SCHWEITZER ENGINEERING LABORATORIES

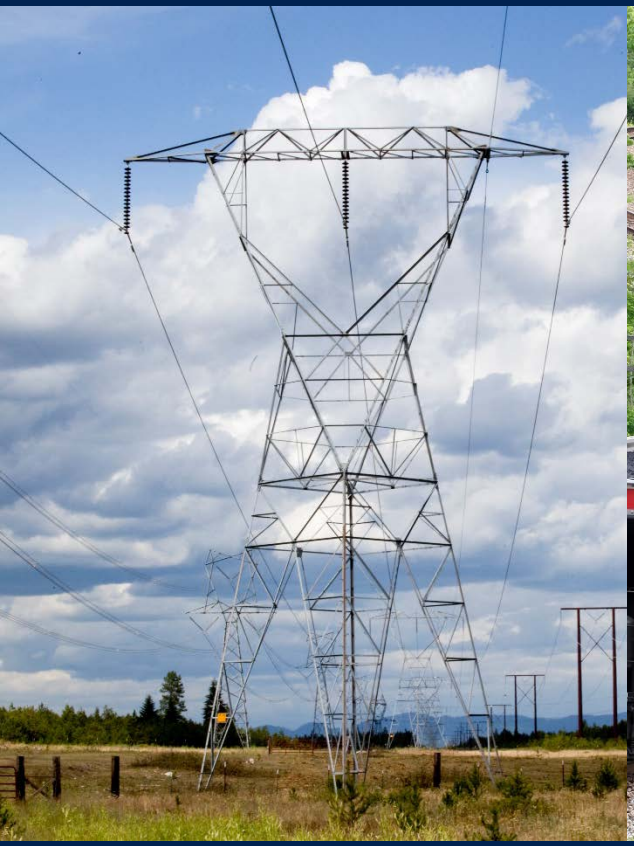
Our Cyber Security History and Future

Trustworthy Cyber Infrastructure for the Power Grid

April 3, 2015

Edmund O. Schweitzer III, Ph.D.
President, Schweitzer Engineering Laboratories, Inc.

Delivering Energy at the Speed of Light

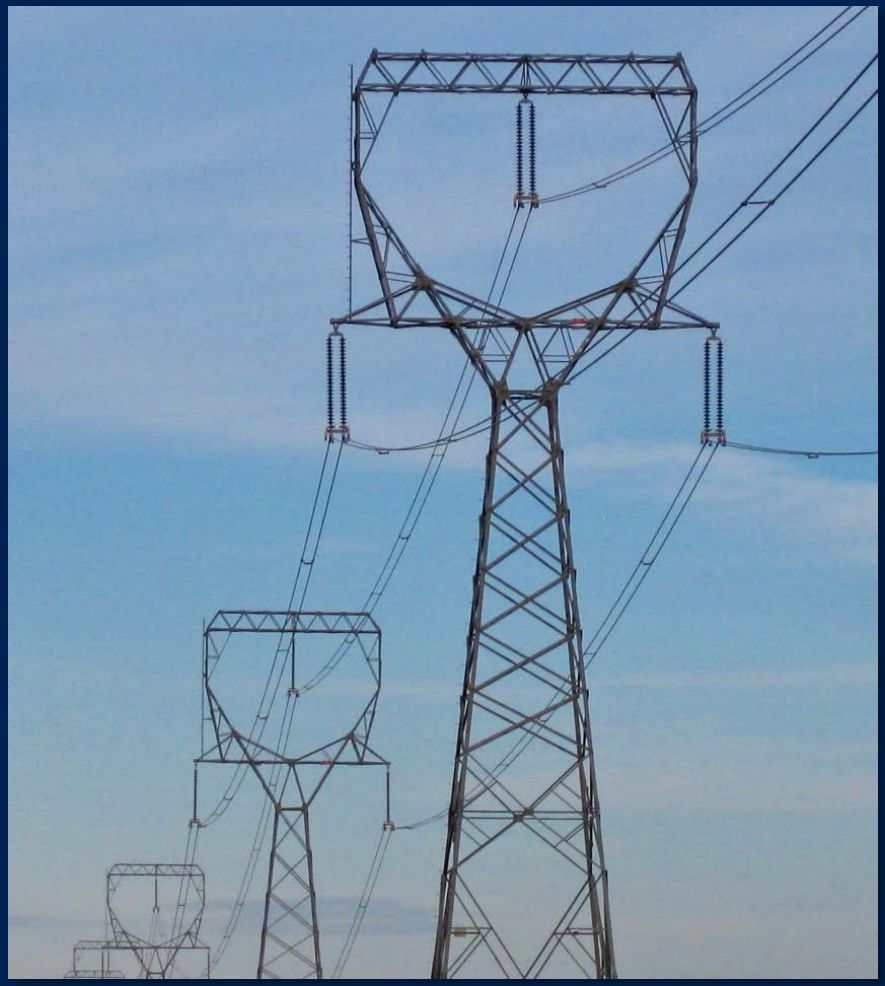


186,000 mi / sec

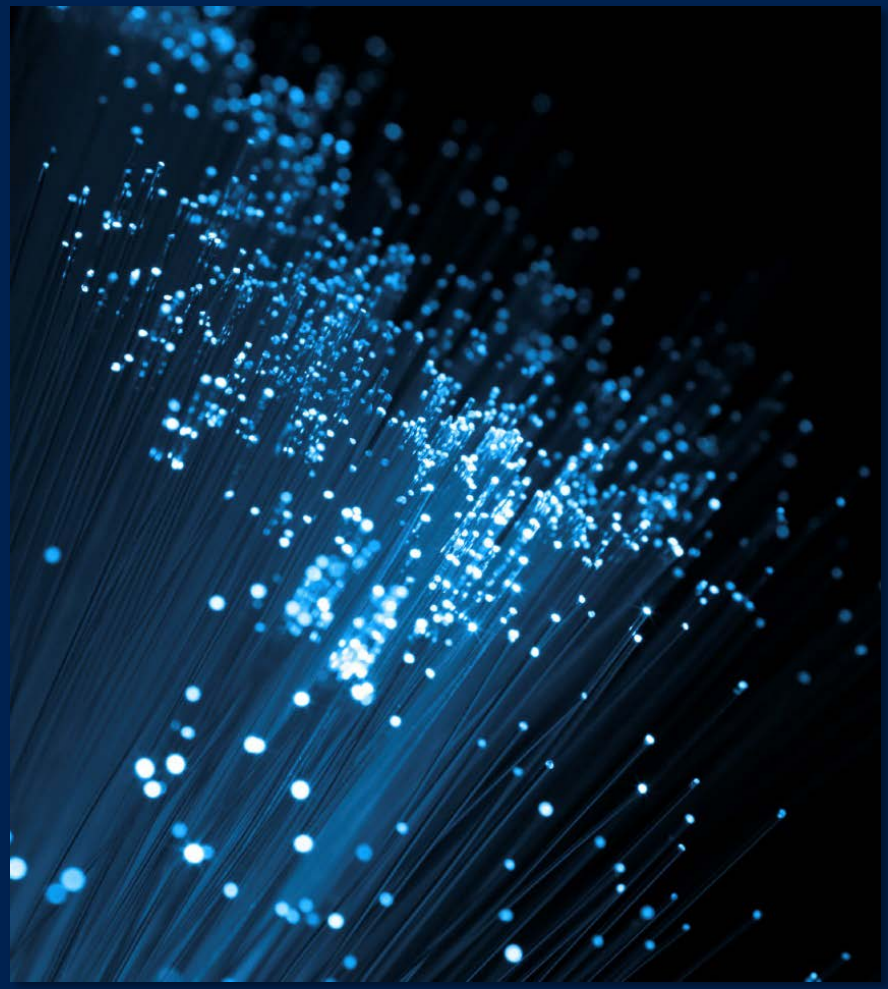
50 mi / hr

30 mi / hr

Faster Than Information in Fiber



300,000 km / sec



200,000 km / sec

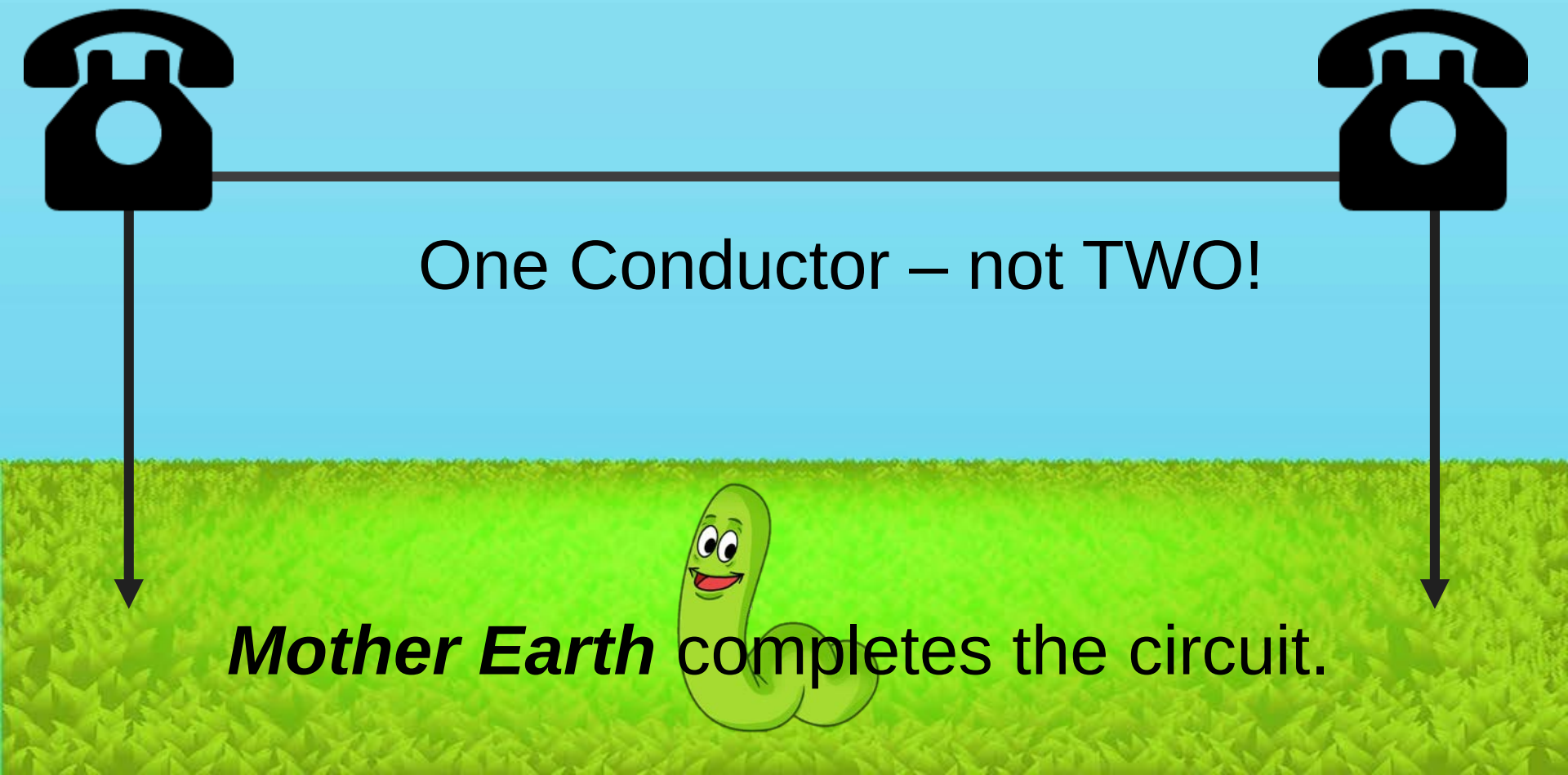
Staying Safe in the Information Age

- What can we learn from history?
- What makes the power system work?
- How can technology contribute?
- Avoiding the weaknesses.
- *Benefiting from the strengths.*

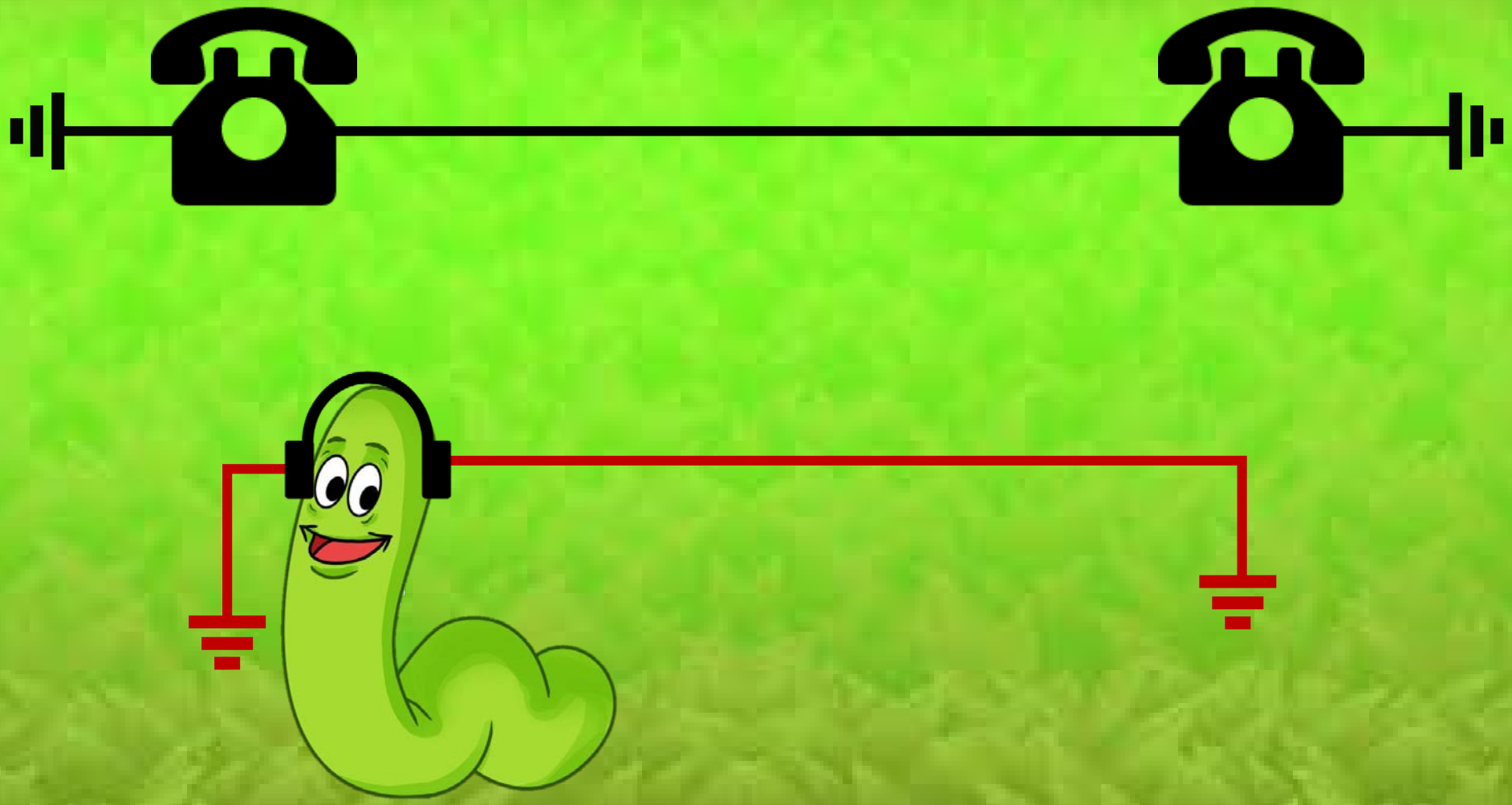
Technology Has Risks

- Earth-return field telephones WW1
- Local oscillator radiation WW2
- False Beacons (Meaconing)

Field Telephones with Single-Pole Earth-Return Save Wire

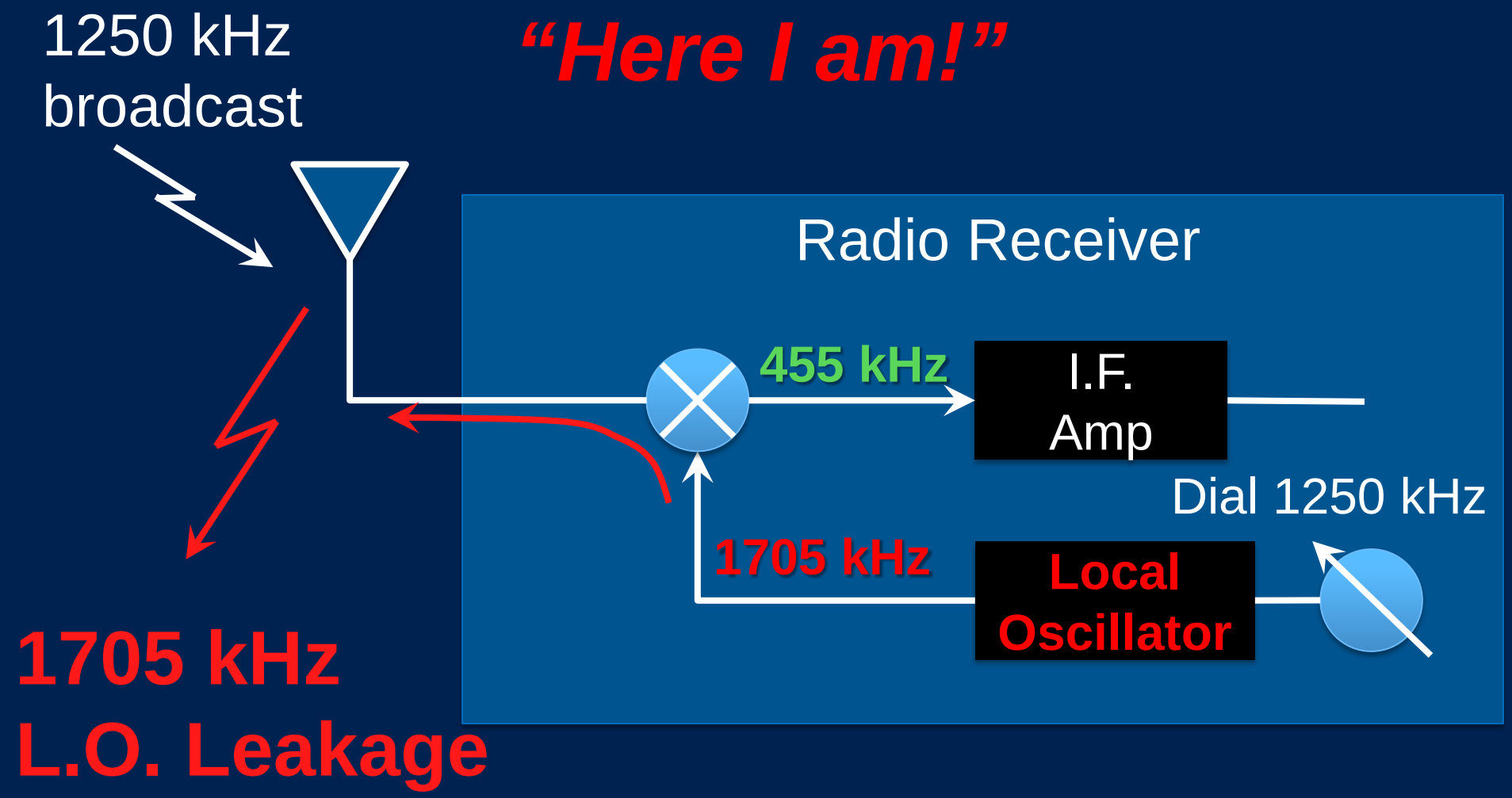


…but the Enemy Can Worm In!



Local Oscillator Leakage Whispers,

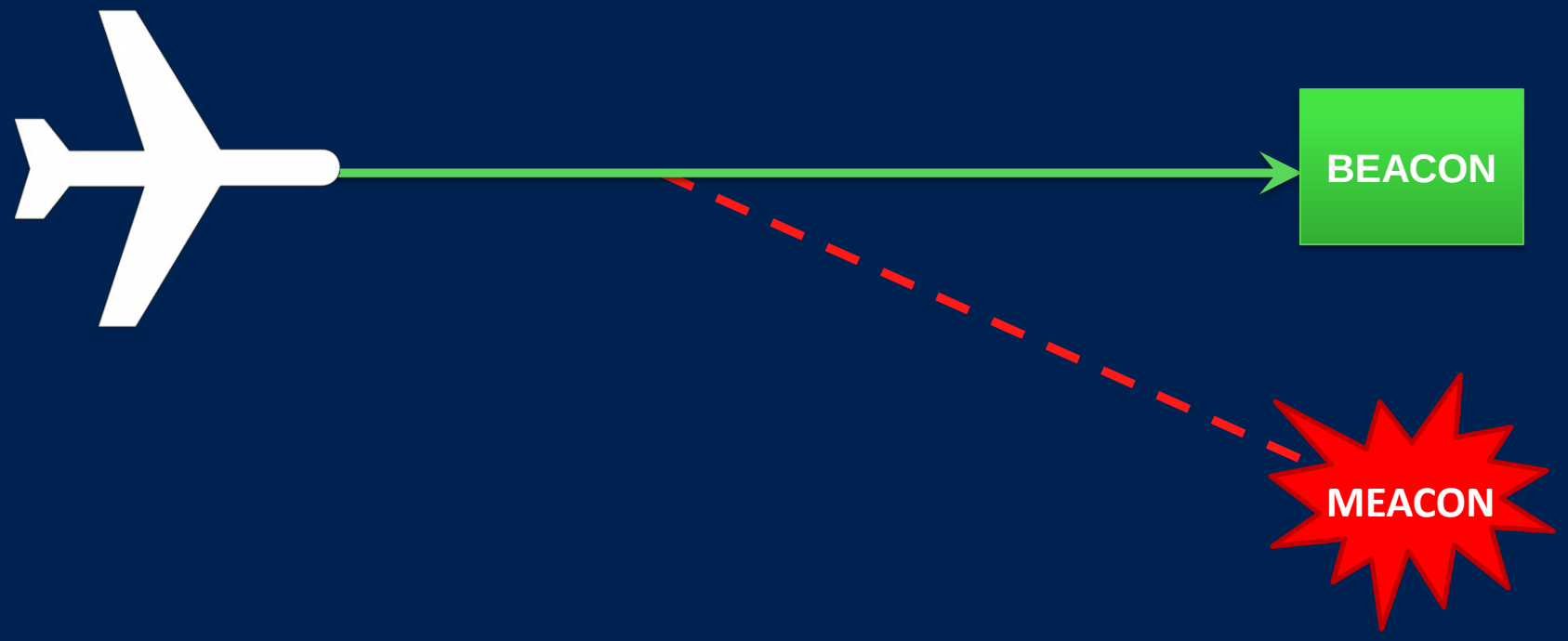
"Here I am!"



1705 kHz – 1250 kHz = 455 kHz

Morale(?) Receiver

Pull Aircraft Off Course With False Beacons

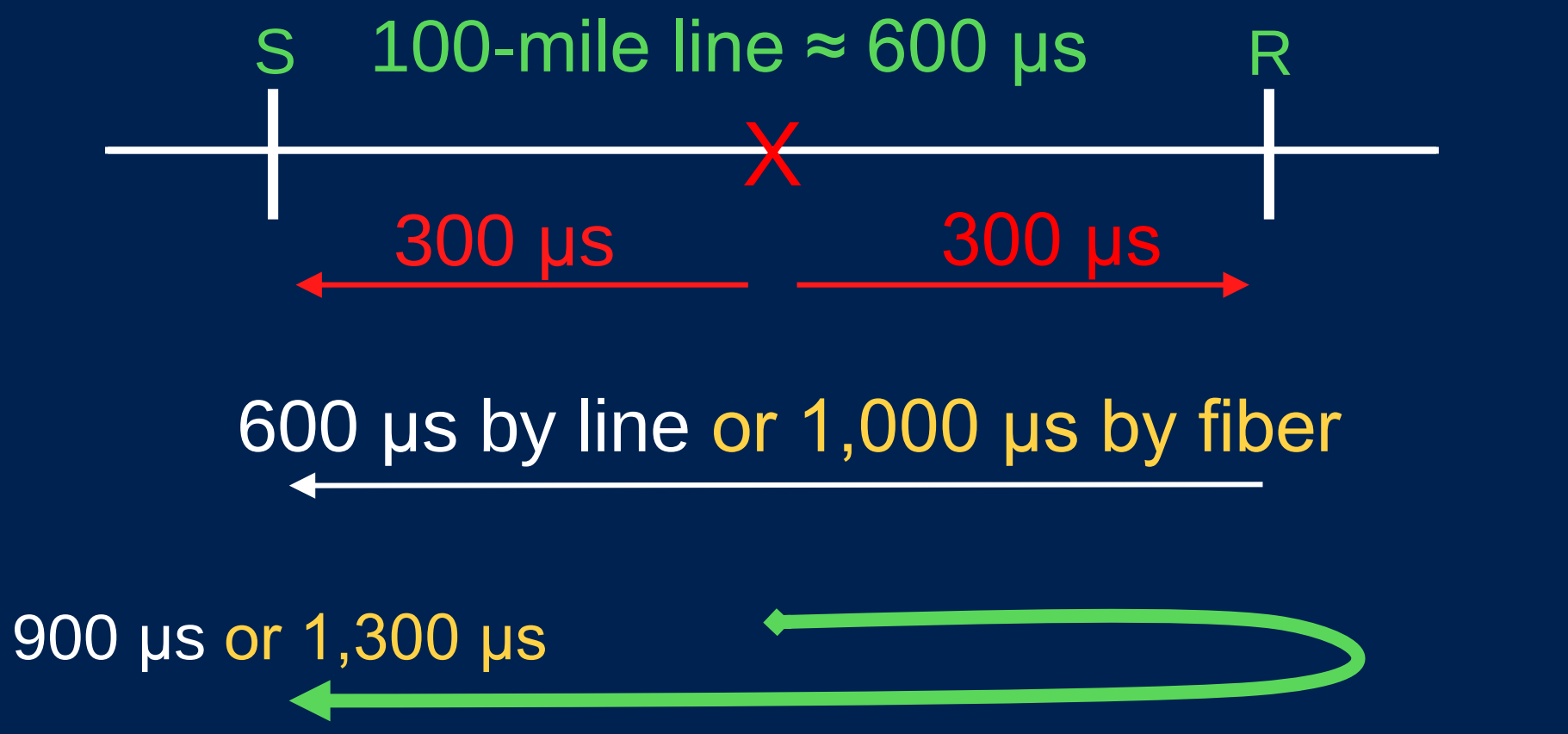


Some Basic Thoughts

- Power systems are inherently stable.
- They can run without “cyber.”
- Protection must always be available.
- Maintaining protection usually means taking primary equipment out of service.
- Faults must be cleared FAST!

Communicate more, depend on it less.

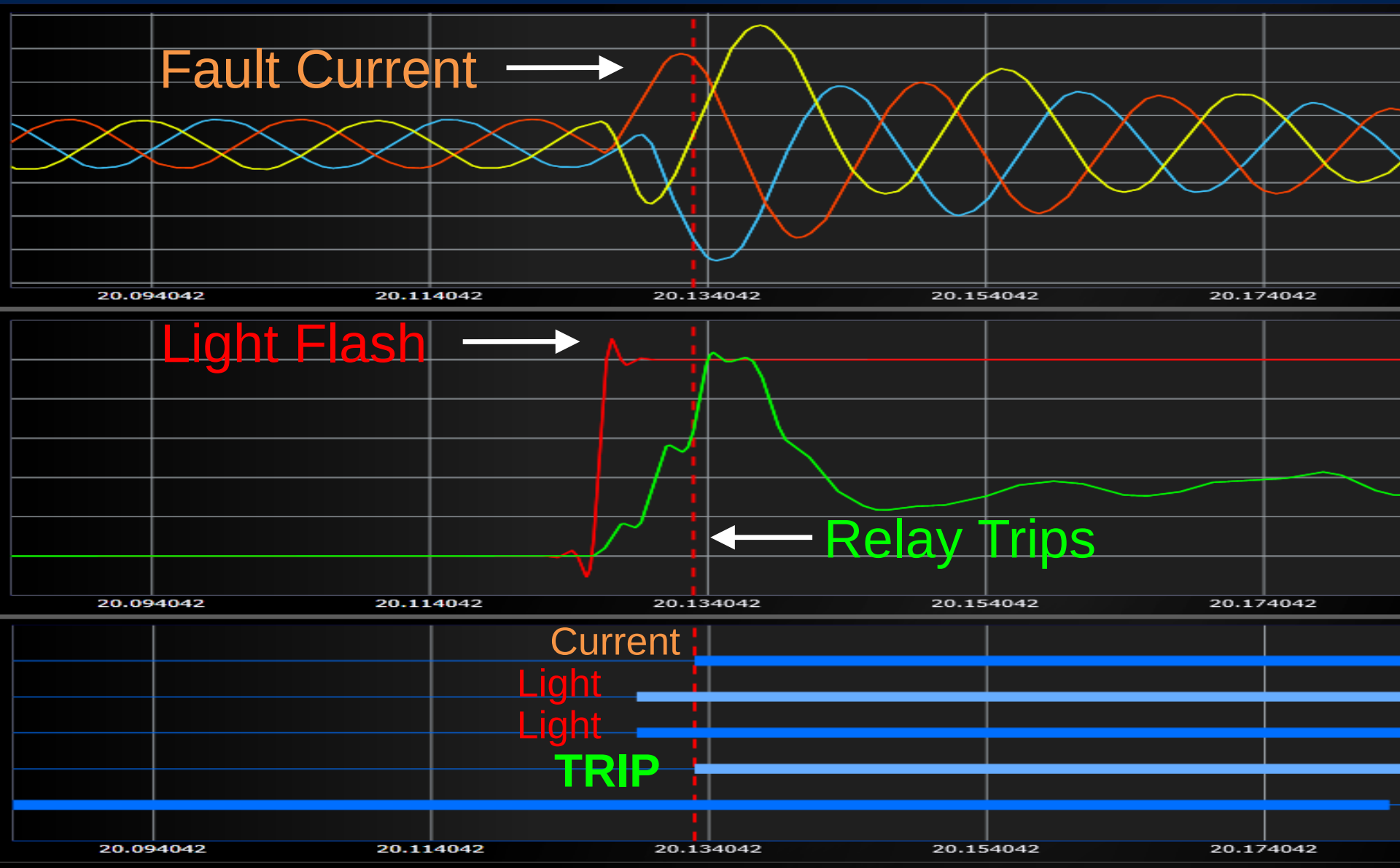
Speed of Light Limits Relay Time



The fastest communications path is the line

Trip *Fast* on Current and Light

Trip in 4 ms

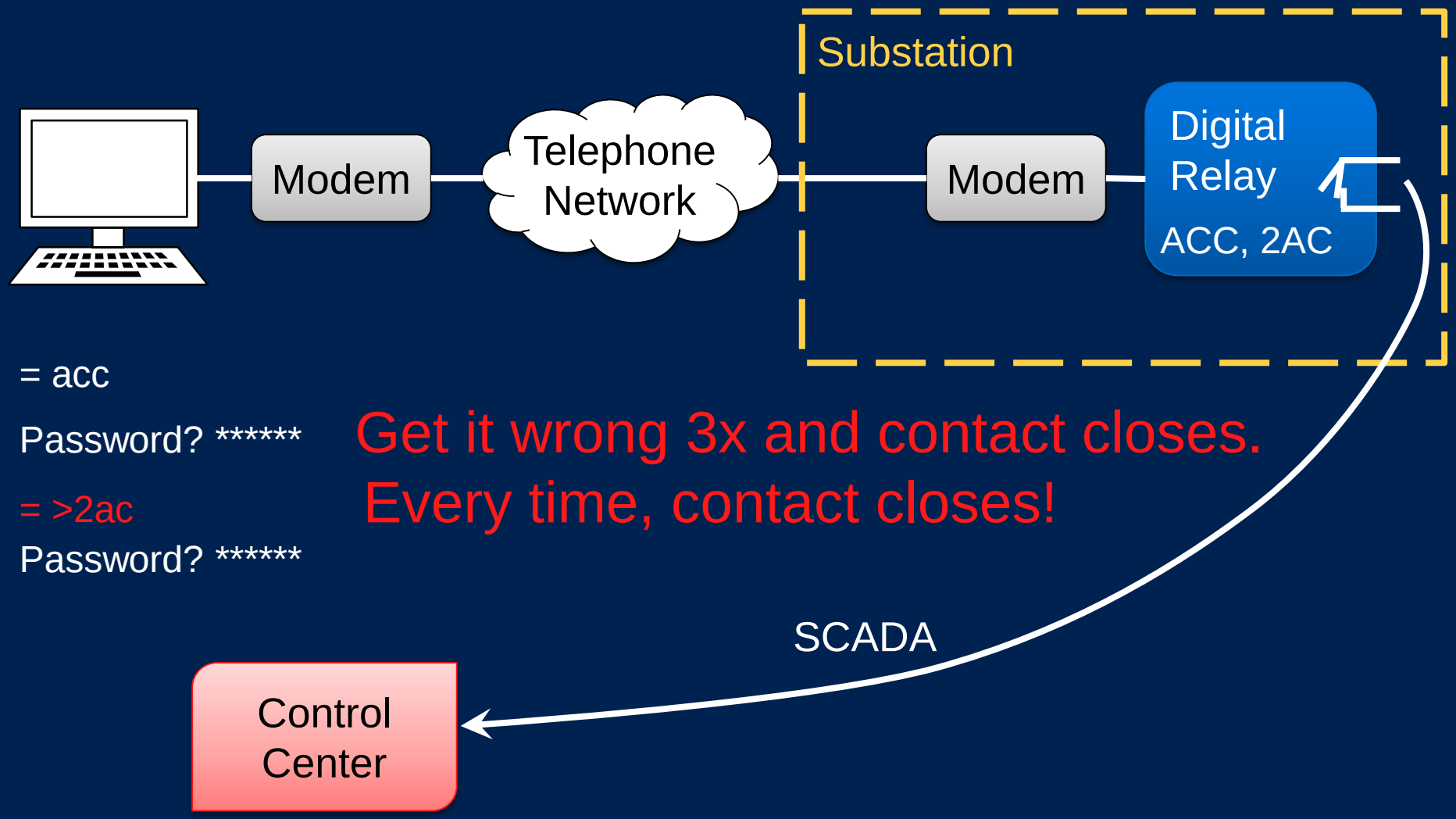

Fault Current
20.094042
20.114042
20.134042
20.154042
20.174042
Light Flash
Relay Trips
20.094042
20.114042
20.134042
20.154042
20.174042
Current
Light
Light
TRIP
20.094042
20.114042
20.134042
20.154042
20.174042

SEL-21 Security in 1984

- Two access levels
- Jumper to disable trip
- Alarm contacts
- Firmware checksums

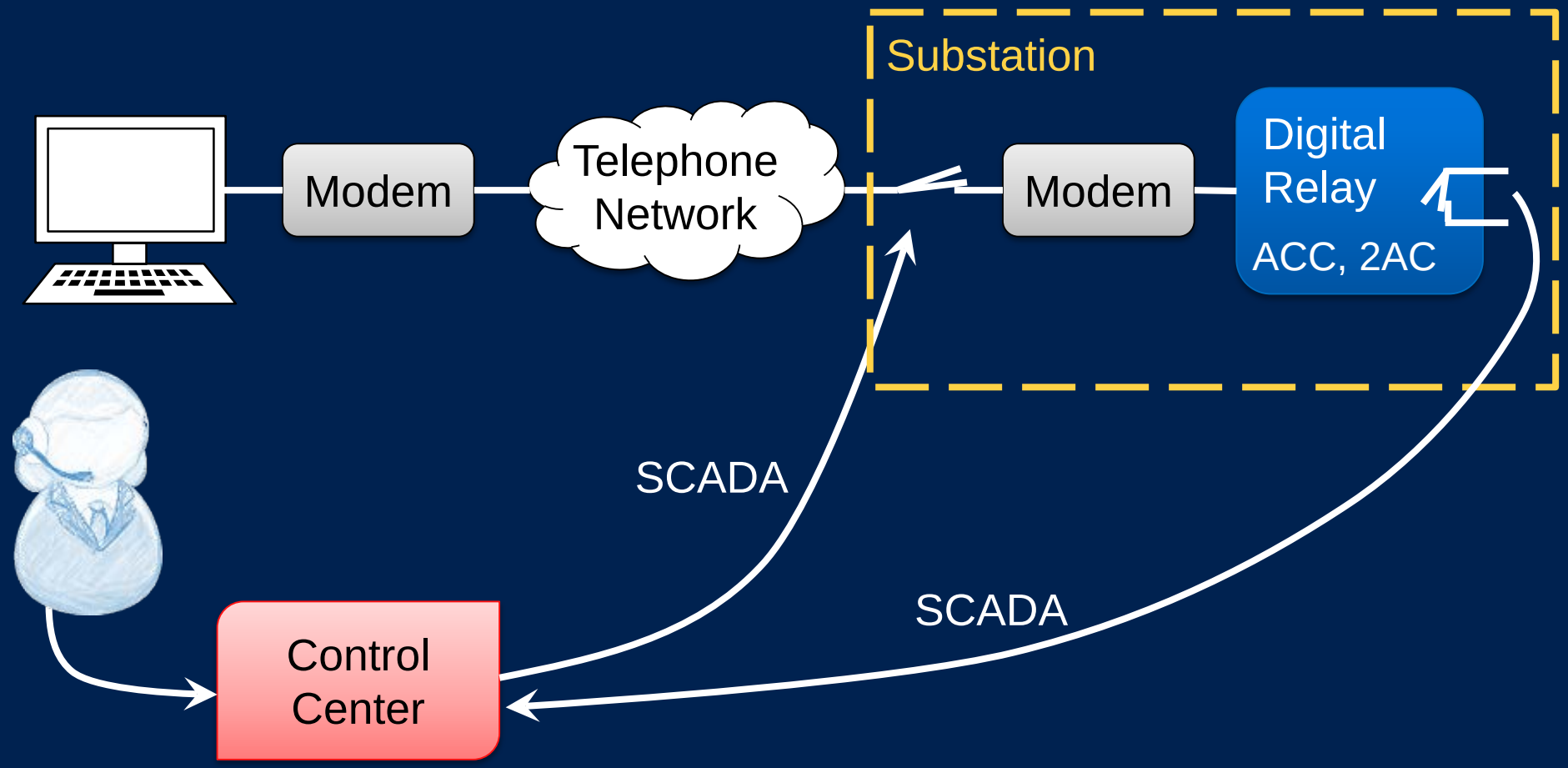

```
*ACC
Password: ? @@@@@@
Invalid Password

Password: ? @@@@@@
Invalid Password

Password: ? @@@@@@
Invalid Password
Access Denied
```

Two-Party Authentication in 1984



SCADA Op Connects Phone Line

You call in; if op knows you, then access



Authentication Slow Could be toll call

Concerns About Intrusions Into Remotely Accessible IEDs, Controllers, and SCADA Systems

27th Western Protective Relay Conference

Spokane, WA

October 24 – 26, 2000

Dr. Paul W. Oman

Dr. Edmund O. Schweitzer

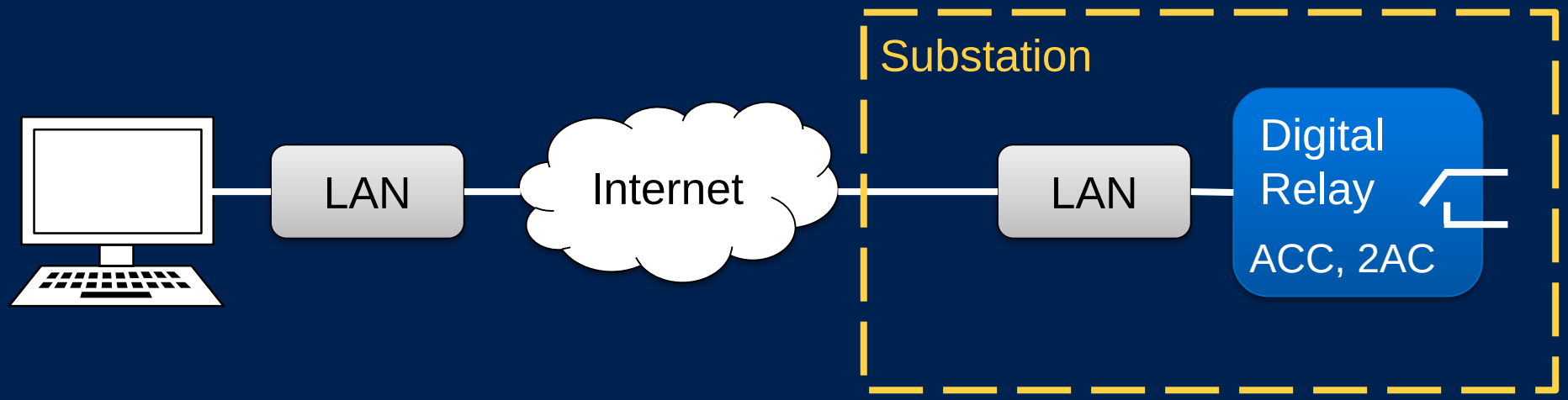
Dr. Deborah Frincke

What's Causing the Increased Risk? WPRC, Spokane, WA Oct 2000

- Pressure to Downsize, Automate, Cut Costs
- Instability in Electric Utility Job Market
- Rapid Growth of Computer Literacy
- Widespread Availability of Hacker Tools
- Shift From Proprietary Systems to Distributed Systems With Open Protocols
- FERC 888 / 889 Requirements
- Increased Access via Modems and Internet
- Increasing Espionage and Terrorism

Connectivity = Convenience + Risk

2001: Relay with Ethernet Port



- Fast and “free”
- Very convenient…to good and bad guys

Q: *“Why would anyone put an Ethernet port on a relay?”* A: *“Market Pressure!”*


THE BEST WAY TO PREDICT
THE FUTURE IS TO
INVENT IT
– Alan Kay

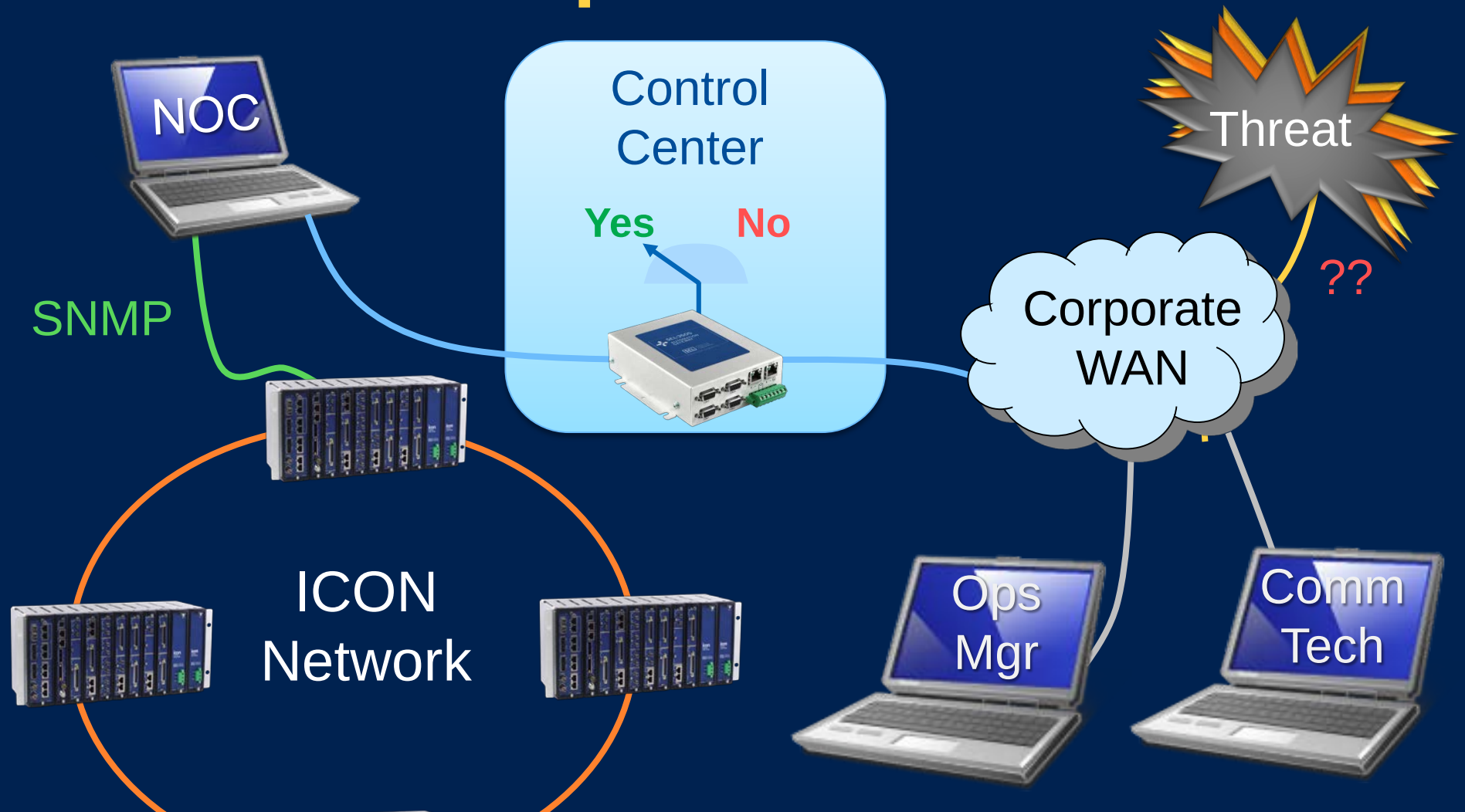
Regulations Fall Short

- Take years to emerge, all the while the tech and threats change.
- One-size-fits-all probably fits no one.
- Tell bad guys what we ***will*** and ***won't*** do.
- Compliance and security are different.

Government: Teach and Advise

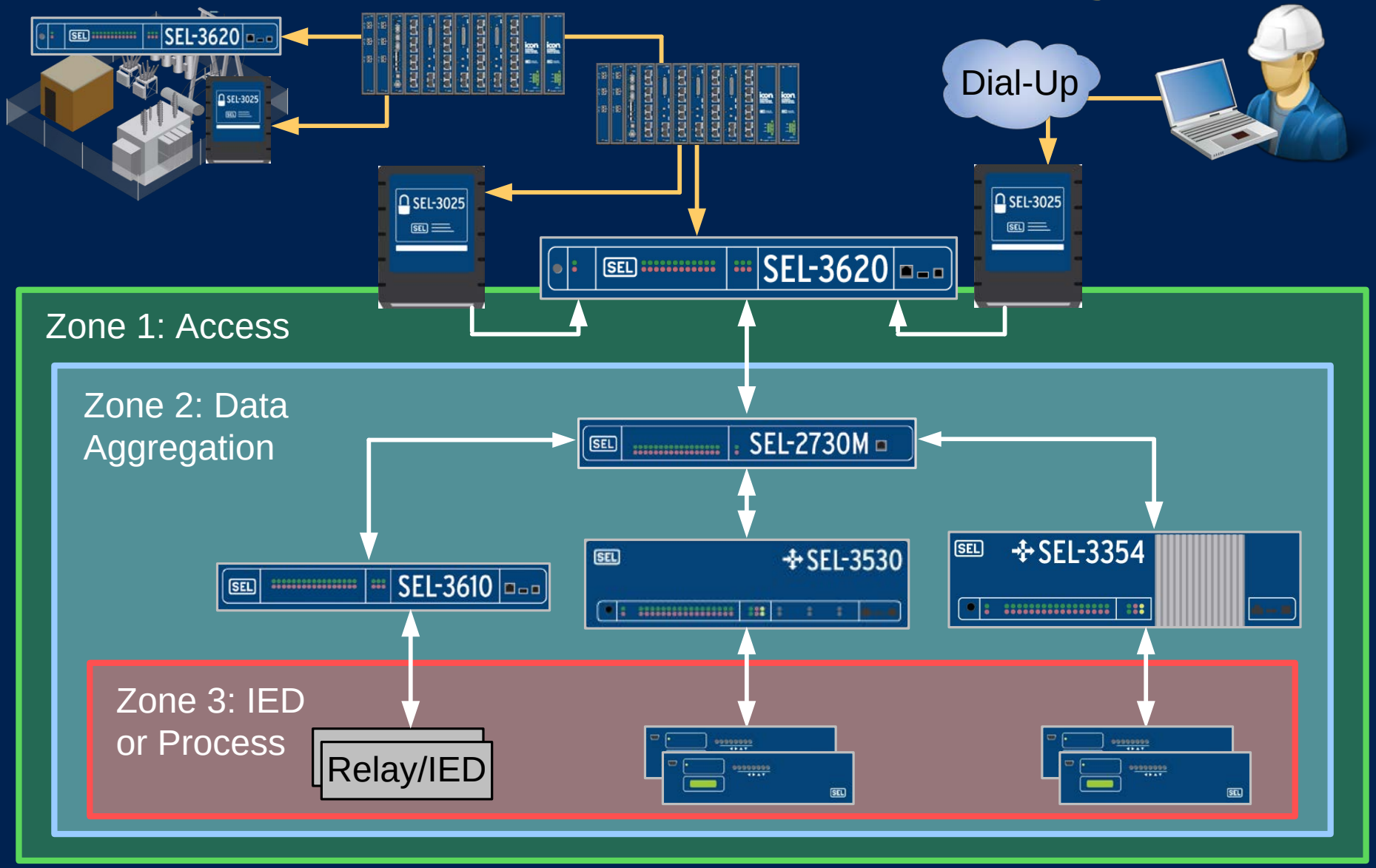
- Teach the threat, with all due respect to sources and methods.
- Advise, on best ways to secure communications and information systems.

SCADA Op Can Enable Link



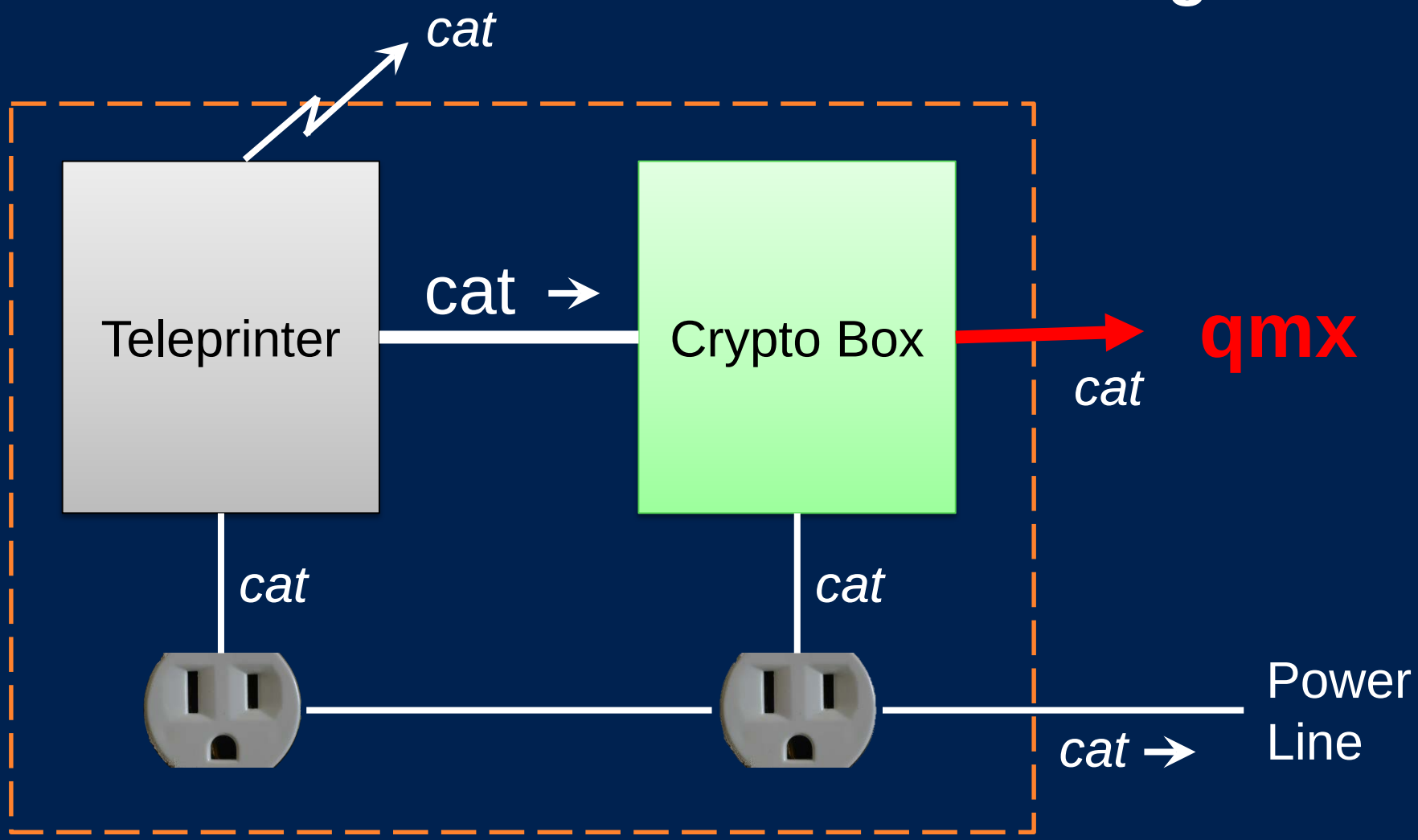
You're only exposed when remote access is required.

Defense-in-Depth for Secure Connectivity

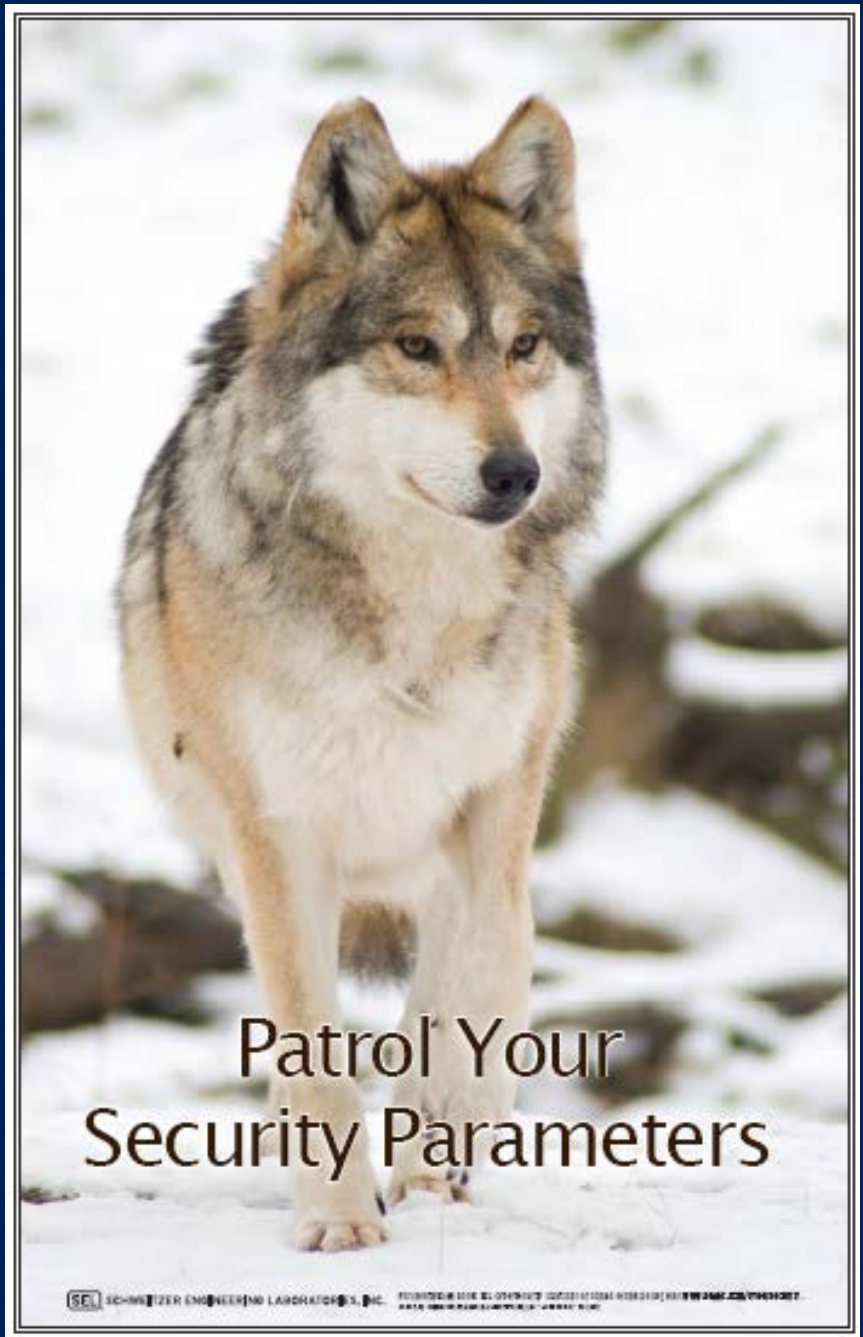


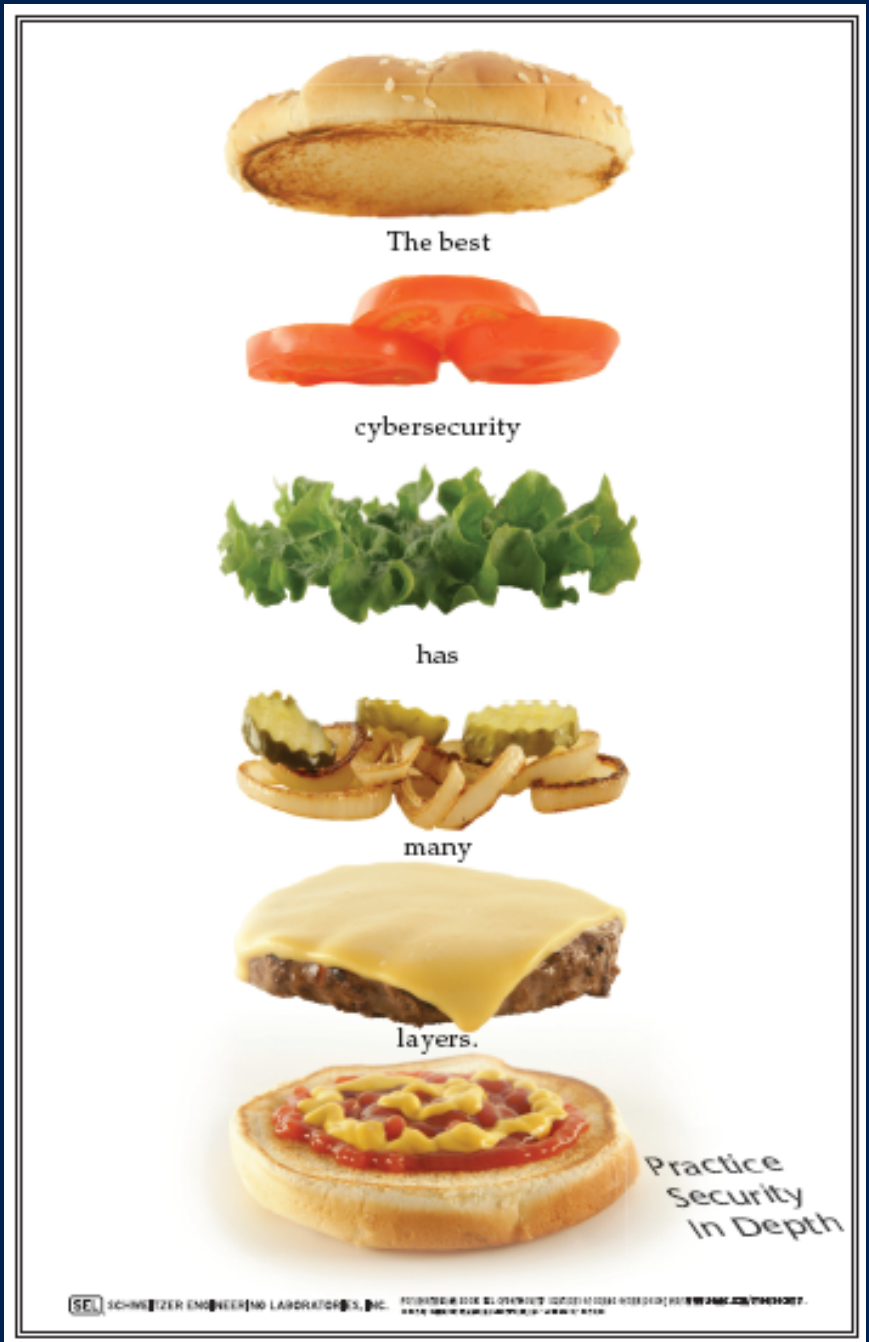
TEMPEST: Shield, Filter, Mask

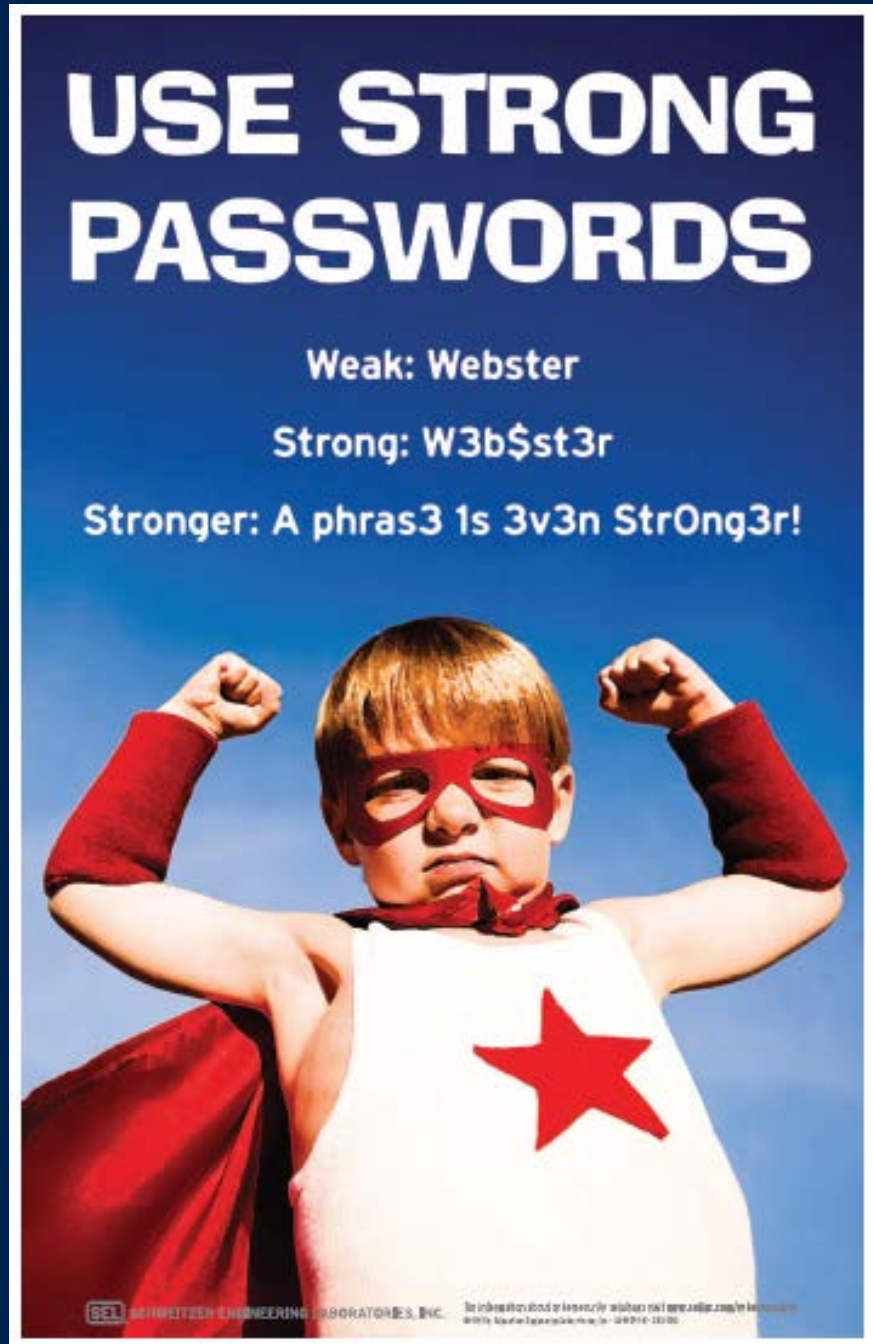
Don't let the "cat" out of the bag



Security Perimeter = "Bag"


Patrol Your
Security Parameters


The best
cybersecurity
has
many
layers.
Practice
Security
In Depth


USE STRONG PASSWORDS
Weak: Webster
Strong: W3b$st3r
Stronger: A phras3 1s 3v3n StrOng3r!
SEL SCHWEITZER ENGINEERING LABORATORIES, INC.


I DON'T SHARE MY TOOTHBRUSH OR MY PASSWORD!
SEL SCHWEITZER ENGINEERING LABORATORIES, INC.

Ships in products, get up to 90 at a time for free!

Physical *and* Cyber Protection

SEL-3622 Security Gateway

Senses *Motion and Door Opening*

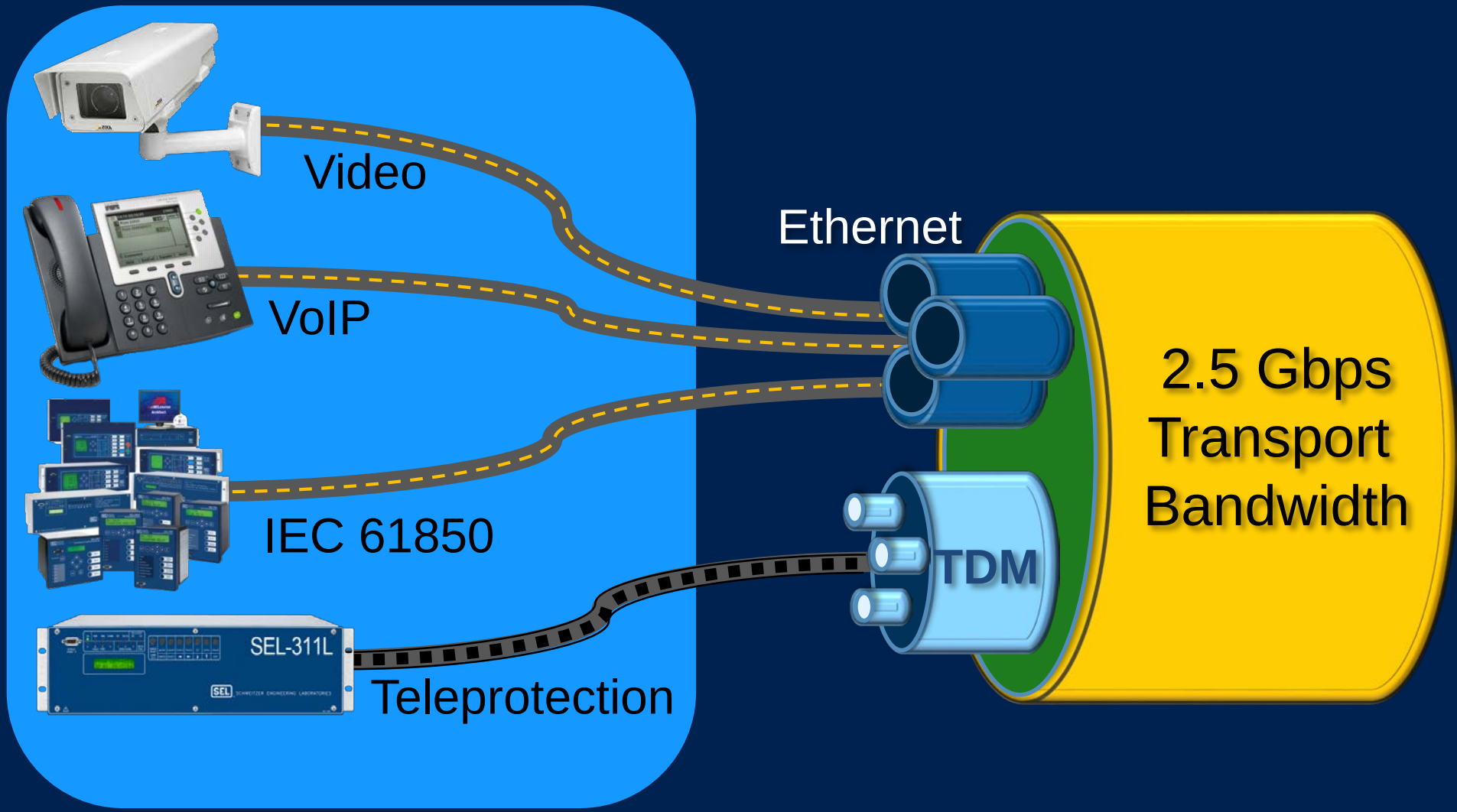
Detect *Light and Cable Disconnect*

Dependable Communications for Critical Infrastructure

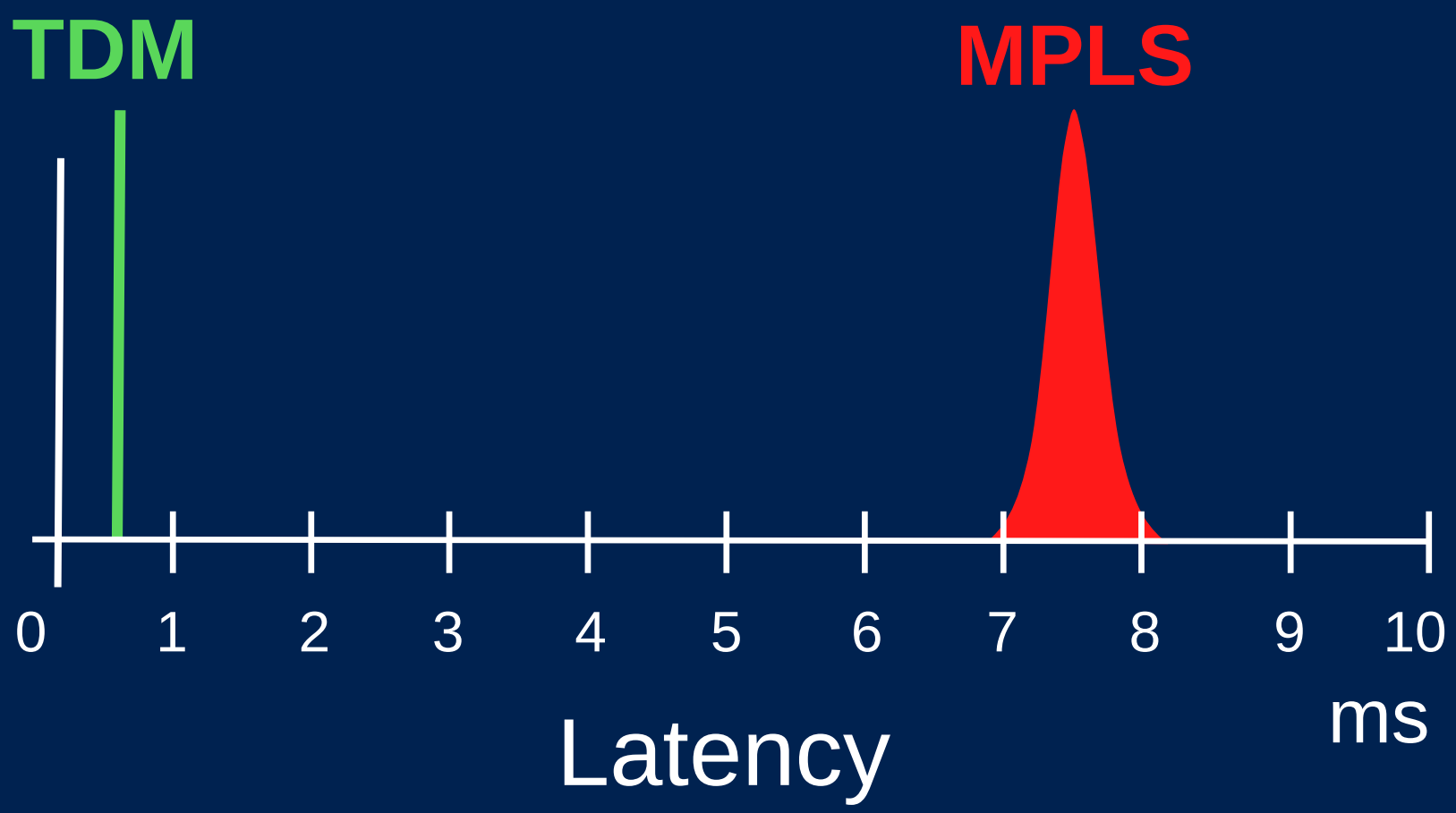
- ✓ Utility rated
- ✓ 5 ms network healing
- ✓ Deterministic communications
- ✓ Absolute microsecond network time
- ✓ Best of TDM and Ethernet features
- ✓ “Clean sheet” design: performance, security quality, manufacturability, and price

icon - The Best of TDM and IP Communication

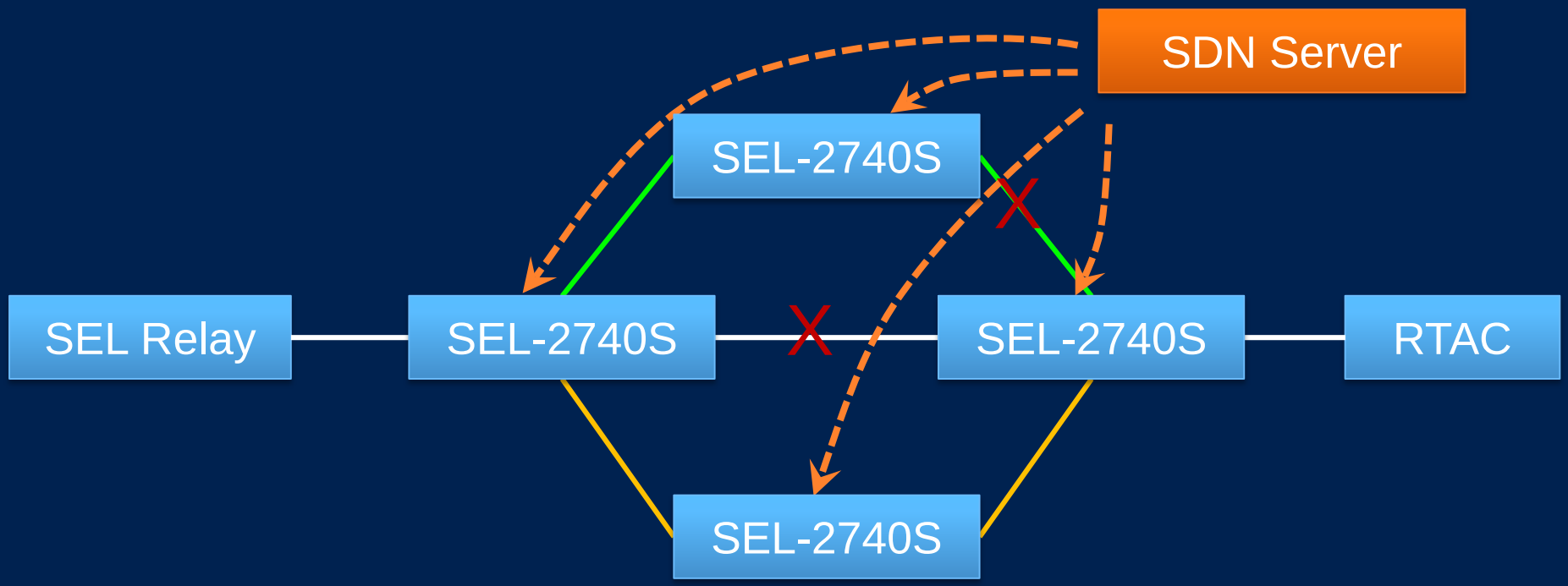
INTEGRATED COMMUNICATIONS OPTICAL NETWORK



We Chose TDM Because It's *Fast* and Doesn't Jitter



Reset Network Complexity With Software-Defined Networking



Primary Path Backup Path Secondary Path

Pilot: “Where Am I?”

- Airspeed, barometric altimeter, compass
- Celestial Navigation
- Charts (Jeppson, flying mail)
- ADF receives NDBs and radio stations
- VOR, DME, ILS; Radar Altimeter
- GPS
- Inertial Navigation Systems

GPS works great, and we have other tools

Power Engineer: “What Time is It?”

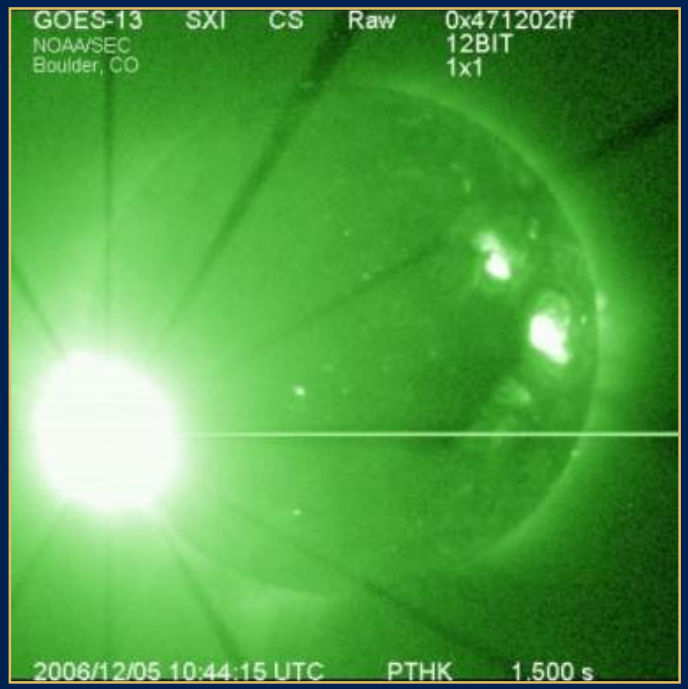
- Substations seldom move
- Satellites <<100 ns
- Terrestrial Network Time <<100 ns
- Disciplined Standards with very low drift rates for excellent holdover
- VLF Broadcasts ~ 1 ms

GPS works great, and we have other tools

GPS Time Is Not Guaranteed!

We need robust solutions.

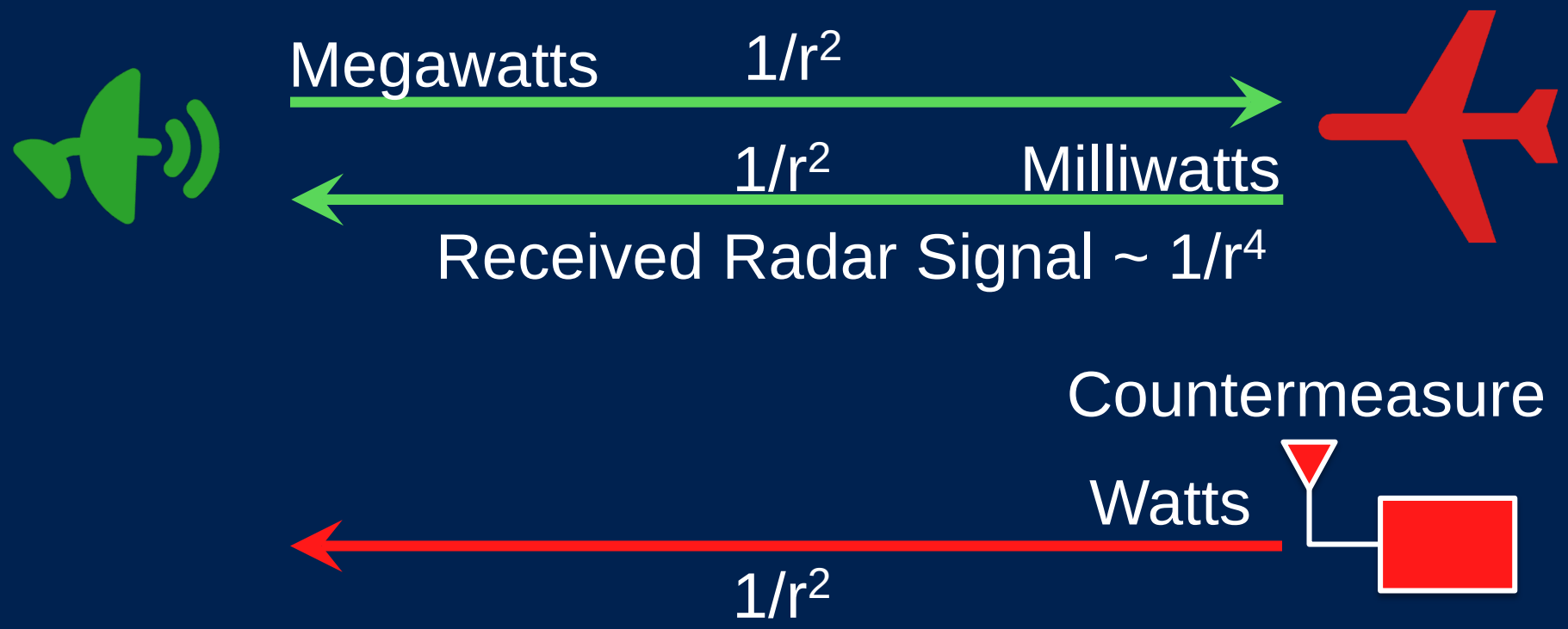
- Jam, spoof, or interfere (NAVWAR)
- Equipment failure
- DoD control
- Solar flares



"On December 6, 2006, a solar flare created an unprecedented intense solar radio burst causing large numbers of receivers to stop tracking the GPS signal."

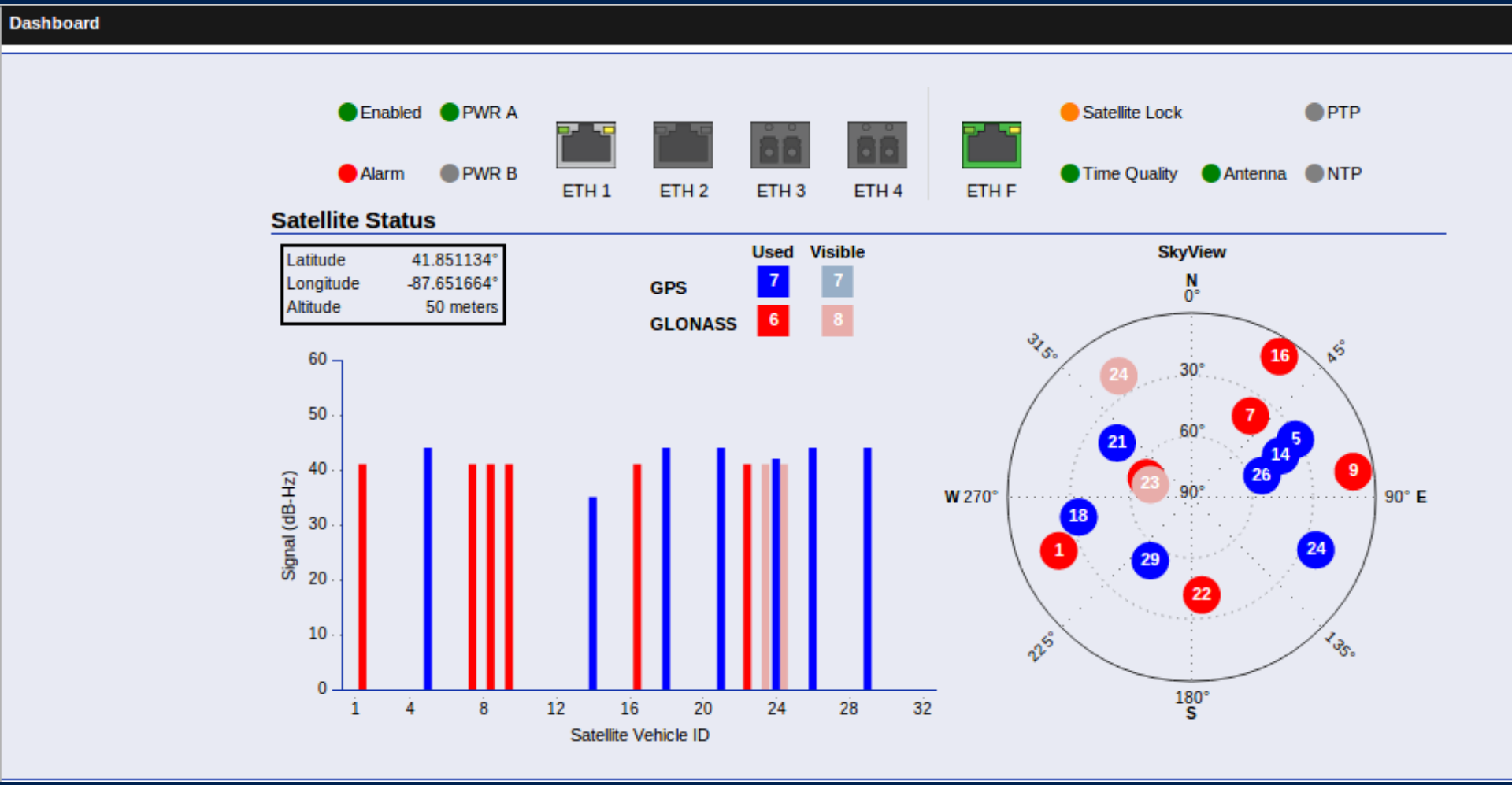
– NOAA Press Release

Detect, Jam, Spoof Radar



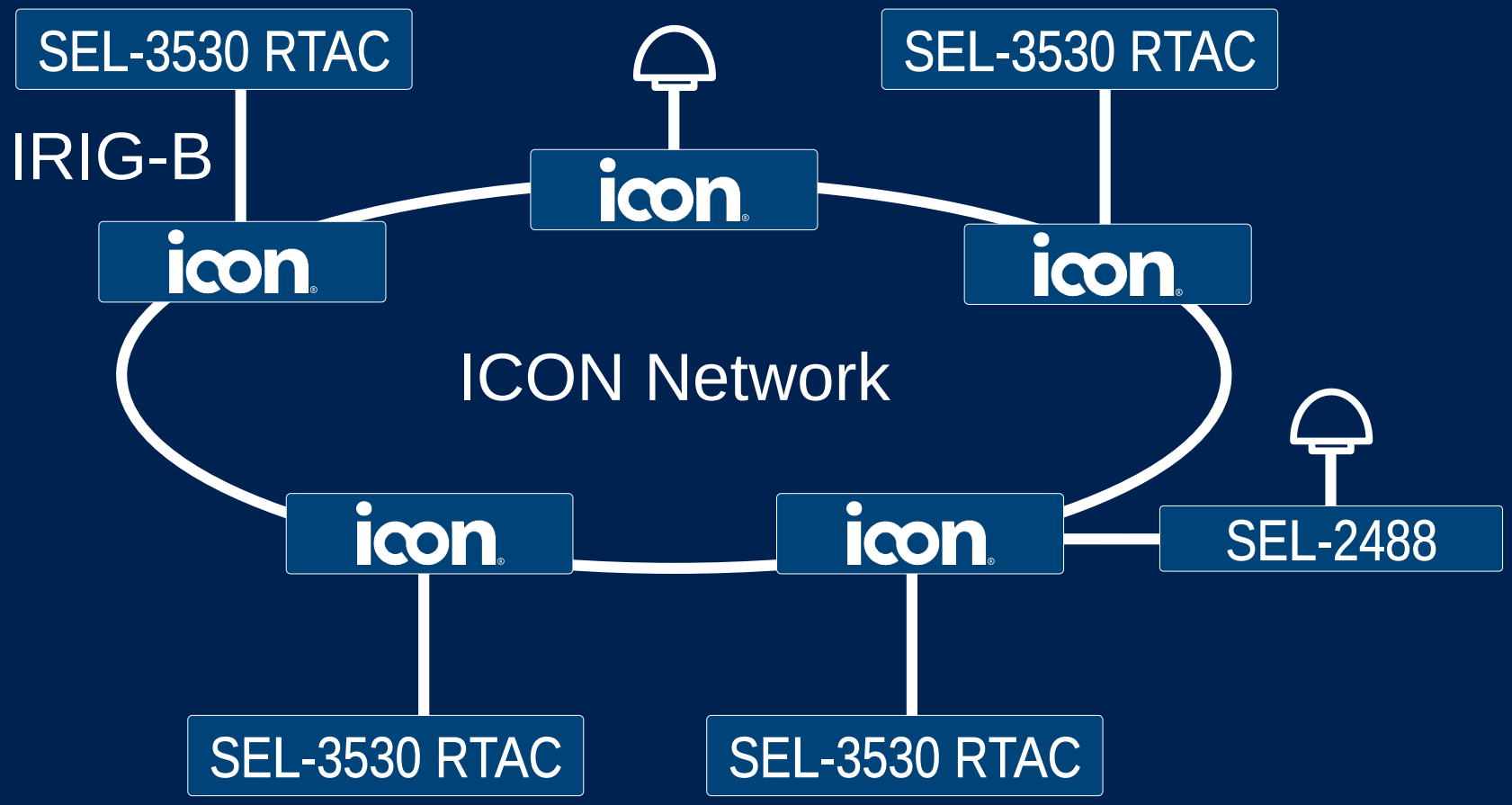
Countermeasure >> Reflection

SEL-2488 Clock Compares Time from GPS *and* GLONASS Satellites



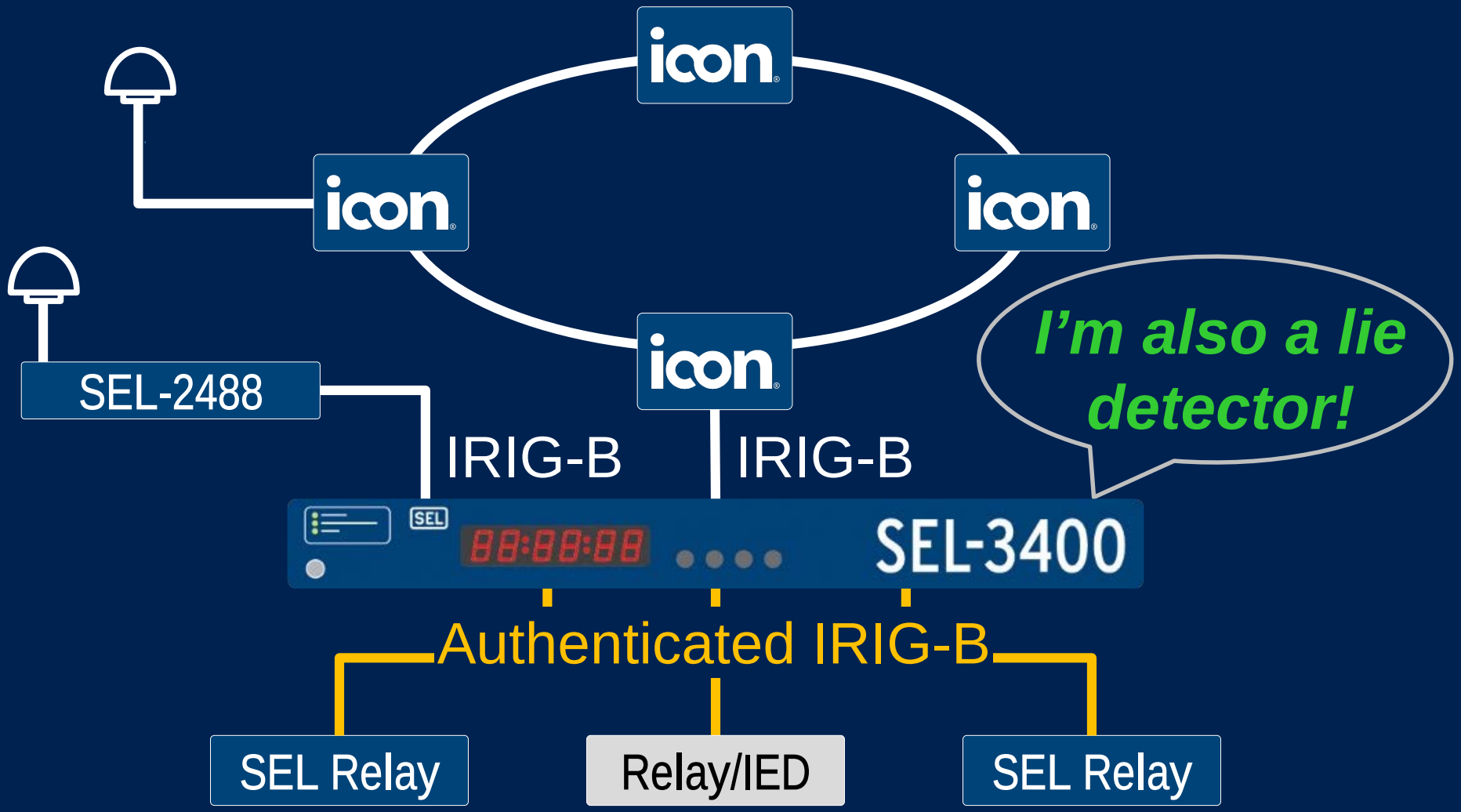
ICON Distributes Precise Time

<100 ns and NO GPS Risks

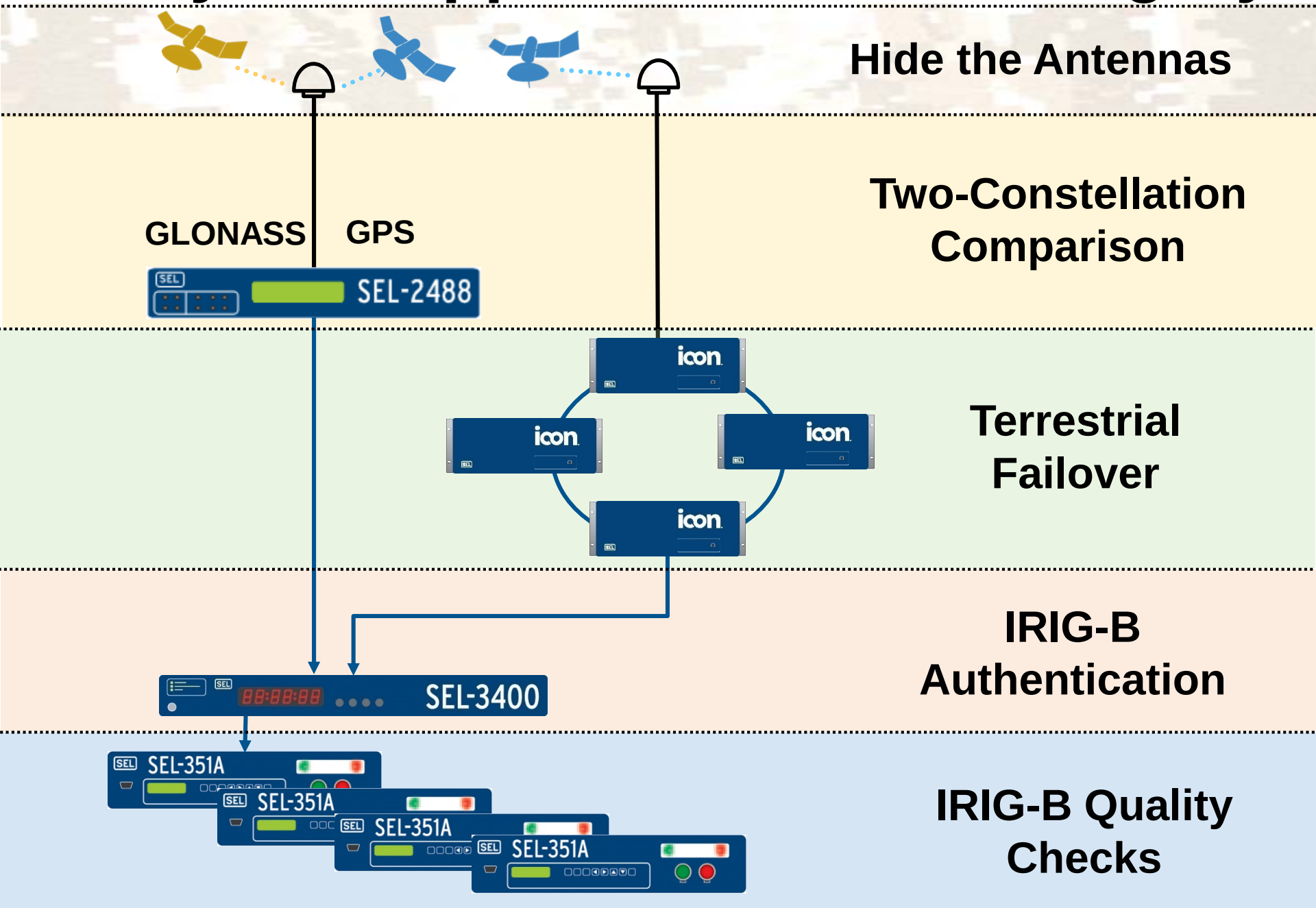


SEL-3400 Authenticates Time

Alarms if Time Differs, but Good Quality Bits



A Layered Approach to Time Integrity



Serious Suggestions

- ***Never*** connect SCADA to Internet
- Operate *private and secure* control networks
- Consider TDM, not just packet comms
- Apply defense in depth; layers of security
- Learn, innovate, educate
- Encourage our government to teach the threat
- Security Plans: *Private and Compartmented*
- Understand the “physics” of electric power

The History and The Future

- Power systems run without “cyber.”
- Computers and communications add to the safety, reliability, and economy of electric power.

We can build cyber-safe solutions!