SCHWEITZER ENGINEERING LABORATORIES

How Would You Know?

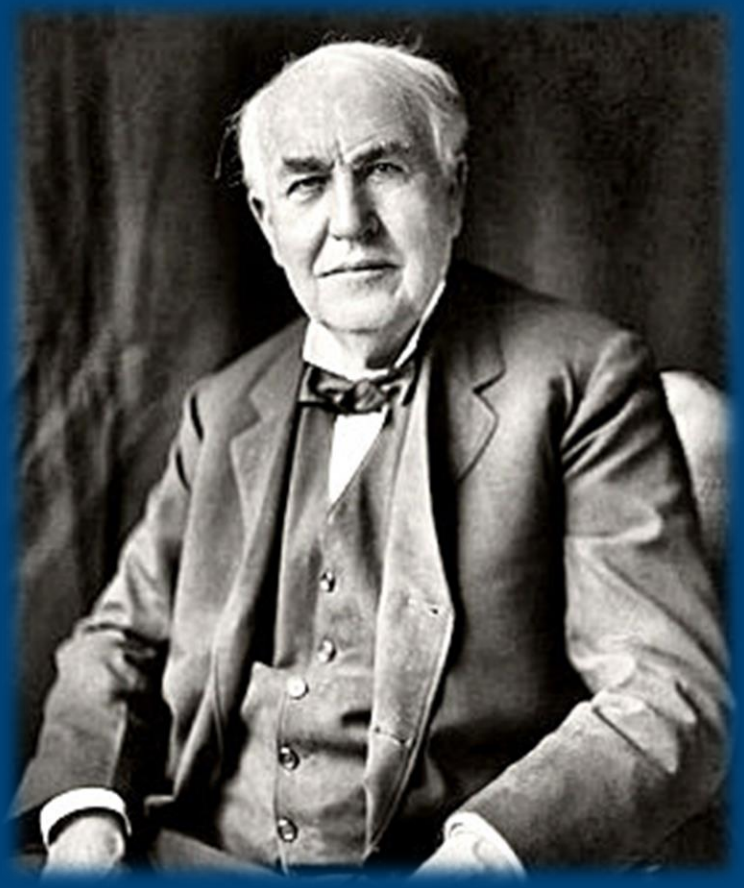
TCIPG Seminar Series on Technologies for a Resilient Power Grid

December 5, 2014

David E. Whitehead, PE
Vice President, Research & Development, SEL

What Are Our Energy Expectations?

- *Customer:* Safe, reliable, and economic delivery of electricity
- *Supplier:* Reasonable return on investment



Thomas Alva Edison
1847 – 1931

Samuel Insull
1859 – 1938

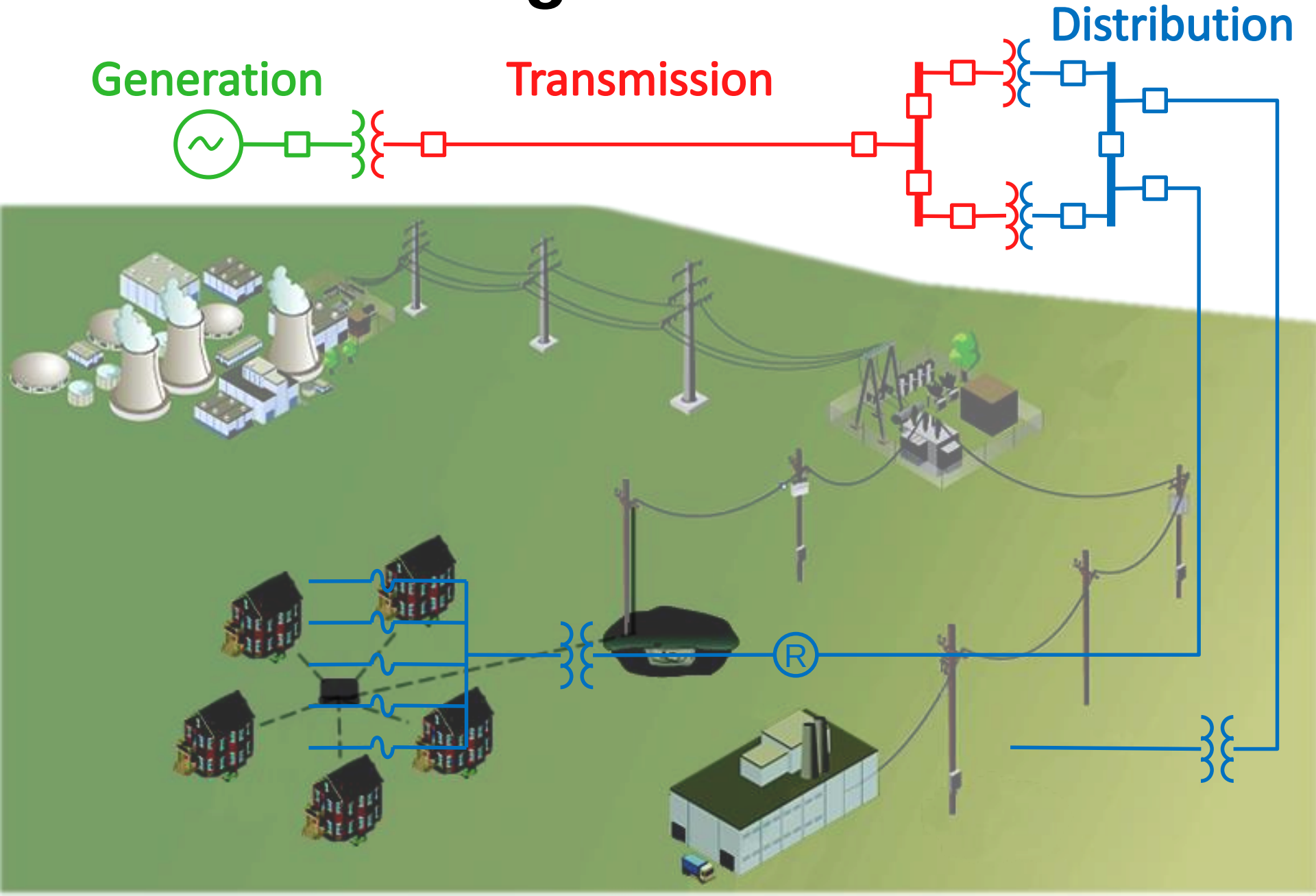
“Unless we can fulfill our primary duty to the public, viz., give absolutely continuous service, we fail in the obligation that we have undertaken to the community in accepting a franchise from the city to manufacture and distribute energy in this community...” -- Samuel Insull

Our Challenges

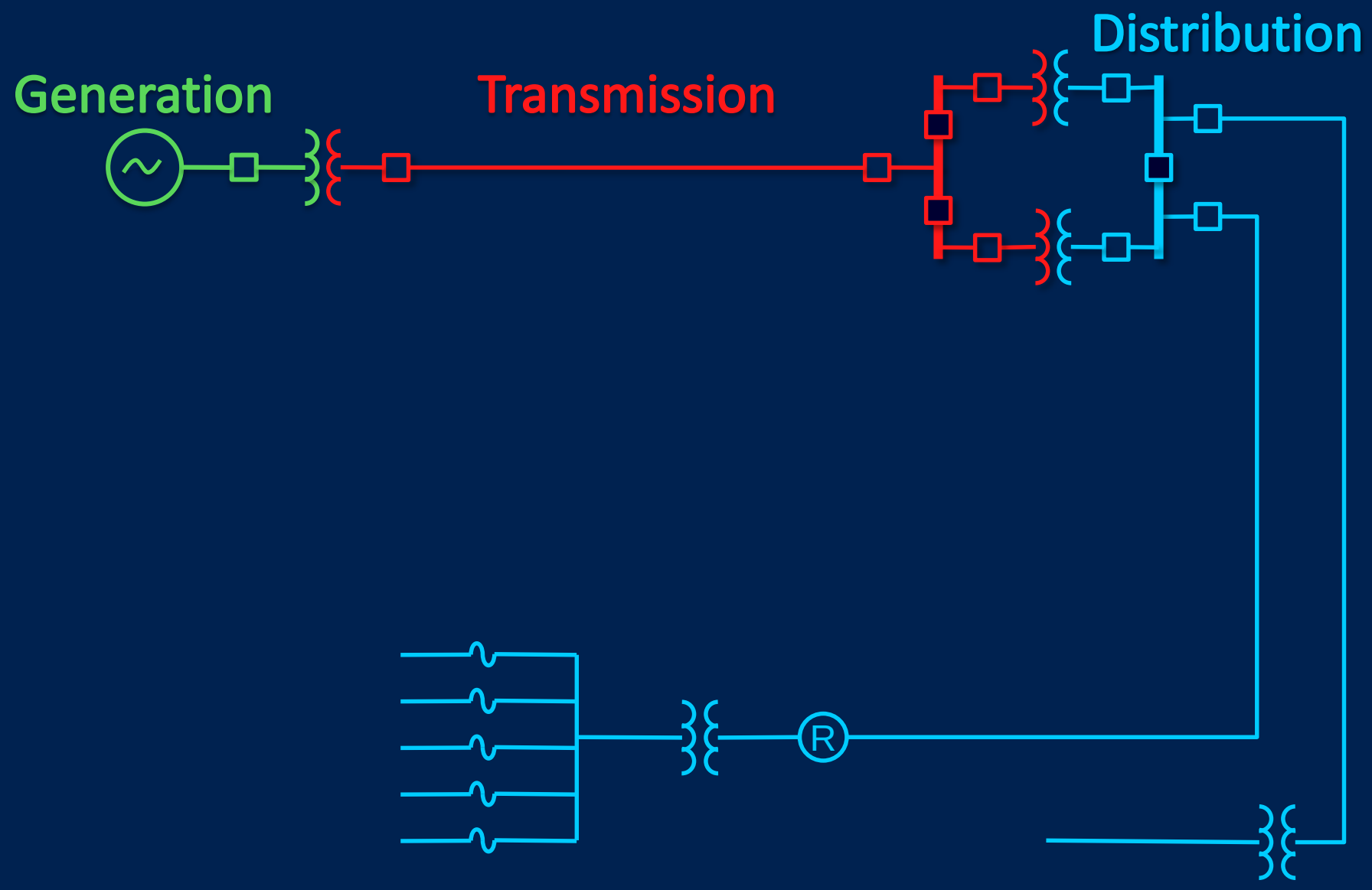
- Hard to build plants, lines, and subs
- Regulations, subsidies, mandates, CO_2
- Intermittent sources, consistent loads
- Loads will increase as economy recovers
- Stability, thermal limits, age of equipment
- Customers less patient with outages
- Aging workforce
- *Cybersecurity*

- Power systems operated for 80 years without cyber controls
- Cyber is a *convenience* not a requirement

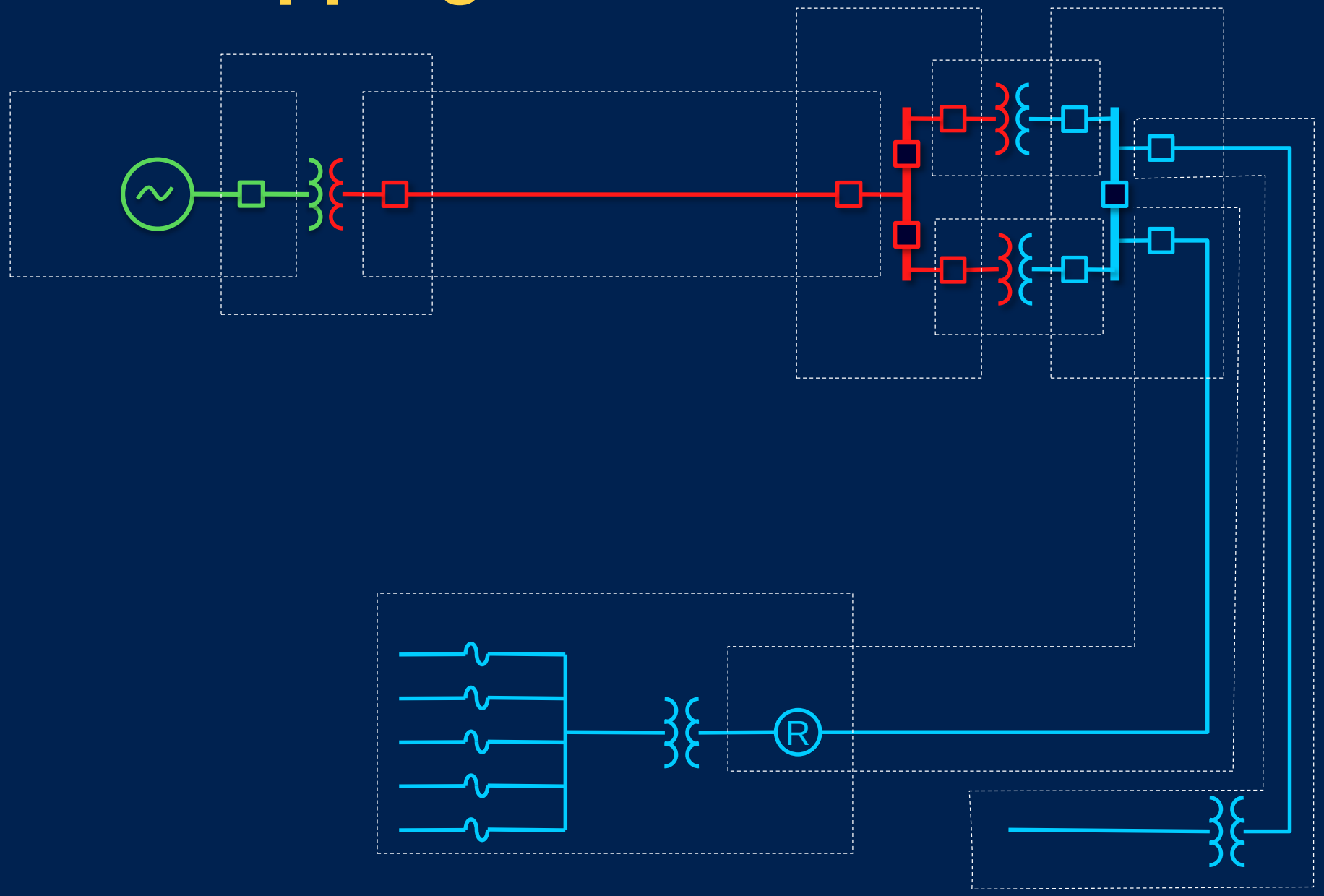
Protecting the Power Grid



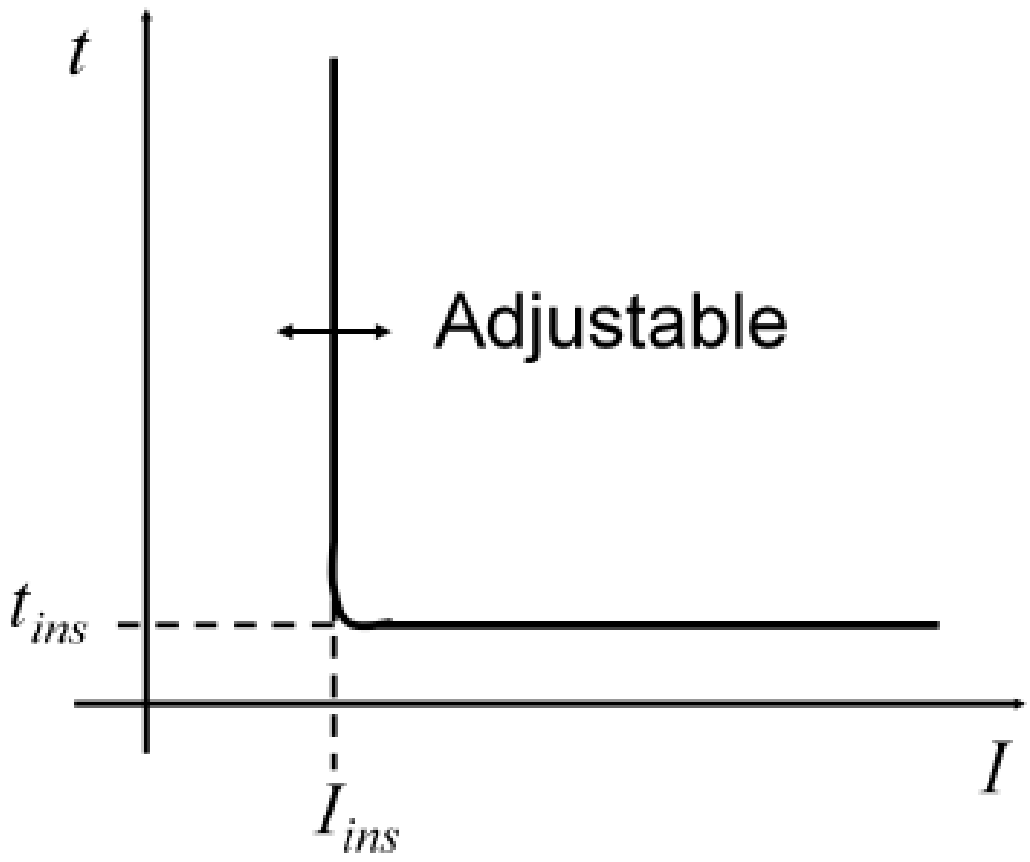
Protecting the Power Grid



Overlapping Zones of Protection

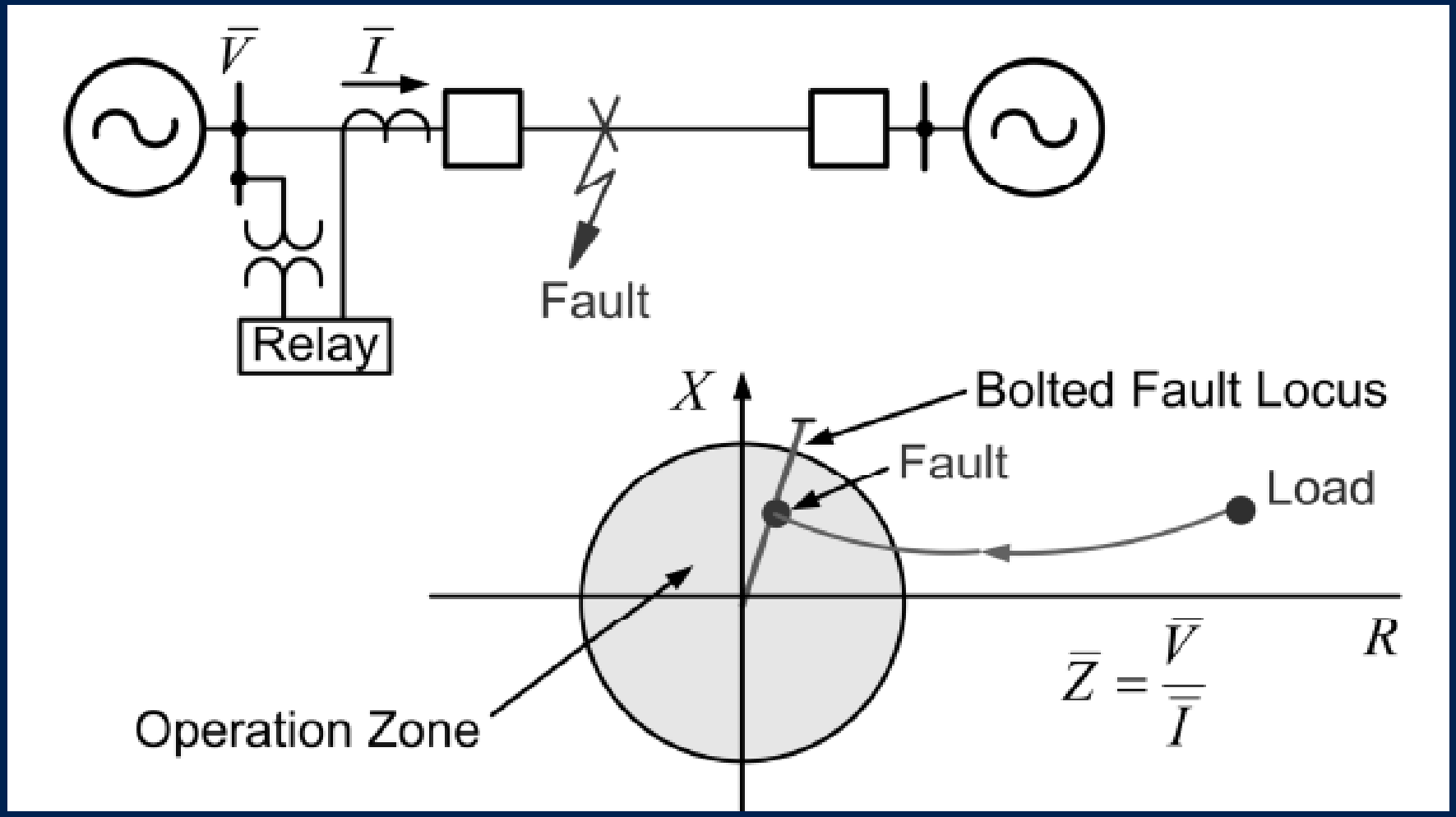


Overcurrent Element (ANSI 50)

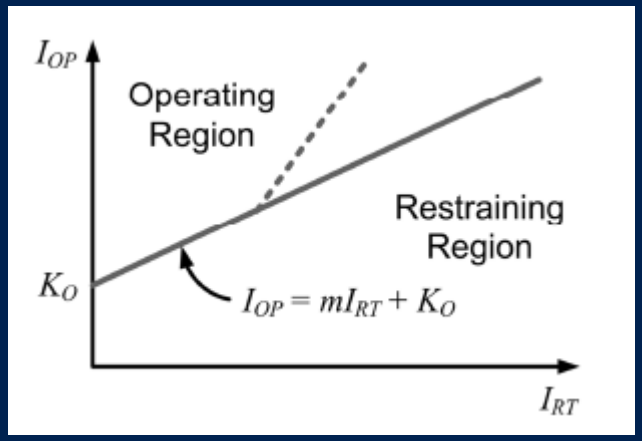


Time t_{ins} < 1.5 cycles

Distance Element (ANSI 21)

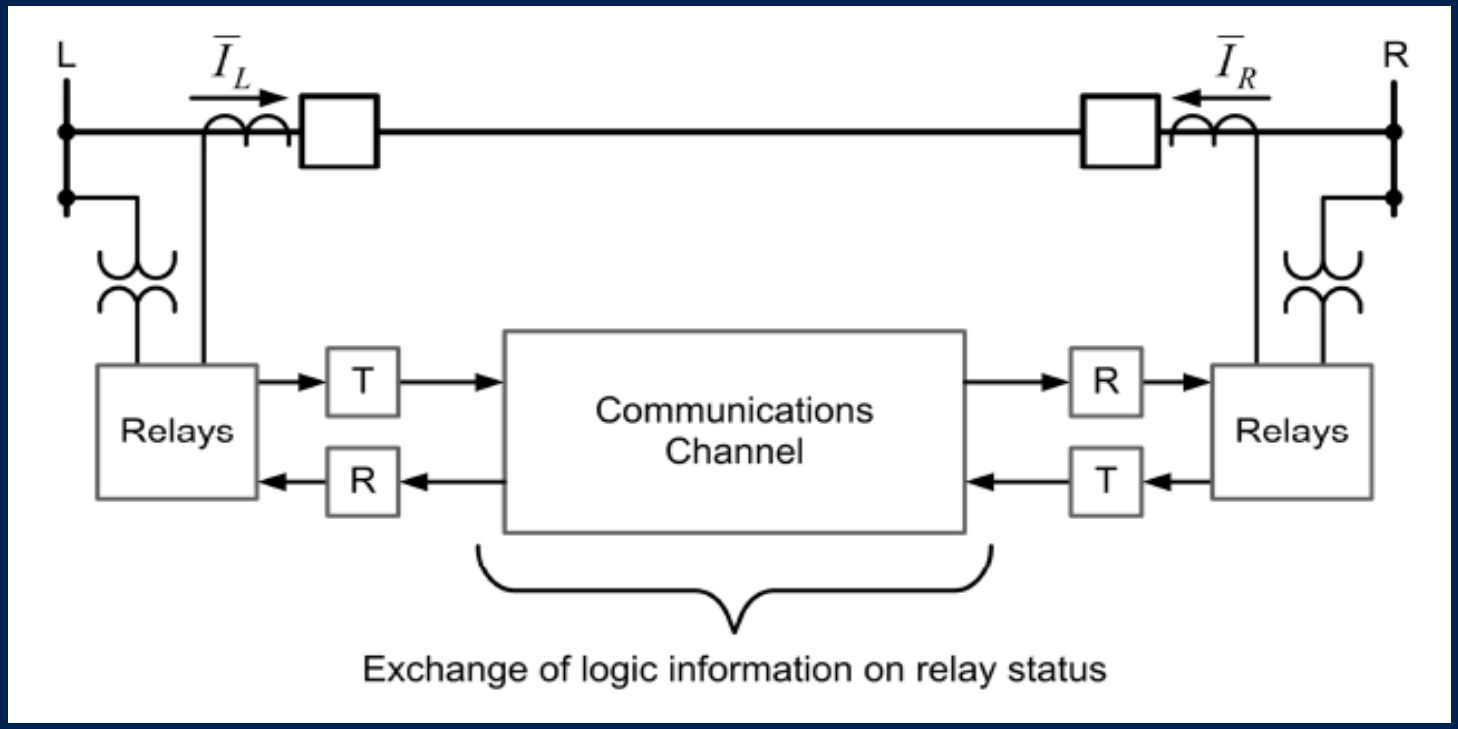


Current Differential Element (ANSI 87)

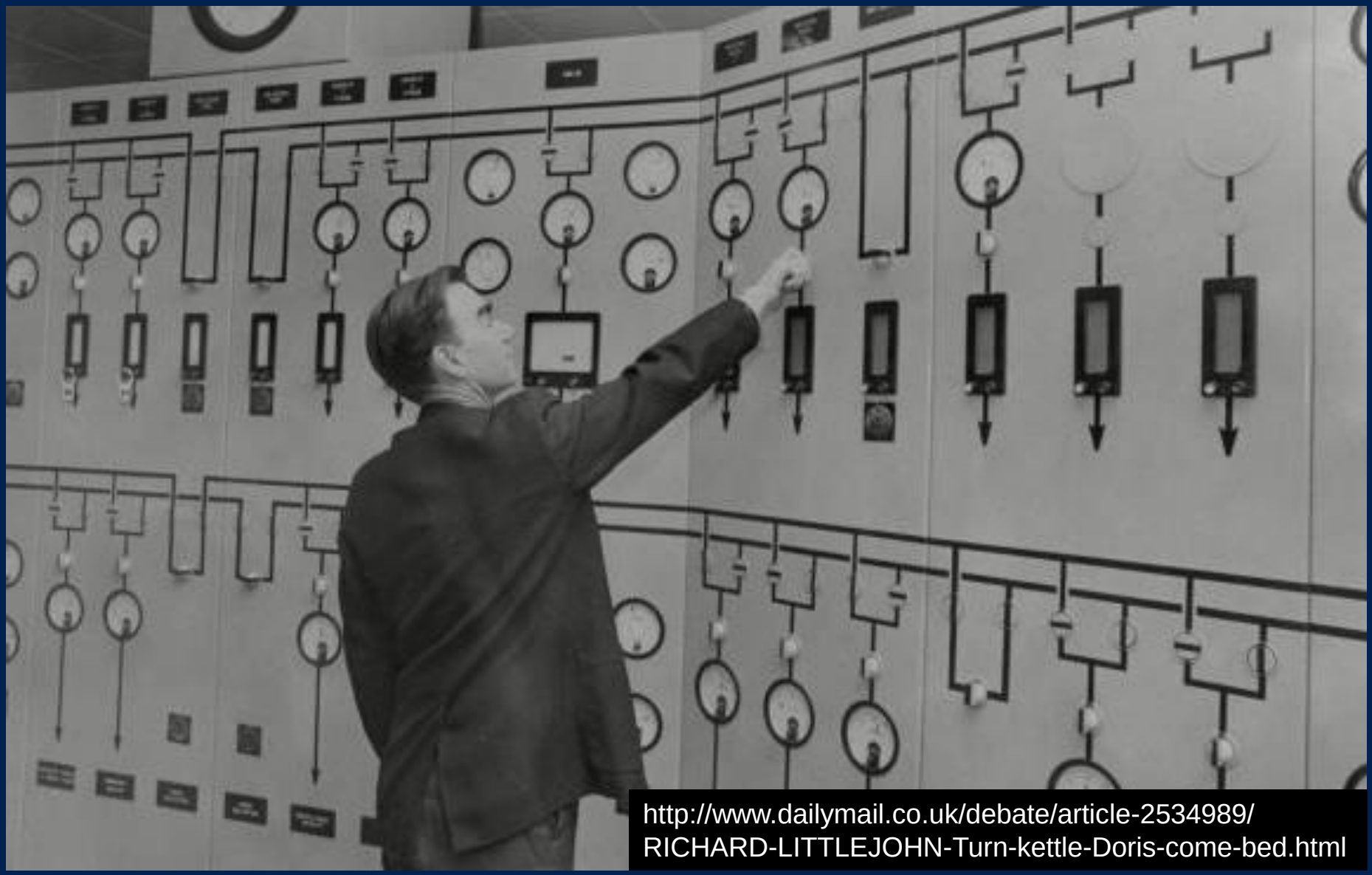


$$I_{OP} = \left|\overline{I}_L + \overline{I}_R\right|$$

$$I_{RT} = k\left|\overline{I}_L - \overline{I}_R\right|$$



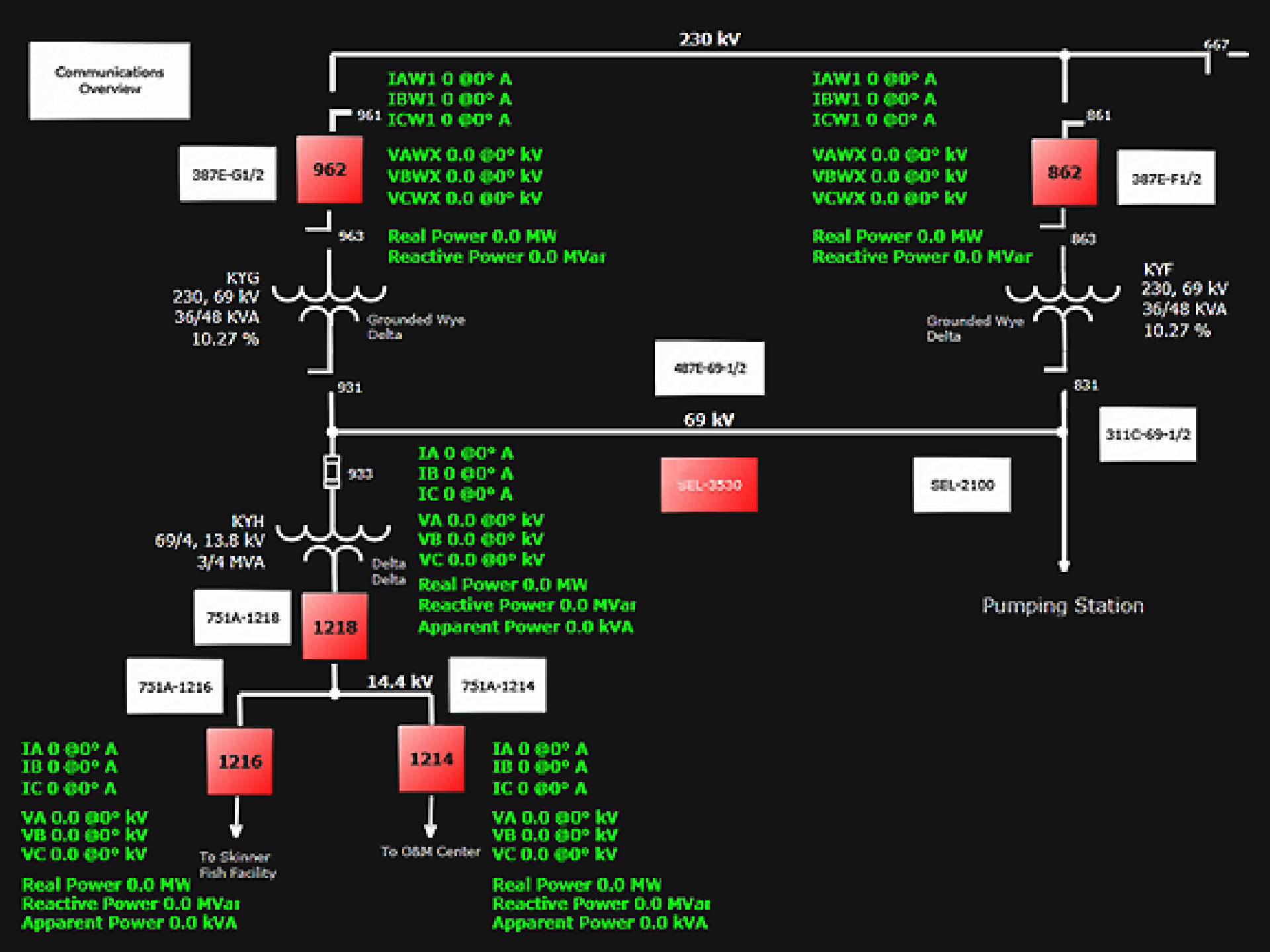
SCADA in 1960s



http://www.dailymail.co.uk/debate/article-2534989/RICHARD-LITTLEJOHN-Turn-kettle-Doris-come-bed.html

Can We Make Our *Cyber Convenience* Secure?

- Cyber information represents a physical system — this is a huge advantage compared to protecting “data” found in a bank account!
- Systems are “over measured”
- Often there are multiple ways to monitor, control, and allow access to systems


Communications Overview
230 kV
667
IAW1 0 @0° A
IBW1 0 @0° A
ICW1 0 @0° A
VAWX 0.0 @0° kV
VBWX 0.0 @0° kV
VCWX 0.0 @0° kV
Real Power 0.0 MW
Reactive Power 0.0 MVar
961
387E-G1/2
962
943
KYG
230, 69 kV
36/48 KVA
10.27 %
Grounded Wye
Delta
861
387E-F1/2
862
863
KYF
230, 69 kV
36/48 KVA
10.27 %
Grounded Wye
Delta
487E-69-1/2
931
831
69 kV
311C-69-1/2
933
IA 0 @0° A
IB 0 @0° A
IC 0 @0° A
VA 0.0 @0° kV
VB 0.0 @0° kV
VC 0.0 @0° kV
Real Power 0.0 MW
Reactive Power 0.0 MVar
Apparent Power 0.0 kVA
SEL-3530
SEL-2100
KYH
69/4, 13.8 kV
3/4 MVA
Delta
Delta
751A-1218
1218
Pumping Station
751A-1216
14.4 kV
751A-1214
1216
1214
IA 0 @0° A
IB 0 @0° A
IC 0 @0° A
VA 0.0 @0° kV
VB 0.0 @0° kV
VC 0.0 @0° kV
Real Power 0.0 MW
Reactive Power 0.0 MVar
Apparent Power 0.0 kVA
To Skinner Fish Facility
To O&M Center

How Would We Know?

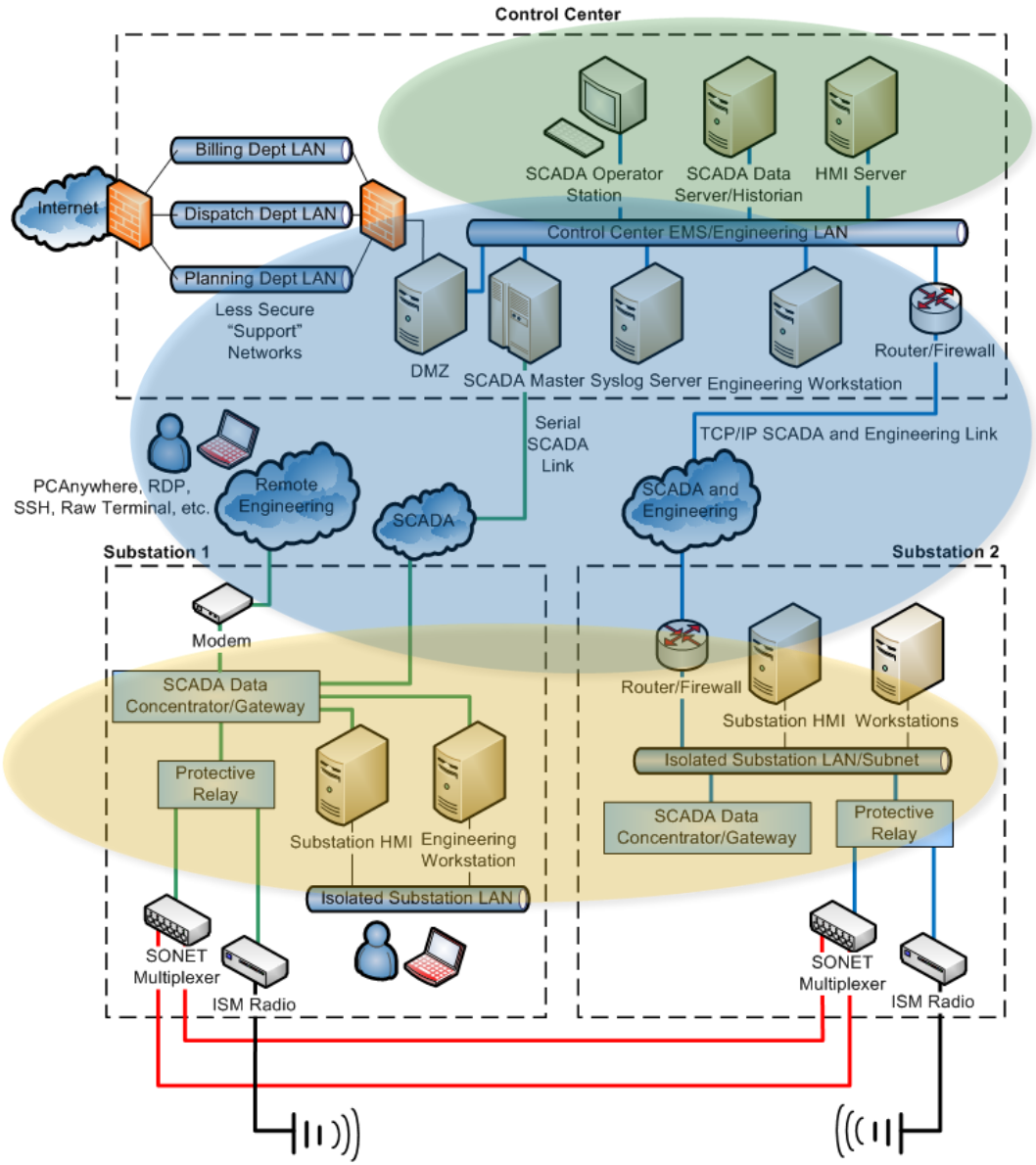
During an electric power industry meeting the question was asked, “How would we know if our system was being cyber attacked?”

Control Systems Consist of Three Layers

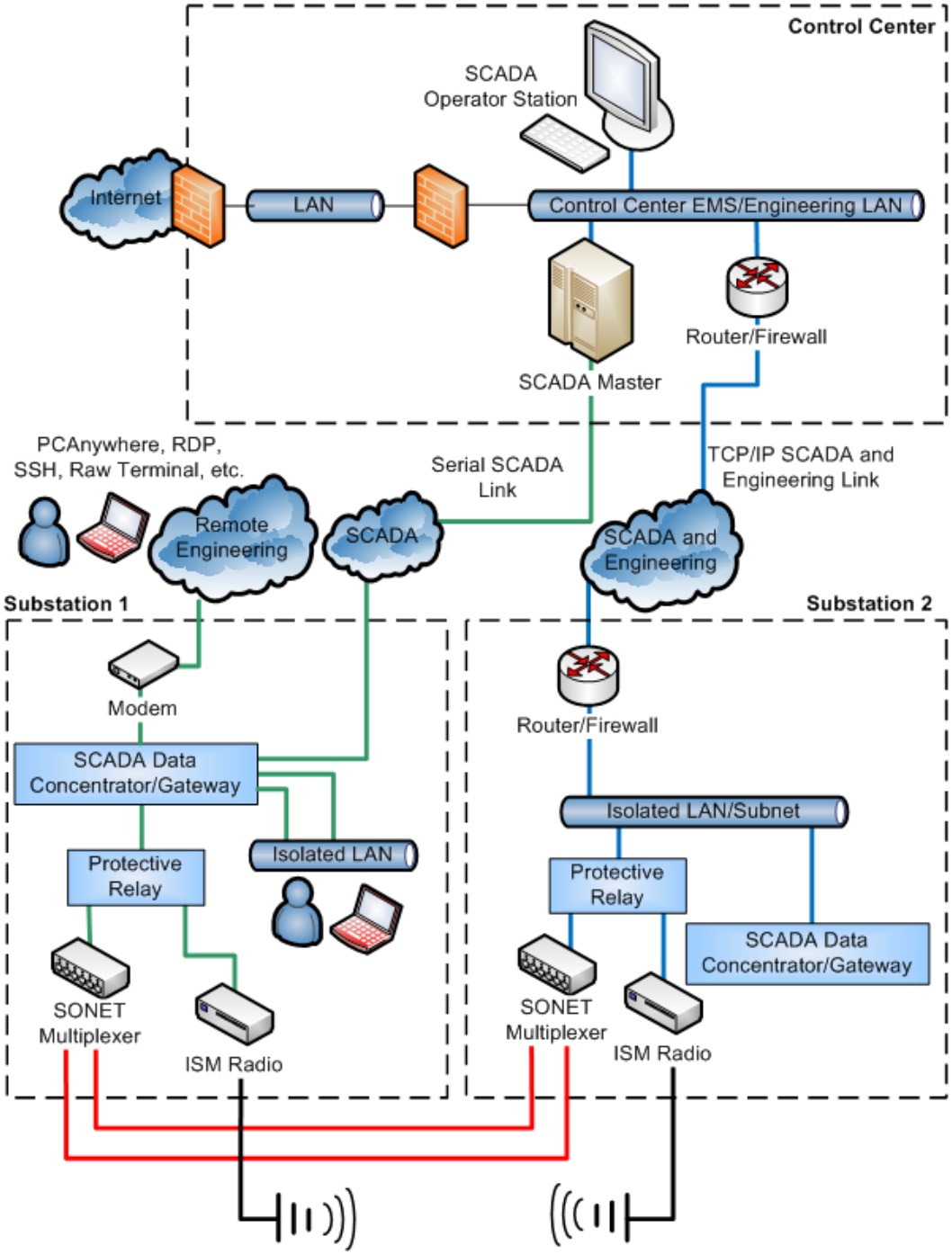
SCADA and EMS Systems

Network Appliances

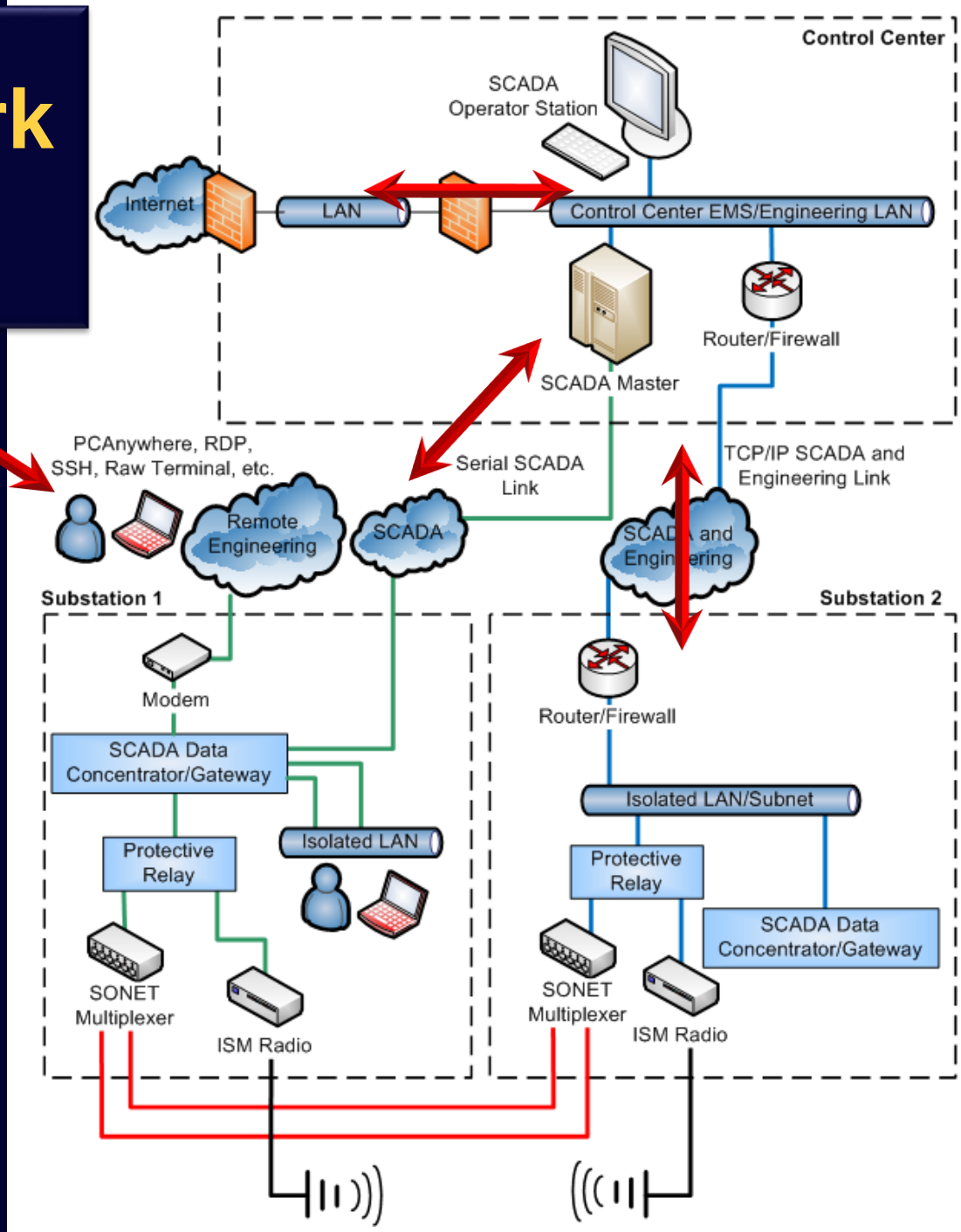
IEDs



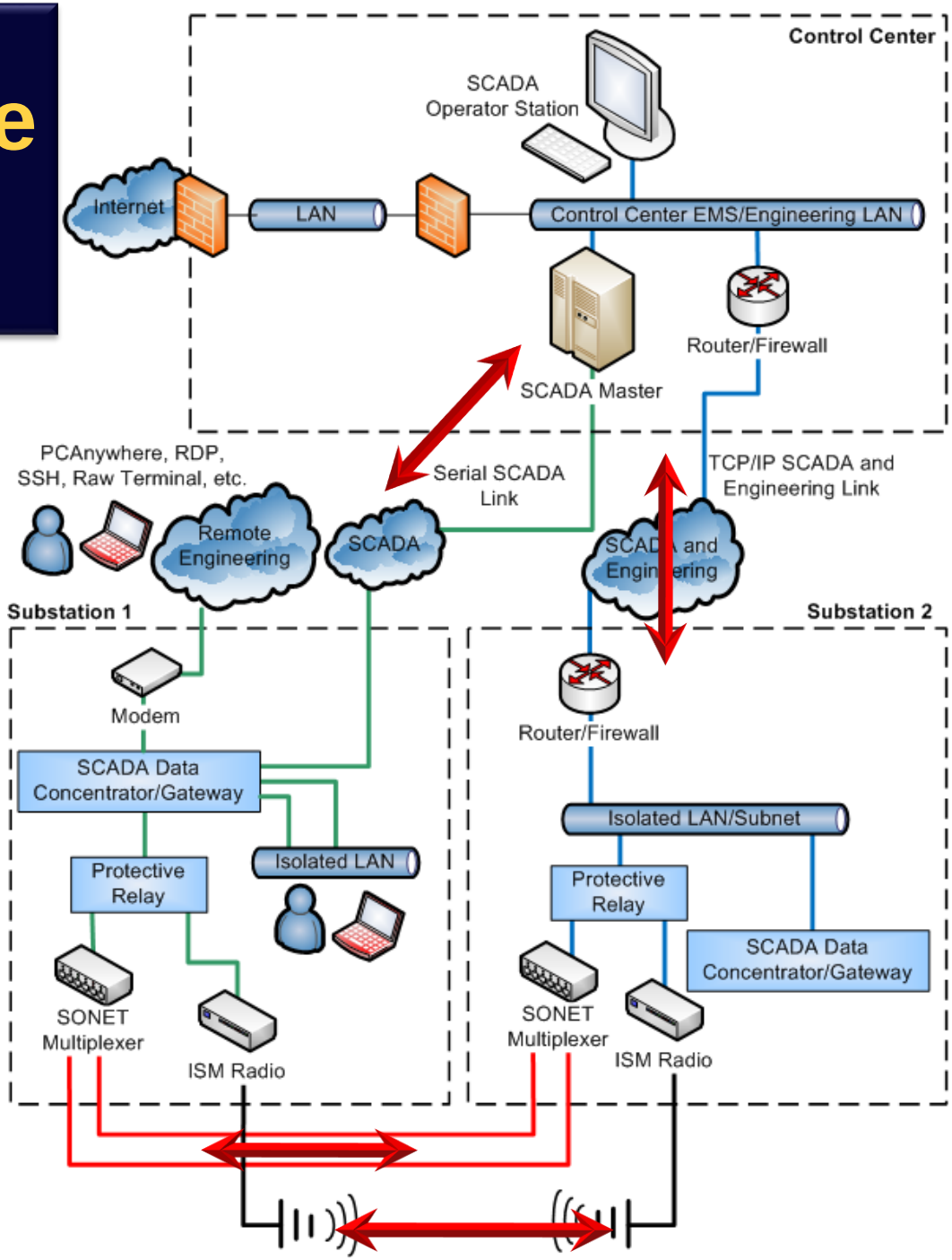
Where Are the Points of Potential Exploits?



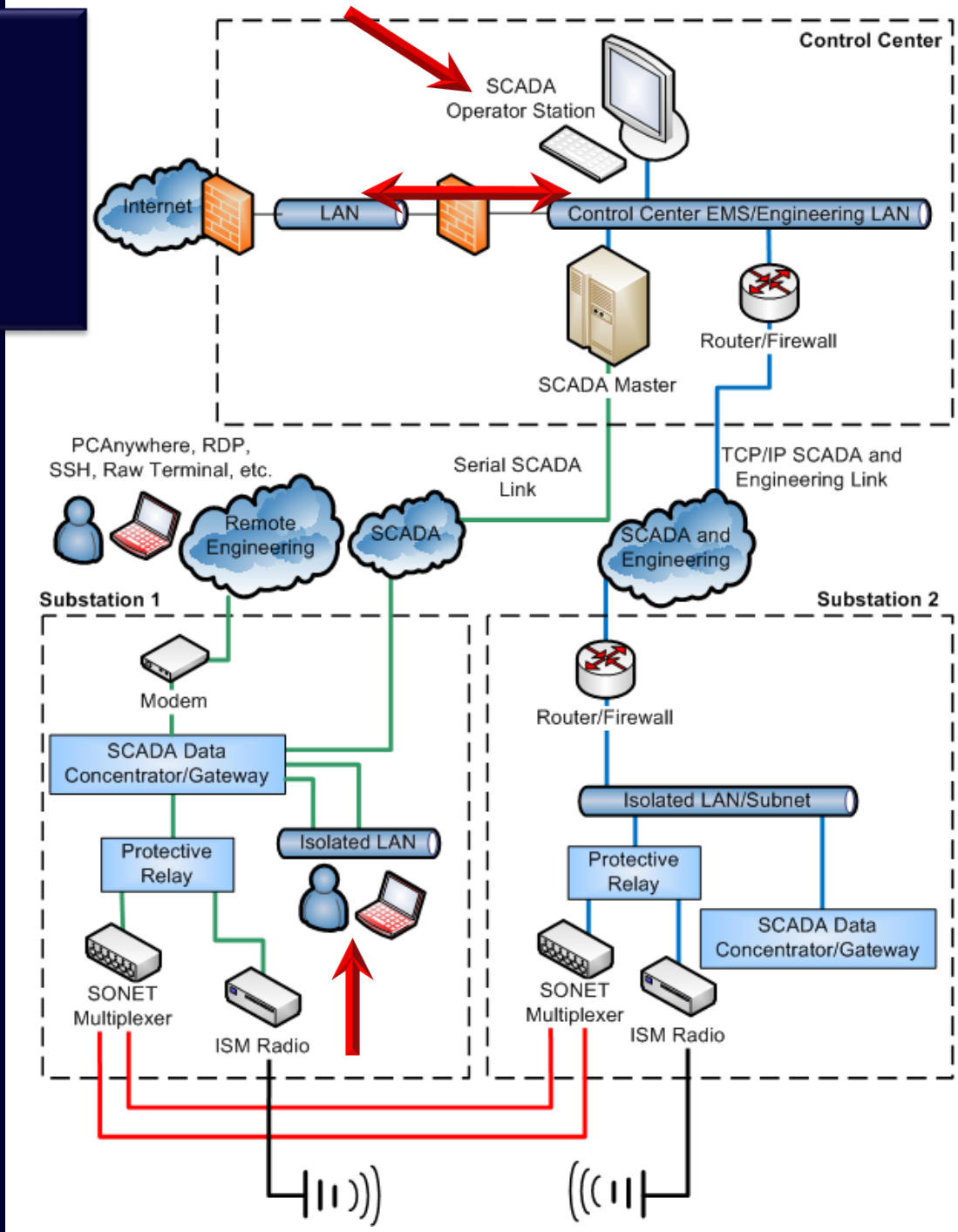
External Network Access



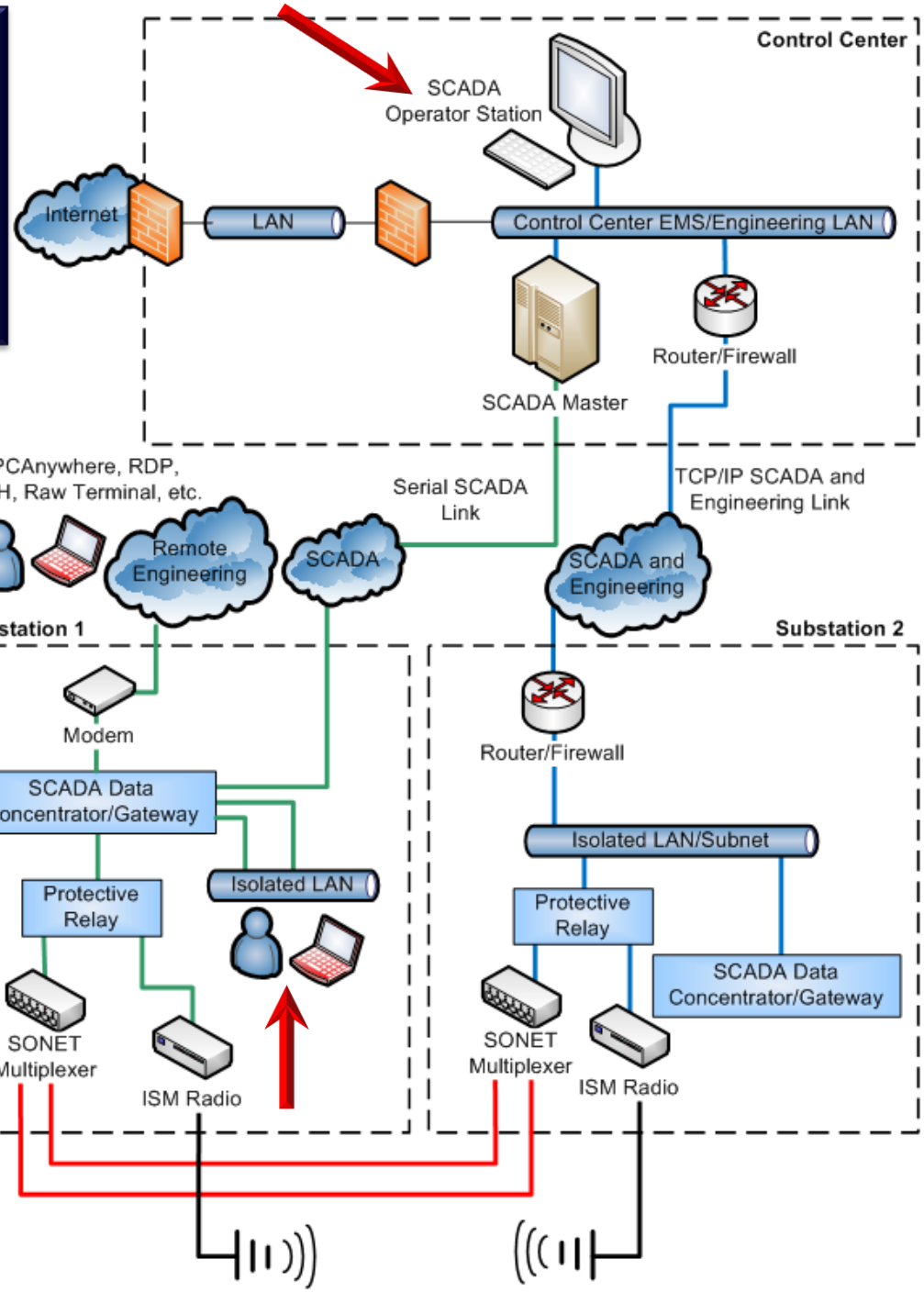
Man-in-the-Middle Attacks



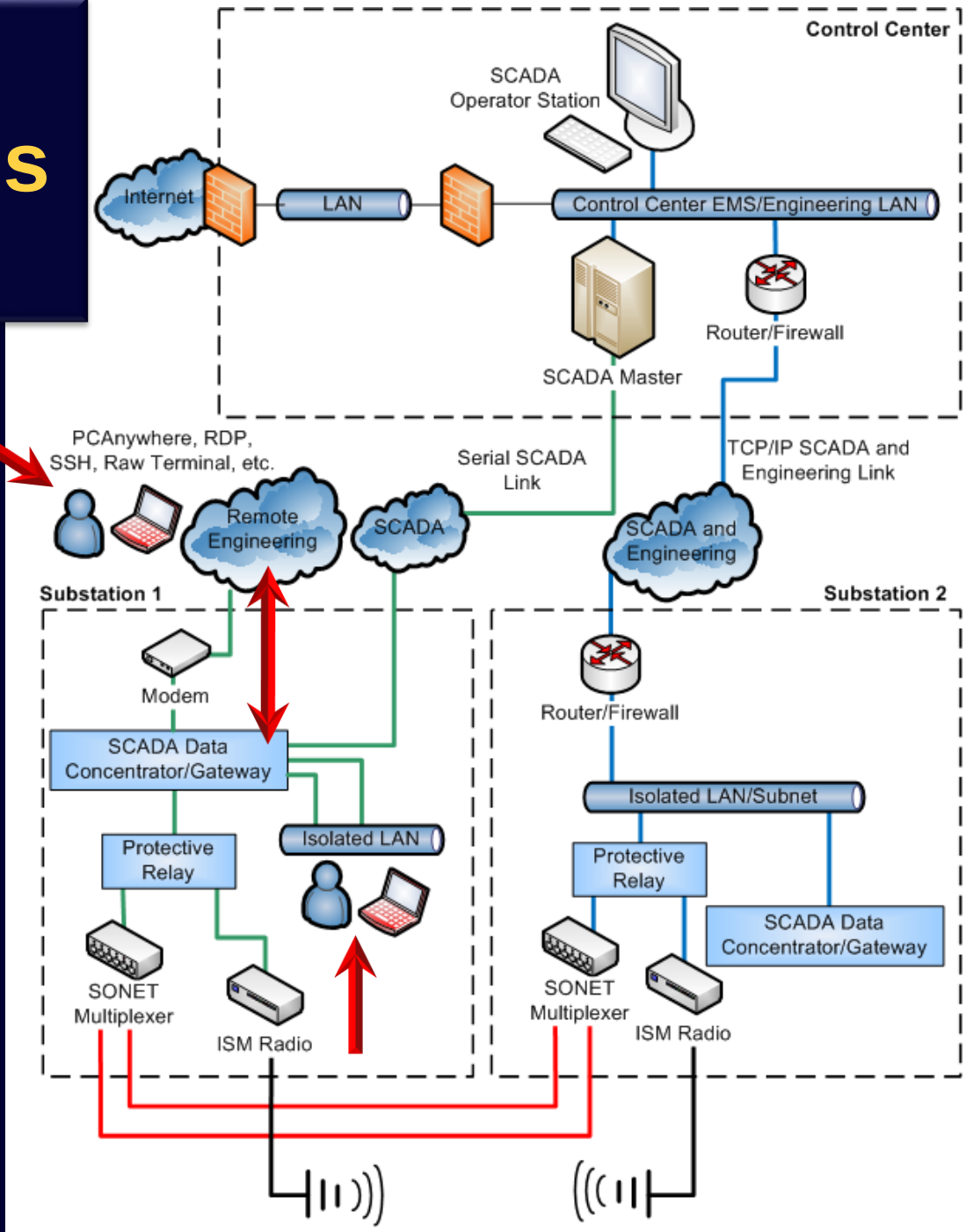
Malware


Control Center
SCADA
Operator Station
Internet
LAN
Control Center EMS/Engineering LAN
SCADA Master
Router/Firewall
PCAnywhere, RDP,
SSH, Raw Terminal, etc.
Serial SCADA
Link
TCP/IP SCADA and
Engineering Link
Remote
Engineering
SCADA
SCADA and
Engineering
Substation 1
Substation 2
Modem
SCADA Data
Concentrator/Gateway
Protective
Relay
Isolated LAN
SONET
Multiplexer
ISM Radio
Router/Firewall
Isolated LAN/Subnet
Protective
Relay
SCADA Data
Concentrator/Gateway
SONET
Multiplexer
ISM Radio

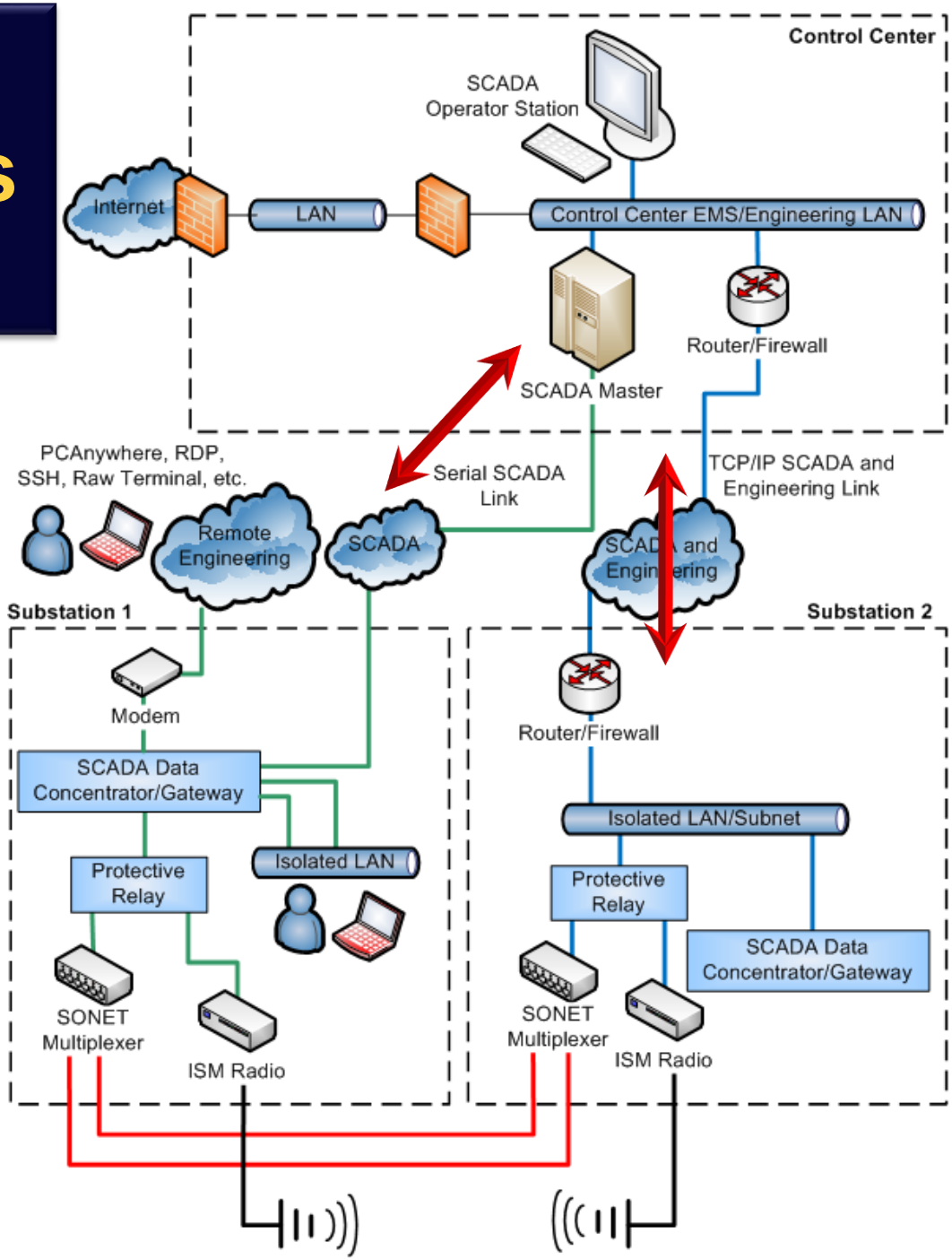
USB Stick Access



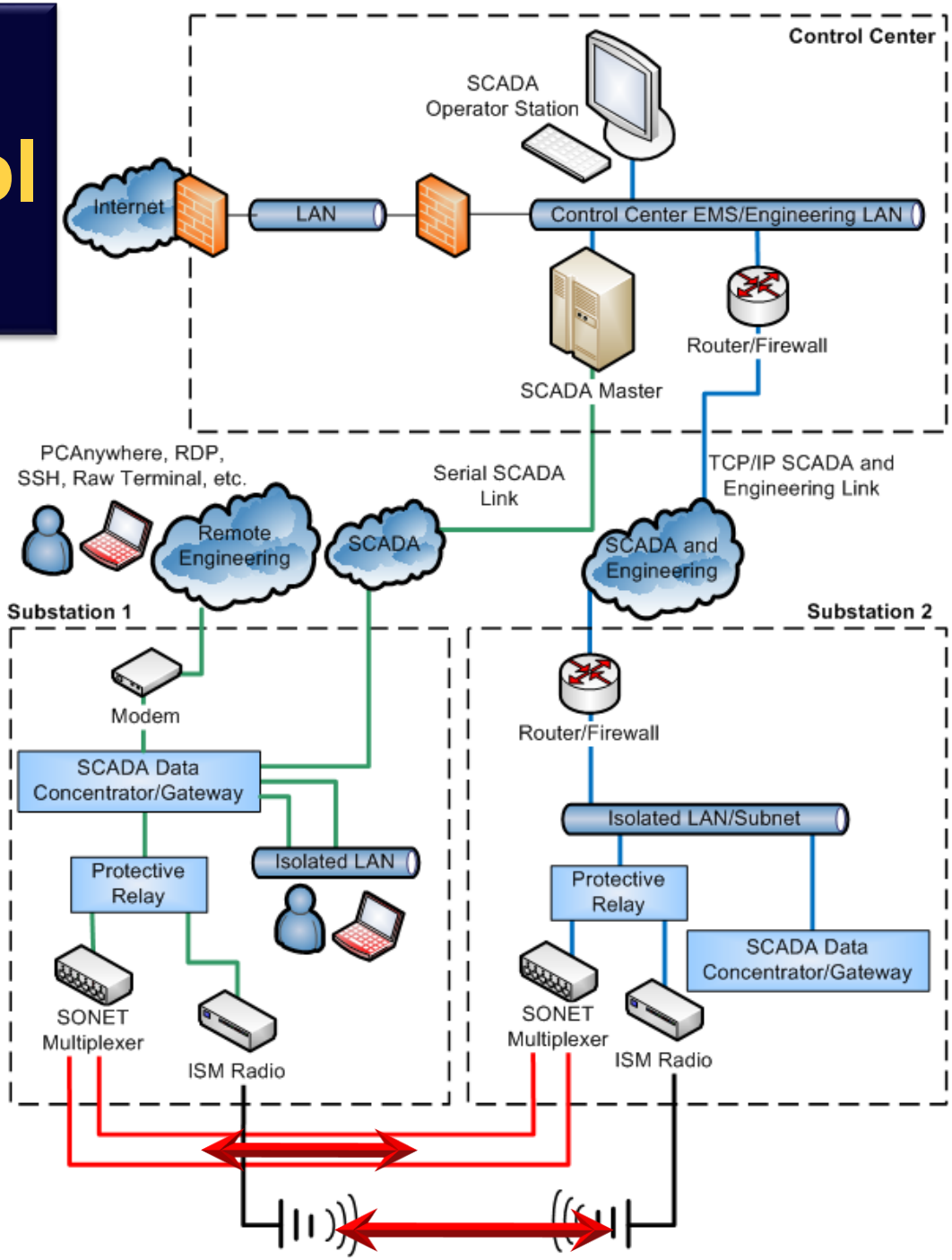
Engineering Communications Access



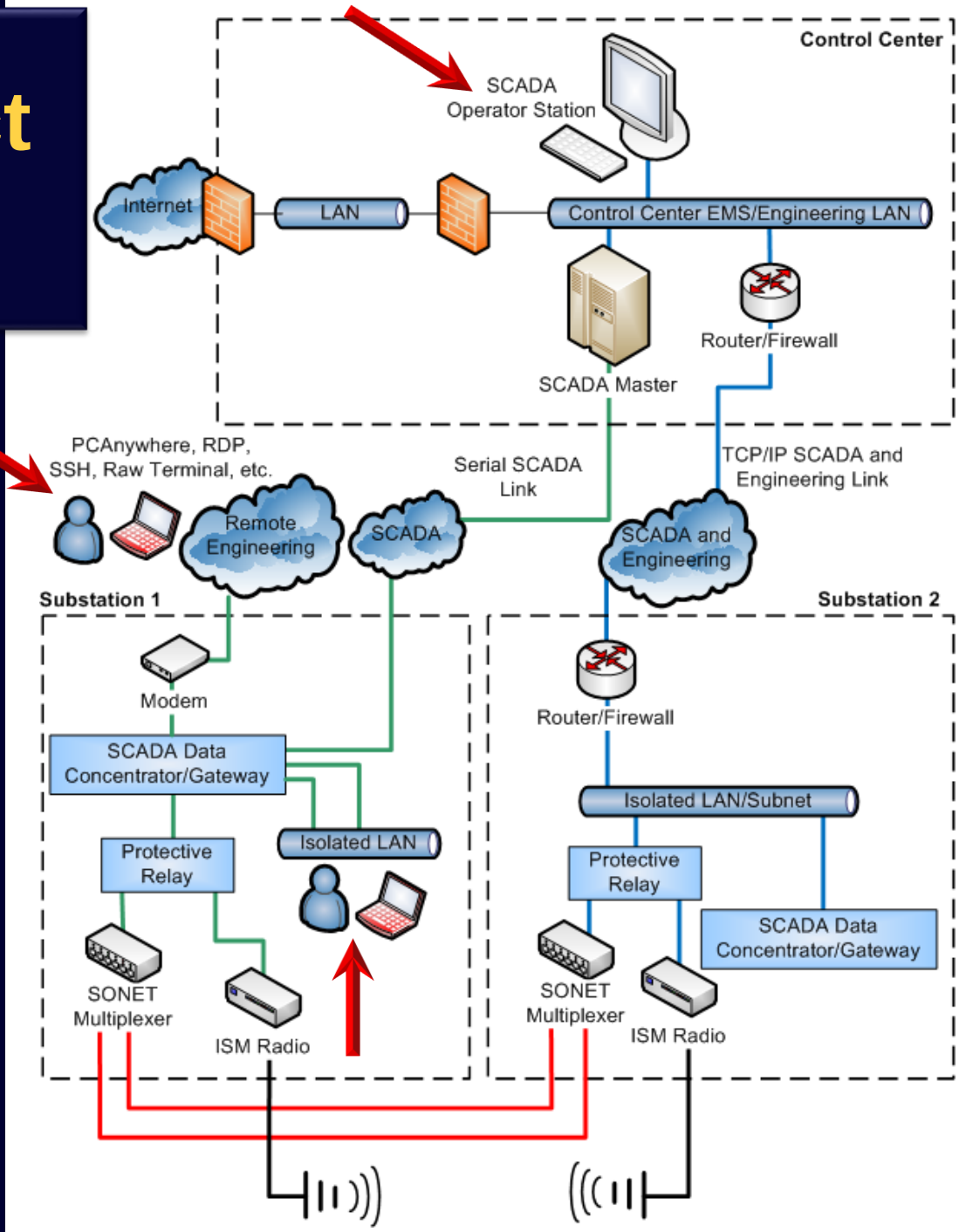
SCADA Communications Access



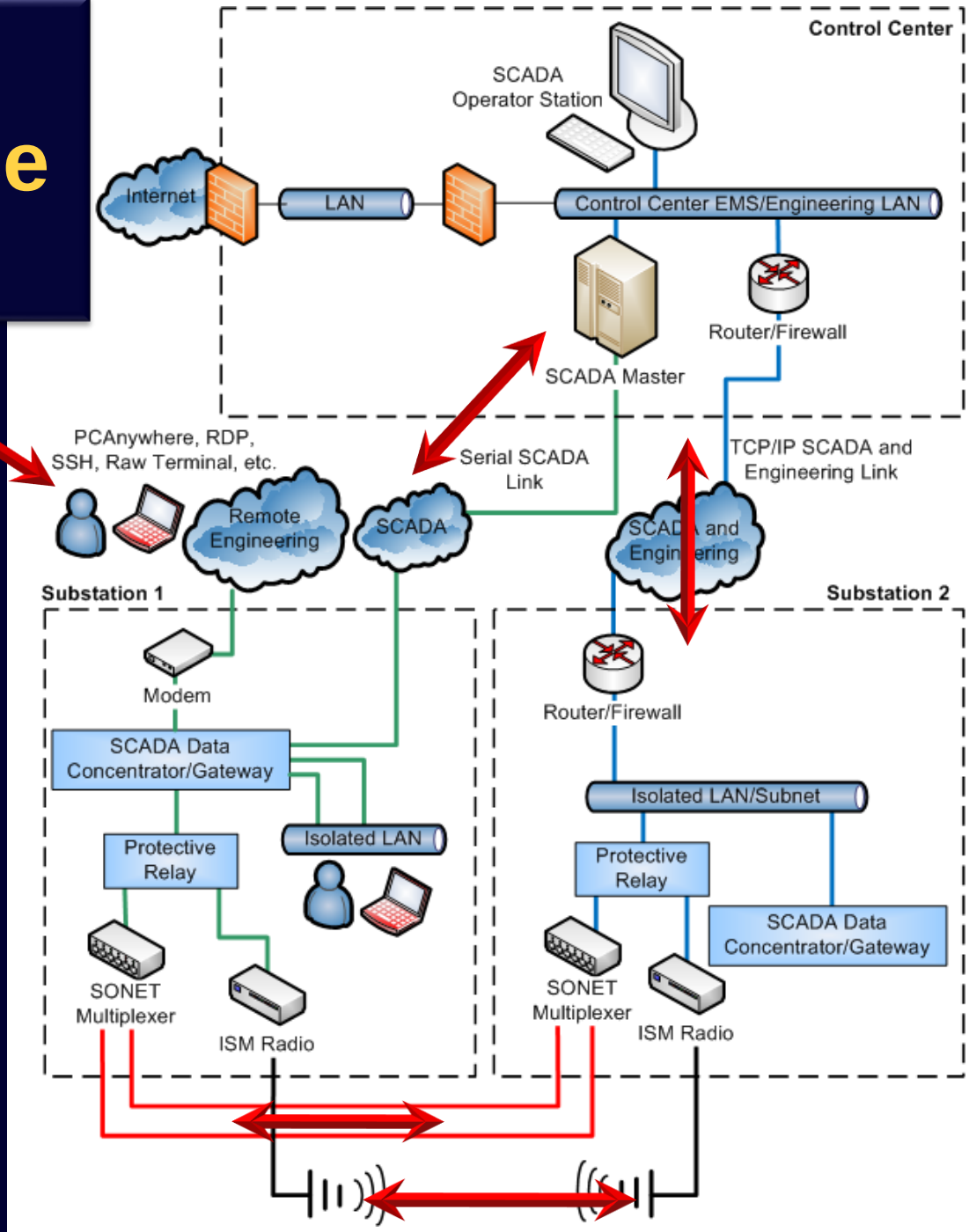
Real-Time Control



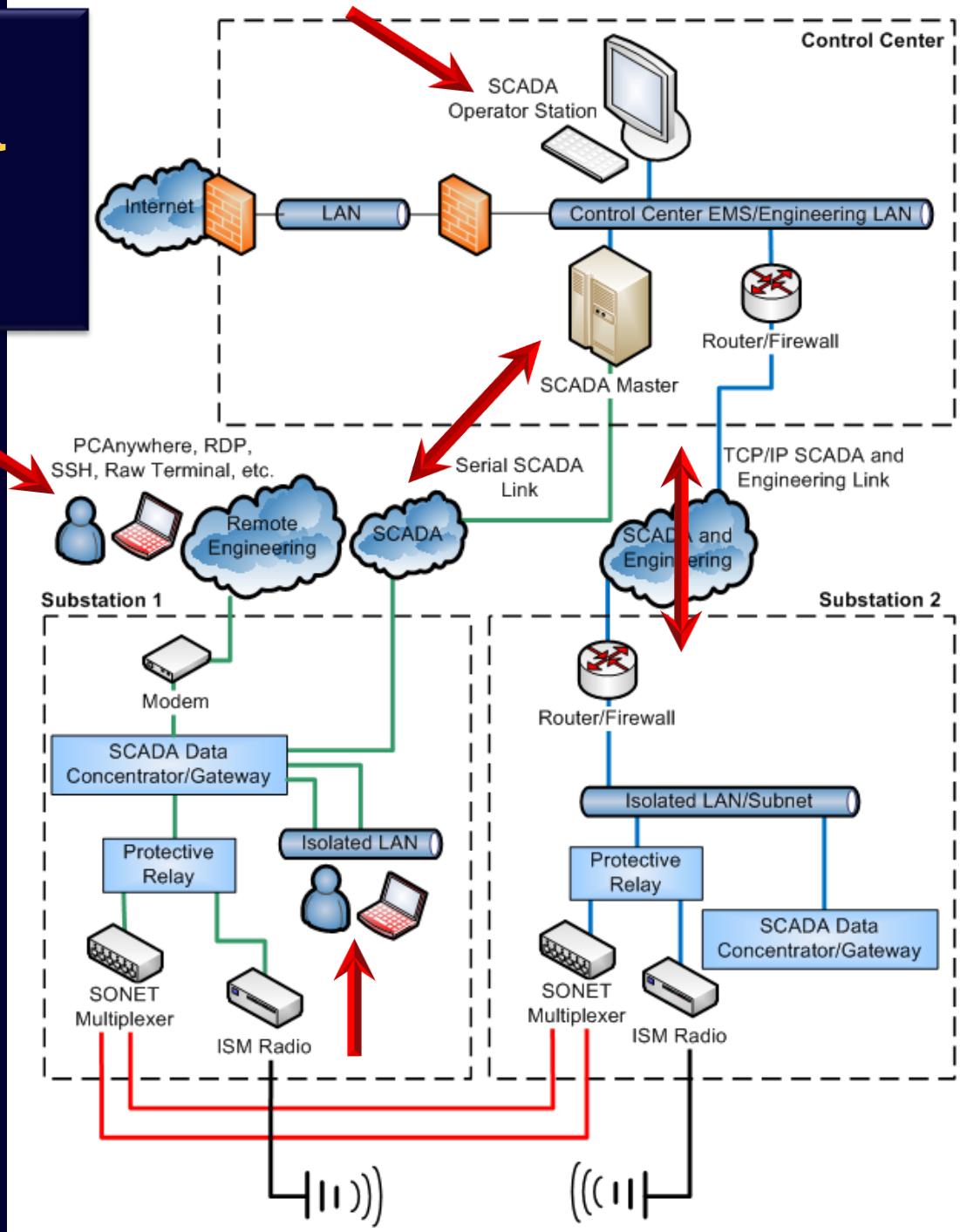
Insider or Direct Access



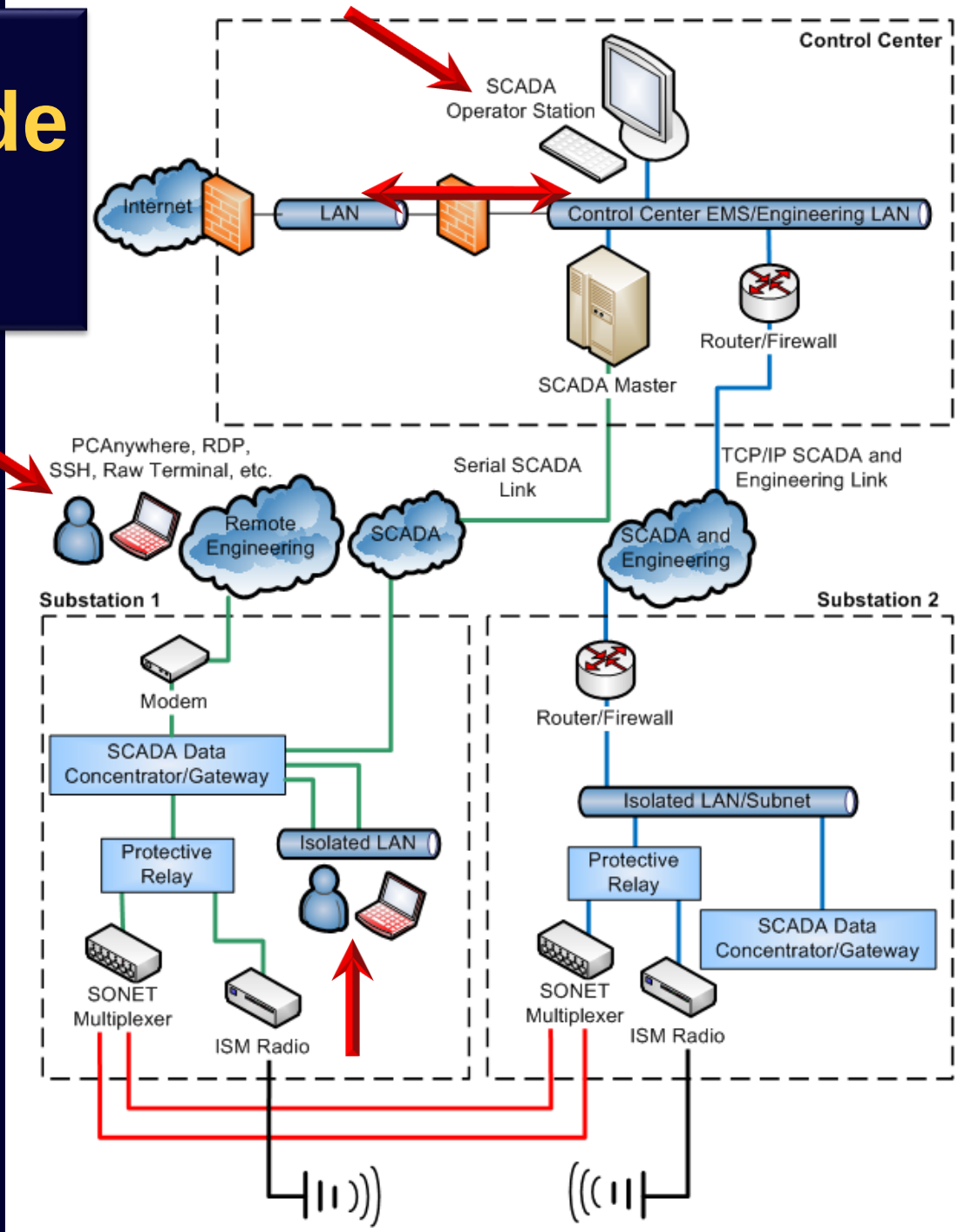
Denial of Service



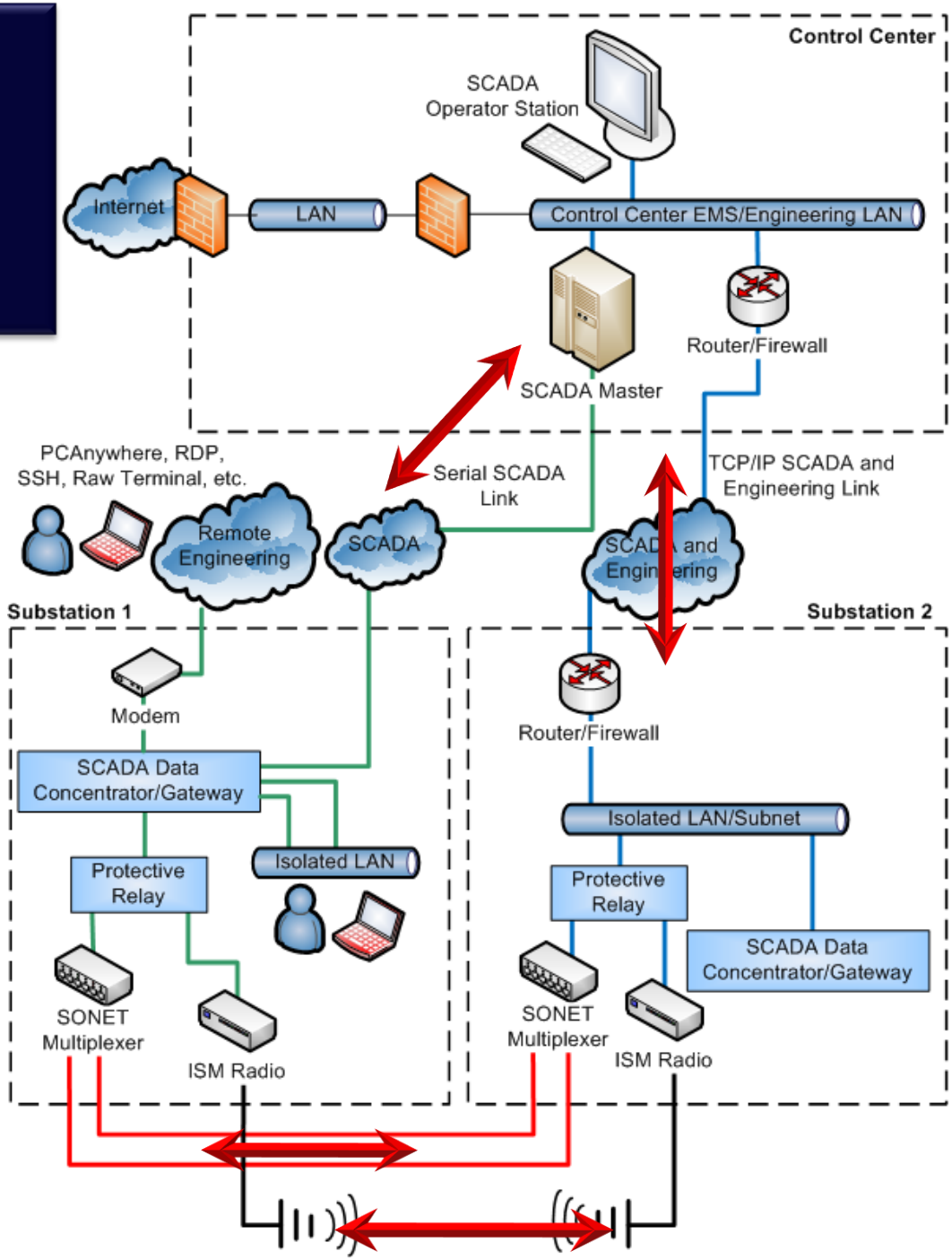
Malicious Data Injection



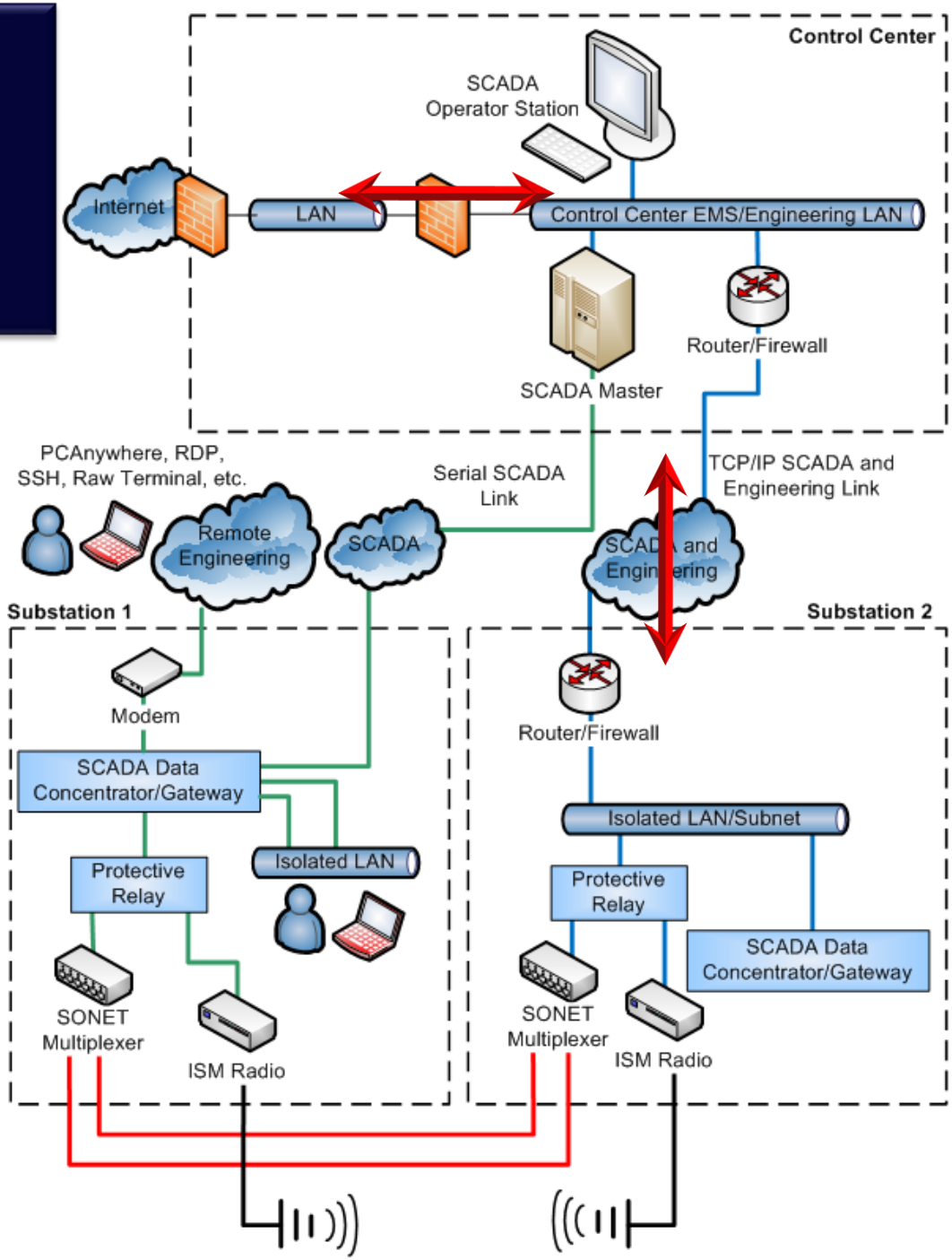
Software Upgrade Exploits



Data Playback



Database Manipulation

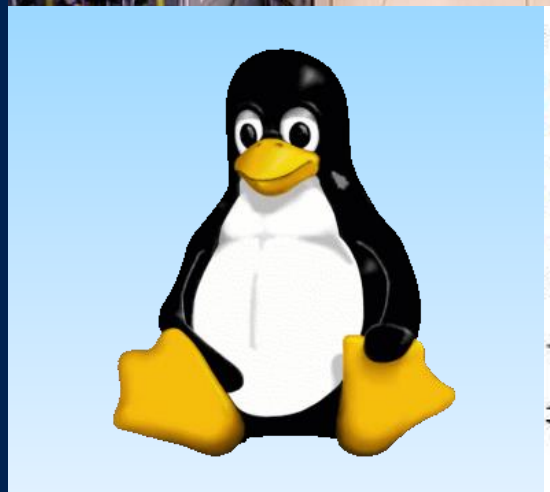


IED Cyber Monitoring Capabilities

- Alarm contacts
- Sequential event reports
- Metering and monitoring
- Communications reports
- Programmable logic and contact I/O

Network Appliance Monitoring Features

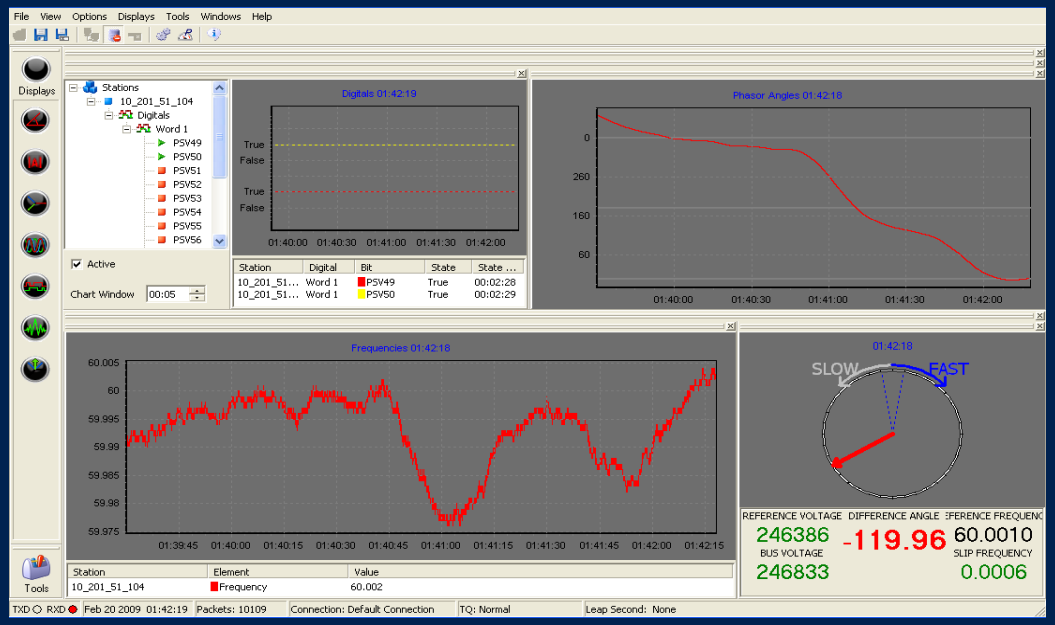
- Network traffic
- Communications alarms
- Computer operating systems logs and audits
- Whitelisting
- Syslogs

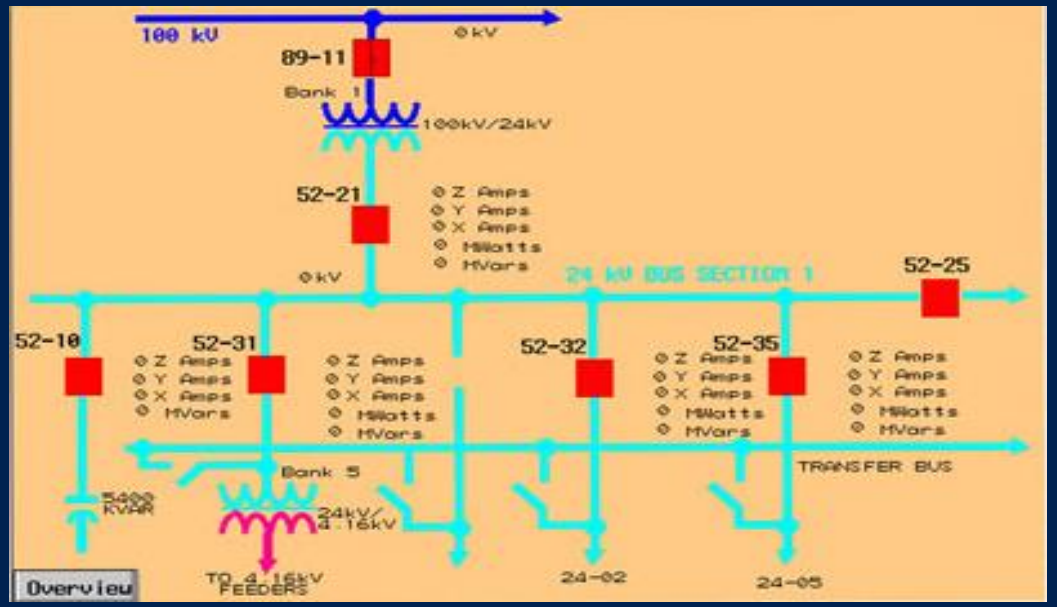


MICROSOFT WINDOWS

SCADA and EMS Monitoring Features

- Logging
- Alarm reporting
- Measurement consistency
- Communications monitoring
- Central collection
- Trending

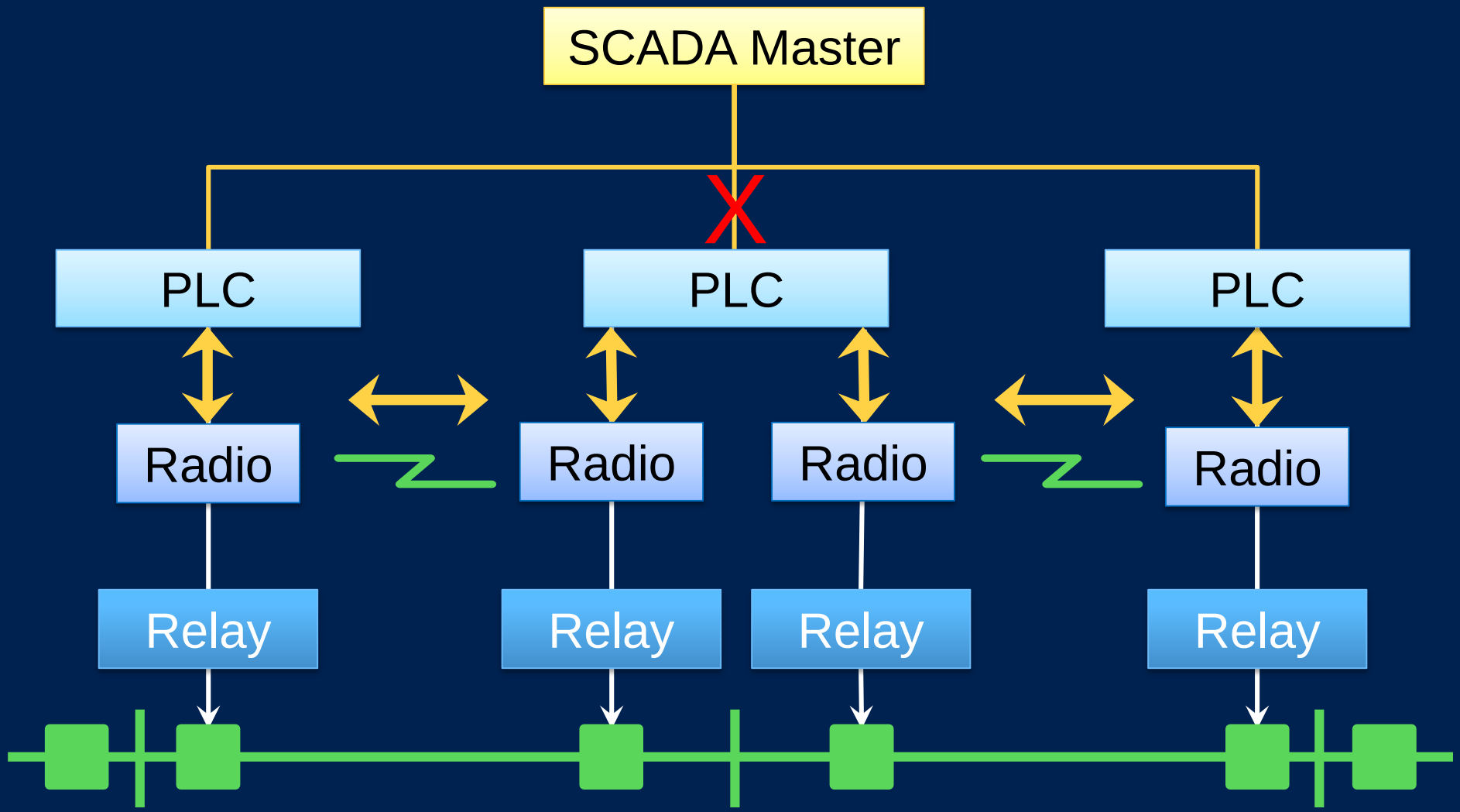




Build on Security Tools and Information in IEDs

- Connect alarms to other system equipment
- Correlate all available time-stamped reports
- Create custom alarm points
- Create secondary communications path to notify when a probe or attack is underway

Secondary Communications Channels



Analyze Redundant and Related Measurements

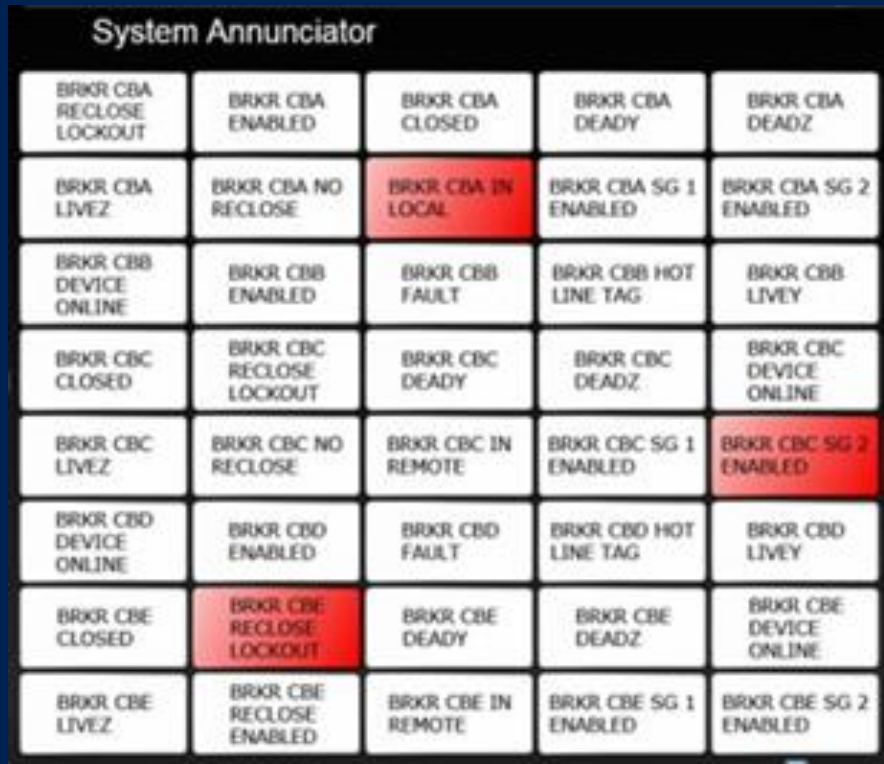
- State estimators purge bad data, this could be a tip-off of an attack
- Synchrophasors and wide-area measurements can be used to detect measurement disagreements
- Use simple meter checks to validate data – fundamental vs. RMS

Implement Best Cybersecurity Practices

- Use cryptography to protect serial and Ethernet connections
- Create clear network segments connected by firewalls
- Isolate control networks with DMZs
- Use static routes
- Disable unused services
- Implement a patch management system
- Baseline IED and system settings

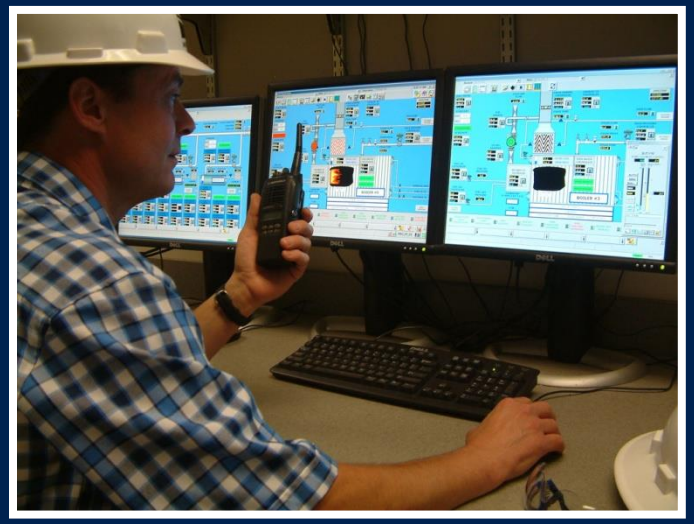
Examine Logs

- Set logs to automatically elevate critical events
- Program IEDs to alarm when settings are changed
- Archive logs for post-event investigations



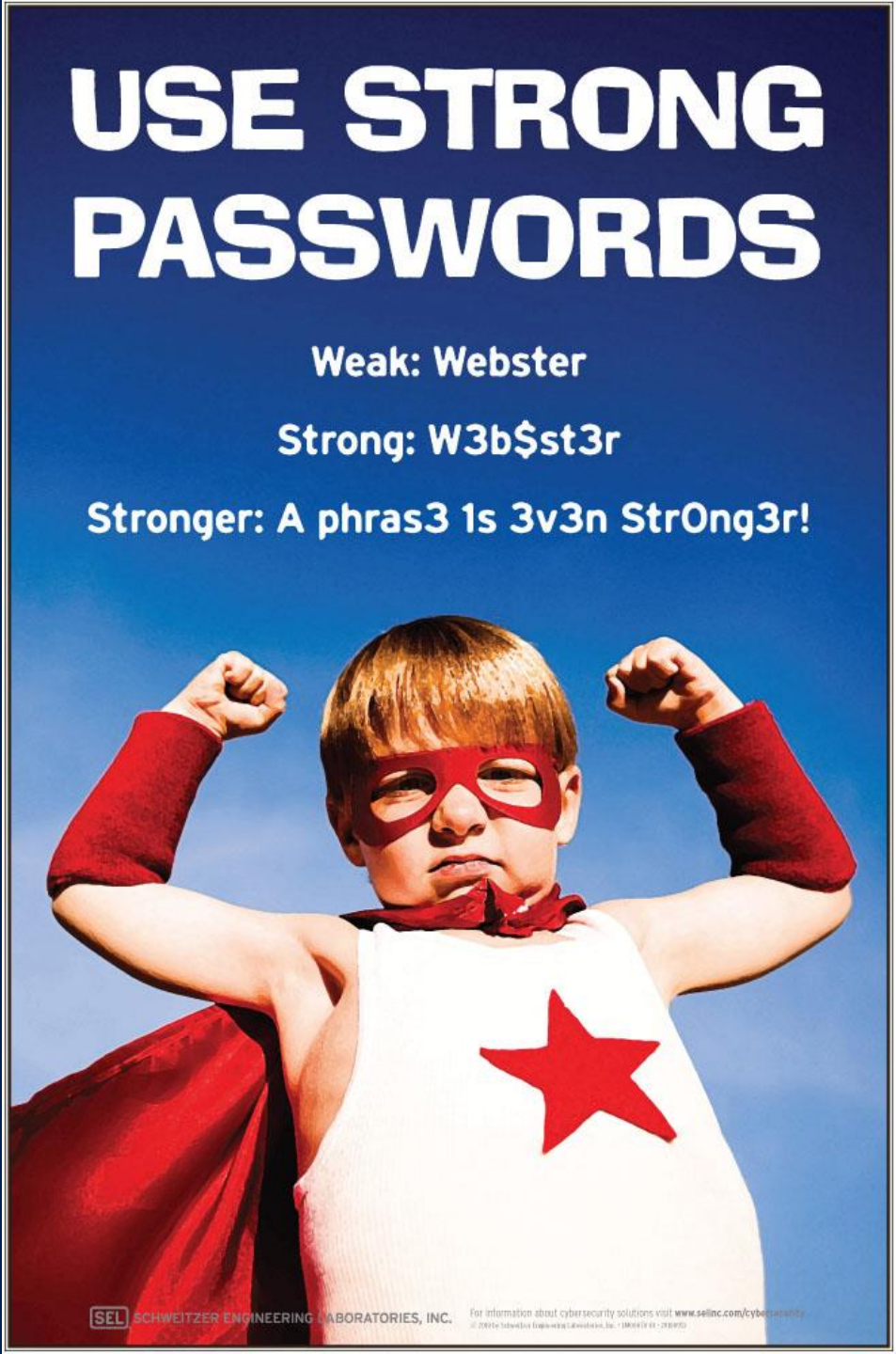
Have an Incident Response Plan

- Prepare organization
- Create a team
- Prepare infrastructure
- Develop and practice remediation plan



Create Security Awareness Program

- Provide regular training
- Notify employees immediately of threats
- Conduct regular security audits



Know Where Your Firmware Came From

Firmware hash(es) for: SEL-411L

Version	MD5 Hash	SHA1 Hash
R100	ed7768da8ff4ffe911e8a1b3e275692e	17d324e009b5d9bff7009c1c505887905023ae96
R101	518482a562cba39d4a1edf60cd066d52	1d6cb984dfab26f68560e3c90aea3f5d05438dcb
R102	2c66996e1348ac45ff61a55cae267f9c	d8ad17e7f19cbbdf77cd2c892cd84ac76f221131
R105	13e9caf2df5422d259acba213609cd2d	d3c0e2e333e4bfe2d2e547902976e400a376bd91
R107	cab2da6dc7ccfc2bb0de126865e6dffa	2ccf15da6bbe1a290295da728990c9380953f25c
R108	fba85253ff790c42c0e8110ce568ad3c	7d18e01a18937915586fd984fe03525d8409c966
R110	b22082179cb943293a54973c868b6cc0	1e9e46bc5894495f164e4e8da70354f40a41a839
R111	a83d2a691fa91e6b54f0d23ca68f668d	329791f4728581a60a1ac26ebe6017cbdee1e22f
R113	5f4bbb953d7b5d150ee770ed813440e1	fcda6d591388f285cf36175f33d7c0ad5f02bc66
R114	2de75b4fa62669937c8e11f073d0a1f9	645a8bd16e91b8748186cc2f9386294b01994d3d
R115	e35586b9933af002a8a7ee278b7e341b	f1eff05a930a3c7345b001671db9c5274c6a626a

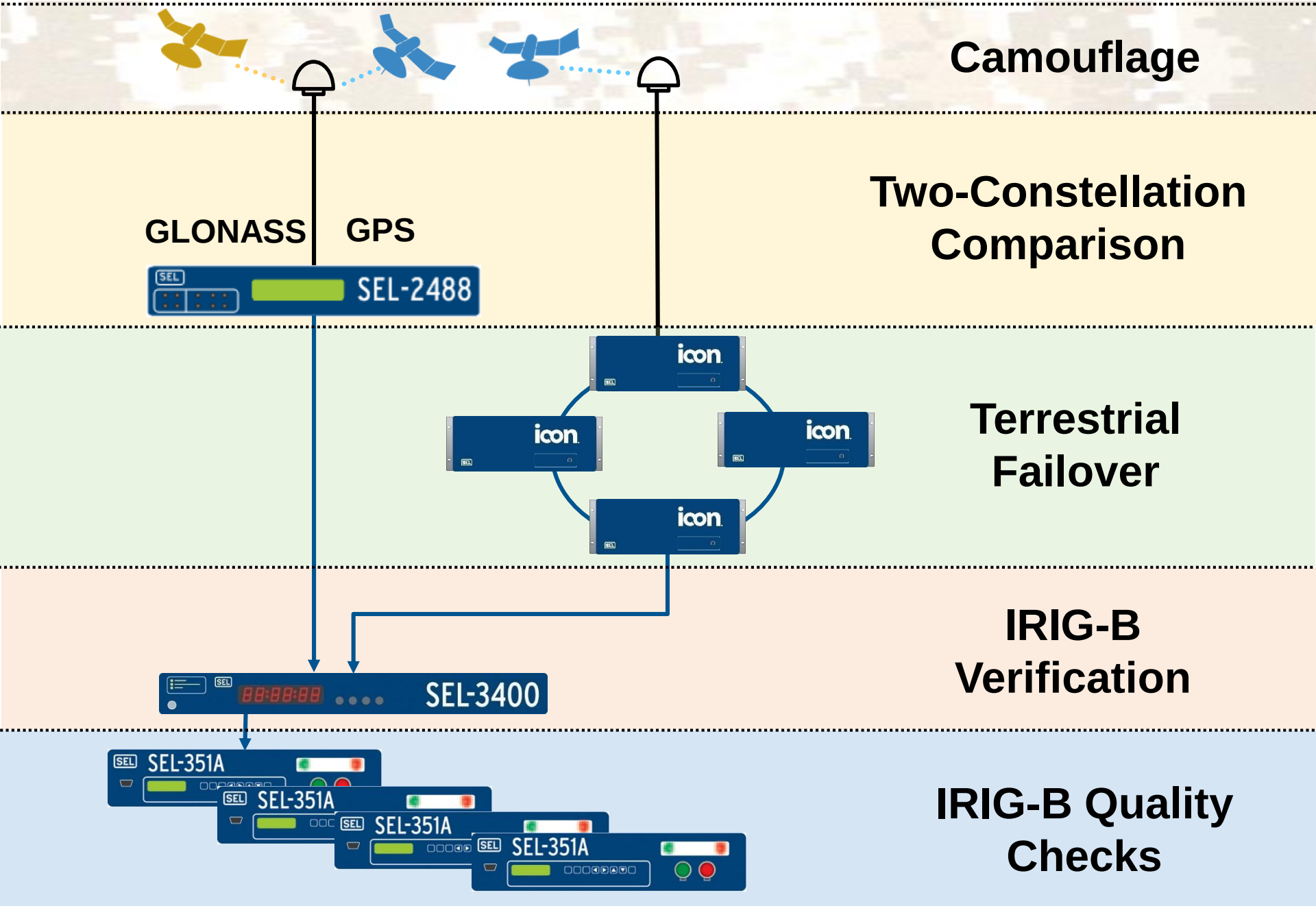
Protect Our Time Systems Too

- Lots of news about GPS spoofing
- Like communications, time is a *convenience*
- How would we know if our time systems were compromised?

Develop Time Distribution Systems Like Our Network Systems

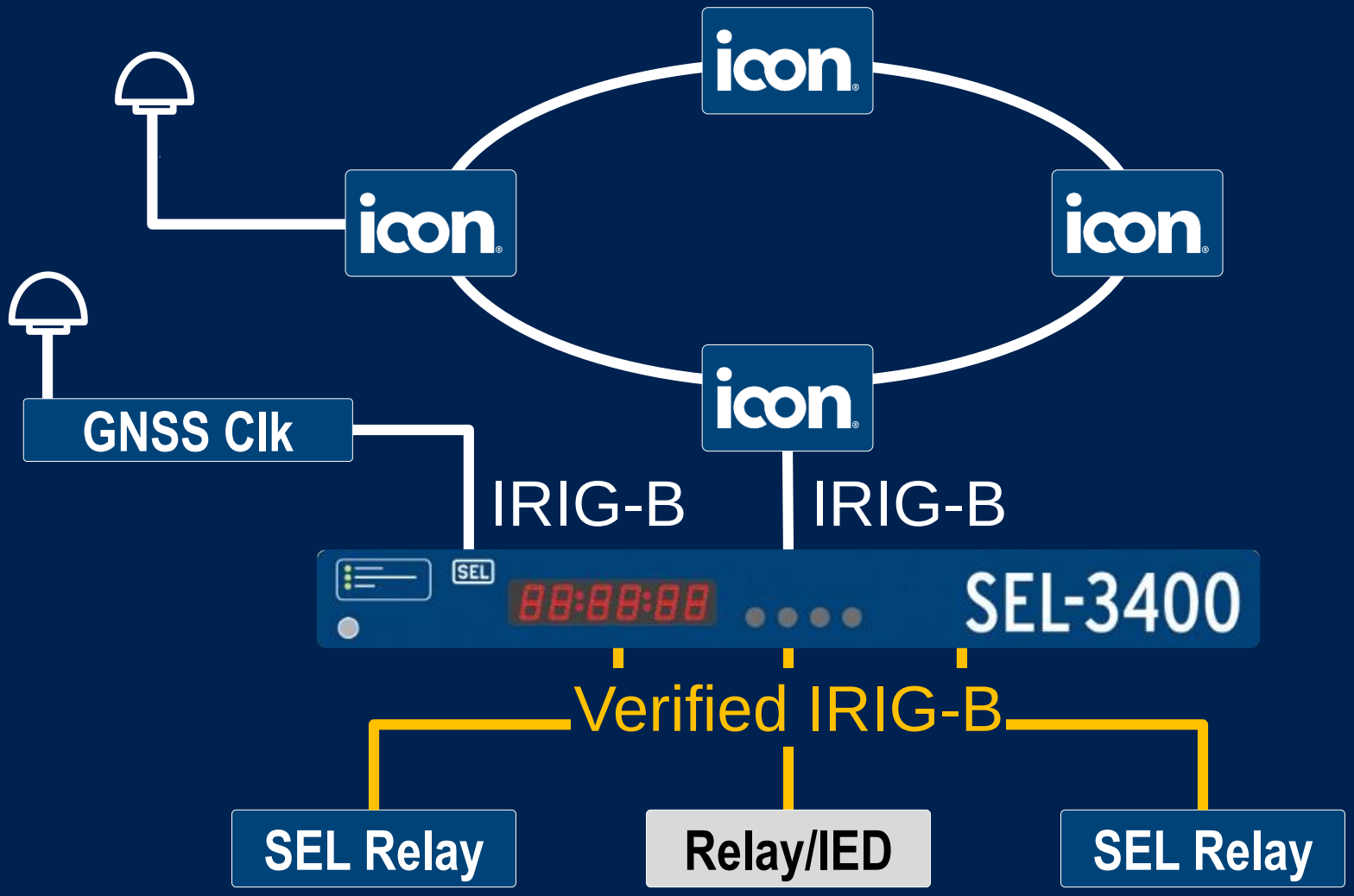
- Design time distribution system with security in mind
- Create fault tolerant systems
- For critical systems, don’t “believe” one time source

A Layered Approach to Time Integrity

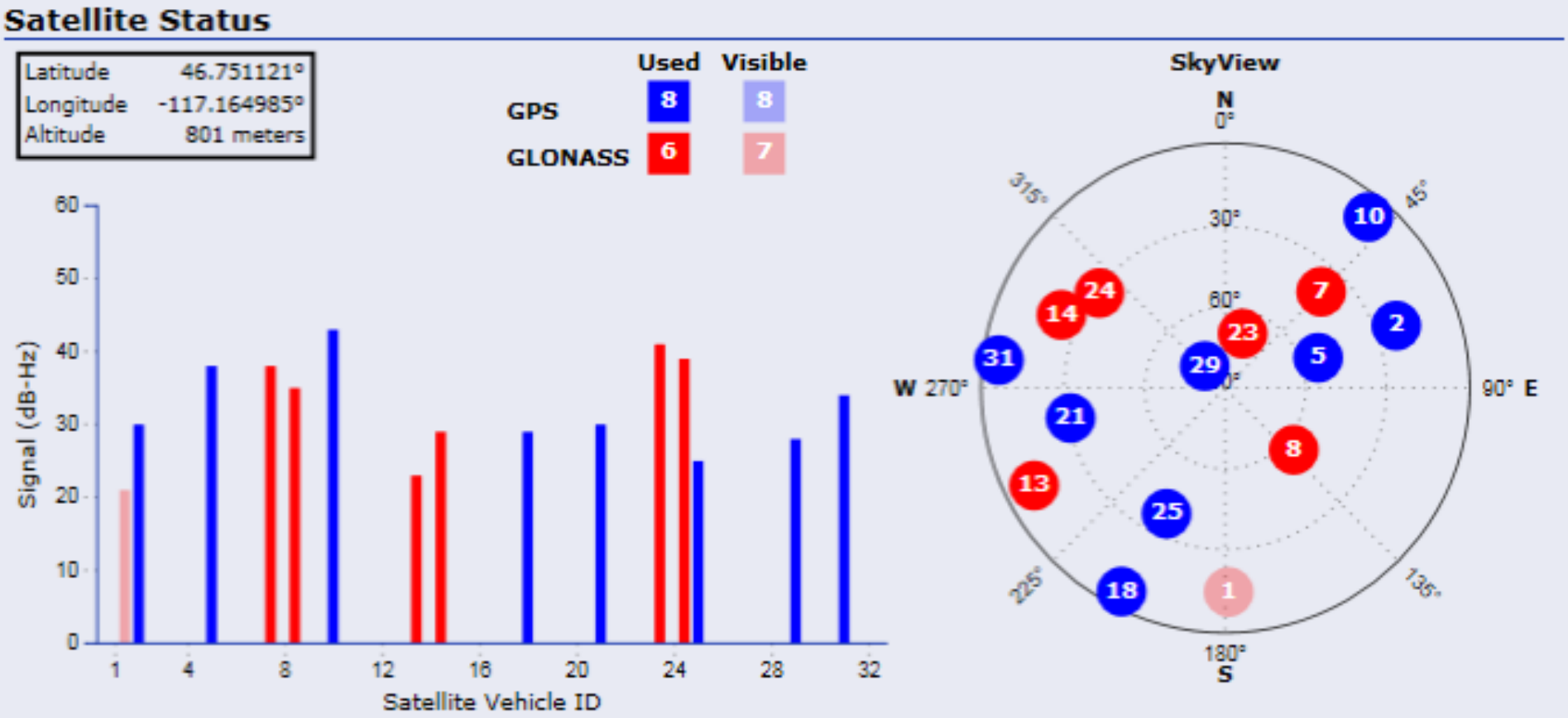


Verifies IRIG-B

Alarms if Time Differs, but Good Quality Bits



Use Multiple Data Sources to Detect Spoofing



What I'd Do

- Never connect SCADA to Internet; audit this
- Operate *private and secure* control networks
- Consider TDM, not just packet comms
- Apply defense in depth; layers of security
- Maintain *PRIVATE* security plans
- Compartmentalize knowledge of system
- *Learn and educate*

Conclusions

- Every cyber intrusion leaves fingerprints
- Most equipment has features that can be used to detect signs of a cyber attack
- Combining features provides consistency checks for wide-area monitoring
- See SEL technical paper “How Would We Know?” at selinc.com

Questions?