Delivering Precise Trusted Time

iPosi
everywhere everytime

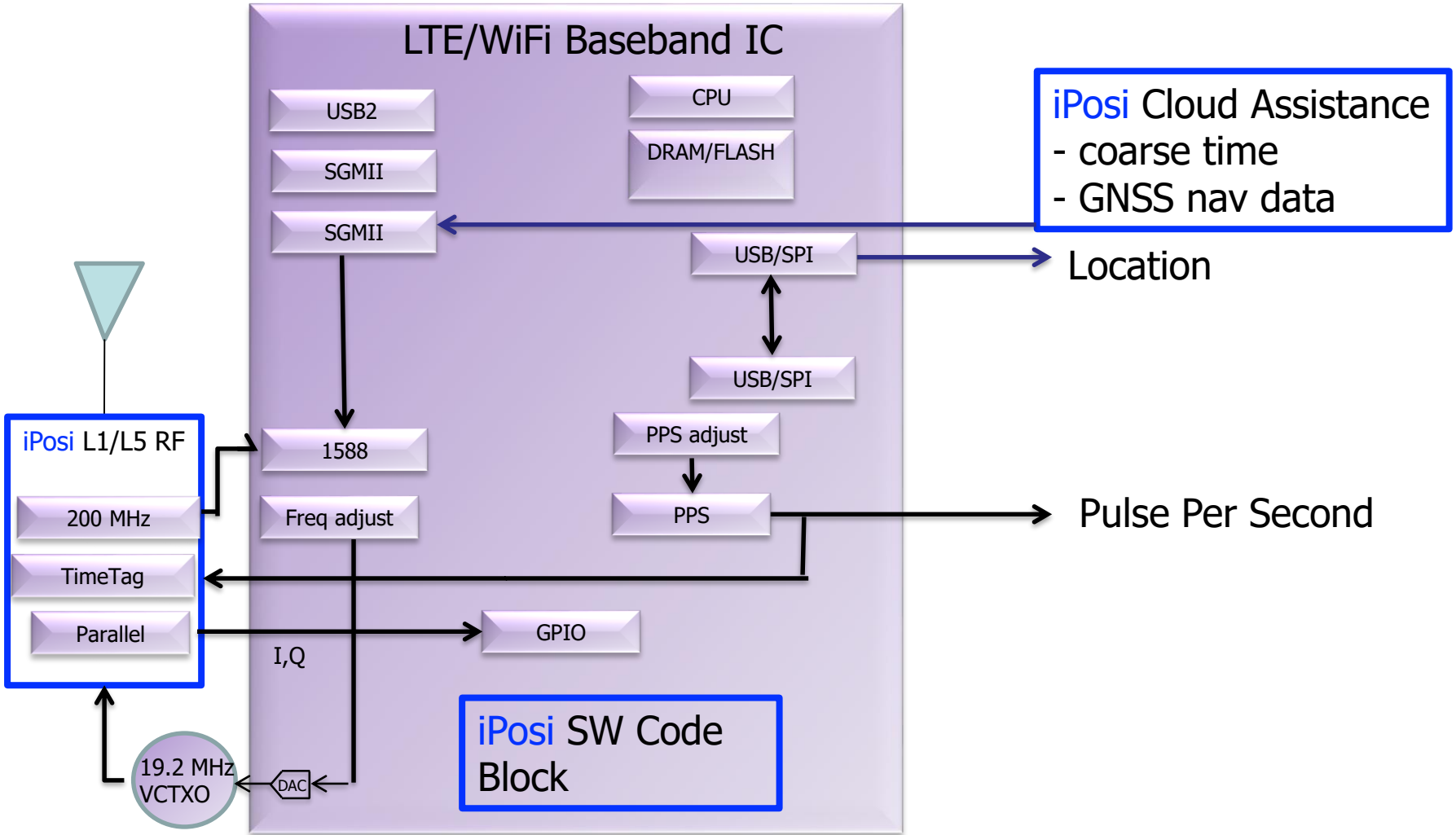
A Proposition to Secure Our Critical Infrastructure and Real-time Networks

Extreme Sensitivity Indoor A-GNSS

We have field tested in 12 cities

Denver
San Francisco (FCC)
Chicago
Santa Clara (FCC)
Boulder
Dallas
Las Vegas
Orlando
Colorado Springs
Los Angeles
Nashville
Austin

Embedded A-GNSS ASIC & SDR for indoor Access Points (LTE/LTE-U/WiFi)



CRITICAL INFRASTRUCTURE REQUIRES PRECISE, SECURE, TRUSTED TIME

Precise Time

- ✓ **Telecom requires < 1.5 μs**
- ✓ **Smart Grid Synchrophasors require < 1 μs**
- ✓ **Financial services (trade execution) require < 100 μs**

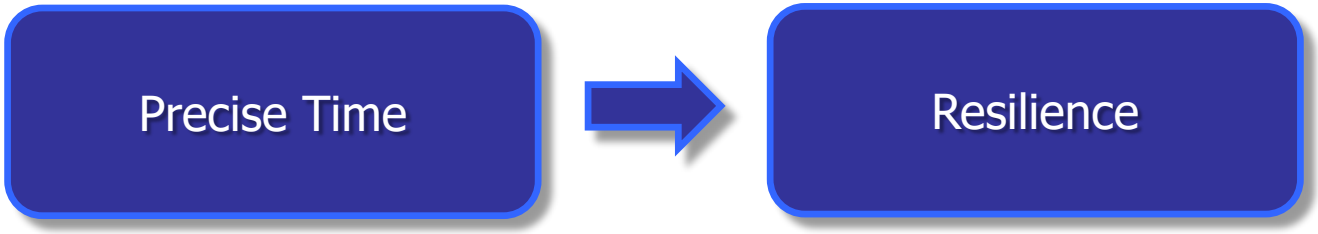
Resilience

- ✓ **PPD 21 (older PDD 63)**
- ✓ **DHS identified 15 of 18 Critical Infrastructure Sectors that use GNSS time**
- ✓ **Operators must preclude impact of GNSS interference events (jamming / spoofing)**
- ✓ **Continuous fallback from independent, diverse sources**

Trusted Time ™

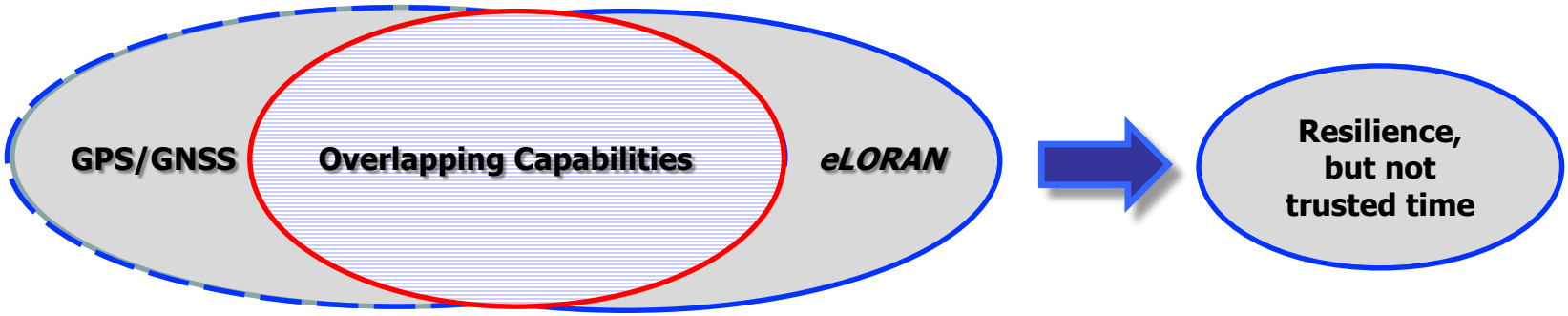
- ✓ **Provides Traceable Tamper-Proof Time**
- ✓ **Sustained resilience against spoofing or jamming / intentional or otherwise**

THE VALUE OF GNSS + ELORAN : *RESILIENCE*, BUT NOT *TRUST*



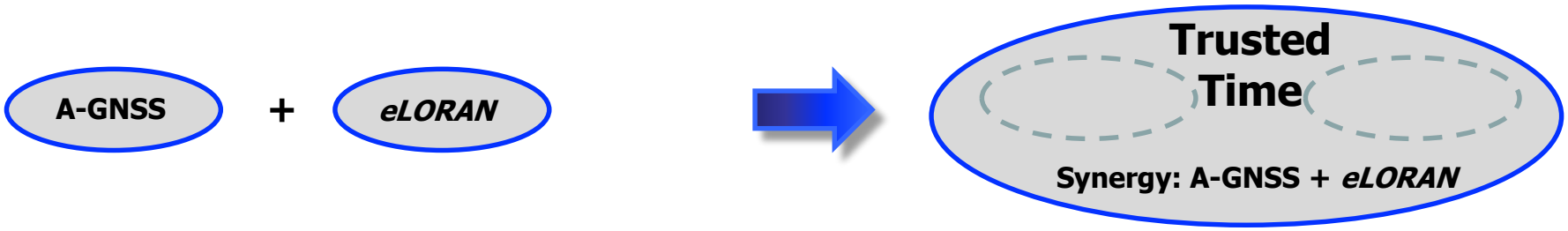
✓ A 'Hybrid' GNSS + *eLORAN* system could do that … but

- Policy makers and industry have regarded a hybrid approach as redundant "7th constellation", costly, falsely competitive, lacking sufficient gain, and
- Lacks the ***trusted time*** feature needed to support critical infrastructures



THE VALUE ADD OF
A-GNSS + *ELORAN* + *NEW SIDE SIGNAL*

- ✓ **Proposition: A-GNSS plus a *new* 'closed' *eLORAN* side signal**
  - Pseudo-random pulse positions modulated via secret key
- ✓ Thwarts 'spoofing' to ensure the reliable delivery of ***Trusted Time***
  (spoofing attacks cannot be thwarted merely by previously knowing rvcr position)
- ✓ Only **four** appropriately located e*LORAN* stations needed for ***Trusted Time***
- ✓ iPosi A-GNSS provides deep **indoor** position and time



Free Bi-Product: Fine-grained *eLORAN* ASF's - improves *eLORAN* PNT accuracy

NEW SIDE SIGNAL ATTRIBUTES

✓The ‘Closed’ side signal is akin to GPS’ P(Y) anti-spoofing code

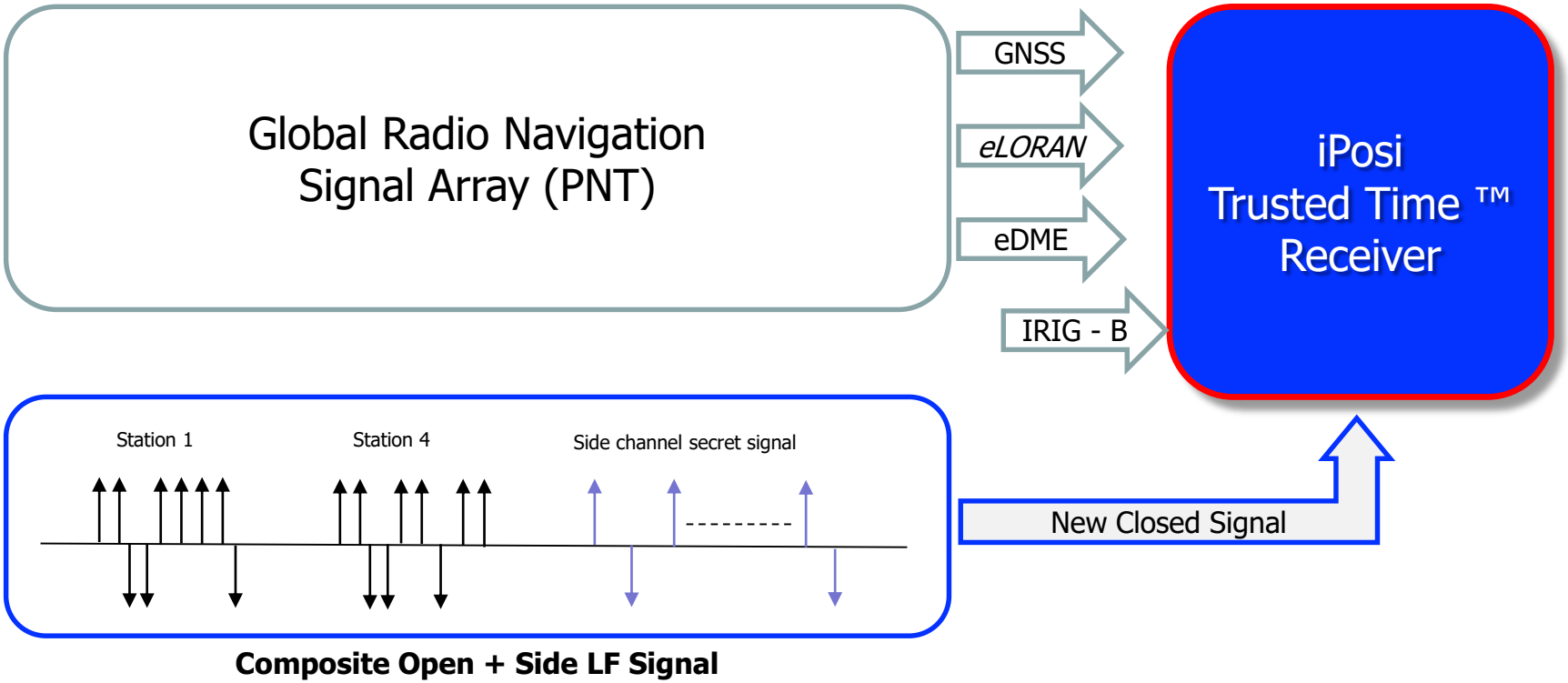
✓ Secures all open GNSS, terrestrial RNAV signals by validating time references

✓ Solution is globally scalable – adapts wherever *eLORAN* is broadcast

✓ LF (100KHz) is an good place to hide the pseudo-random Side Signal

- Lightning strikes are common in the LF channel

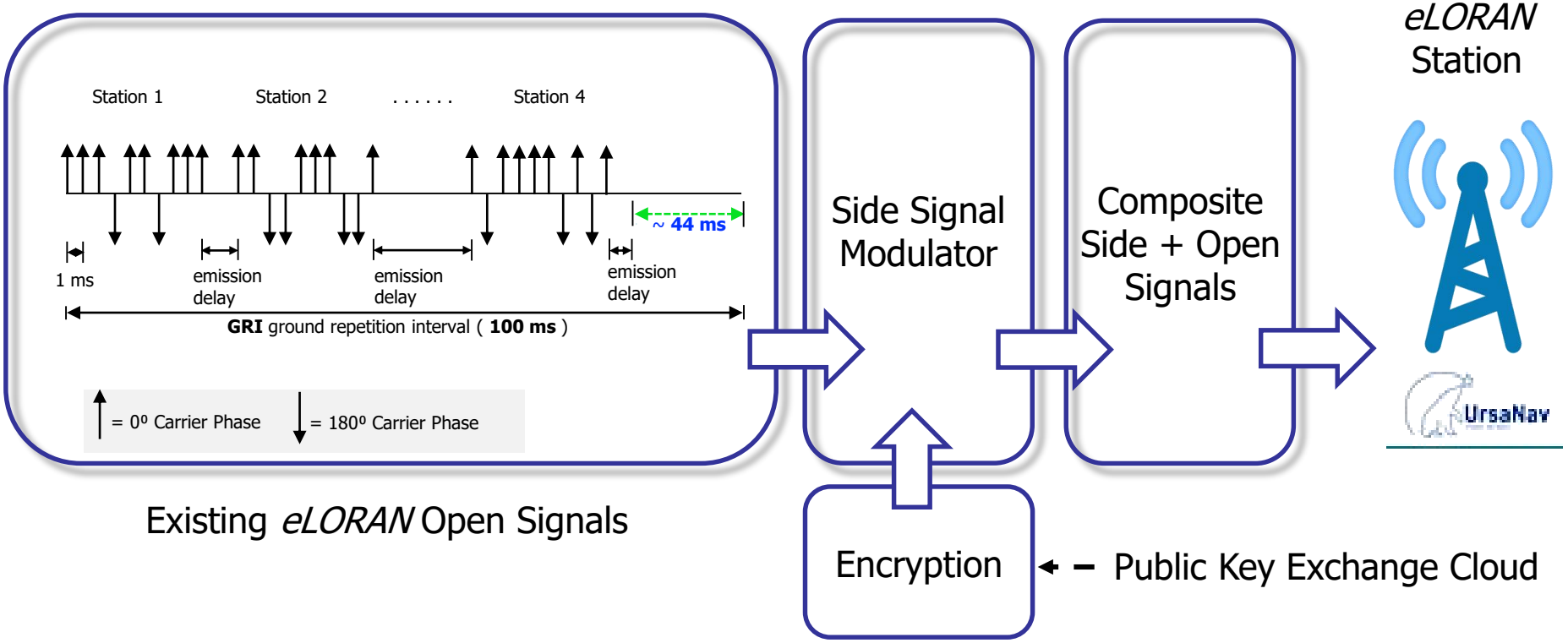
'CLOSED' SIDE SIGNAL VALIDATES ANY OPEN PNT SIGNALS



Composite Open + Side LF Signal

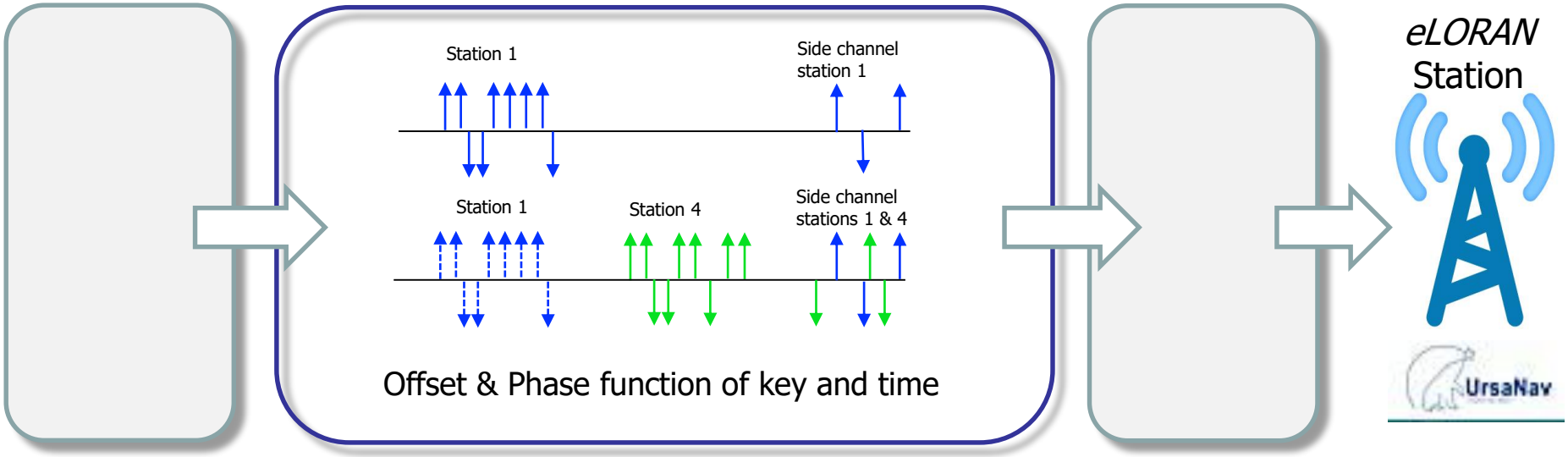
- ✓ Encrypted key incorporated into iPosi assistance, & delivered over IP network
- ✓ Fixed indoor/outdoor receivers today; later will address non-stationary receivers
- ✓ If attacked, receiver ignores open signals and tracks closed signal exclusively

"UNDER THE HOOD": A CLOSER LOOK …



- ✓ Closed Side-Signal: Placed at end of GRI interval
- ✓ Per-station key securely disseminated via IP. Makes Side-Signal un-spoofable
- ✓ 'Closed' Side-Signal fully compatible with UrsaNav's *eLORAN* 'open' signals

ONE LAST LOOK UNDER THE HOOD …



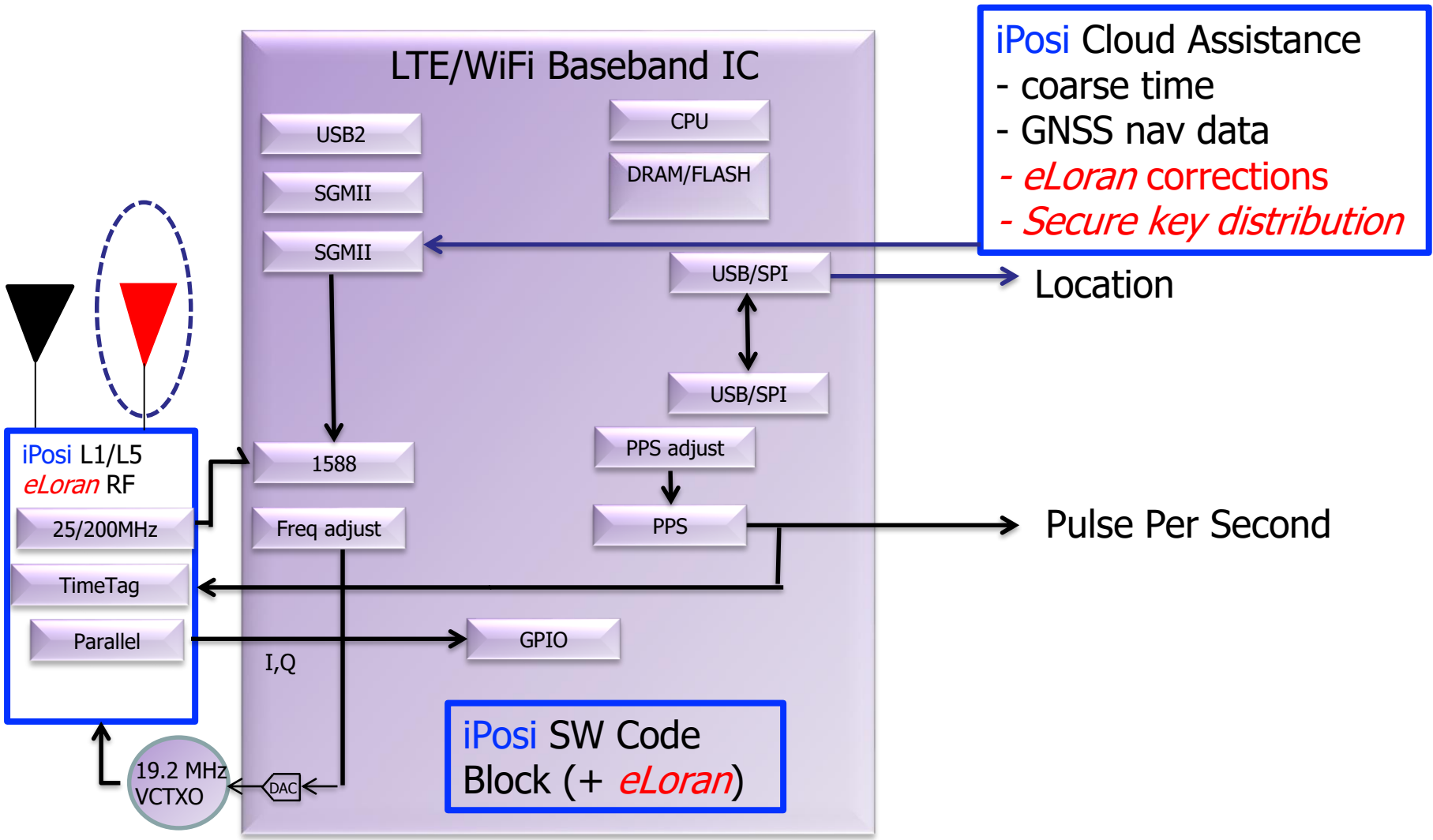
Existing eLORAN Open Signal Modulation

iPosi End-to-End On air Signals

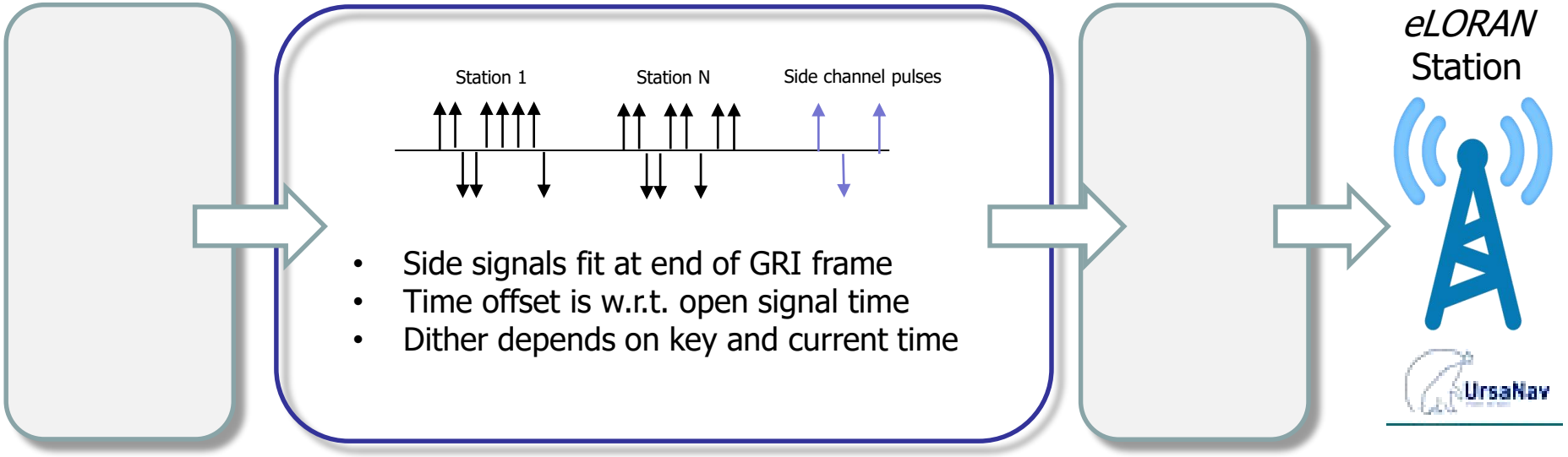
Composite Side + Open Signal

- ✓ **Microsecond-grade** time transfer to **indoor** points at up to 1000km
- ✓ Link budget supports **outdoor** embedded receivers up to 1600km
- ✓ Building losses are 0-30 dB for **Loran** vs 15-47 dB at **L1** or 15-40 dB at **L5**
- ✓ iPosi SDR platform flexibly adds *eLORAN* to its L1 & L5 signal suite

Embedded A-GNSS ASIC & SDR for indoor Access Points (LTE/LTE-U/WiFi)



WE LIED, HERE'S MORE DETAIL…



Existing *eLORAN* Open Signal Modulation

iPosi End-to-End Side Signals

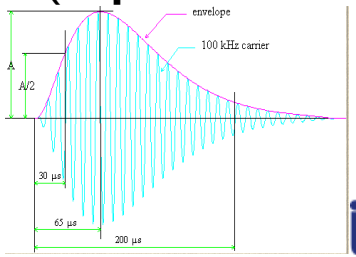
Composite Side + Open Signal

✓ Indoor SNR for GNSS is improved by providing real-time *data* assistance – via IP

✓ However, a receiver under attack will maintain 1 < μs accuracy ***without*** IP network

✓ 'Closed' Side-Signal: Pseudo-randomized pulse sequence (in **position** and **phase)**

- Fully compatible with *eLORAN* signals
- Side Signals use standard LORAN pulse waveform



SUMMARY OF PROPOSAL

✓ Two great technologies form new resilient critical infrastructure service: **Trusted Time**™

✓ **Inexpensive** 4-station US launch platform uses UrsaNav's LF station network

✓ Provides **Indoor** reception; reduces cost; further hardens against jamming

✓ Sustains Trusted Time while under spoofing attack

✓ One Closed signal secures all GNSS

✓ Field trials, before YE 2017

✓ Application, industry-specific trials, dates TBD