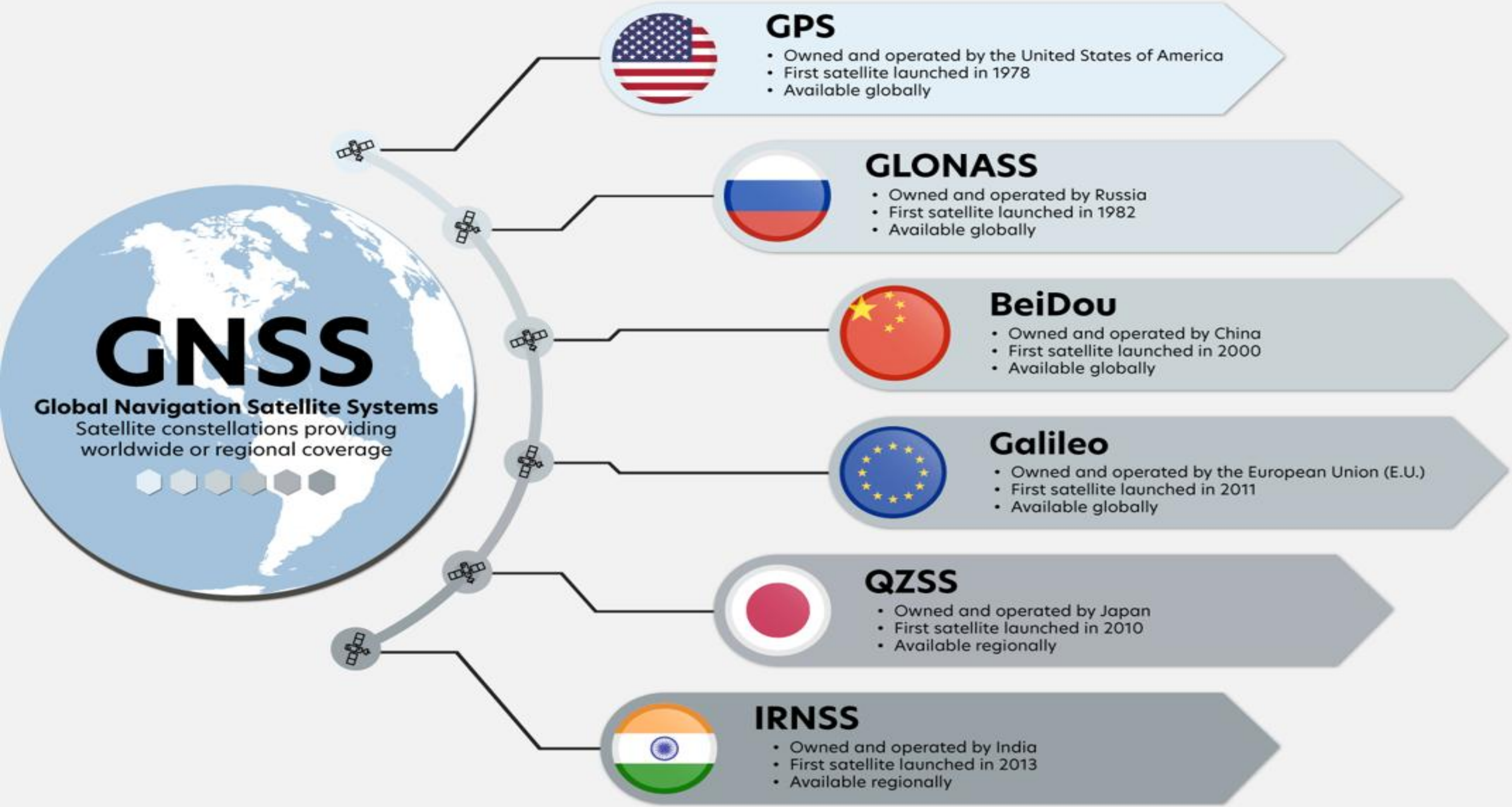
FrontLine Cyber Solutions

Messing with Time

March 2026

What is GNSS

- GNSS stands for **Global Navigation Satellite System**, a term for satellite constellations providing autonomous geospatial positioning, navigation, and timing (PNT) services with global coverage.
- These systems, including GPS (US), GLONASS (Russia), Galileo (EU), and BeiDou (China), transmit signals from space that receivers use to determine 3D locations
- Position, Navigation, Time (PNT)
  - Receivers detect and decode signals to determine position, speed, and precise time.



GNSS

Global Navigation Satellite Systems

Satellite constellations providing worldwide or regional coverage

GPS

- Owned and operated by the United States of America
- First satellite launched in 1978
- Available globally

GLONASS

- Owned and operated by Russia
- First satellite launched in 1982
- Available globally

BeiDou

- Owned and operated by China
- First satellite launched in 2000
- Available globally

Galileo

- Owned and operated by the European Union (E.U.)
- First satellite launched in 2011
- Available globally

QZSS

- Owned and operated by Japan
- First satellite launched in 2010
- Available regionally

IRNSS

- Owned and operated by India
- First satellite launched in 2013
- Available regionally

How Dependent Are We?

- An estimated 4 billion people, along with countless devices, rely on Global Positioning System (GPS) signals worldwide.
- These range from smartphones, self driving cars and personal locators to critical infrastructure like banking systems, power grids, and cell towers, all relying on at least 24 (currently 32) satellites for navigation and timing

GNSS Signal

GNSS or GPS in the US, signals are highly vulnerable to interference because they are extremely weak upon reaching Earth, having traveled over 20,000 kilometers.

Not new news but did you know that they are easily disrupted by jamming (blocking) or spoofing (faking) using inexpensive, readily available devices, posing significant threats to aviation, shipping, critical infrastructure, and navigation?

So, how easy do you think it is?

Problem…was then and is still here

“In the future, grid systems will require sub-microsecond level accuracy at power substations to implement automatic network management and protection relay functions, and to support fault detection and performance measurements.

Today grid systems rely on GNSS clocks as time reference sources and atomic clocks as a backup in case of outages.

GNSS receivers are low-cost, reliable, high-precision timing sources that can be implemented in a large number of intelligent grid sensors (i.e. Phasor Measurement Units), to enable real-time automatic control of the grid.”

Experiment

Power grid relies on GPS time for synchronized accuracy…. Timing is everything,

Access to more generators and transmission paths between grids means less chance of an outage. Thus, synchronization among the nine major power generating and transmission grids in the United States is vital to make power sharing work.

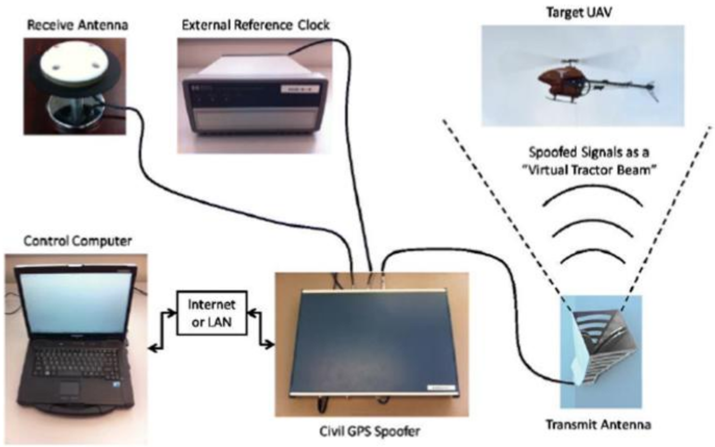
So, our question was “could we cause a power grid to shut down by simply manipulating the GPS signal? Not jam it

- jamming is easy
- devices are designed to continue working.

Our Focus

A civil GPS spoofer produces counterfeit versions of the authentic GPS signals and tricks a target receiver into tracking these counterfeit signals.

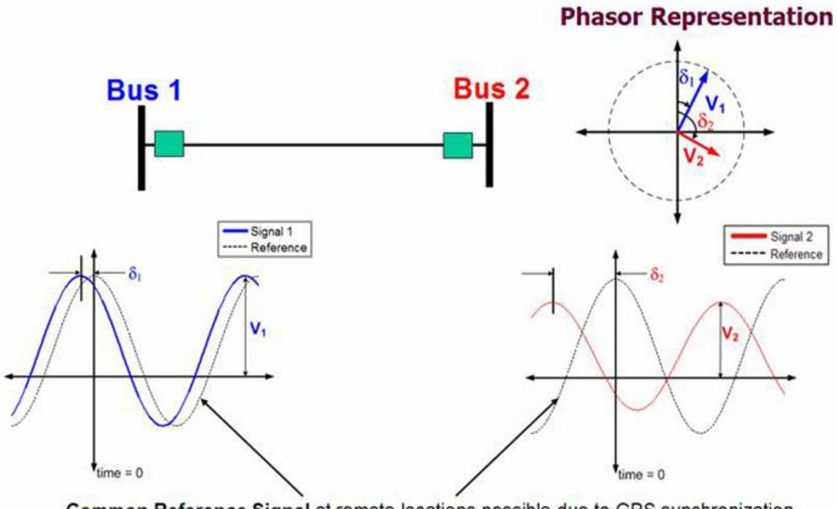
The typical goal of a spoofer is to influence the position-velocity-time (PVT) solution output by the target receiver to cause some ill-effect in downstream equipment which depends on the PVT solution



Target

Partnering with the the University of Texas, we set out to conducted a functional test and evaluation of the effects that spoofed GPS timing signals can have on synchrophasor measurements produced by phasor measurement units (PMUs)

Why PMU? PMUs are part of protective relays.



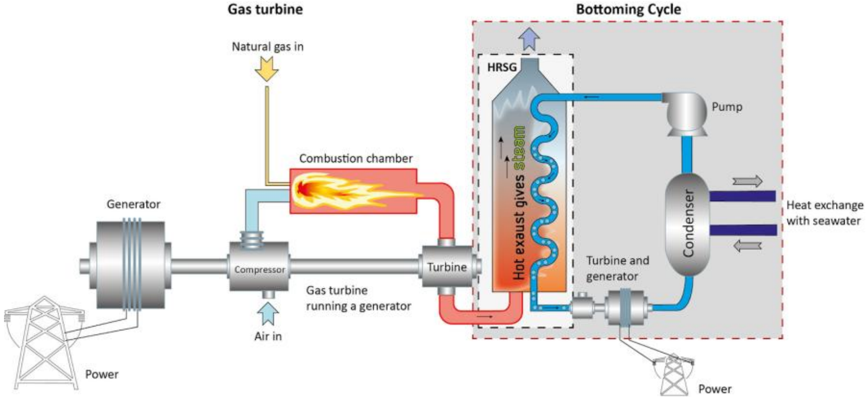
Common Reference Signal at remote locations possible due to GPS synchronization

Why PMUs / Protective Relays

Protective relays act as the "brains" of electrical power systems by continuously monitoring parameters like current, voltage, and frequency to detect abnormal conditions or faults.

When a fault is detected, they instantly send a signal to trip circuit breakers, isolating faulty equipment to prevent damage, improve safety, and maintain system stability

Going to use the system against itself



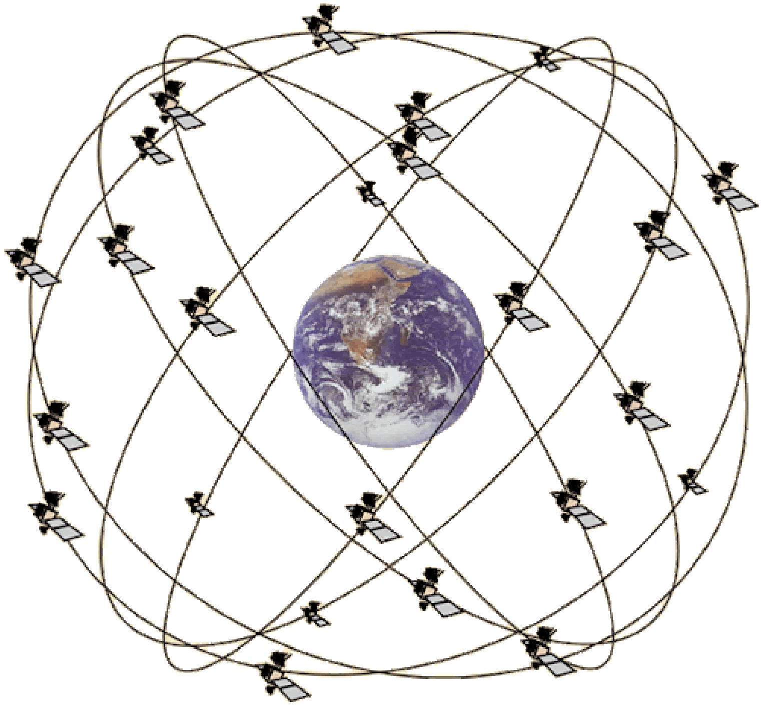
Explained the Why, Now the How

Snapshot at current space picture

- Orbital dynamics

Software aligns perfectly to create our "virtual world"

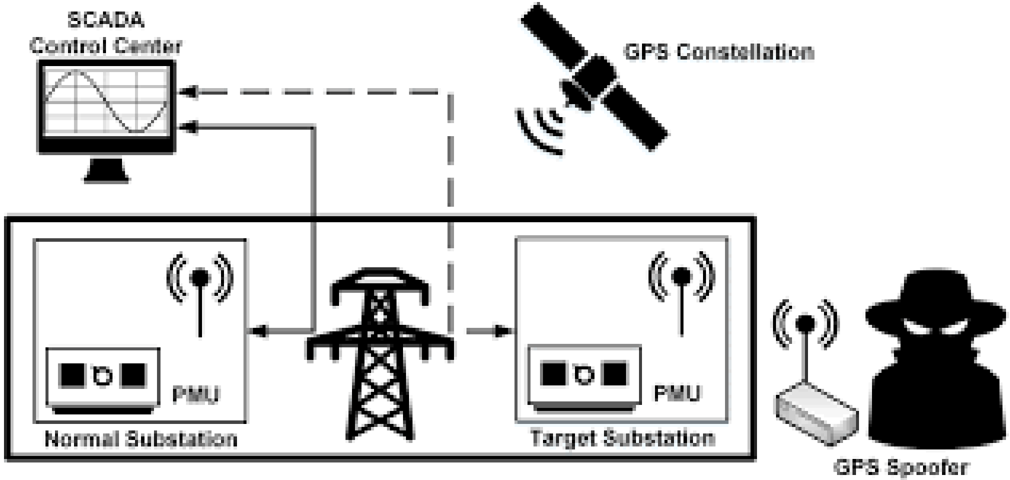
The spoofer produced signals that are initially nearly perfectly aligned with the authentic signals at the target receiver but with low enough power that they remained far below the target receiver's noise floor



The How

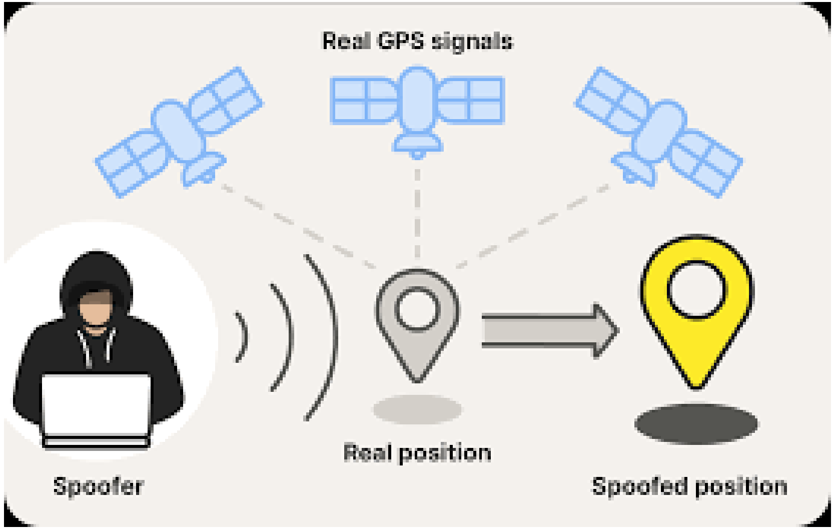
The spoofer then raised the power of the spoofed signals slightly above that of the authentic signals

At this point, the spoofer had taken control of the target receiver’s tracking loops and slowly led the spoofed signals away from the authentic signals, carrying the receiver’s tracking loops with it



The How

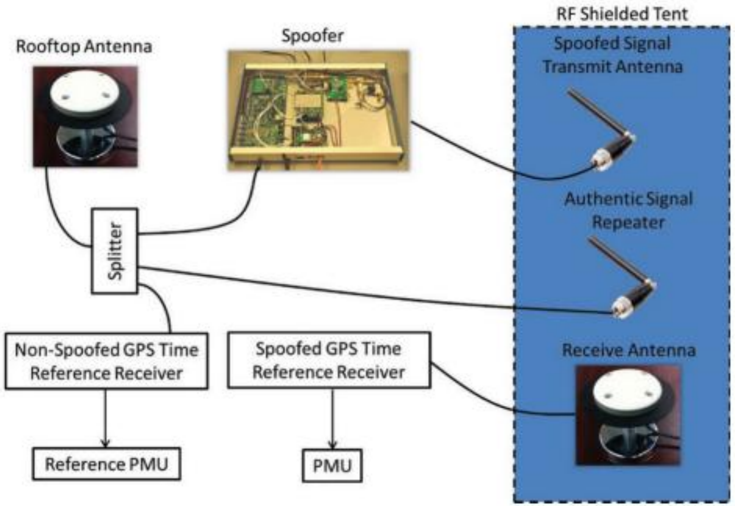
Once the spoofed signals had moved more than 600m in position or 2 µs in time away from the authentic signals, the target receiver was considered completely captured and at the mercy of the spoofer



The How

The spoofer was then able to manipulate the timing of the receiver, and thus the synchrophasor measurements produced by the PMU, more aggressive, provided it stayed within the dynamic range of the target receiver’s tracking loops.

This enabled the spoofer to introduce arbitrarily large errors, given enough time, in the phase angle measurements produced by the PMU

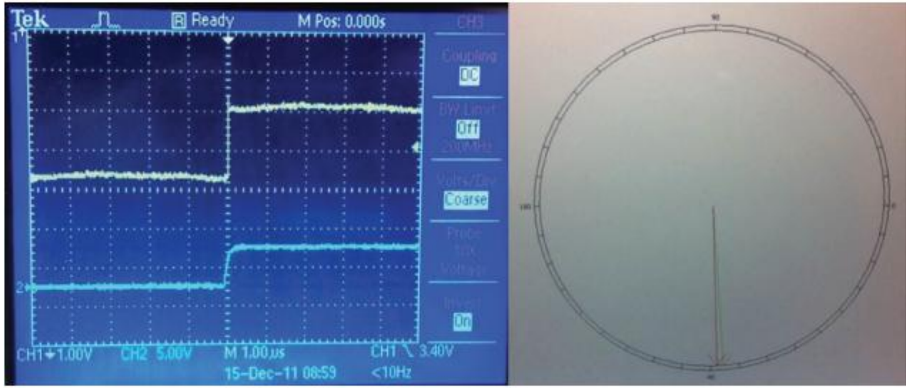

RF Shielded Tent
Rooftop Antenna
Spoofer
Spoofed Signal Transmit Antenna
Authentic Signal Repeater
Splitter
Non-Spoofed GPS Time Reference Receiver
Spoofed GPS Time Reference Receiver
Receive Antenna
Reference PMU
PMU

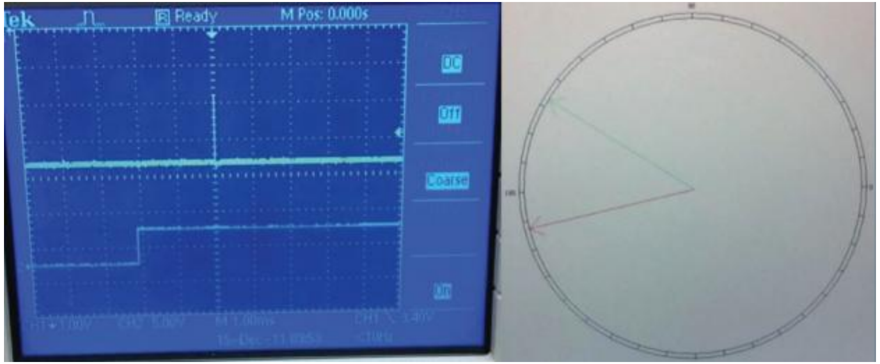
How Long Did it Take Us?

We demonstrated that a timing error of a few tens of microseconds can easily be induced by a spoofer in about **11 minutes** from the start of the attack for a typical PMU without giving any indication of foul-play

This spoofer-induced timing error causes a PMU to violate the maximum phase error allowed by the applicable standard for PMUs

IEEE Standard is <u>**.573**</u> degrees…..we took it out **10 degrees**



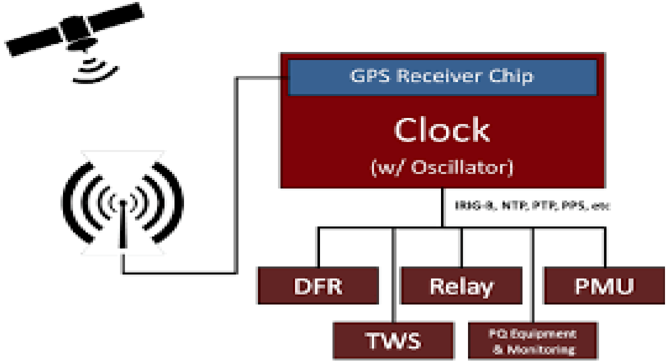


Blackout

When protective relays trip, they immediately detect electrical faults (like short circuits or overloads) and signal a circuit breaker to open, isolating the faulty equipment within milliseconds to prevent damage and ensure safety

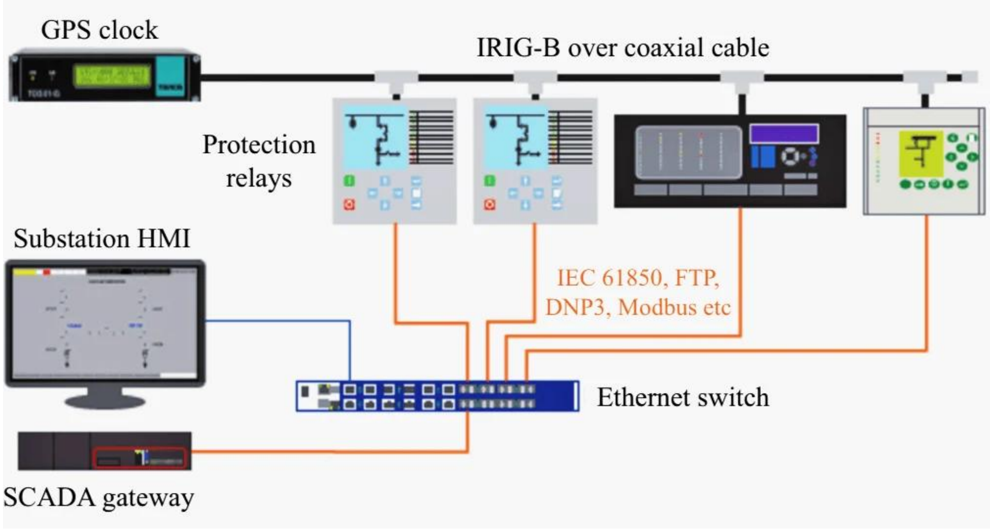
The specific part of the power system, such as a generator or a substation bus, is immediately shut down and the line de-energized

Better or worse? AI?



What’s next?

- There is NASPI
- People are hardening the network but at the wrong place
- Us….we improving and expanding on this technology
- We don’t believe in “impossible”, we’re doing what they said can’t be done with GPS…..until the next briefing



Questions?