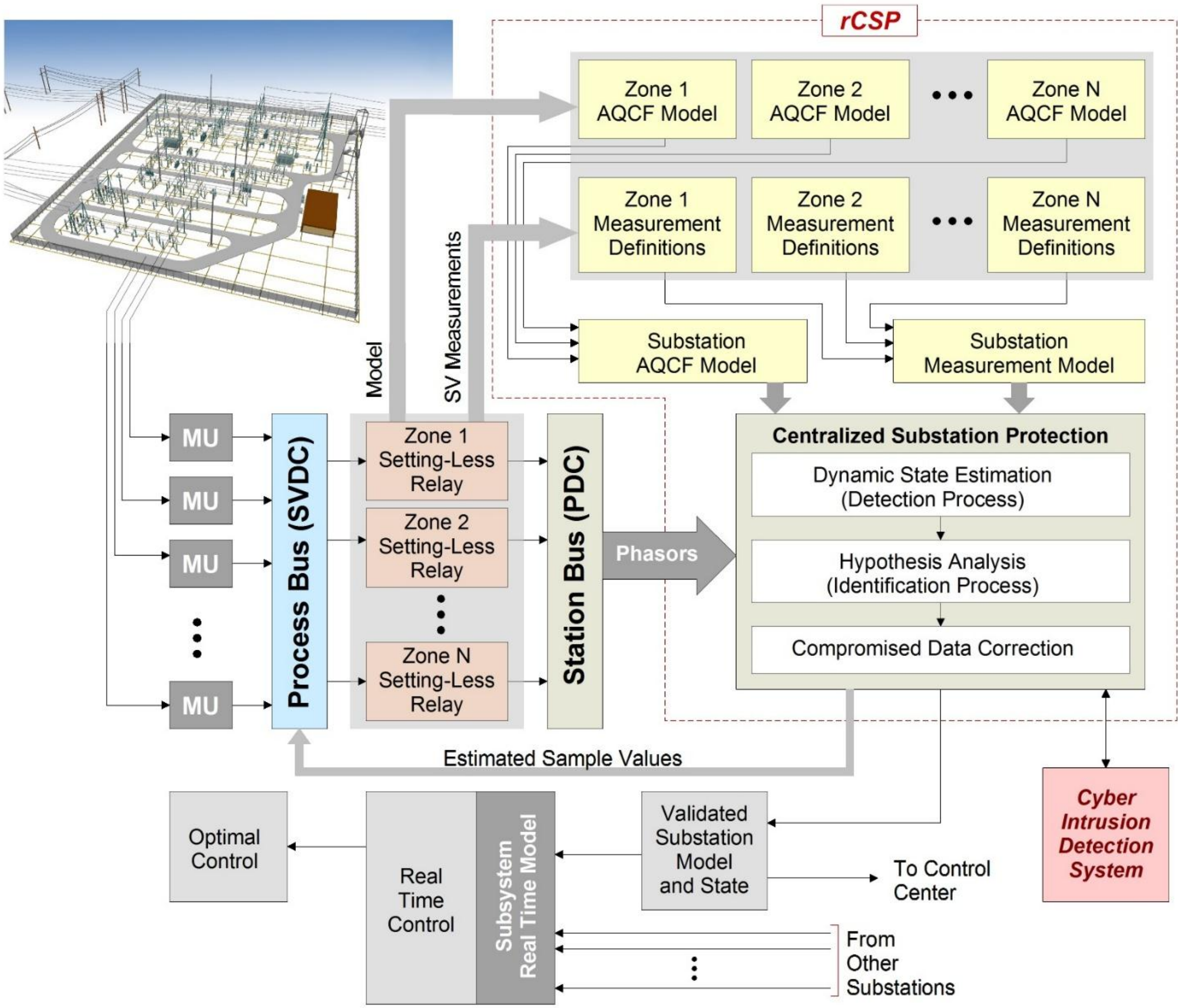


The integrated model enables co-simulation and evaluation of the complex interactions between the two systems.

Most importantly enables (1) immediate detection and blockage of adversary data and (2) context based authentication or blockage of commands via the cyber system in a seamless and timely manner. **Time response** of the authentication process is an extremely important issue.

ARPAe Project - (GT, SouCo, NYPA, EPRI)

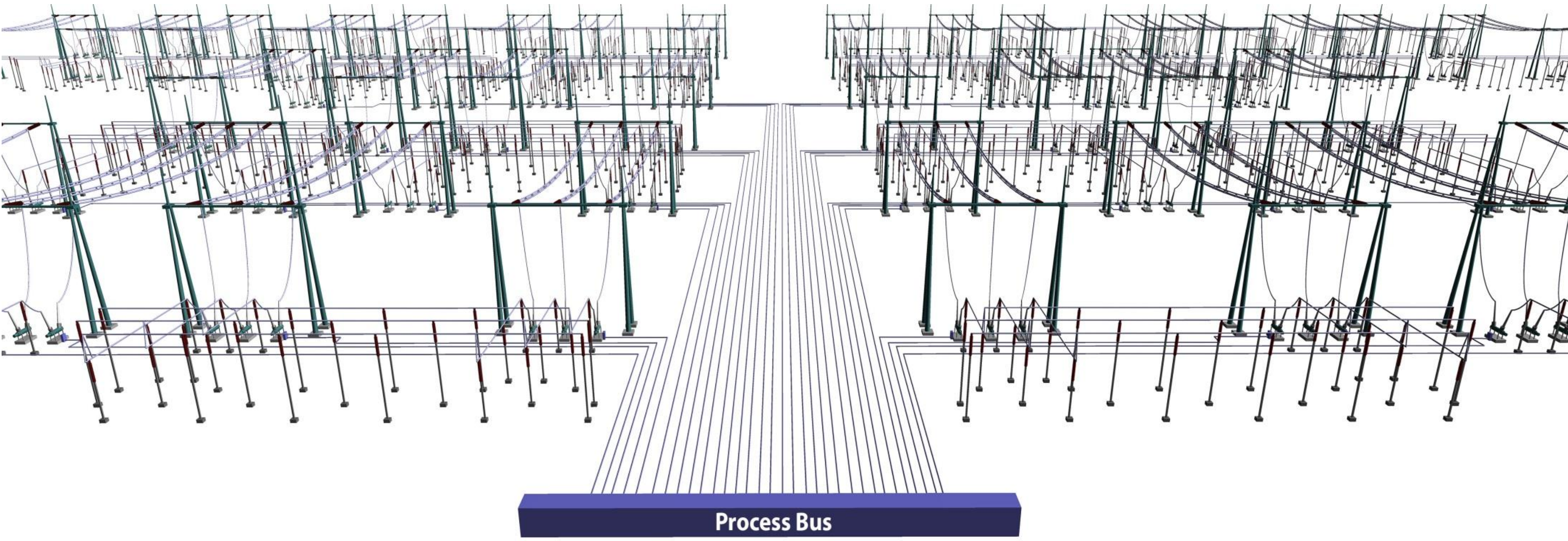
Resilient Centralized Substation Protection and Control (rCSP)



Core Technology: Dynamic State Estimation Based Centralized Protection Scheme

Data Integrity

1. Instrumentation Channel Errors
2. Hidden Failures
3. Cyber Data Attacks



Effects of Input Data Accuracy

Quality of Data is Affected from (a) Instrumentation Channel Errors, (b) Hidden Failures and (c) cyber data attacks. All Affect Performance of protective relays (legacy relays and setting-less relays).

Relays and merging units are becoming more accurate by using higher resolution in data acquisition and higher sampling rates.

Errors from instrumentation channels remain practically the same. Instrumentation channel errors have been much higher than the errors introduced by the data acquisition even in earlier generations of sensor less systems.

Merging Units offer a unique opportunity to perform error correction within a merging unit → MU provides corrected data in primary quantities.

Error correction enables more reliable detection of cyber data attacks

Impact of Hidden Failures/Cyber Attacks

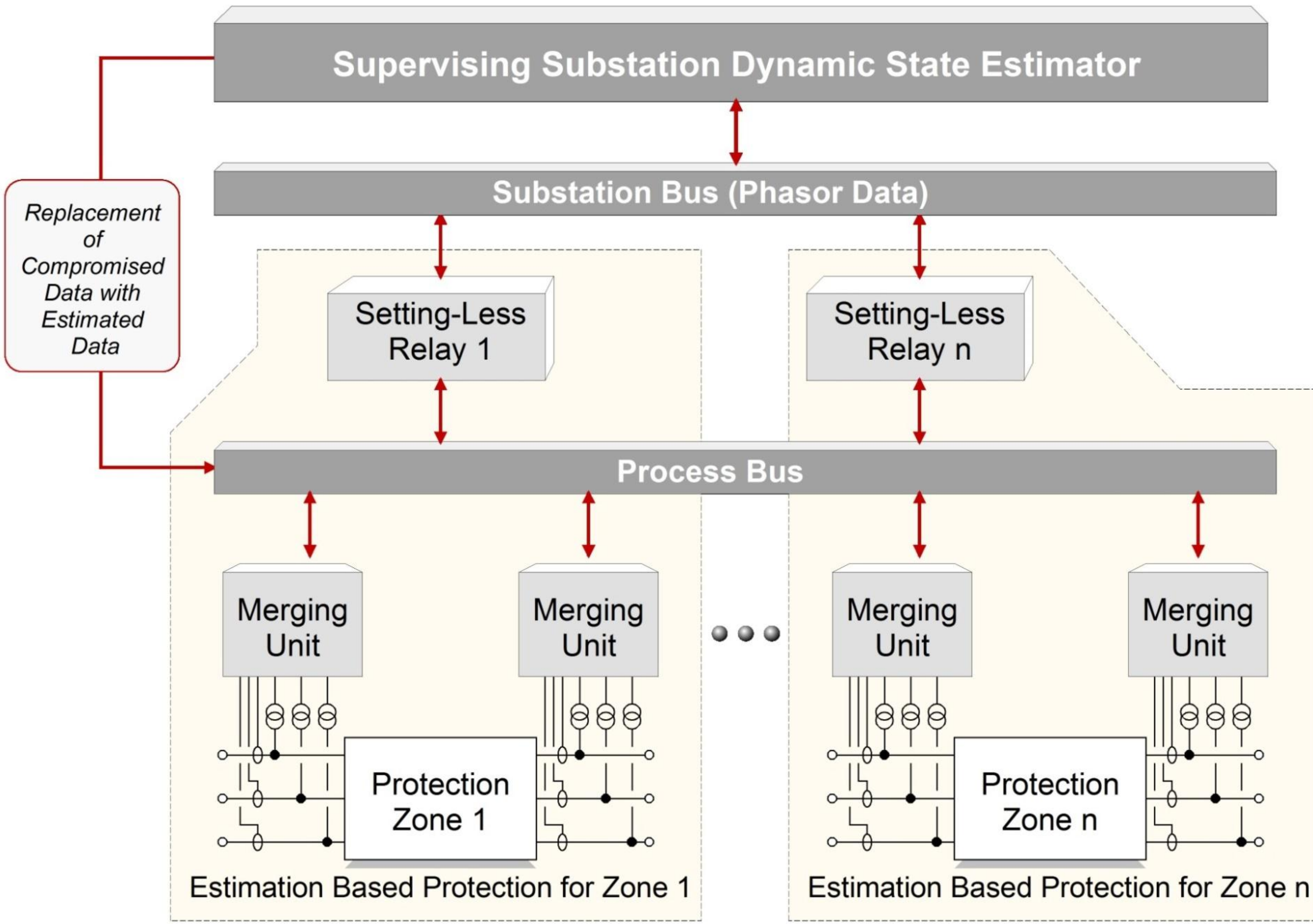
Hidden failures and cyber attacks corrupt the data “seen” by a relay, legacy or setting-less protective relay.

Hidden failures/cyber attacks will cause relay mis-operation whether it is a legacy or a setting-less protective relay.

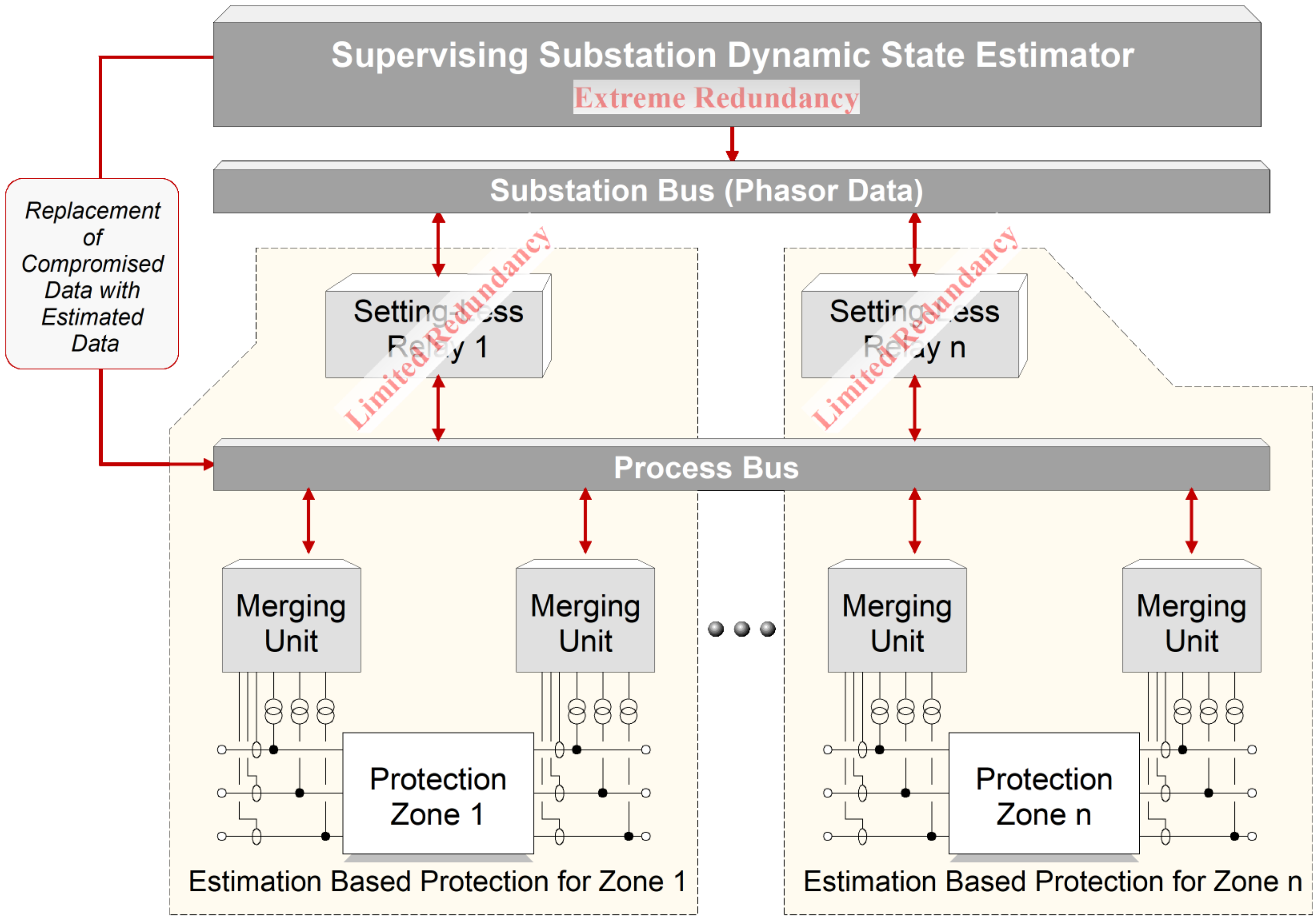
Need to identify hidden failures/cyber attacks and avert relay mis-operations.

Present State of Art: Some legacy relaying schemes can identify some hidden failures and inhibit relay operation. No capability to take corrective action. No capability to detect data alteration by cyber-attacks.

Proposed Method for Securing Data



Proposed Method for Securing Data



Dynamic State Estimation Based Centralized Protection Scheme (rCSP)

Hypothesis Testing: Observations

- At substation level redundancy is high (over 2000%)
- System is continuously running.
- Probability of simultaneous failure events is low

Hypothesis Testing: Mechanics

- Identify suspect measurements from residuals
- Group suspect data with certain criteria
- Determine “faulted devices” from setting-less relays output

Dynamic State Estimation Based Centralized Protection Scheme (rCSP)

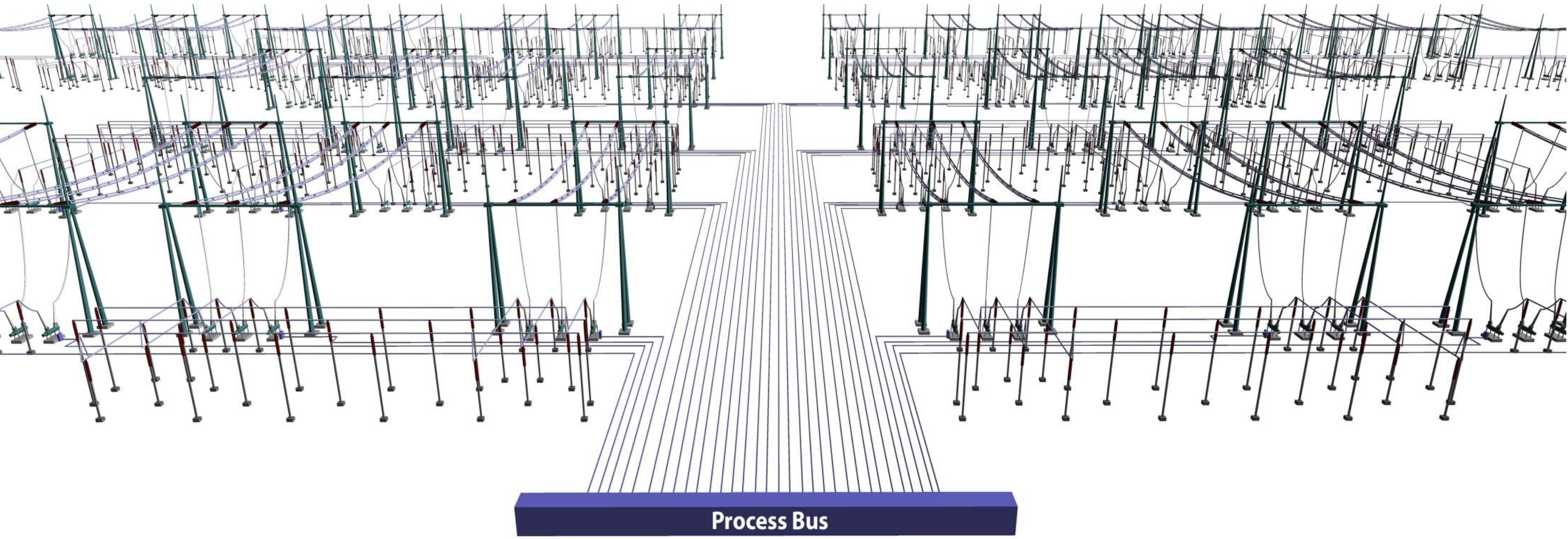
Hypothesis Type 1 (H1): (determine if a hidden failure exists) Remove suspect measurements and rerun DSE. If probability high → removed measurements are bad → identify root cause → issue diagnostics → replace bad data with estimated values. End hypothesis testing. Otherwise go to **H2**.

Hypothesis Type 2 (H2): (determine if a fault decision is correct). For the reported faulted device, remove all internal device measurements and remove the faulted device model from the substation model. Then rerun DSE. If probability high → the device is truly experiencing an internal fault. Allow zone relay to trip the faulted device. End hypothesis testing.

Hypothesis Type 3 (H3): (simultaneous hidden failure and fault) This test combines type 1 and type 2 hypothesis testing to cover the case of a simultaneous fault and a hidden failure. If affirmative, end hypothesis testing. Otherwise go to H4.

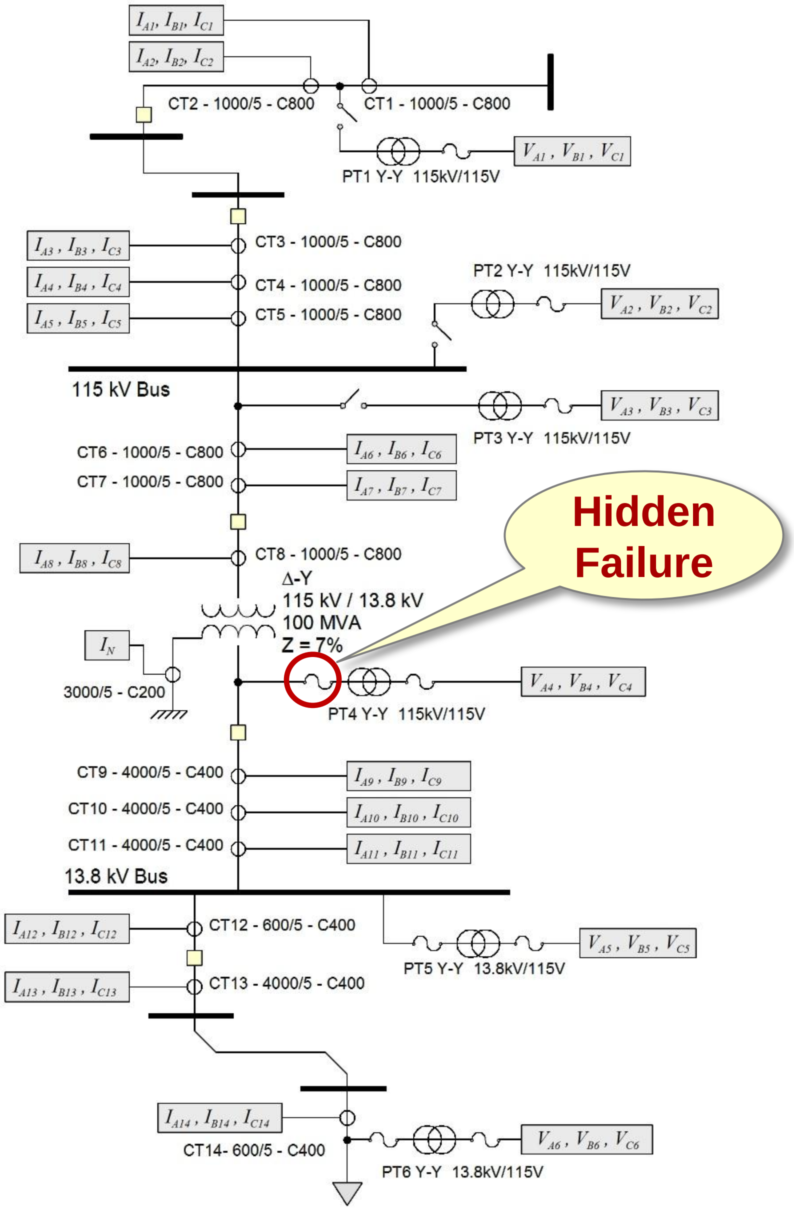
Hypothesis Type 4 (H4): (cyber attack) Remove data originating from an IED. Then rerun DSE. If probability high → the IED has been compromised.

Examples of Intrusion

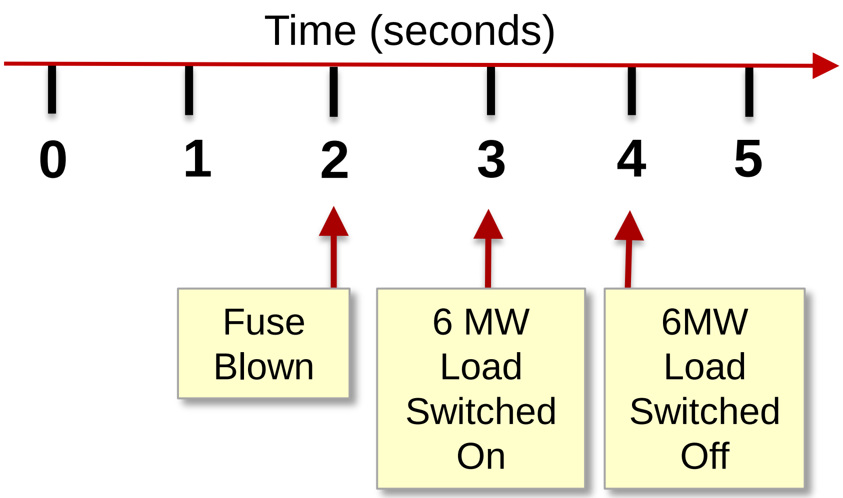


Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A



Sequence of Events

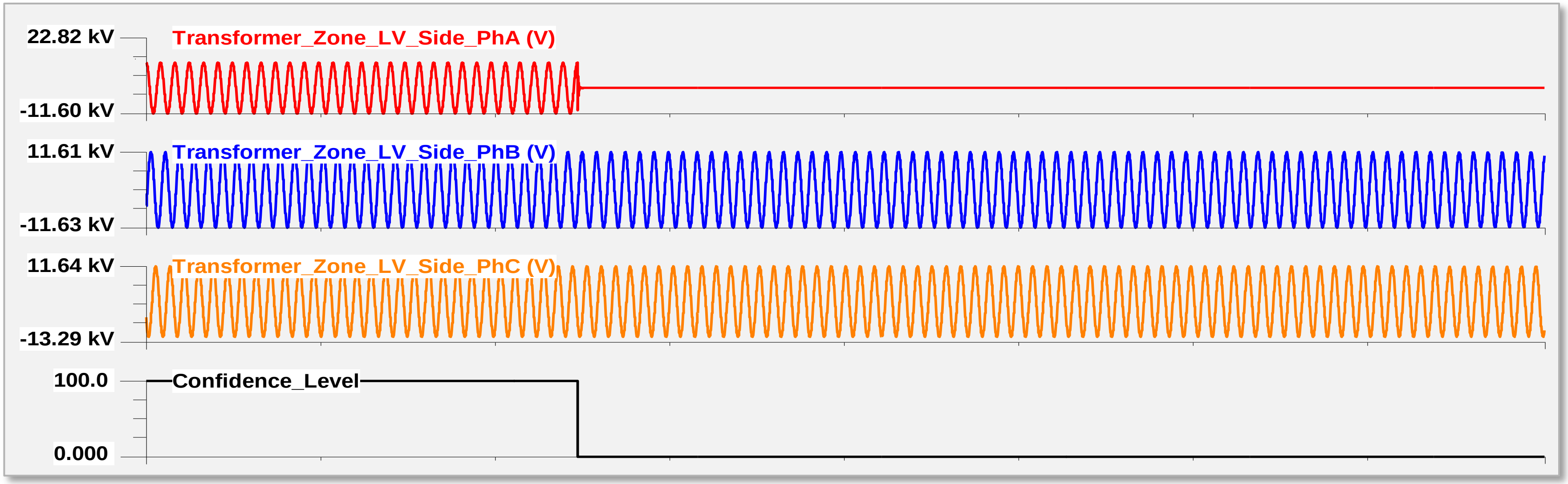


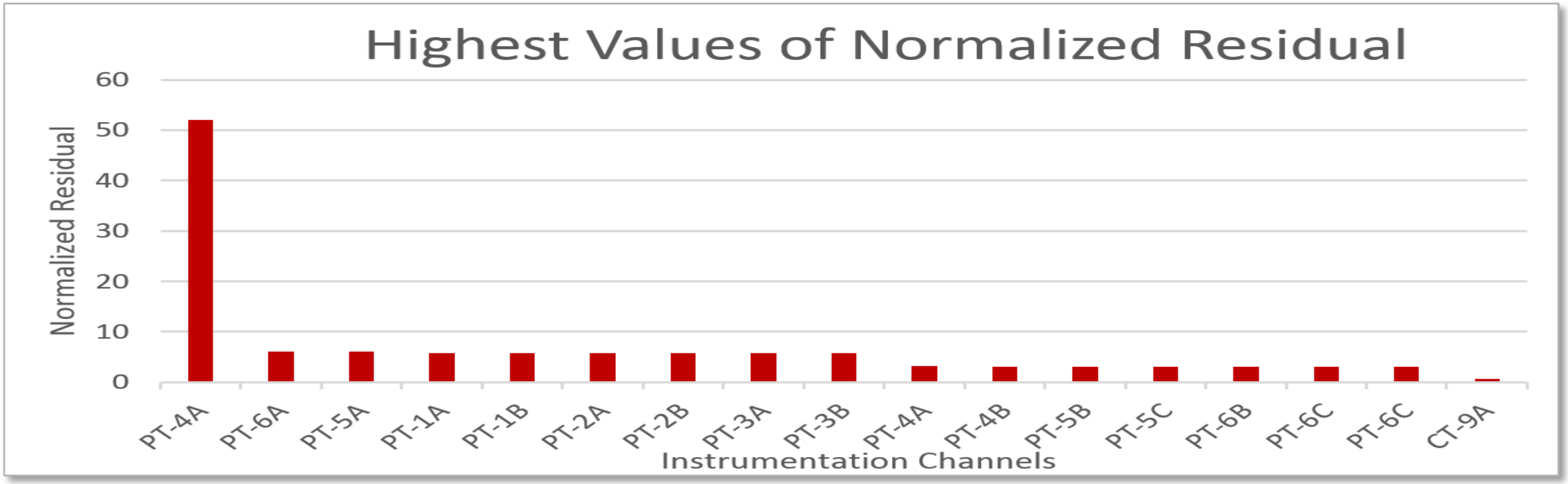
5 Protection Zones:

- 115 kV Transmission Line
- 115 kV Bus
- 115/13.8 kV , 36 MVA Transformer
- 13.8 kV Bus
- 13.8 kV Distribution Line (one of the two)

Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A Setting-less Relay of Transformer Zone

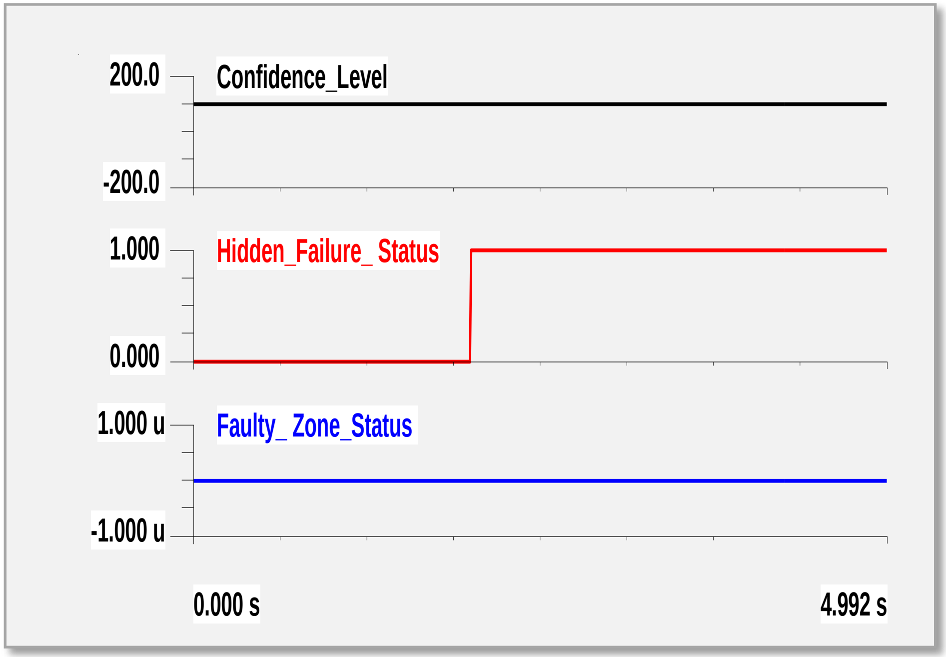


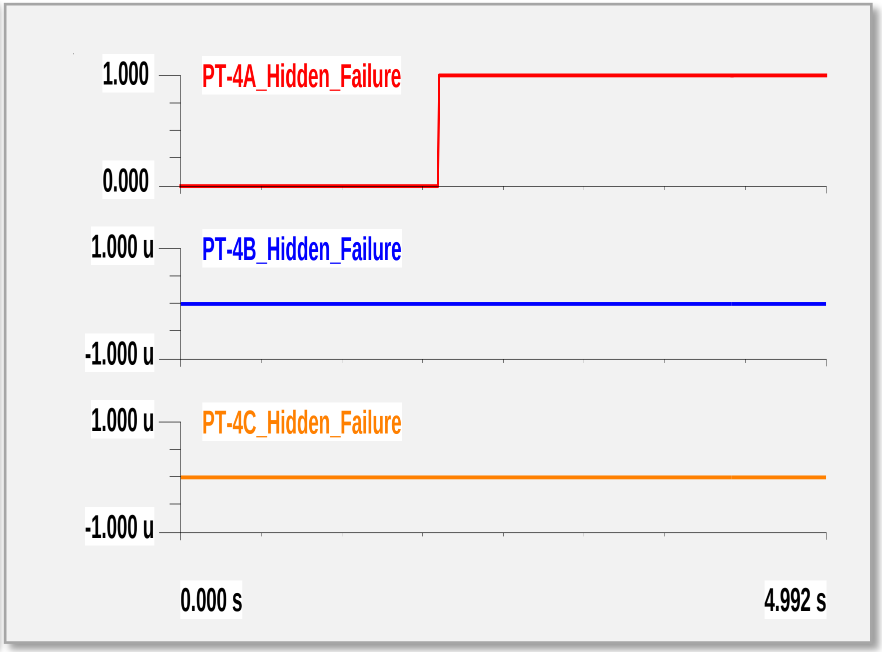


Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A

Centralized Protection Scheme :

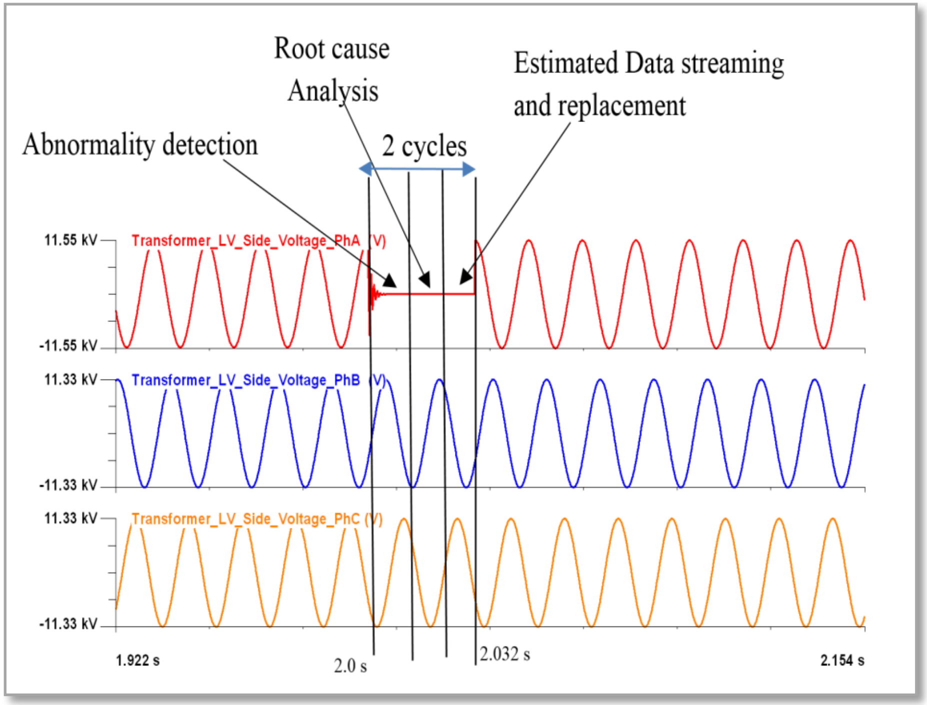


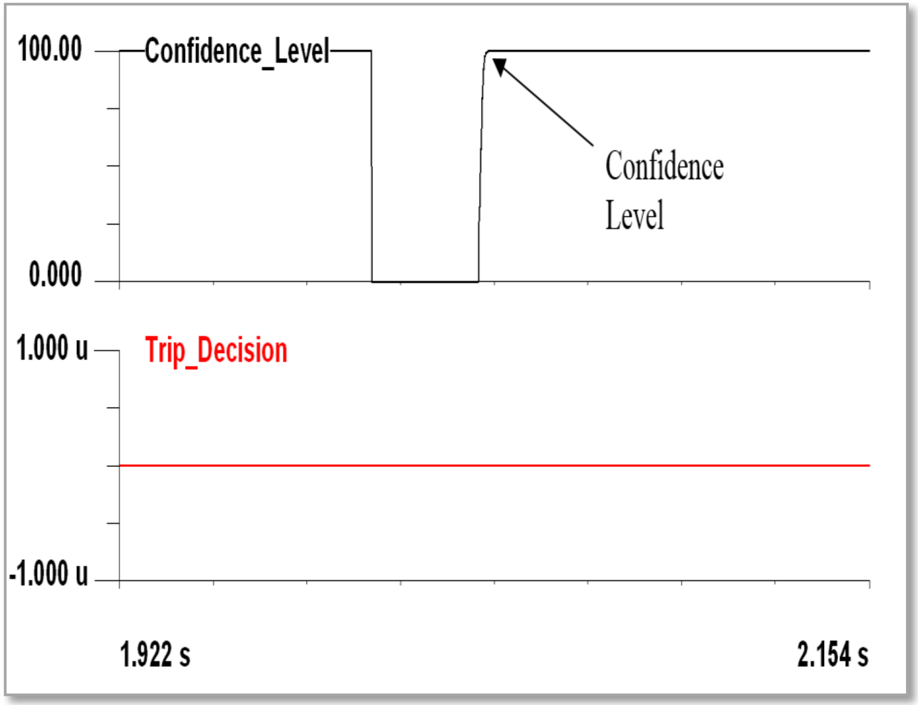


Numerical Example

Case1: Primary Fuse Blown Y-Y, PT-4A

Compromised Data Correction :

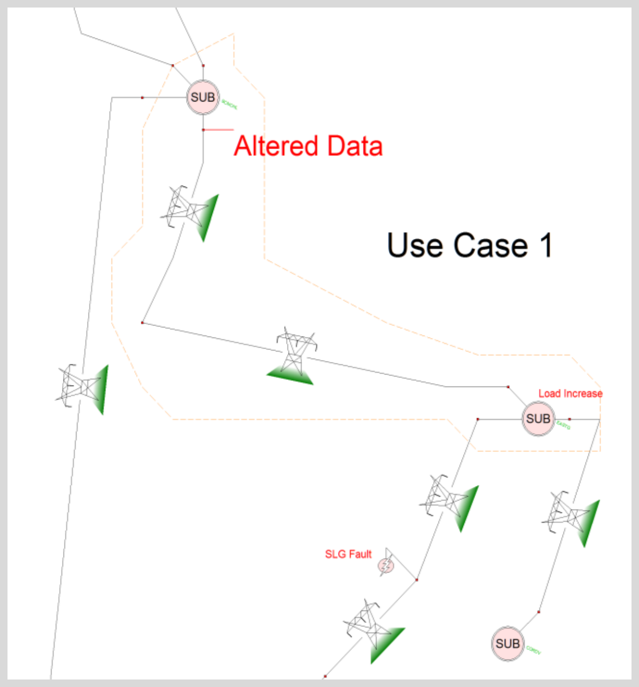




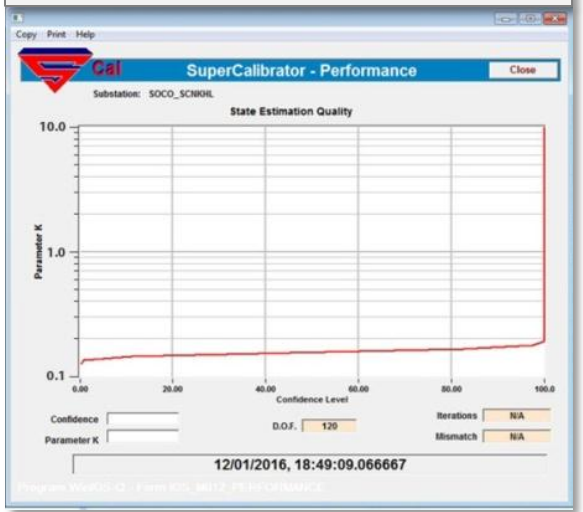
Example of Intrusion Detection

Data Attack Experiments:

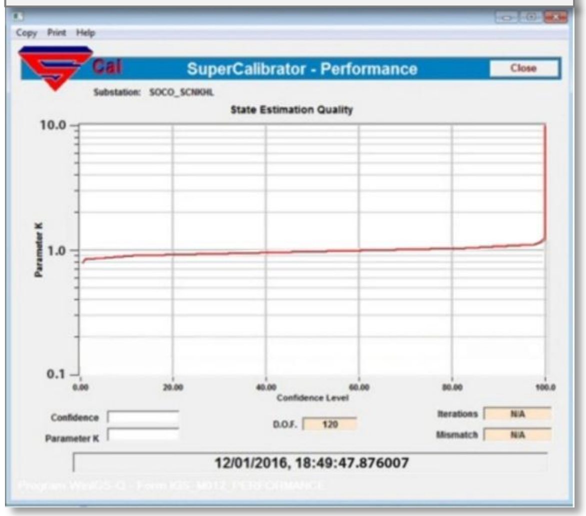
- Attackers were given access to system.
- They stage their own attacks, system does not monitor their activity.
- Attack → Change Relay Settings: from 1200:5 to 2400:5



Before Attack



After Attack



Example of Intrusion Detection

Performance Characteristics:

- Detection of data attack is almost instantaneous (25 ms or less). It is detected at the first execution of the dynamic state estimation after the attack. Dynamic state estimation executes once per 16.66 ms.
- Identification of compromised device is also fast (an additional 8 ms) by hypothesis testing. It also provides probability of certainty.
- Corrective actions: (a) quarantine compromised device, (b) block any access to the system, (c) sanitize and restore.
- Assuming that attacks can occur at one device at a time, an attack can be foiled and stopped in real time.

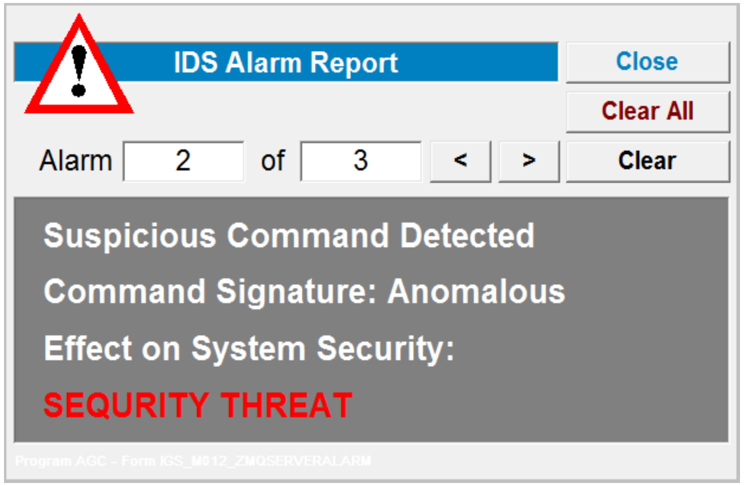
Context Based Command Authentication

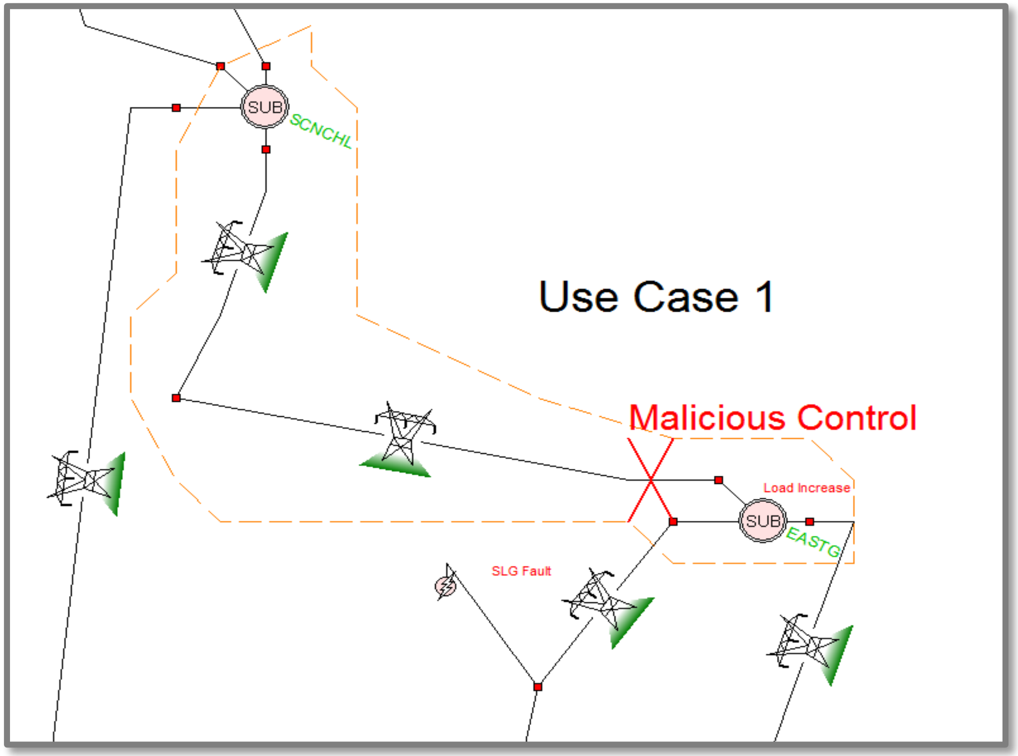
- Capture command,
- Determine effect of command on system using real time model and faster than real time simulation and
- Authenticate/Block command on the basis of the effects on the system.

Example of Intrusion Detection

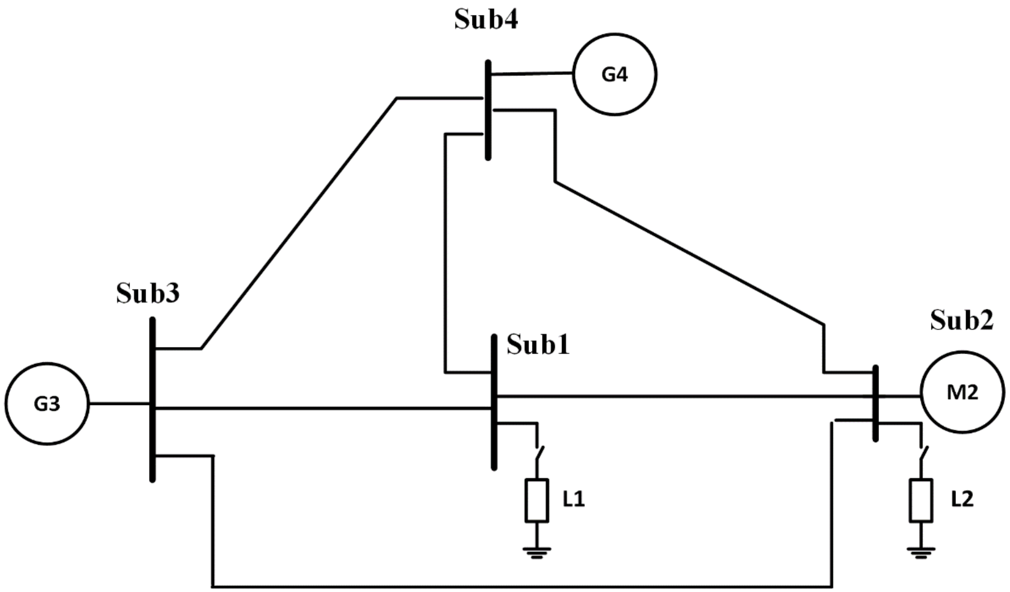
Attack Experiments: Attackers were given access to system. They stage their own attacks, system does not monitor their activity.

Attack: at time t = 2.5 sec, a malicious control is sent to open the breaker of the Eastgate-Scenic Hills line in the Eastgate substation

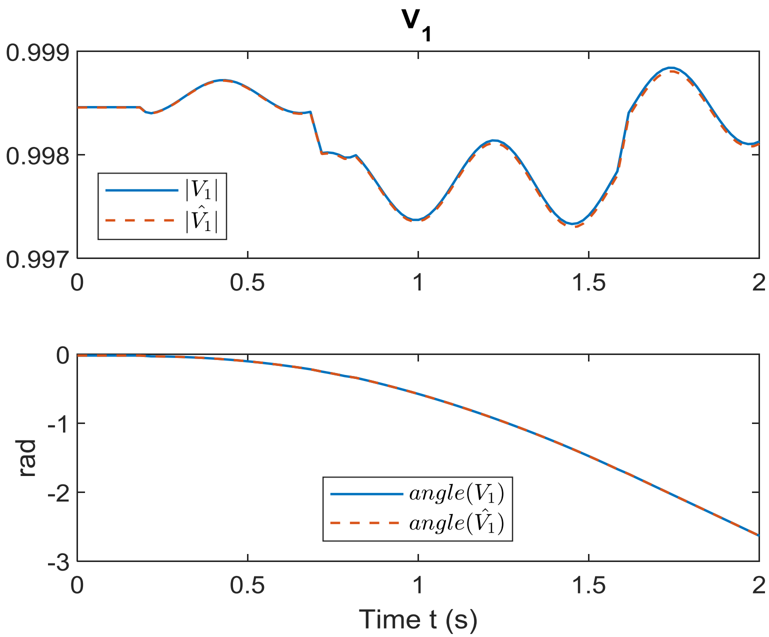




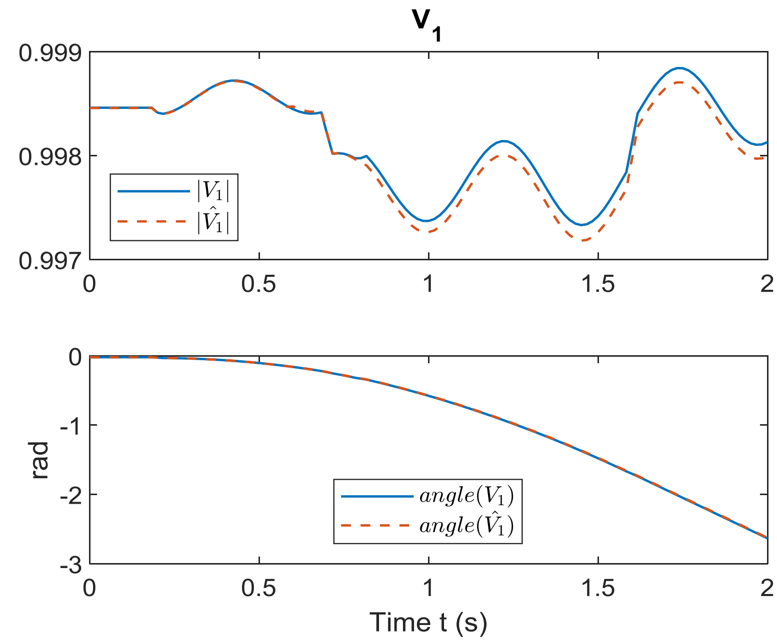
Numerical Example of GPS Spoofing Detection



Without GPS Spoofing



With GPS Spoofing



SouthernCo - Georgia Tech Work

Implementation of DSE on Three SoCo Substations

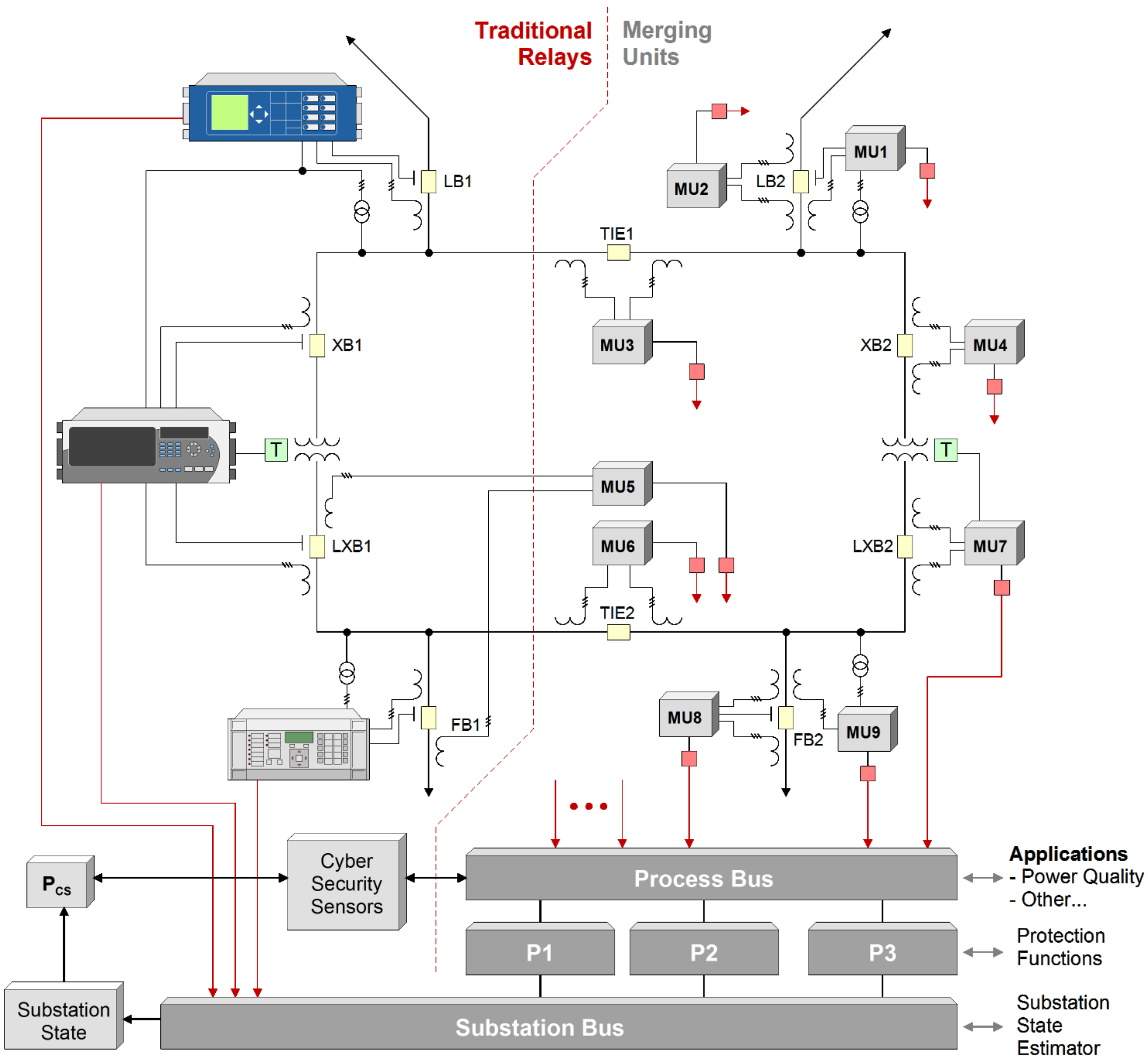
Additional Benefits

Reduced Control House Size

Reduced Wiring

GT Laboratory (PSCAL)

Dedicated Lab for Protection, Control & Cyber Security Testing: Continuous Operation of Fully Automated Substation: Complete Substation Cyber Infrastructure



Configuration is a full replica of the IT infrastructure of a modern substation with multi-vendor equipment

Combines numerical relay architecture with new architectures based on merging units.

It is driven by a high fidelity simulator capable of reproducing real life conditions

Unique capability for simultaneous testing of protection, control and cyber security

Enables realistic testing of Intrusion Detection System in an almost field conditions environment using the PB-PCcoM approach.

Additional Cyber Security
Encrypted Hash generated by MU and embedded in streaming data

Concluding Remarks

The industry supported by IEEE and CIGRE Efforts Move Towards the DIGITAL SUBSTATION.

The entire process is becoming fully automated (many efforts towards autonomy) with self healing capabilities against data errors, hidden failures and cyber attacks.

The technologies under development offer three distinct benefits:

(a) Drastically improved operational reliability

(b) Reliable defenses against cyber attacks

(c) Reduced Cost

Τέλος