

# How Would We Know?

Edmund O. Schweitzer III, David Whitehead,  
Allen Riskey, Rhett Smith

*Schweitzer Engineering Laboratories, Inc.*

# 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?”

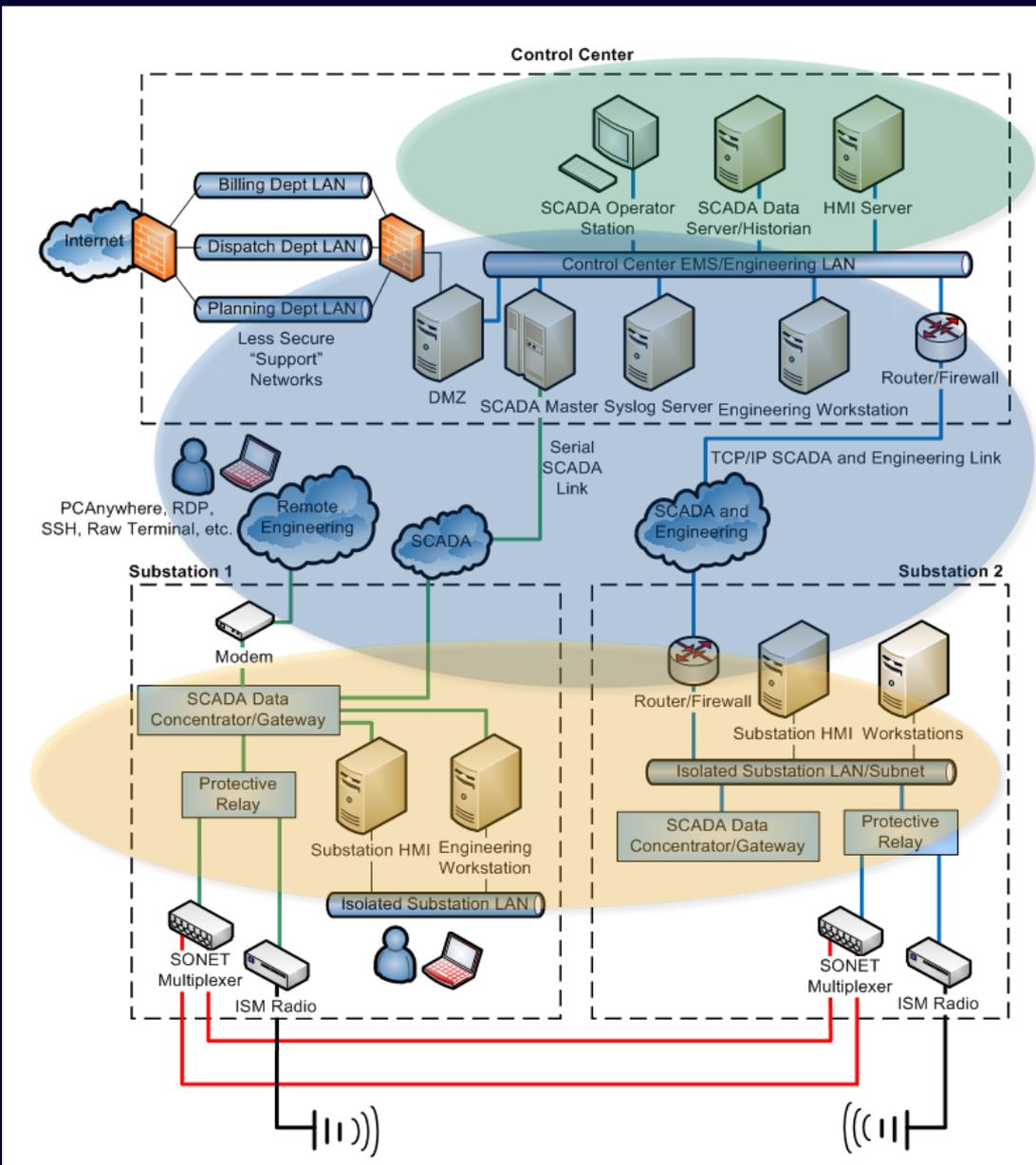


# Control Systems Consist of Three Layers

SCADA and EMS Systems

Network Appliances

IEDs



# IED Cyber Monitoring Capabilities

- Alarm contacts
- SER
- Event reports
- Metering and monitoring
- Communications reports
- Programmable security points
- Unsolicited SERs



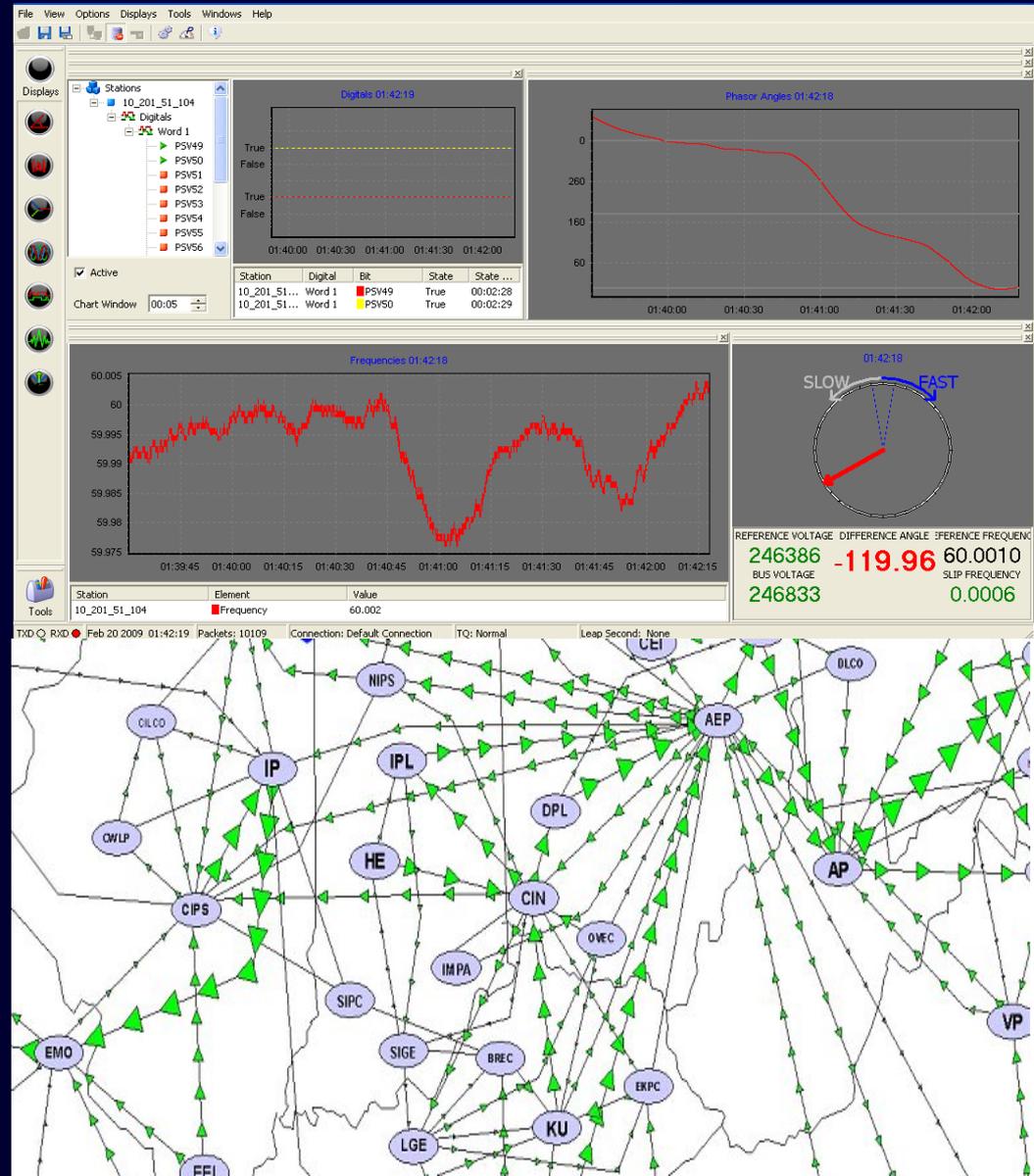
# Network Appliance Monitoring Features

- Network traffic monitoring
- Communications alarms
- Computer operating systems

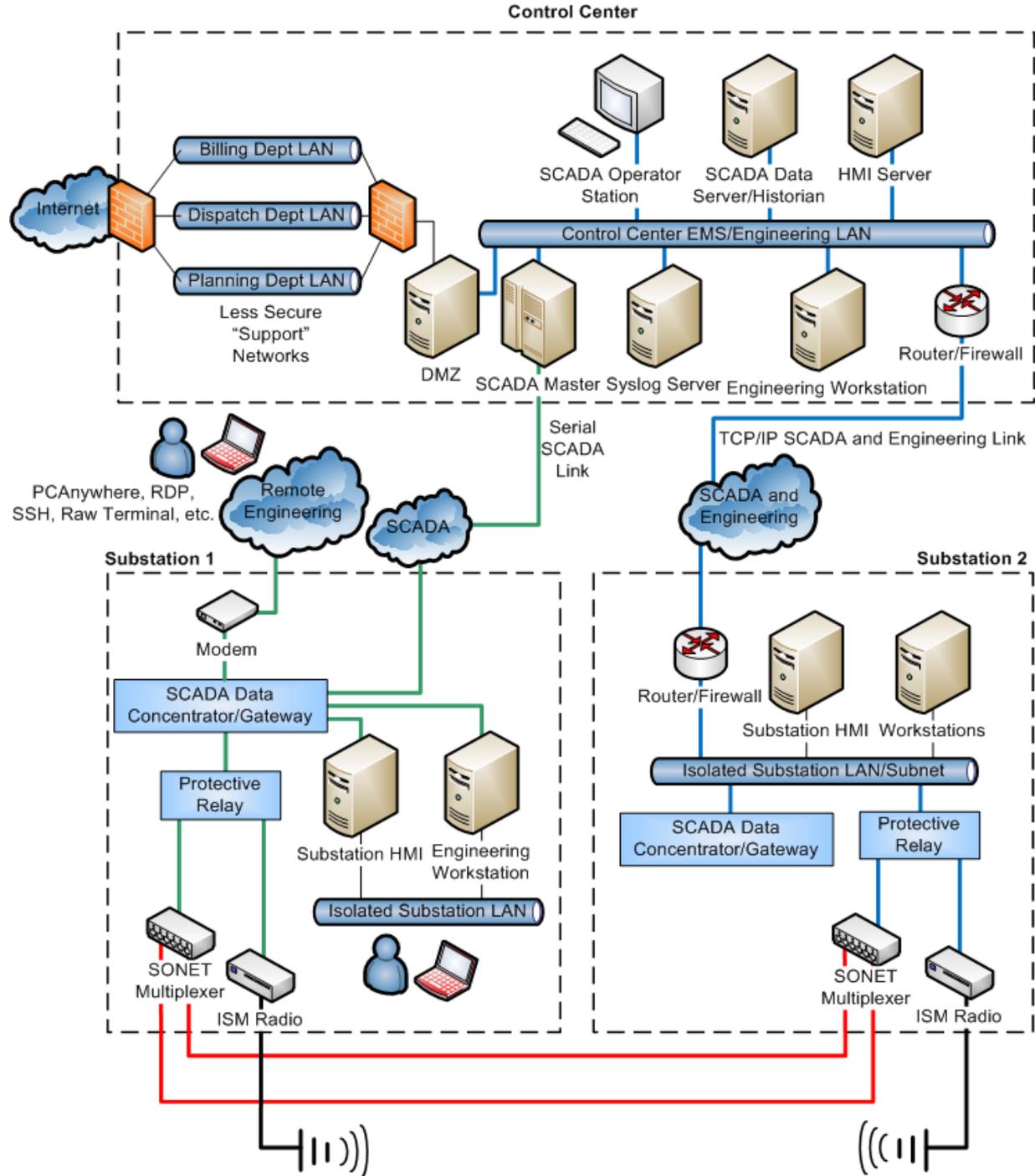


# SCADA and EMS Monitoring Features

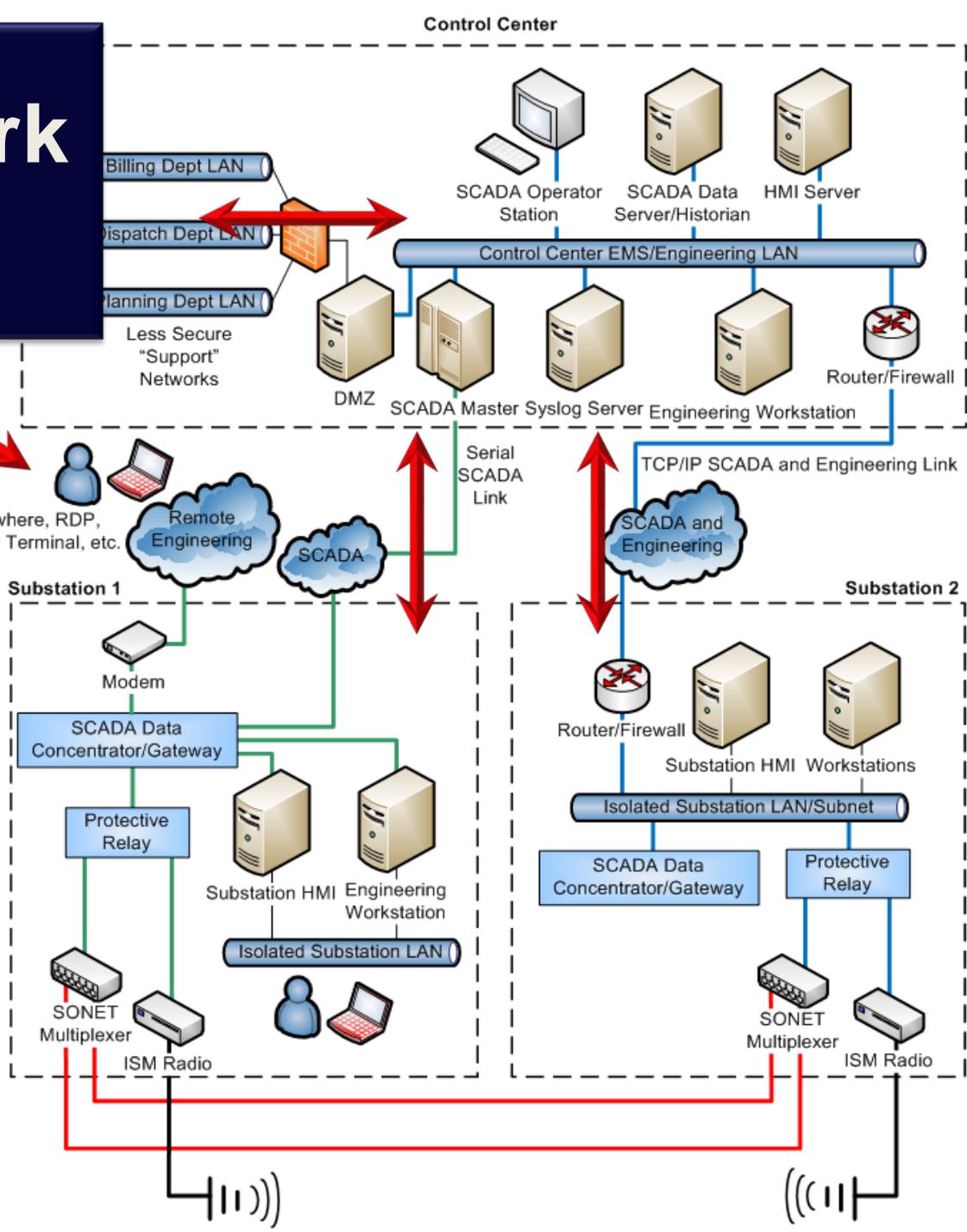
- Logging
- Alarm reporting
- Measurement consistency
- Communication monitoring
- Central logging



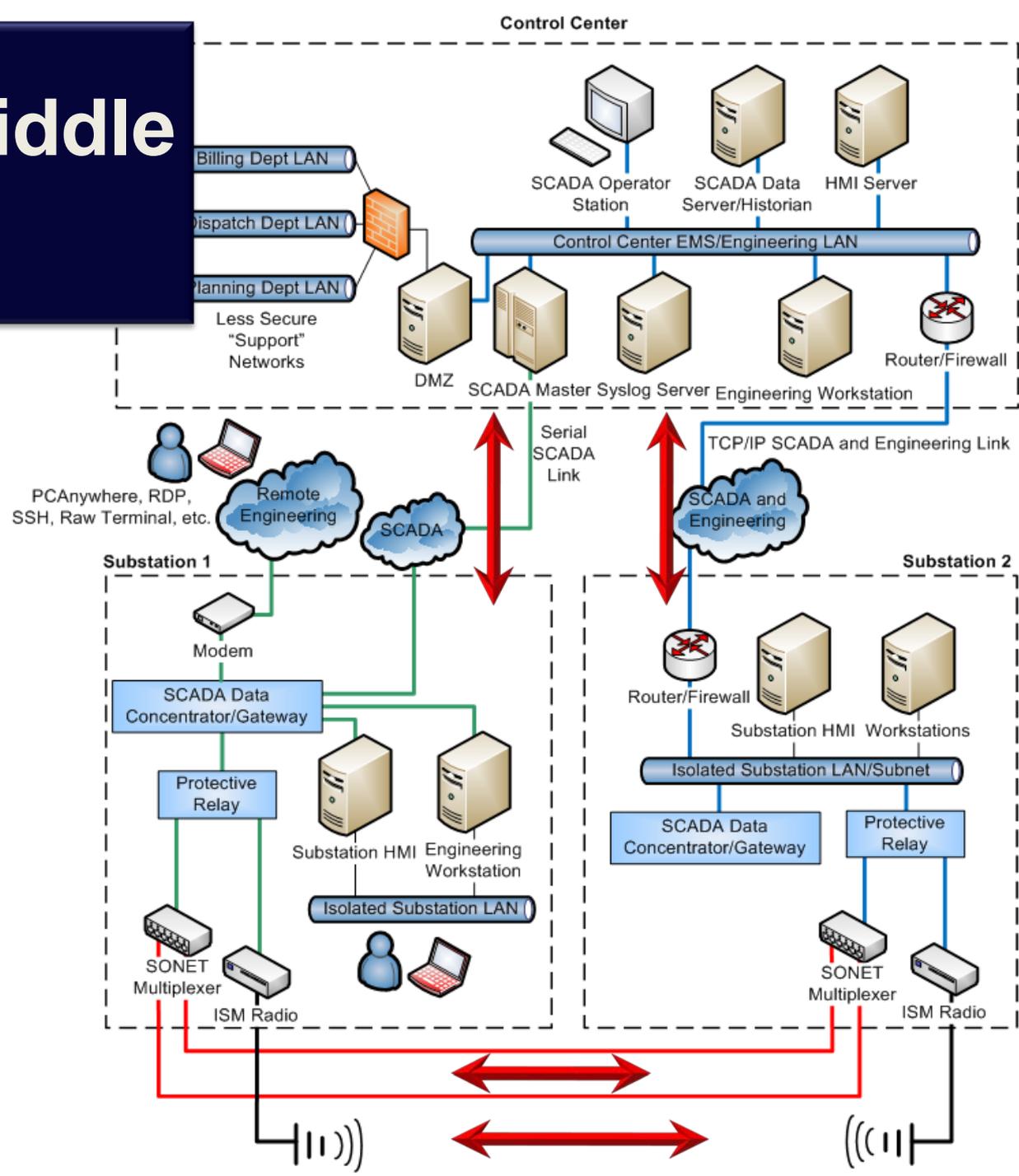
# Where Are the Points of Potential Exploits?



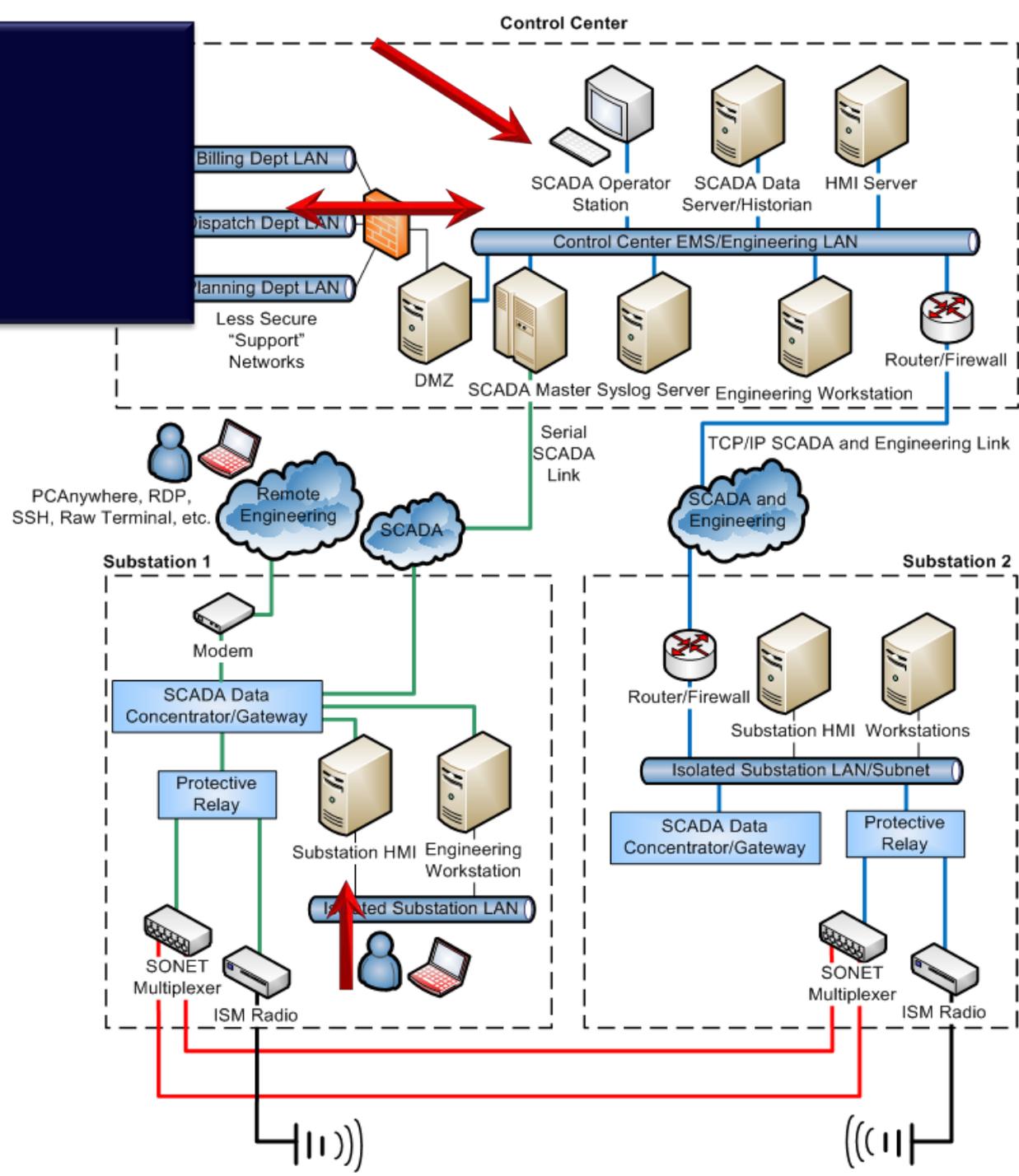
# External Network Access



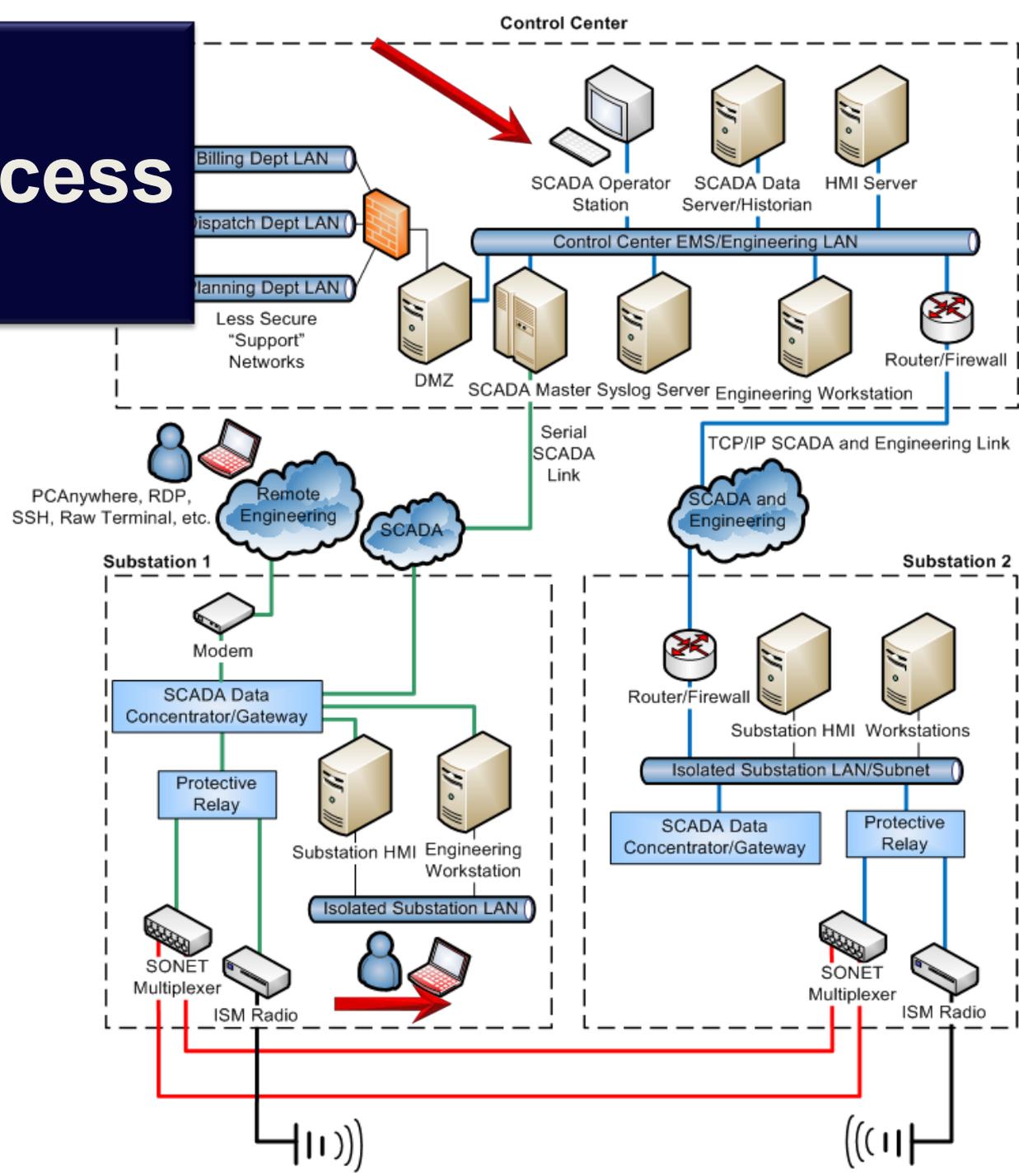
# Man-in-the-Middle Attacks



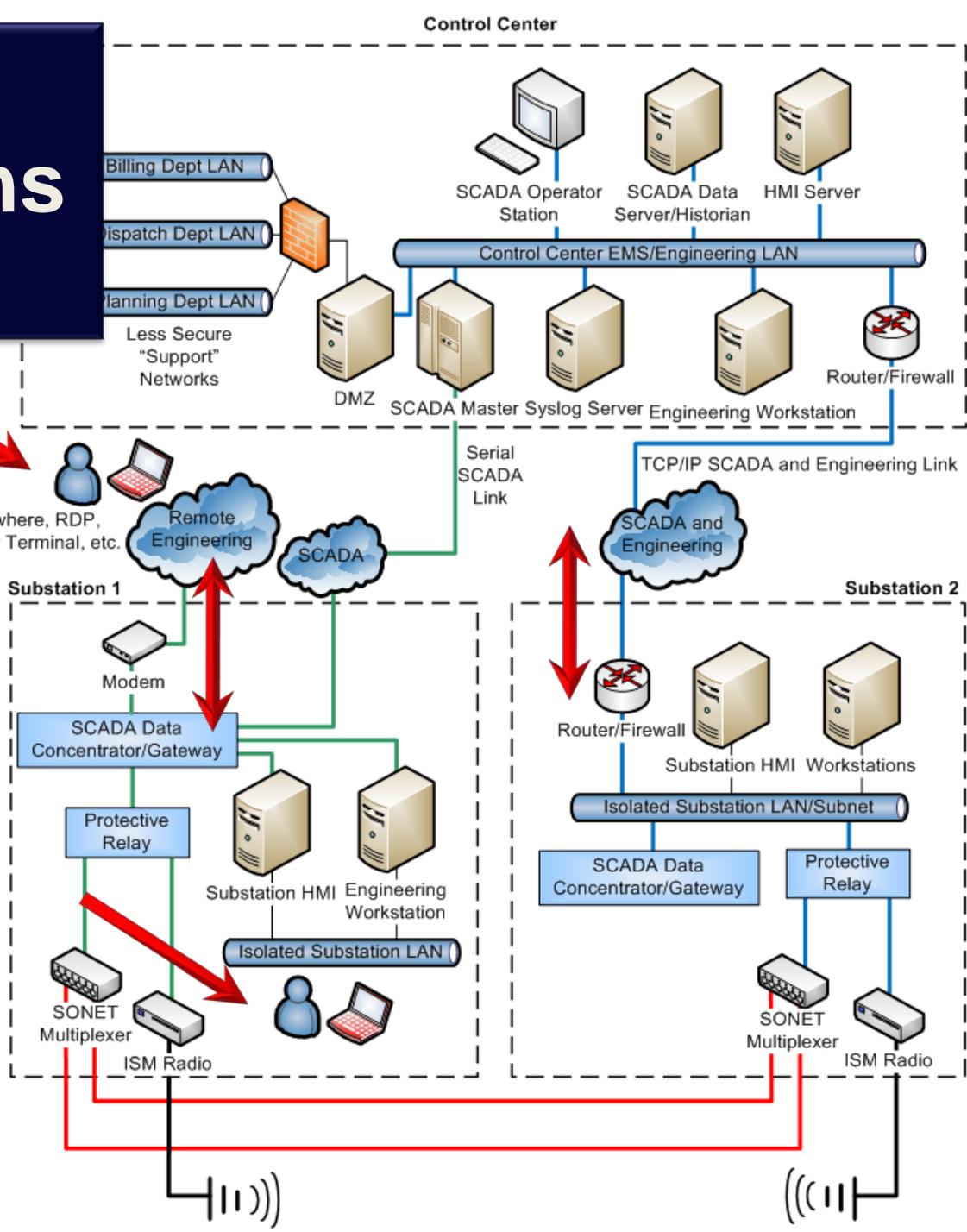
# Malware



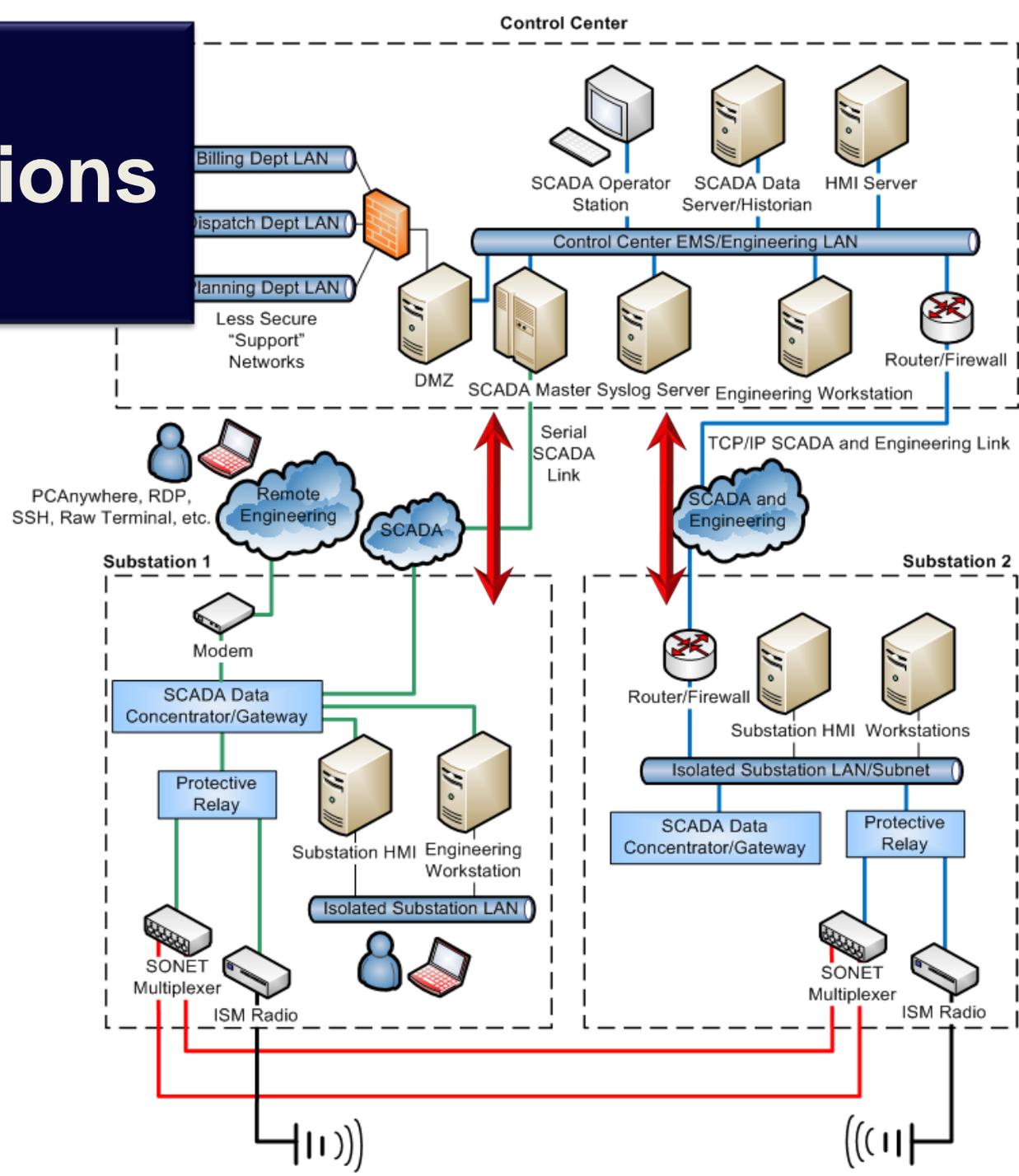
# USB Stick Access



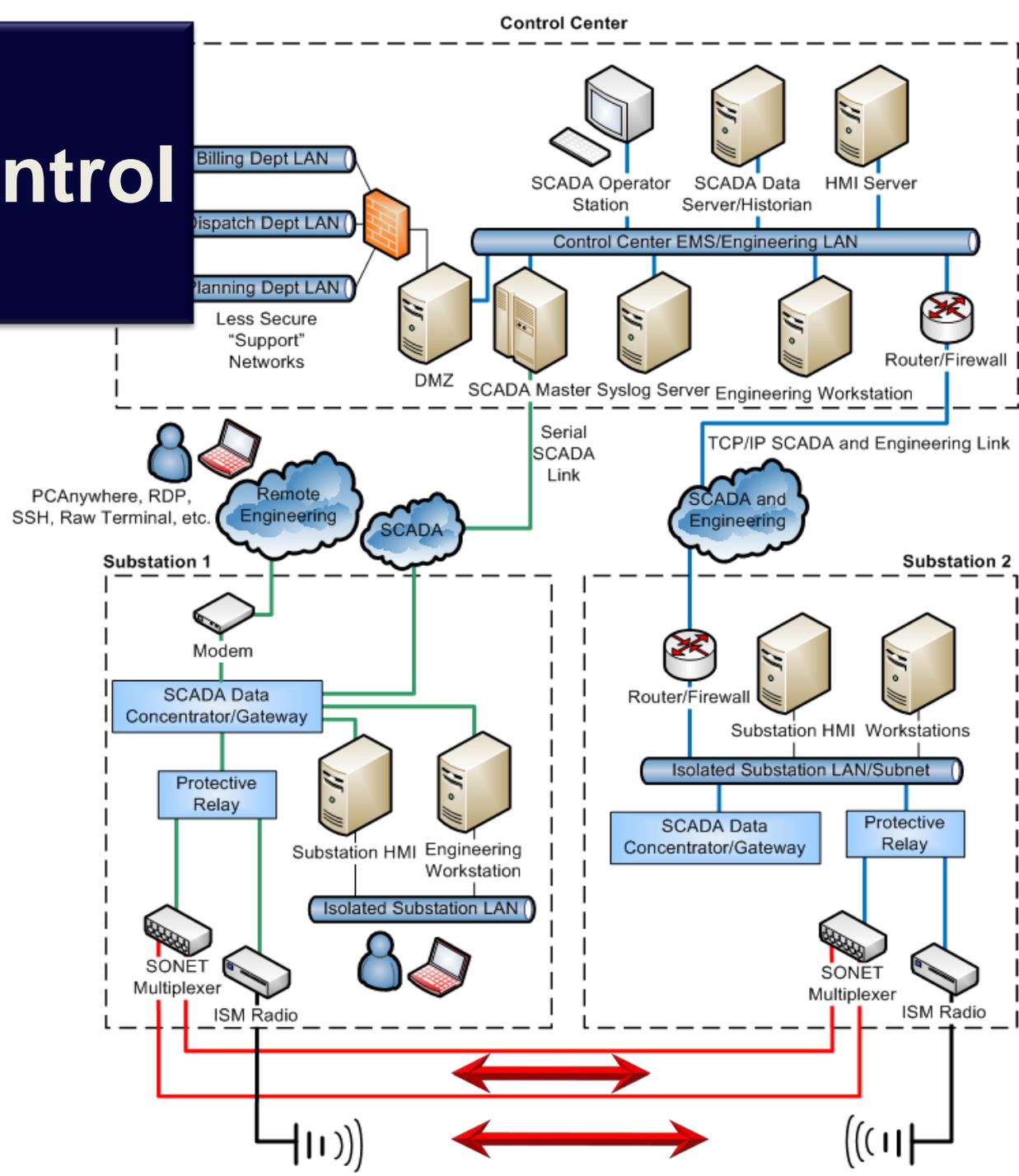
# Engineering Communications Access



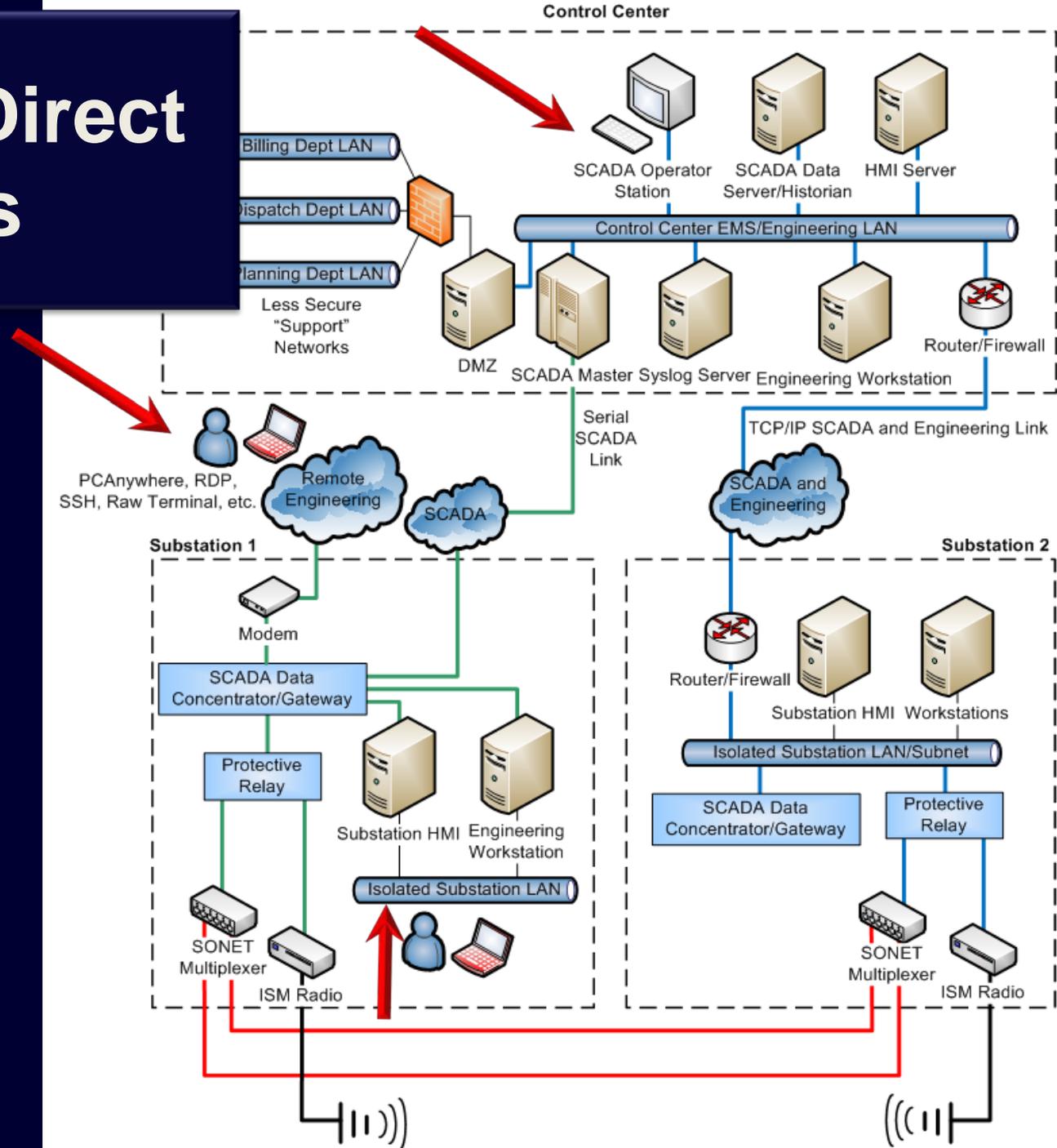
# SCADA Communications Access



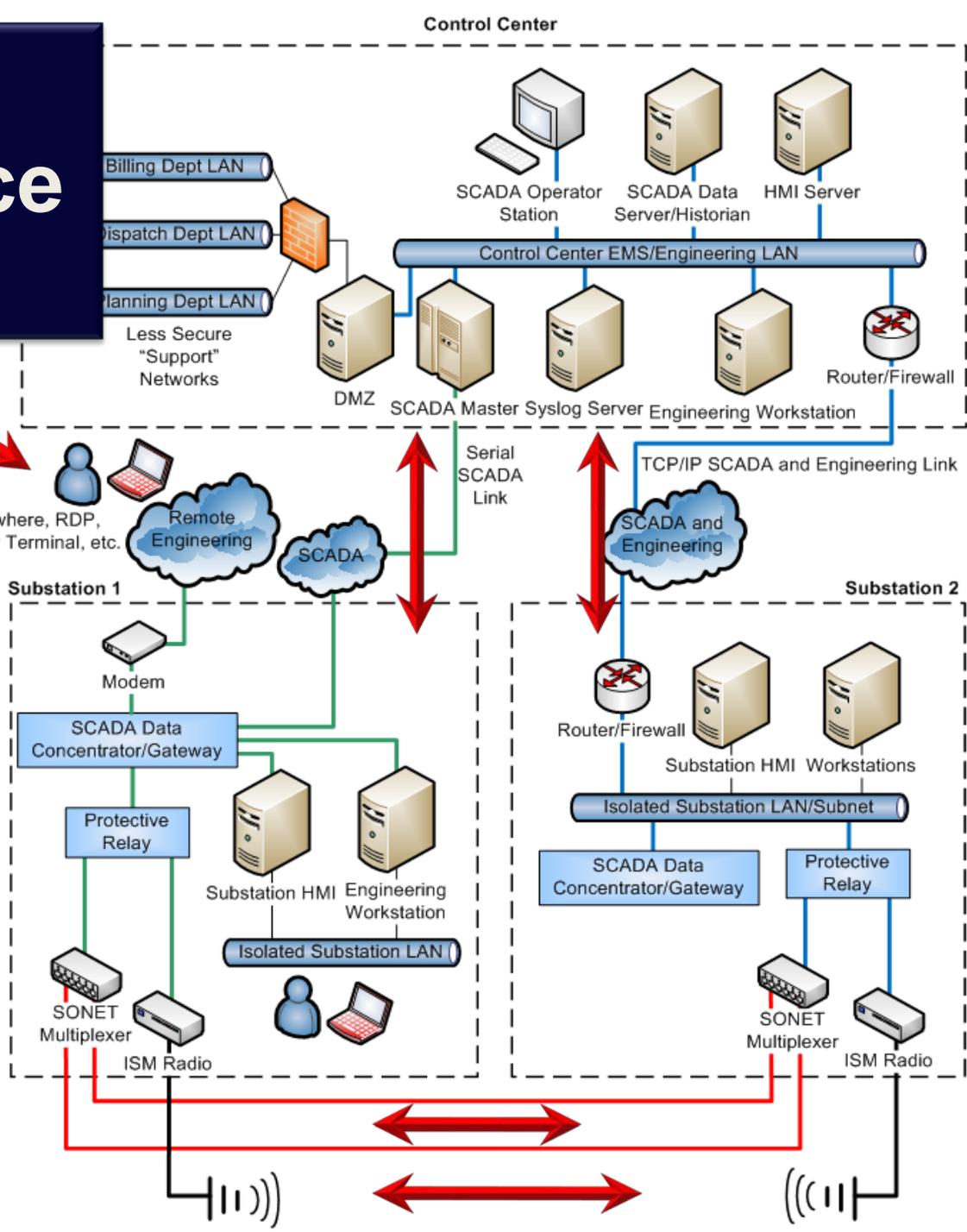
# Real-Time Control



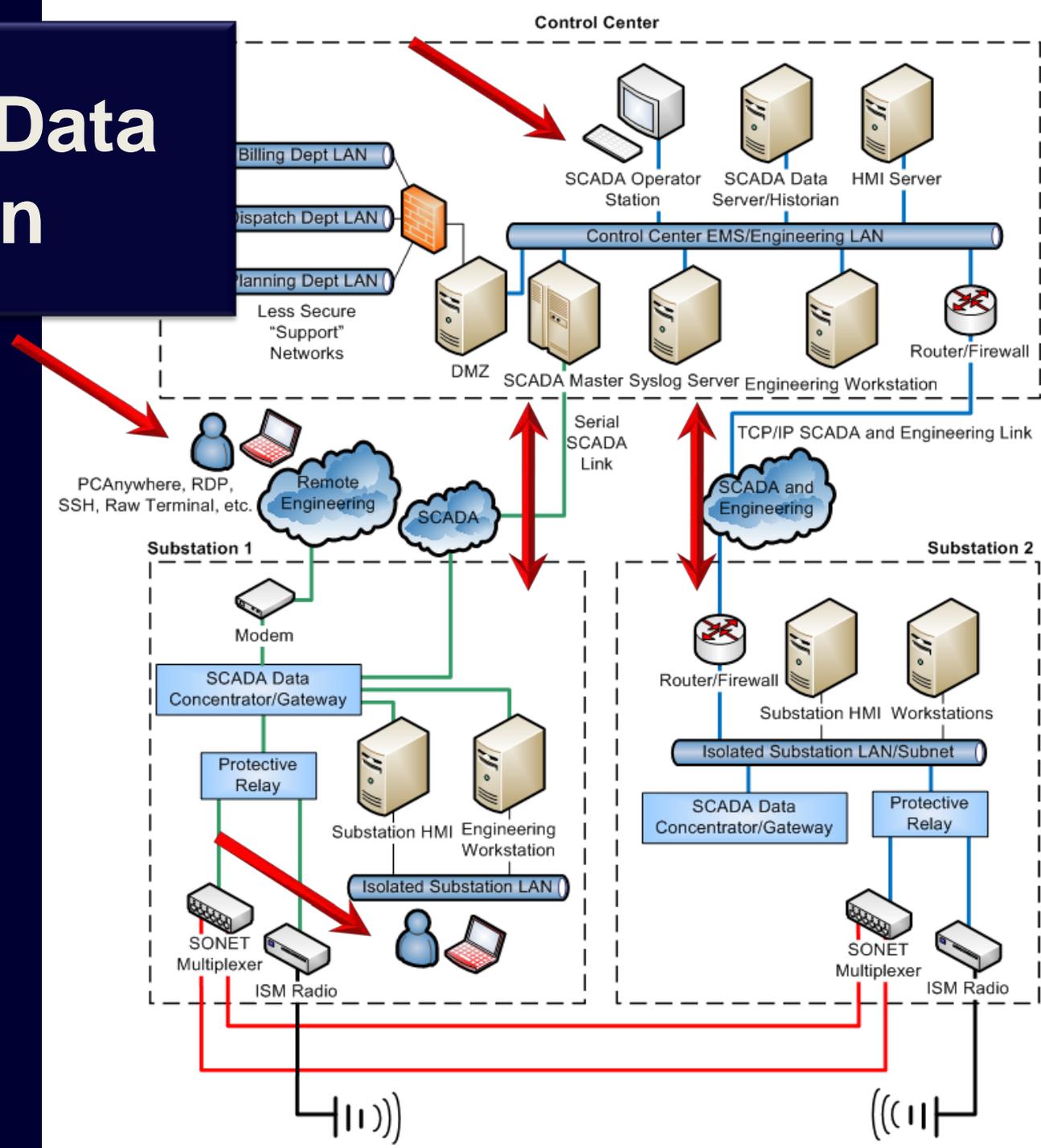
# Insider or Direct Access



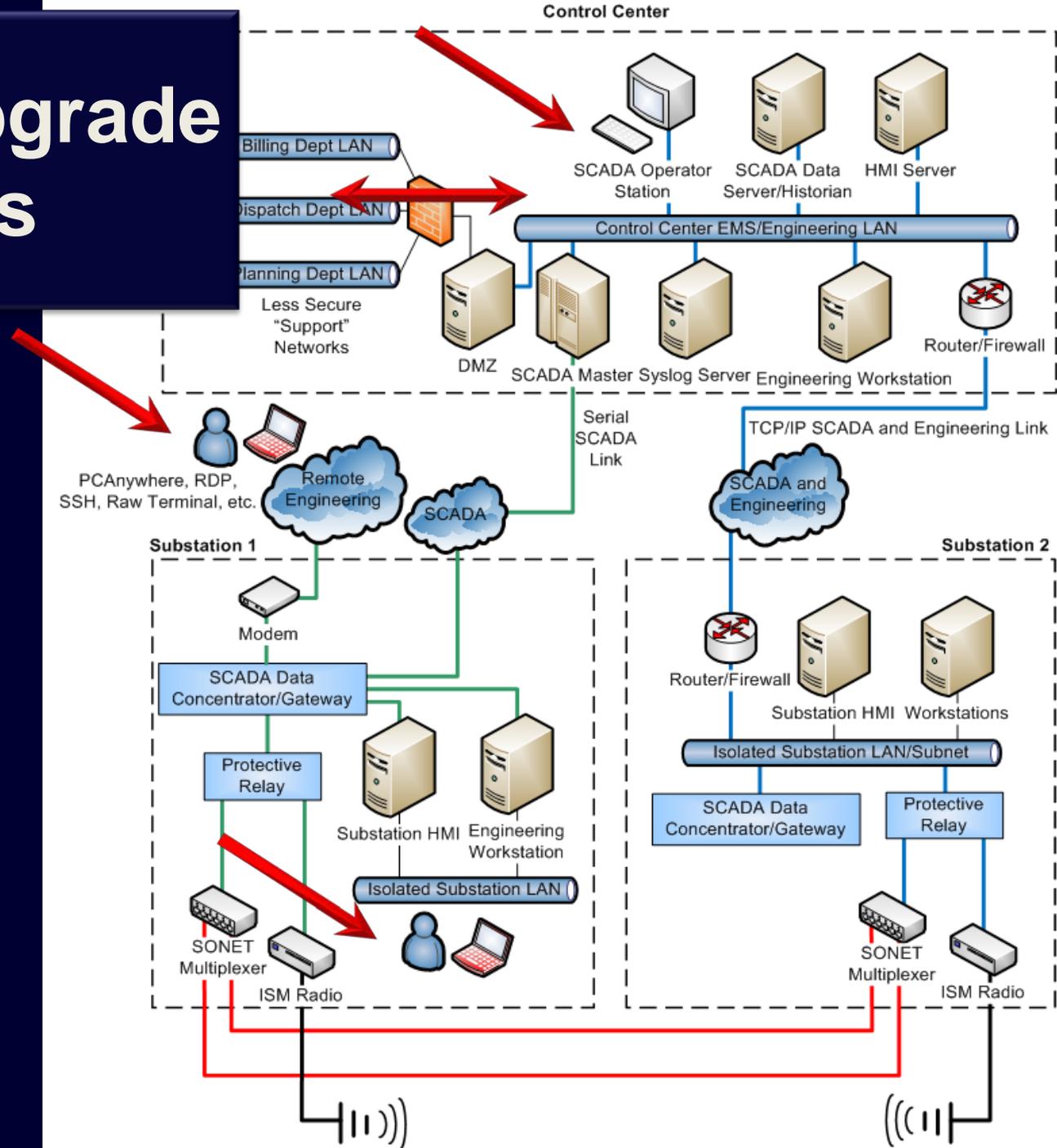
# Denial of Service



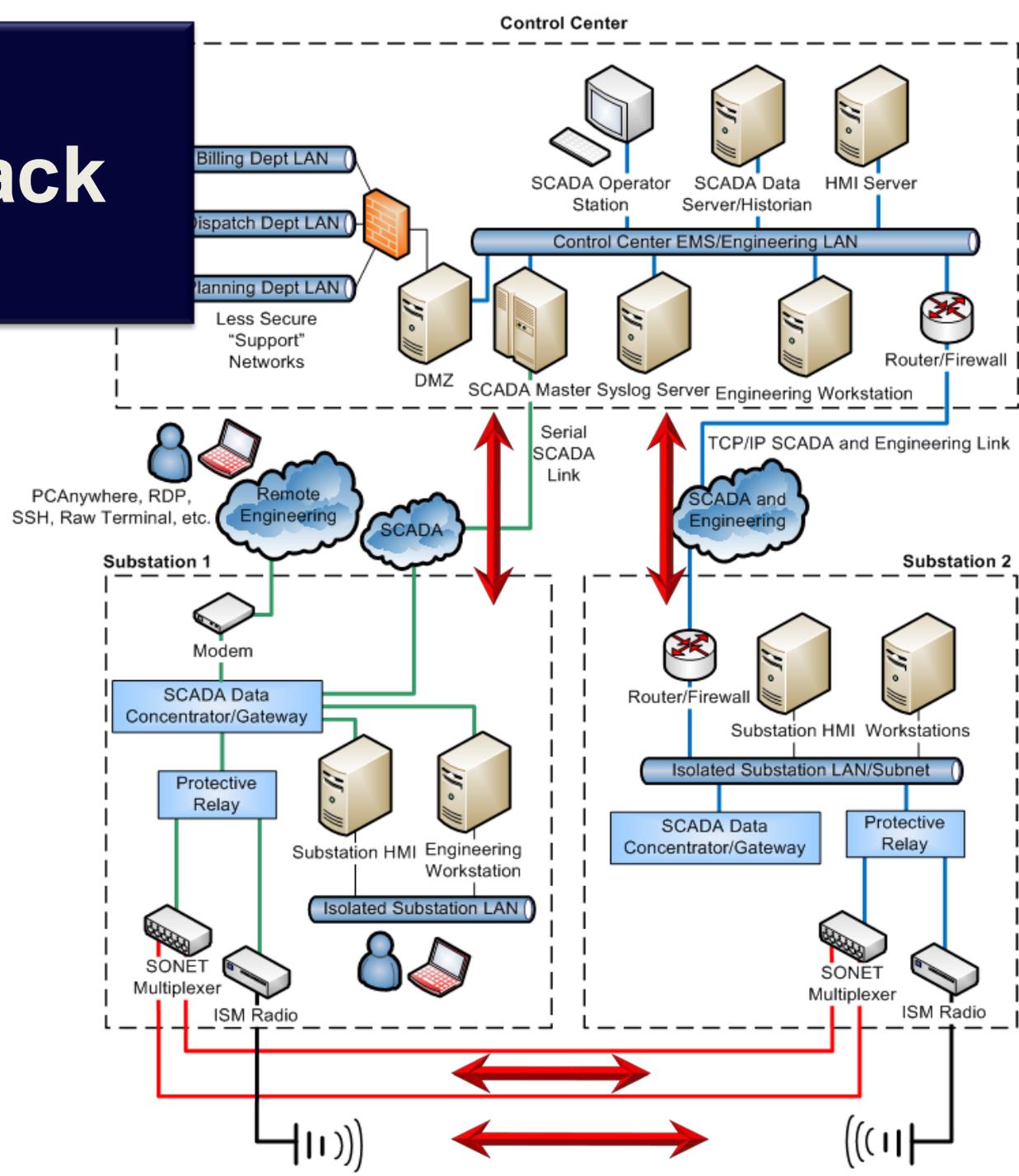
# Malicious Data Injection



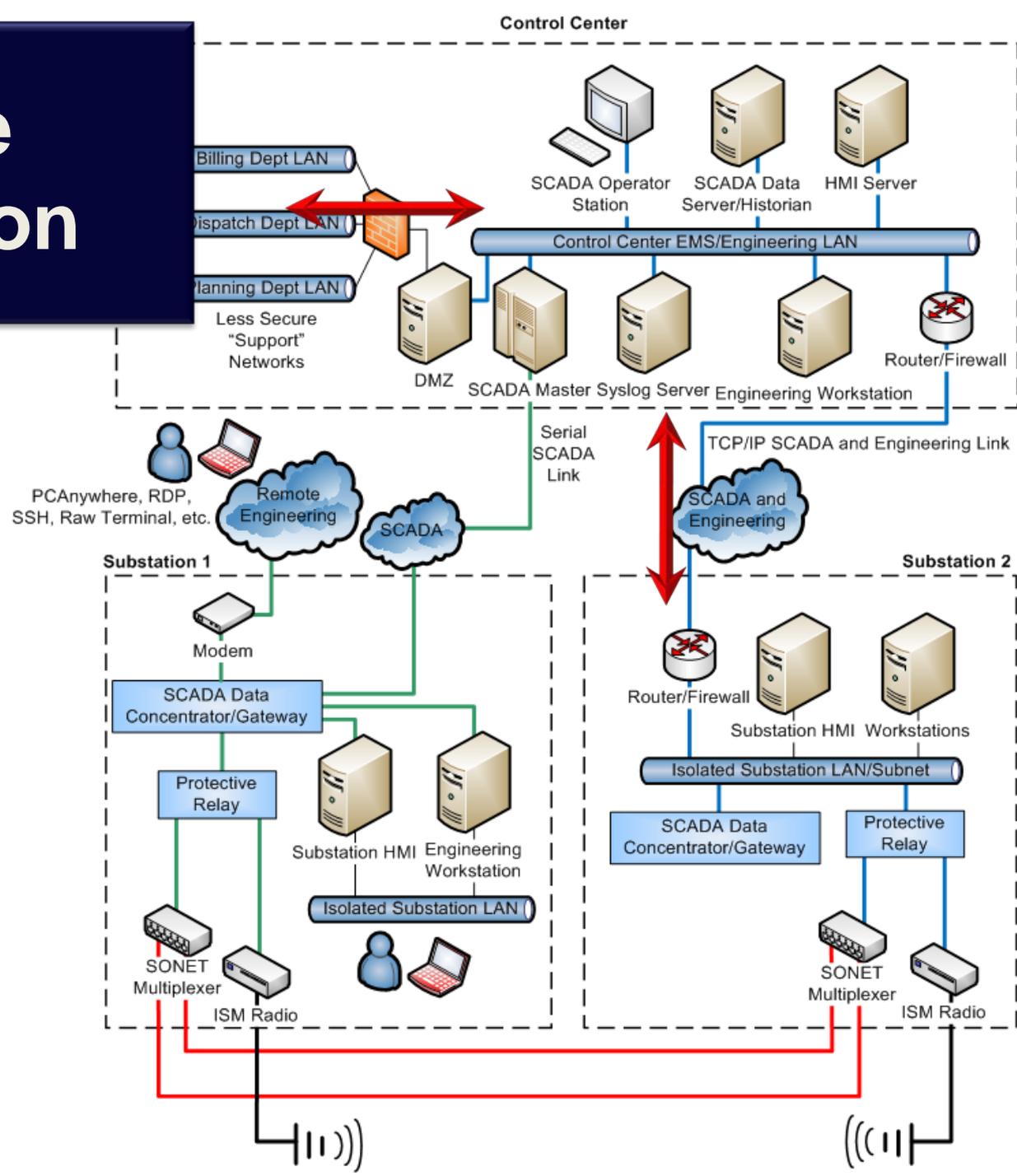
# Software Upgrade Exploits



# Data Playback



# Database Manipulation



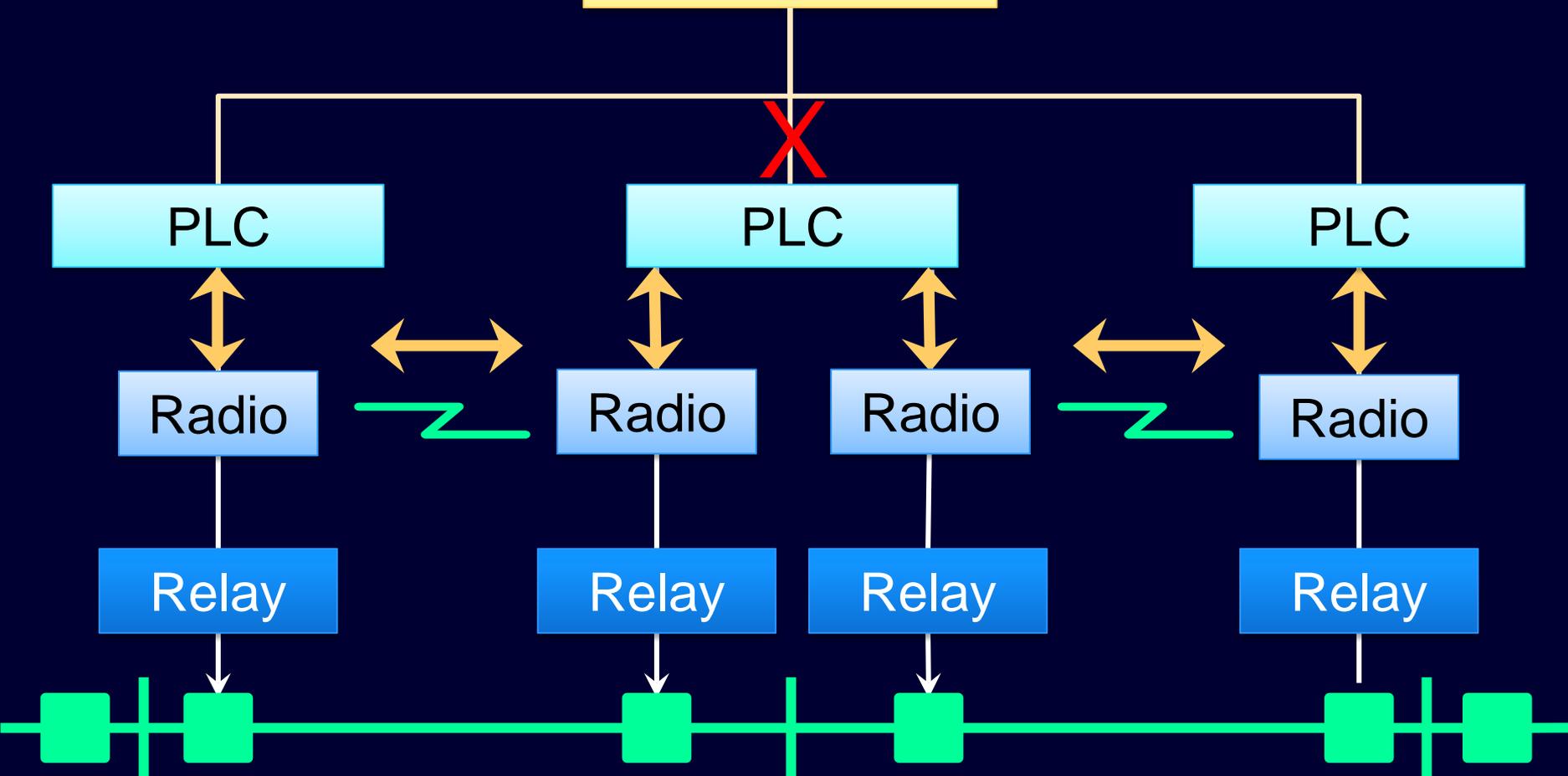
# Build on Security Tools and Information in Your IEDs

- 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



# Develop Secondary Communication Channels

SCADA Master



# 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 IT Cyber Security Practices

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

# Examine Logs

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

System Annunciator				
BRKR CBA RECLOSE LOCKOUT	BRKR CBA ENABLED	BRKR CBA CLOSED	BRKR CBA DEADY	BRKR CBA DEADZ
BRKR CBA LIVEZ	BRKR CBA NO RECLOSE	BRKR CBA IN LOCAL	BRKR CBA SG 1 ENABLED	BRKR CBA SG 2 ENABLED
BRKR CBB DEVICE ONLINE	BRKR CBB ENABLED	BRKR CBB FAULT	BRKR CBB HOT LINE TAG	BRKR CBB LIVEY
BRKR CBC CLOSED	BRKR CBC RECLOSE LOCKOUT	BRKR CBC DEADY	BRKR CBC DEADZ	BRKR CBC DEVICE ONLINE
BRKR CBC LIVEZ	BRKR CBC NO RECLOSE	BRKR CBC IN REMOTE	BRKR CBC SG 1 ENABLED	BRKR CBC SG 2 ENABLED
BRKR CBD DEVICE ONLINE	BRKR CBD ENABLED	BRKR CBD FAULT	BRKR CBD HOT LINE TAG	BRKR CBD LIVEY
BRKR CBE CLOSED	BRKR CBE RECLOSE LOCKOUT	BRKR CBE DEADY	BRKR CBE DEADZ	BRKR CBE DEVICE ONLINE
BRKR CBE LIVEZ	BRKR CBE RECLOSE ENABLED	BRKR CBE IN REMOTE	BRKR CBE SG 1 ENABLED	BRKR CBE SG 2 ENABLED

# Have an Incident Response Plan

- Develop plan to repair or restore system configuration
- Train all stake holders so they know what to do
- Practice response plan



# Create Security Awareness Program

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

# USE STRONG PASSWORDS

Weak: Webster

Strong: W3b\$st3r

Stronger: A phras3 1s 3v3n Str0ng3r!



# Conclusions

- Every cyber intrusion leaves finger prints
- Most equipment has features that can be used to detect the signs of a cyber attack
- Combining features provides consistency checks for wide area monitoring and security-in-depth.
- Use the concepts of this paper to answer the question “How would we know?”