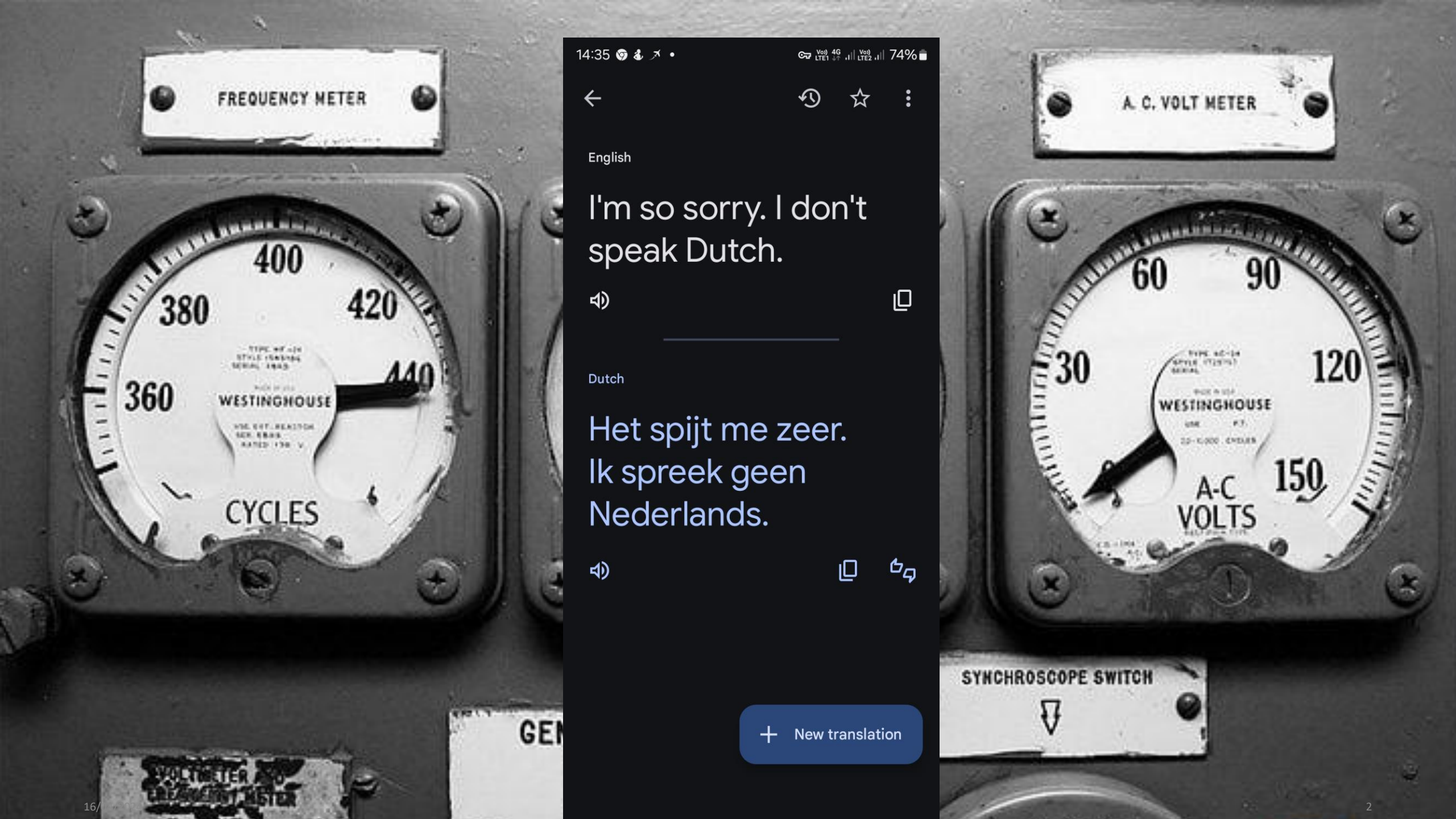
Zero by Design - secure, resilient & traceable time

Christian Farrow B.Sc.(Hons) MIET MInstP

11/04/2024

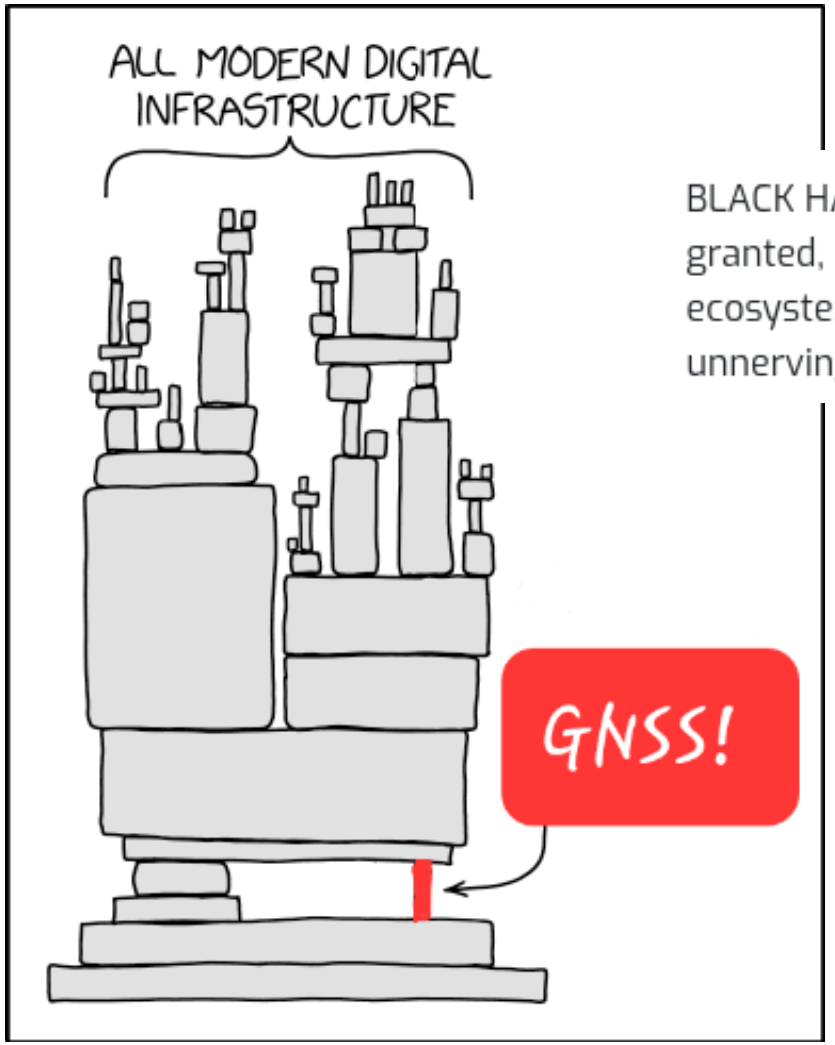
chronos TECHNOLOGY


FREQUENCY METER
400
380
420
360
440
WESTINGHOUSE
CYCLES
A. C. VOLT METER
60
90
30
120
150
WESTINGHOUSE
A-C
VOLTS
SYNCHROSCOPE SWITCH
14:35
74%
English
I'm so sorry. I don't speak Dutch.
Dutch
Het spijt me zeer. Ik spreek geen Nederlands.
New translation

Time underpins everything...

- Distributed Sensor Networks
  - Voltage, Current
    (and derivatives - Power etc.)
    Phase Angle, Temp, Battery SoC
- IT/OT Networks
  - NTP/PTP reference clocks
    Time-stamping of events
- GNSS clocks everywhere
  - "*Its biggest strength is its biggest weakness*"
    Phenomenal uptime, global availability

Dependency



- With apologies to Randall Munroe https://imgs.xkcd.com/comics/dependency.png

DARKREADING The Edge DR Tech Sections Events

Vulnerabilities/Threats | 3 MIN READ NEWS

What Happens If Time Gets Hacked

Renowned hardware security expert raises alarm on the risk and dangers of cyberattackers targeting the current time-synchronization infrastructure.

Kelly Jackson Higgins
Editor-in-Chief, Dark Reading

November 11, 2021

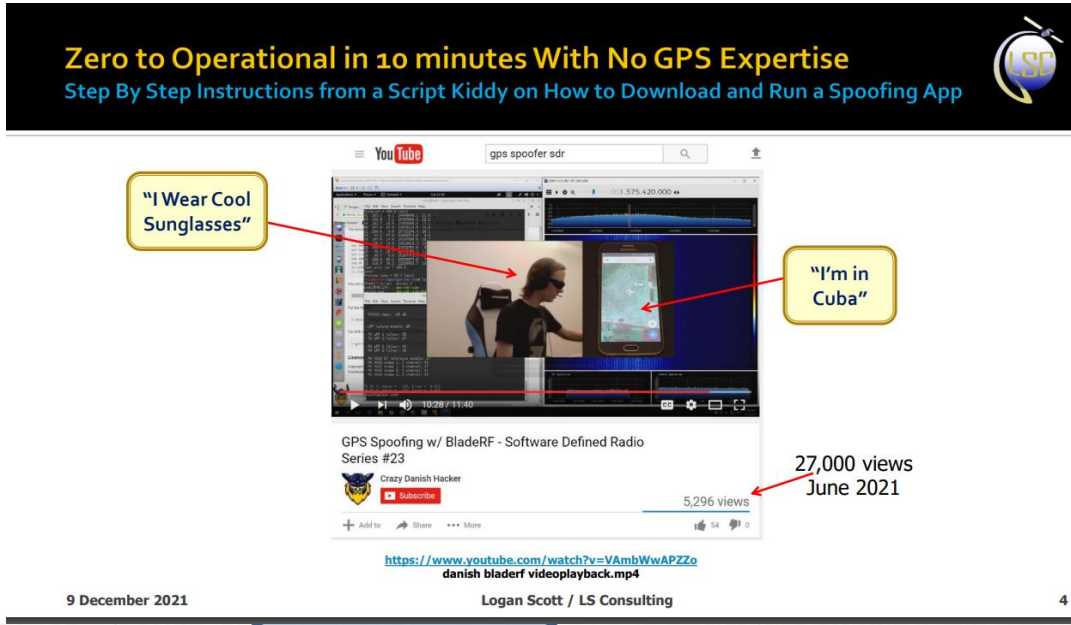
BLACK HAT EUROPE 2021 - London - Most people take time synchronization for granted, but it operates on what hardware security expert Adam Laurie calls a "fragile ecosystem." Laurie, a renowned hardware hacker, here today demonstrated an unnervingly simple way to alter time on a clock.

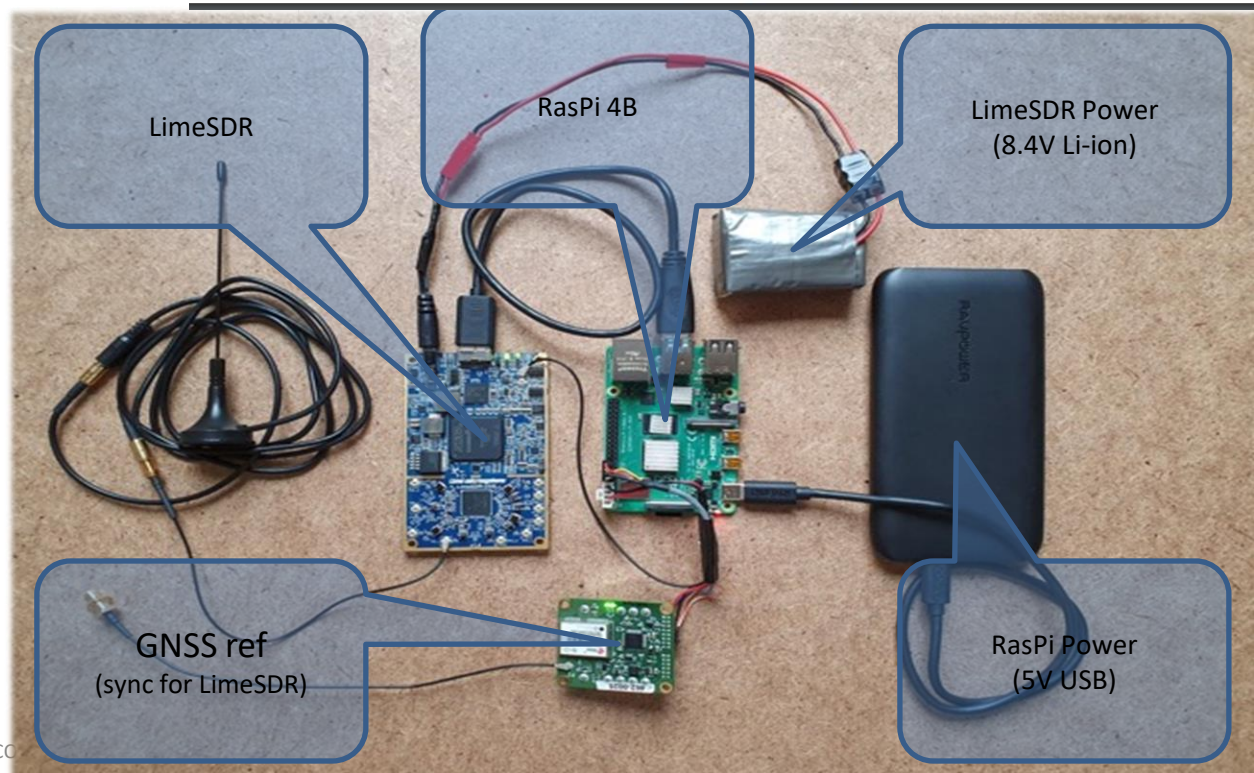
Adam Laurie's time-hacking demo at Black Hat Europe.

BLACK HAT EUROPE 2021 - London - Most people take time synchronization for granted, but it operates on what hardware security expert Adam Laurie calls a "fragile ecosystem." Laurie, a renowned hardware hacker, here today demonstrated an unnervingly simple way to alter time on a clock.

Cyber Security for Time

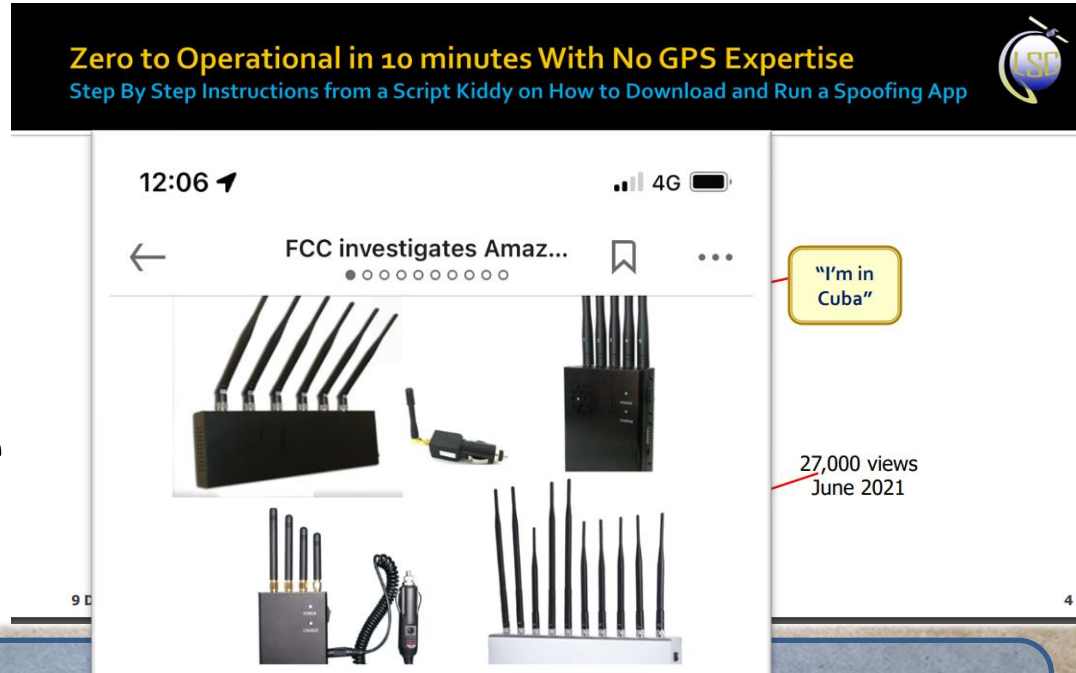
- Not just threats from the network... GNSS RF signal inherently vulnerable
- Jamming (DoS) - Spoofing (MITM)
- Space-based attacks, Space Weather

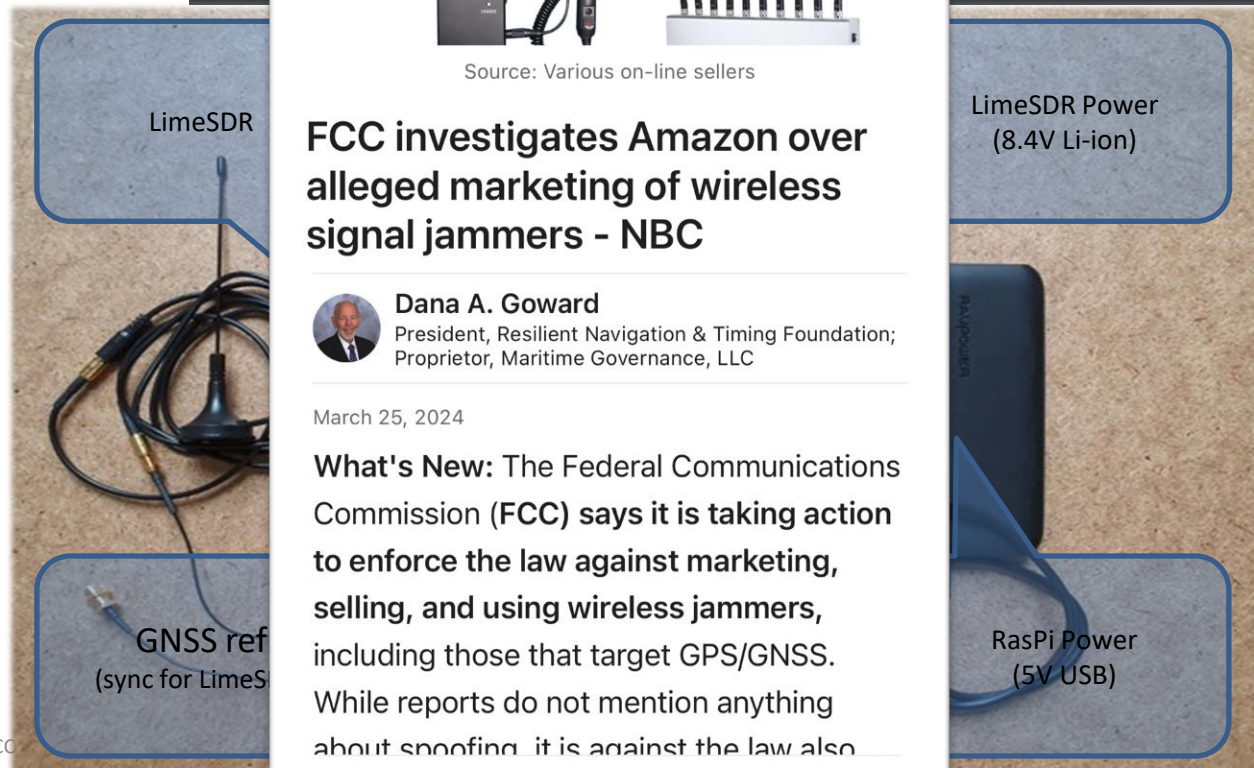




Cyber Security for Time

- Not just threats from the network... GNSS RF signal inherently vulnerable
- Jamming (DoS) - Spoofing (MITM)
- Space-based attacks, Space Weather

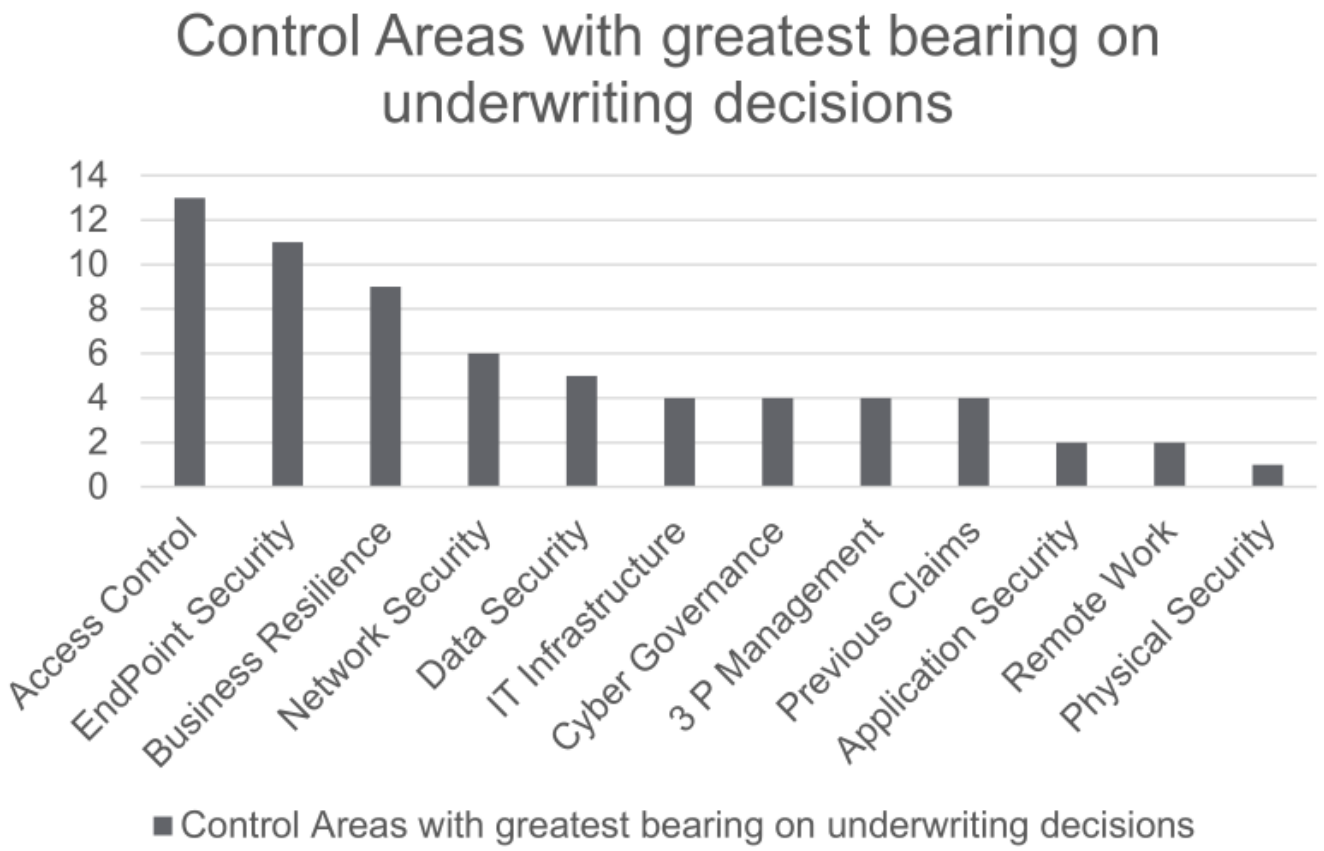




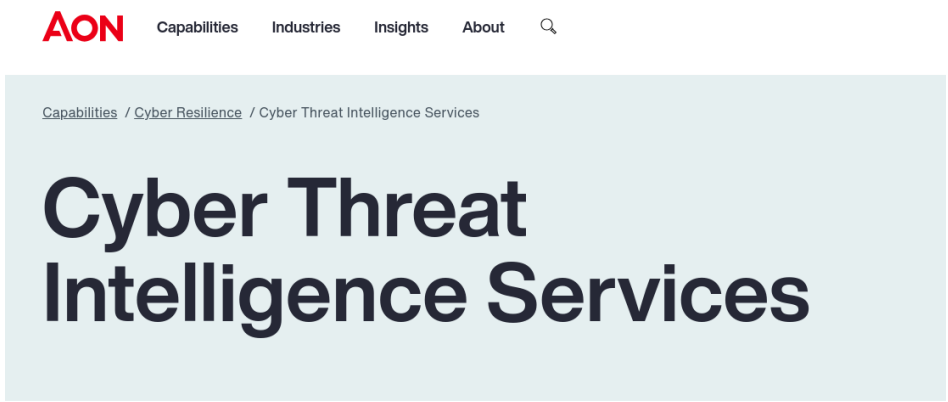
AON 2023 report

- "Access Control"

Insurers closing their books for cyber-insurance!



2021-22 was the worst year ever for Losses, with the books virtually closing to new policies towards the end of 2022..Source AON 2023



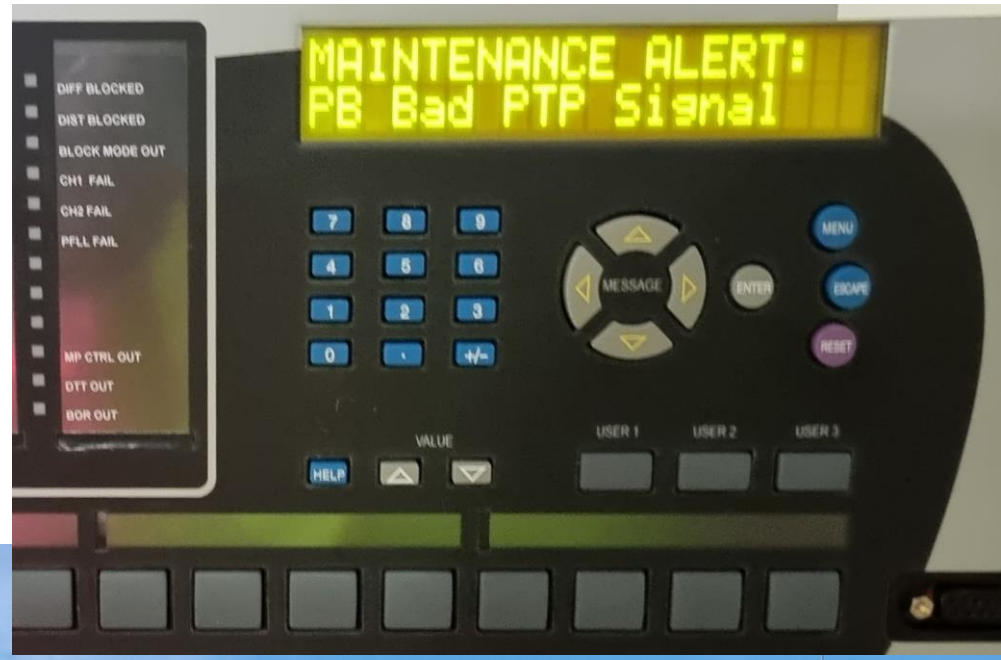
What is Cyber Threat Intelligence?

Cyber Threat Intelligence helps identify online threats and business risks to individuals and organizations. We tailor our Cyber Threat Intelligence engagement to your organization's needs, leveraging tactical and strategic intelligence and turning

Credit: AON 2023 report:
https://www.aon.com/2023-cyber-resilience-report/

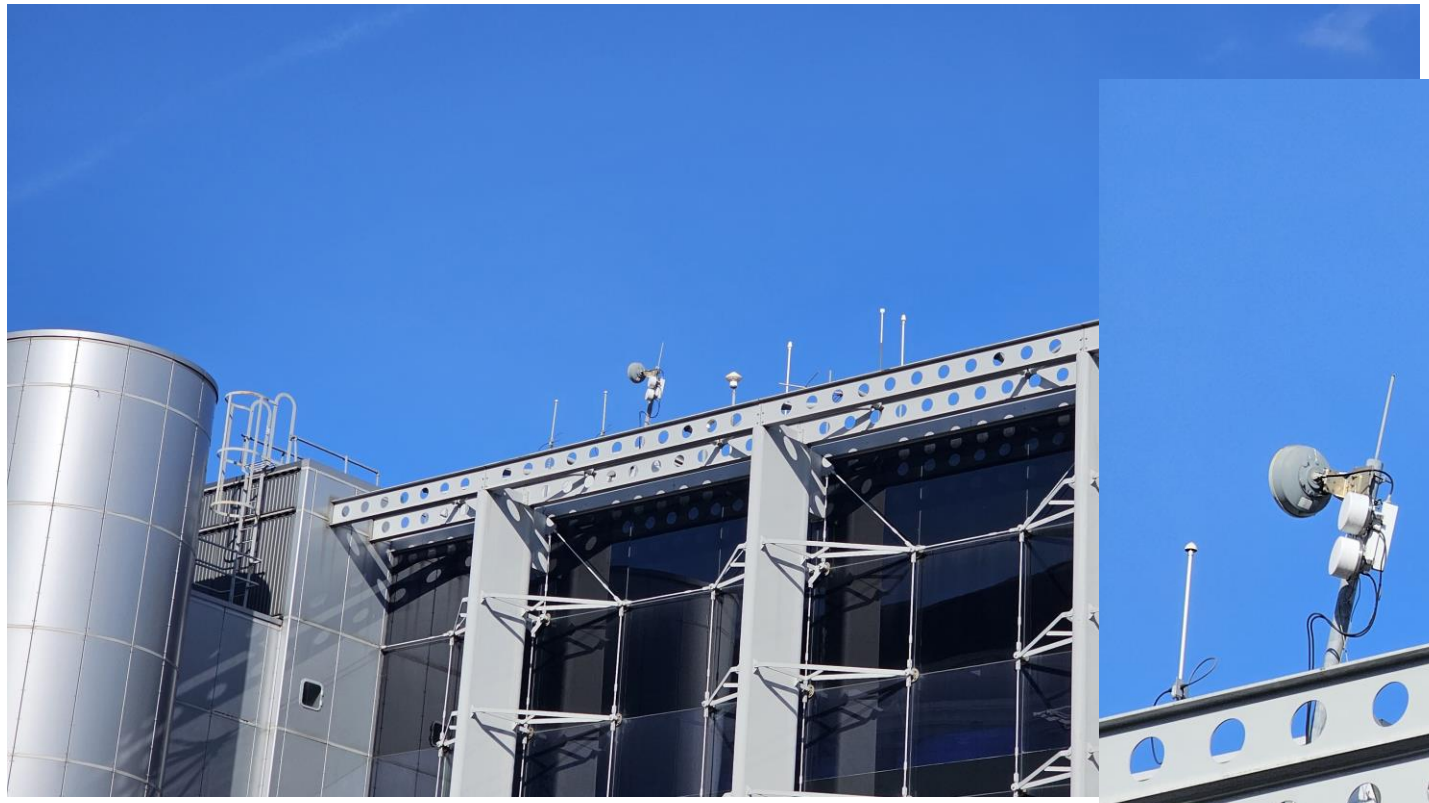
Case Study: GNSS Antenna Proliferation

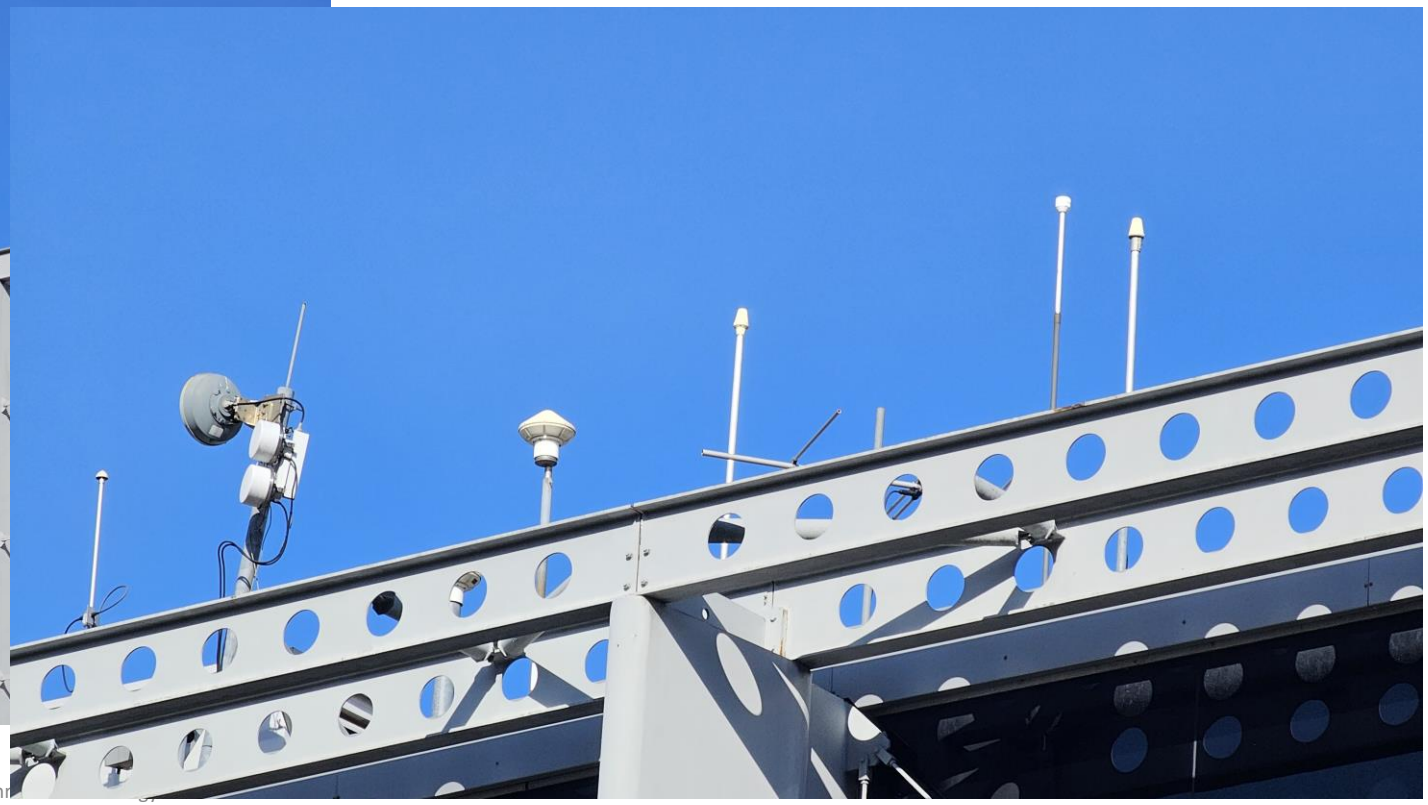
- "Digital Substation"
  - GNSS proliferation driven by
    - Redundancy, "rack-based" functionality
    - Incompatible PTP profile or lack of support - *C37-238-2011 or -2017 or 61850-9-3 or (S)NTP*



Data-centre antennas (proliferation?)

- Cloud compute (+ some flavours of edge compute also?)
  "*It's secure, it's in the cloud*" - *there's no such thing!*





Resilient Timing: Best Practices

- Own your own timescale
- Trust no one
- Test Everything

Resilient Timing: Best Practices

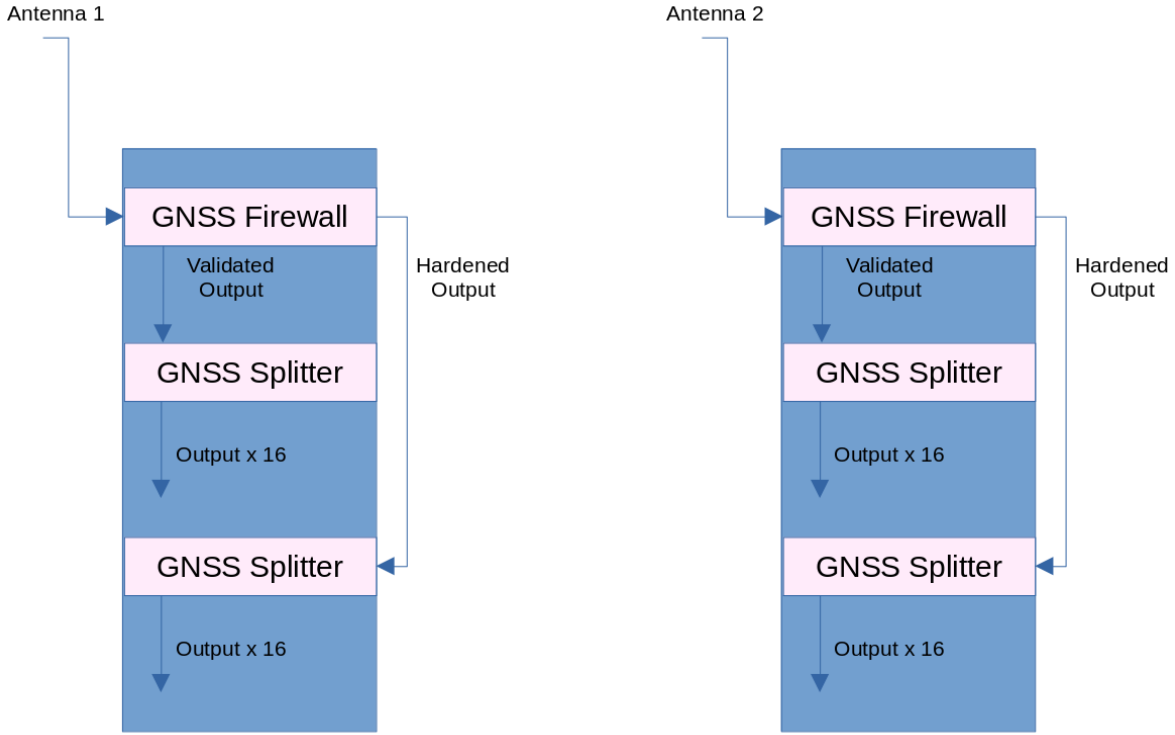
"Zero Trust"
&
"Secure by Design"

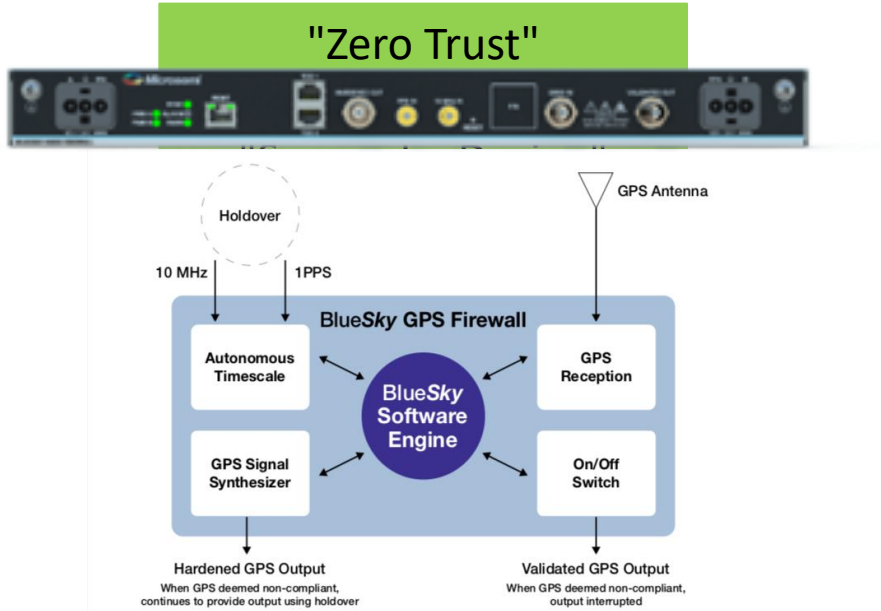
- Own your own timescale
  - Bring some trusted sources/autonomy in-house
- Trust no one
  - Be careful accepting timing from outside sources
- Test Everything
  - Test & Monitor permanently

ISO/IEC 27001 and 27002
ISO/IEC 15408
IEC 62443
ISO/SAE 21434
ETSI EN 303 645
NERC/NIST CSF/Cyber Essentials

Case Study: GNSS antenna nonproliferation (!)

- Single antenna (x 2) *(GNSS over fibre?)*
  GNSS Firewall + GNSS signal distribution inside building – splitter output drives existing system(s) directly





Evolution of ITU reference clocks

- Initially Frequency only (Plesiochronous International Digitial Links!) - 1 x 10^{-11}
- Later Frequency + (Traceable) Time/Phase - 100ns or 30ns error to UTC
- Better (x10) frequency - 1 x 10^{-12}
- Frequency + Time/Phase + "**tuned holdover**" - <100ns error to UTC for 14 days (>40 days under study)
- GNSS independence "Coherent Network" - (inter)national lab style, geographically distributed architecture

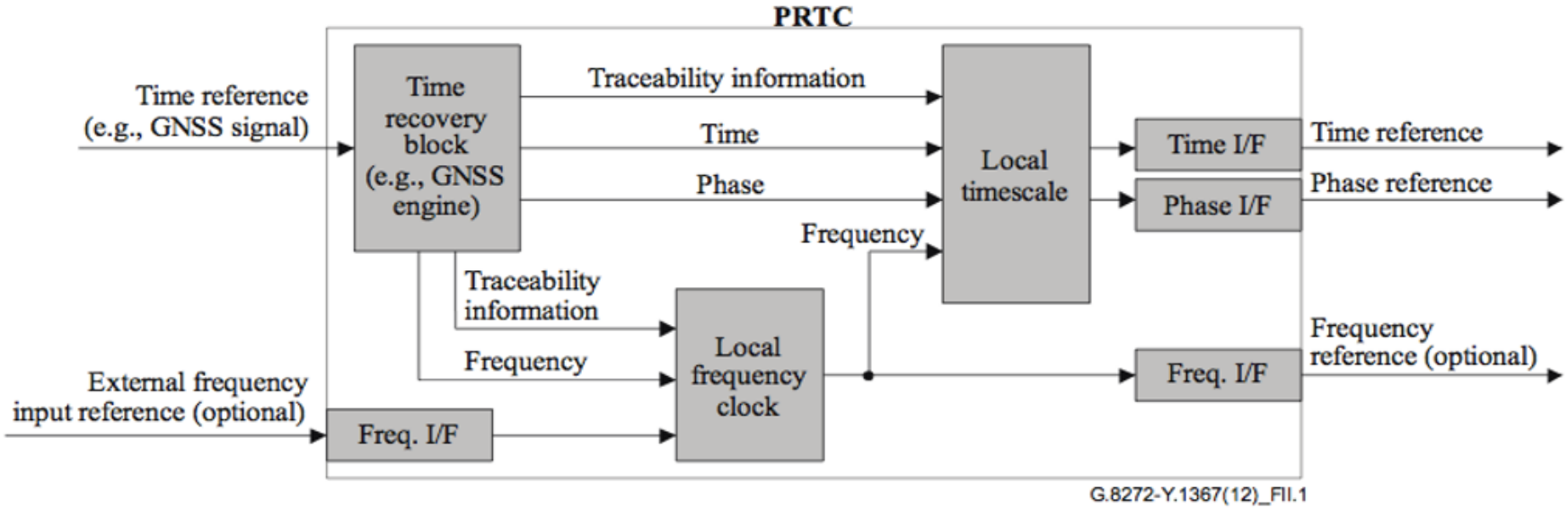
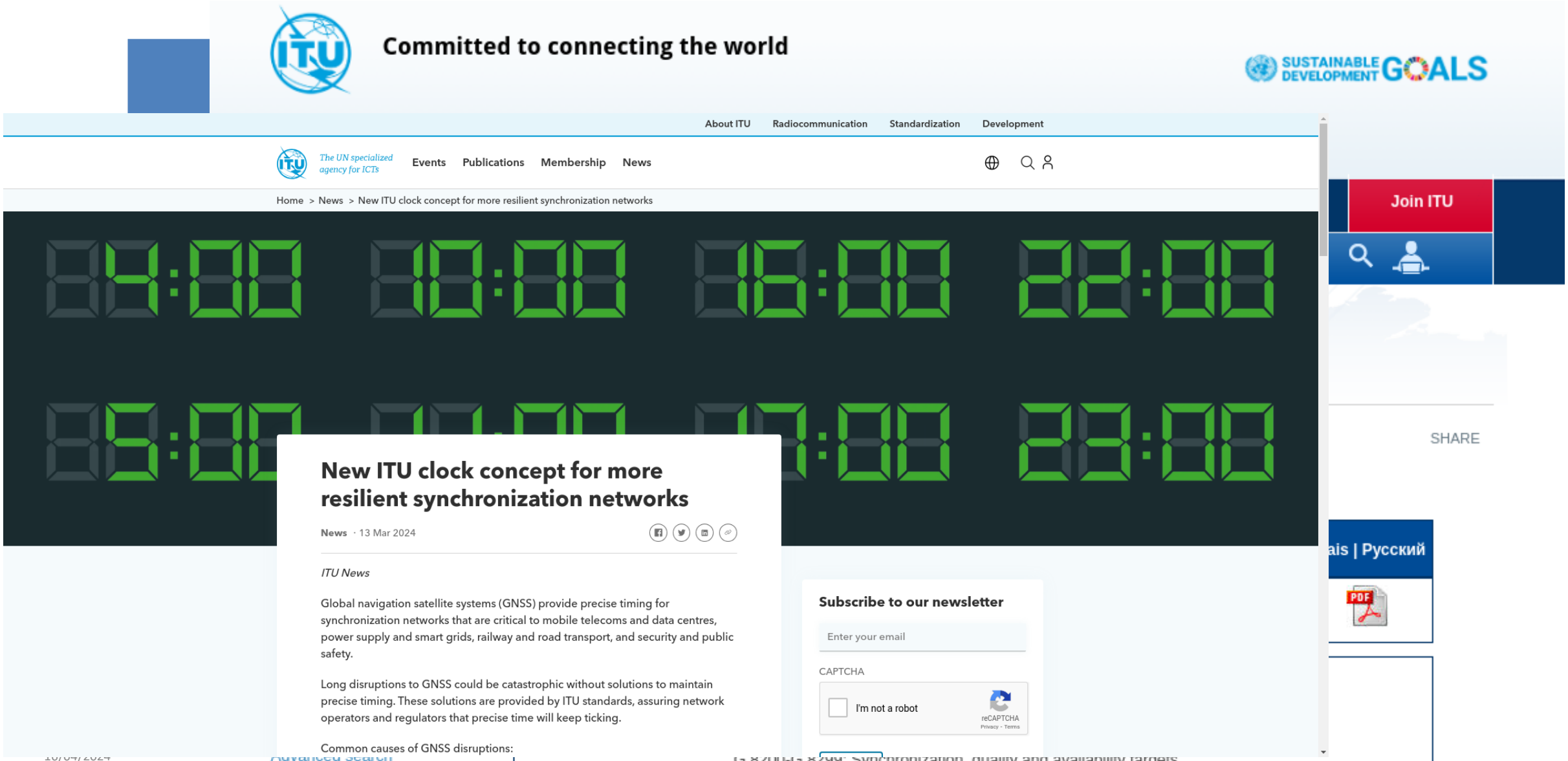


Figure II.1 – PRTC functional model

Evolution of ITU reference clocks



Evolution of ITU reference clocks

Clock Type	ITU-T Recommendation	Date
PRC – Primary Reference Clock	G.811	1976 – CCITT Orange Book
PRTC - Primary Reference Time Clock	G.8272	2012
ePRTC – Enhanced Primary Reference Time Clock	G.8272.1	2016
ePRC – Enhanced Primary Reference Clock	G.811.1	2017
cnPRTC – Coherent Network Primary Reference Time Clock	G.8272.2	2024

PRC/ePRC - Frequency only, Caesium clock
PRTC-A – single band GNSS
PRTC-B – multi-band GNSS (ionospheric delay compensation)
ePRTC – clock combiner GNSS + Caesium
cnPRTC – ePRTC with PRTC-B meshed at the network layer

cnPRTC

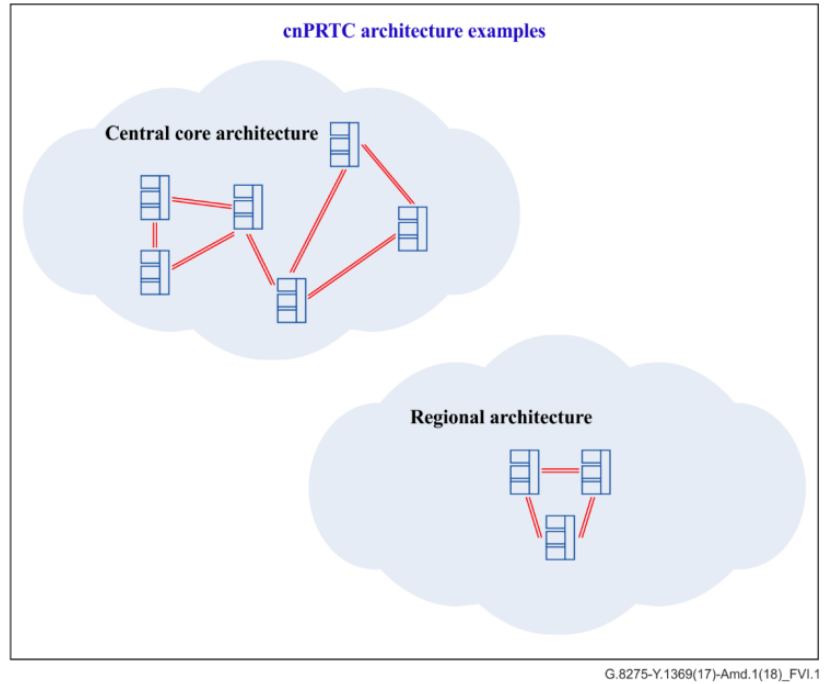


Figure VI.1 – Coherent network PRTC architecture examples

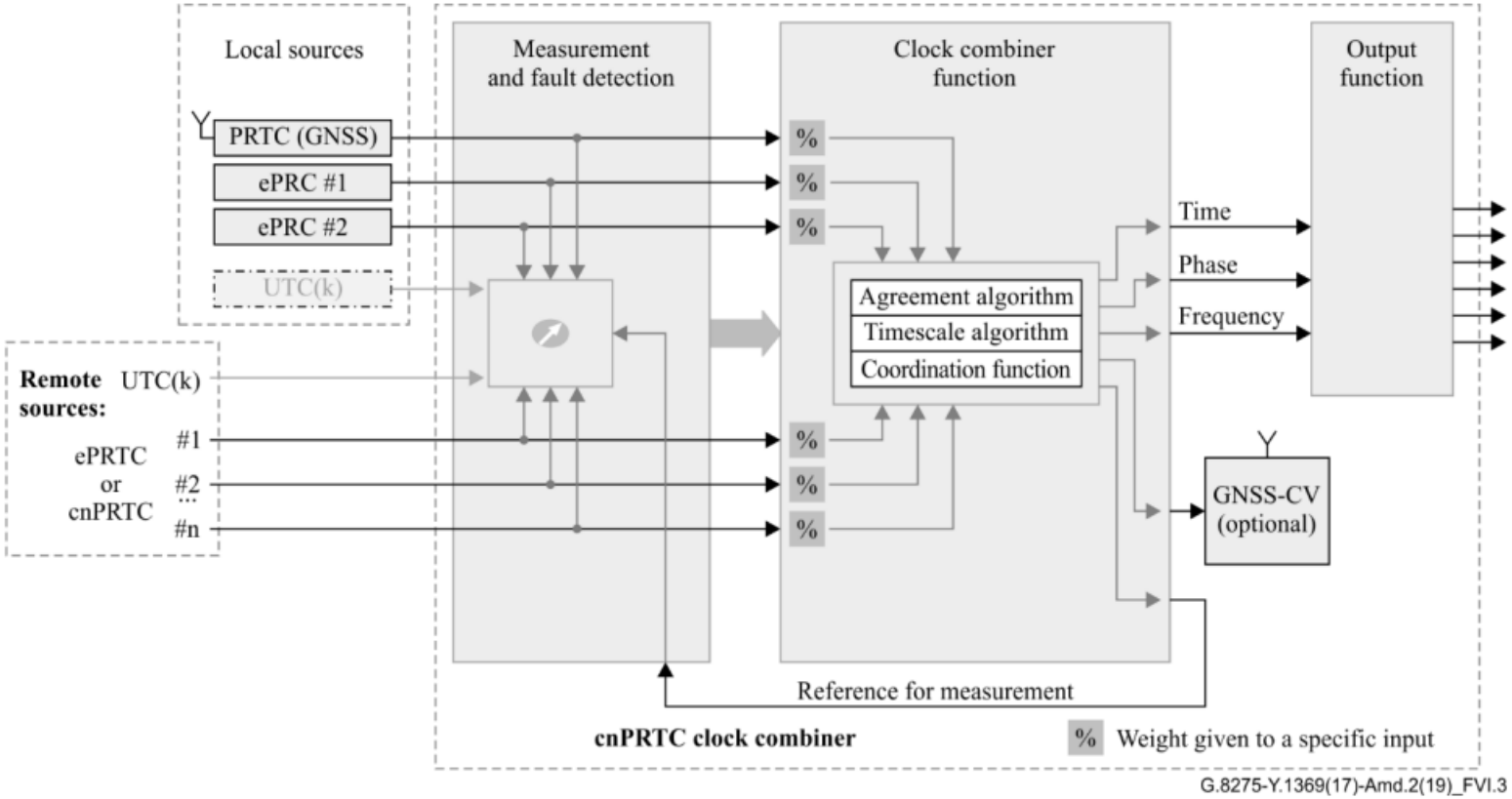
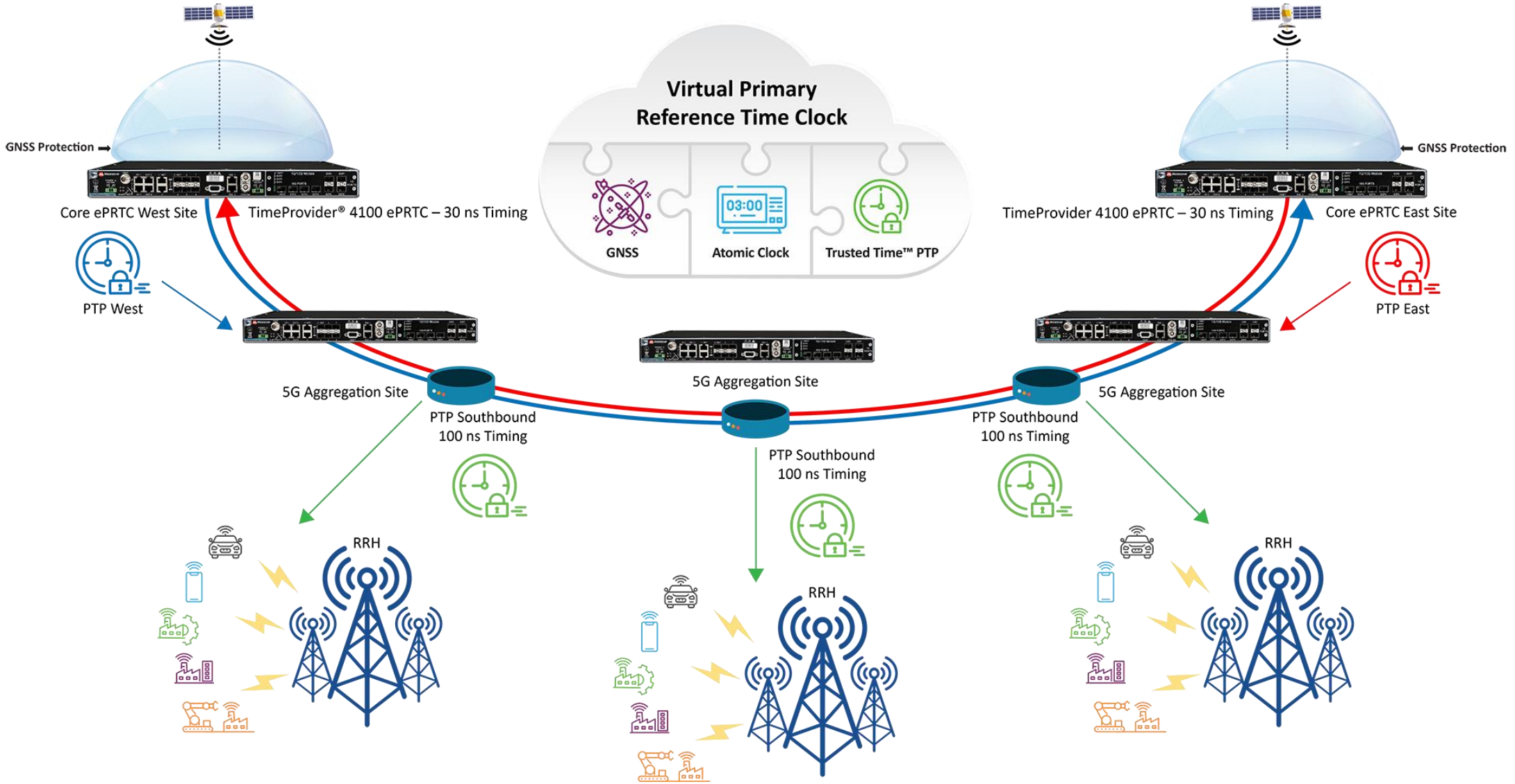


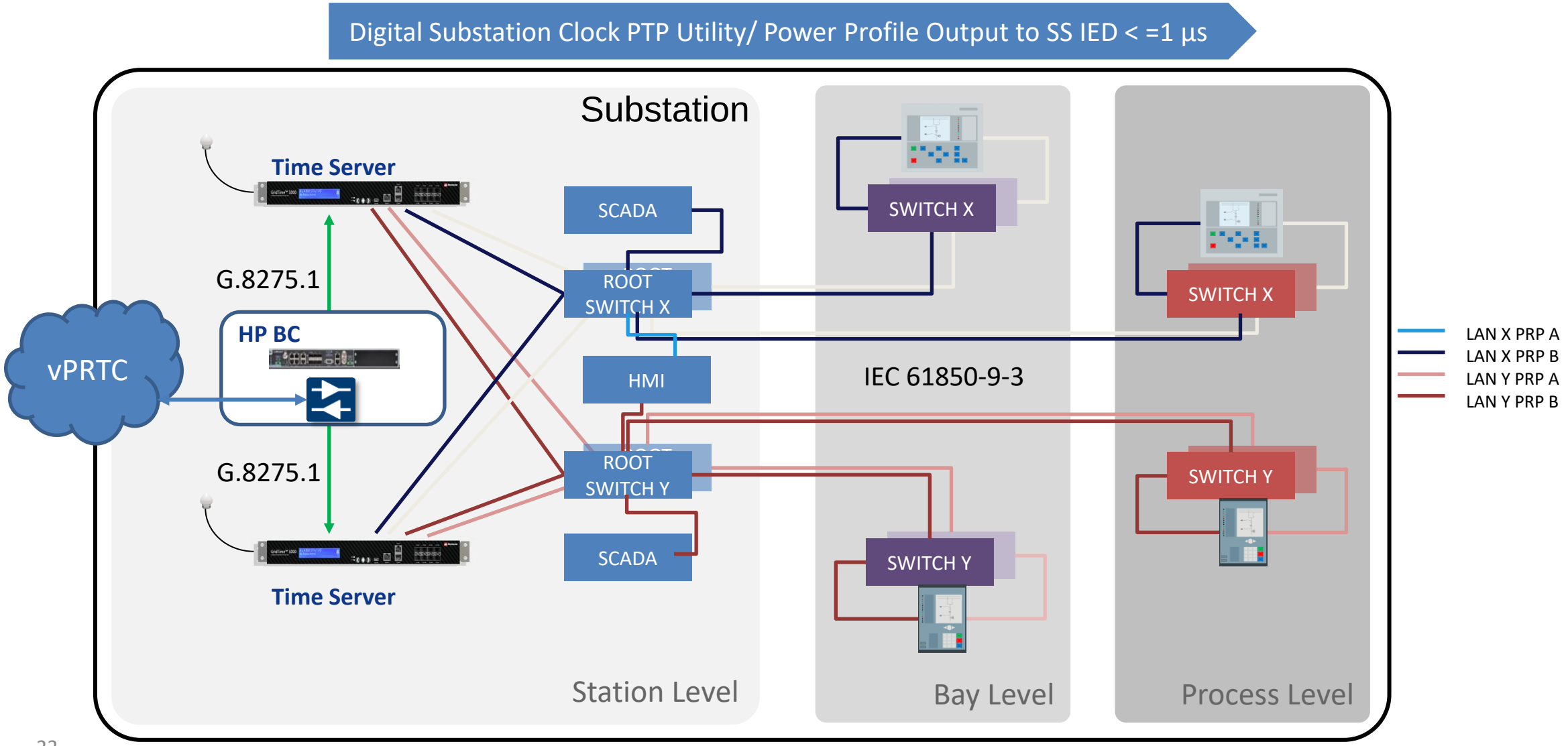
Figure VI.3 – Coherent network PRTC functional block diagram

"Resilient Primary Clock concepts acc. to ITU-T with measurement results", Helmut Imlau, ITSF 2022, Düsseldorf

"The Network is The Clock" - vPRTC



"The Network is The Clock" – vPRTC to substation



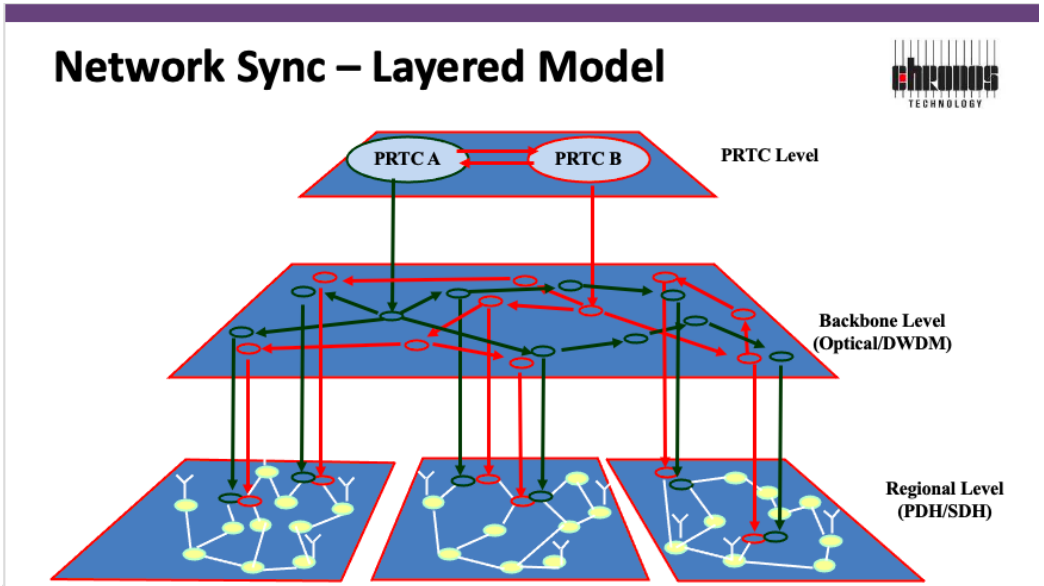
Utilise Telecom Network to provide *YourOwnTime™*

- New ePRTC clock specifications* networked via dedicated fibre (DWDM/OTN etc.) & HP-BC can provide ~5ns of error to UTC across the whole network

* ITU G.8272.1 - GNSS+Cs <100ns error to UTC 14 days

- Every substation that has Telecom optical network access can have access to *YourOwnTime™*

- *YourOwnTime™* can be primary or a backup to be used if GNSS interference is present



Resilient Time: Summary

"Zero Trust"
&
"Secure by Design"

- Resilience increasingly means security, availability & autonomy for time
- ITU-T vPRTC telecom network architectures can supply resilient & trusted time everywhere – if business silos can be overcome!
- "GNSS Firewall" features appearing in newer GNSS receivers – but don't forget the "legacy" installed base!

Digitale onderstations: leer & ervaar!

Hoe digitalisering de energietransitie versnelt | CIGRE B5 & D2

CIGRE Nederland

11 april 2024

Thank you for your attention

Christian Farrow B.Sc(Hons) MIET MInstP

Chris.Farrow@Chronos.uk :: @Chronos_ChrisF :: https://chronos.uk

CHRONOS TECHNOLOGY