12TH EUPOS TECHNICAL MEETING

Intentional and natural threats to CORS infrastructure

Detecting jamming and spoofing in the network,
and keeping users fixed through ionospheric storms.

Jacek Pietruczanis

Trimble · Warsaw, 7–8 October 2026

Two types of threat

INTENTIONAL

Jamming and spoofing

Somebody puts energy in the band, or a false signal on it. RF interference is now routine in parts of Europe.

Trimble Pivot Platform 5.3
Jamming and Spoofing detection

NATURAL

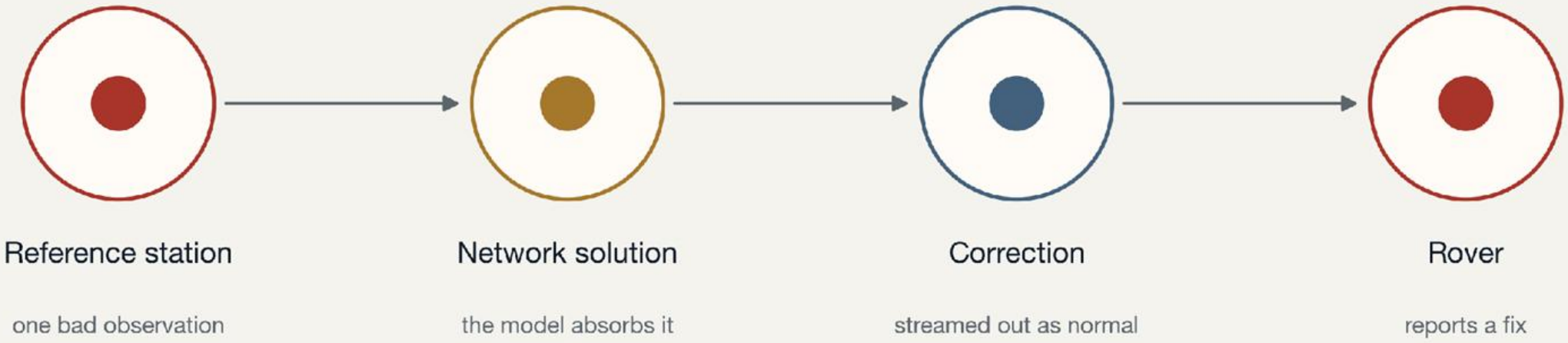
Ionospheric disturbance

Solar Cycle 25 has peaked, and the declining phase still produces the strongest storms. Rovers lose their fix.

Trimble IonoGuard VRS
Pivot Platform 5.2 and later

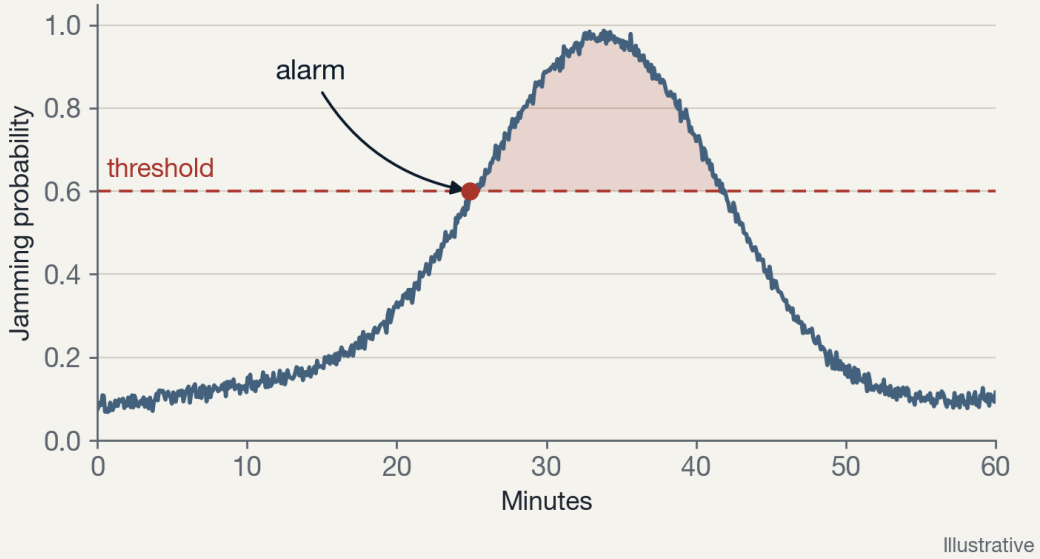
Both arrive as a bad observation at a station you operate.

It does not stay at the station

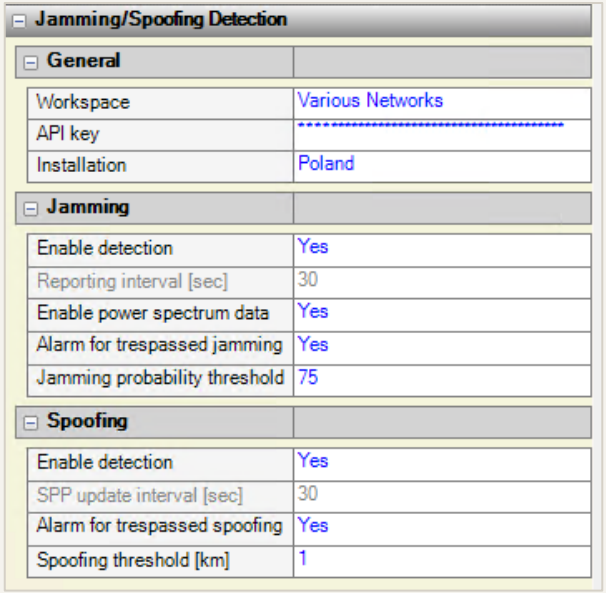


In one event we analyzed, jamming probability rose on L1 while tracking still looked healthy — and GPS, GLONASS and Galileo fixing degraded anyway, because the affected observations were still in the solution. The station never went offline. The rover did not see any degradation.

It raises an alarm. It also cleans the solution



Illustrative



THE ALARM

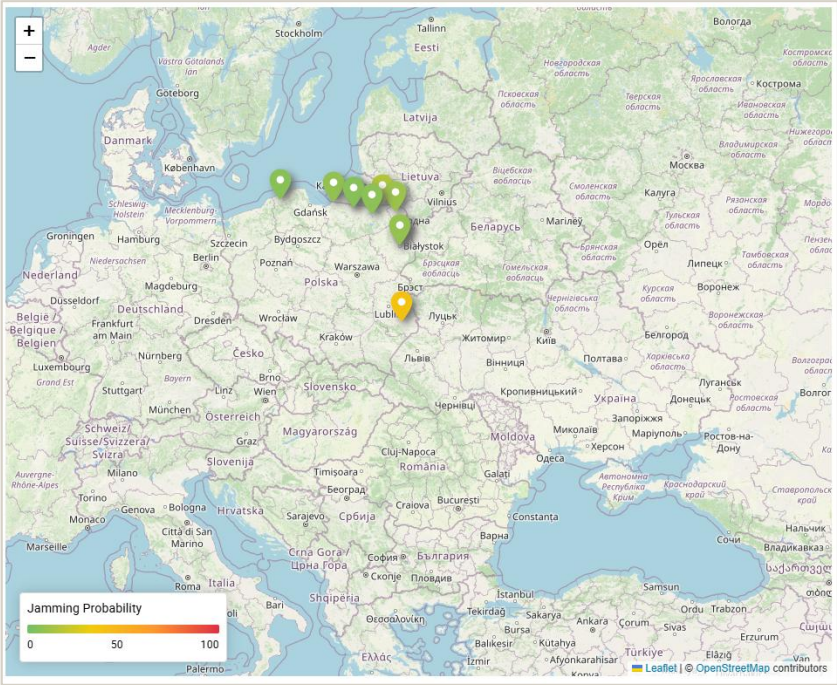
- Probability (based on 4 indicators: signal level, how steady it stays, loss of lock, and the spectrum) crosses the threshold and Alarm Manager tells you.

YOUR THRESHOLDS

Set per installation in Device Manager: jamming probability, and spoofing distance in kilometres.

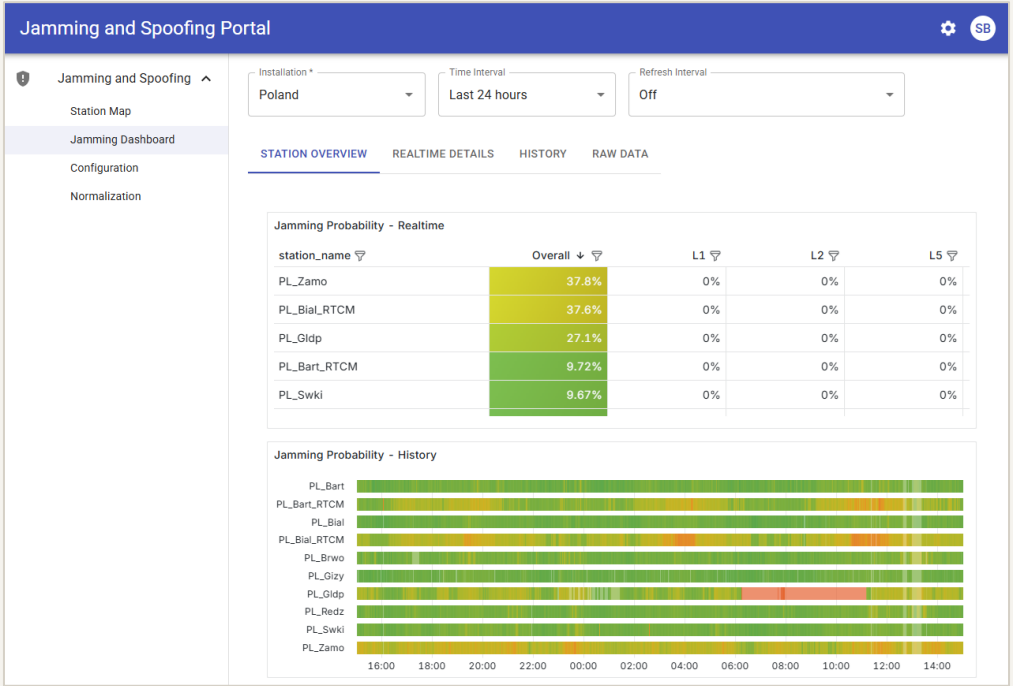
Mitigation already runs inside Raw Data Analysis

Your network, your workspace, your data



STATION MAP

Every station, coloured by jamming probability. Green through to red.



STATION OVERVIEW, REALTIME DETAIL, HISTORY AND RAW DATA

A hosted workspace linked to your own Pivot installation. Your data, nothing for you to build or host.

It runs on the network you already have

No new hardware

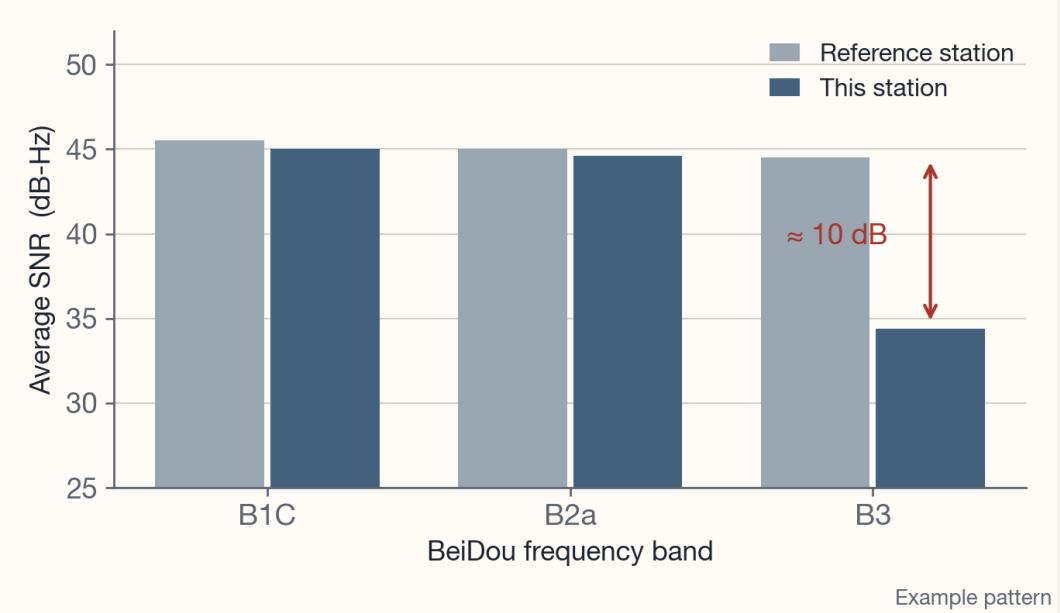
Trimble Alloy, with the Pivot Platform you already run. Nothing to install at the site.

Calibrated, not guessed

Indicator base levels per band, validated against Trimble RTX integrity stations. Trimble maintains the calibration.

It can detect bad CORS station setup, too

The example on the right is not a jammer: one band roughly 10 dB low. Antenna or cable.



Keeping the user fixed through a solar storm

The network sends more

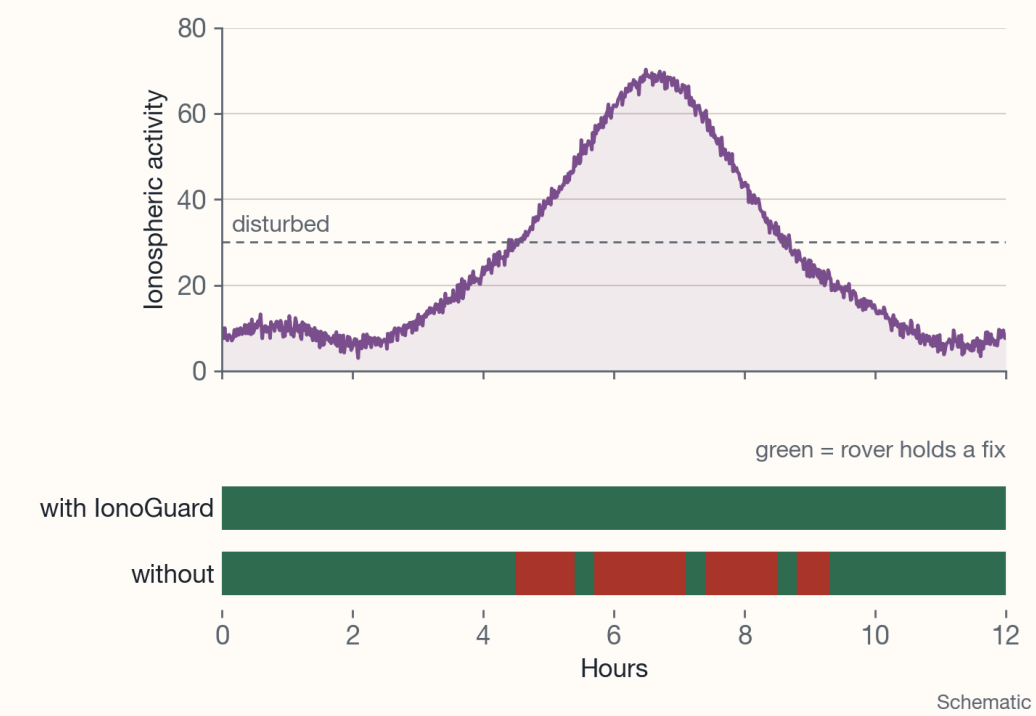
Pivot 5.2 and later put per-satellite ionospheric information into your VRS corrections, in CMRx and RTCM.

The rover uses it

A ProPoint rover combines it with its own measurements, tracks frequencies independently, and recovers carrier lock faster.

The result

A fix that holds through disturbance, where the same rover on ordinary corrections would drop out.



Schematic

If you have Trimble Pivot 5.2, it is a service you can offer your own users.

Xona Space Systems

Xona Pulsar is a LEO constellation

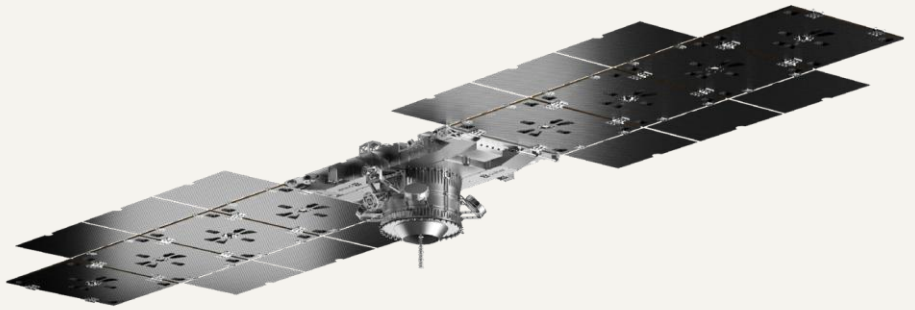
258 satellites planned in low Earth orbit, roughly twenty times closer to the ground than GNSS.

Harder to drown out

About a hundred times the received signal power, and a demonstrated live-sky reduction in jammer effectiveness.

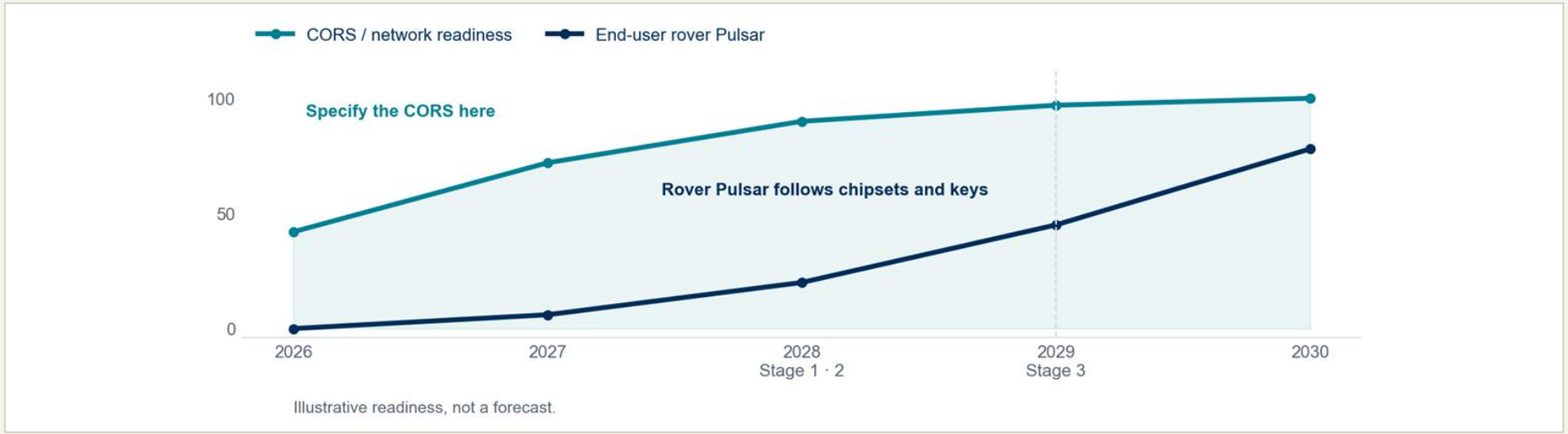
Built to be authenticated

Authenticated ranging, with a dynamic anti-spoof watermark on the signal itself.



Two signals in L-band — X1 and X5 — the band your infrastructure is already built around.

The value arrives at the reference station first



Heard on L-band

The band your choke ring and Zephyr 3 Geodetic already cover.

Into the network

Tracked, archived and quality-checked at the reference, in Pivot.

The collaboration

Xona builds the constellation. Trimble makes it usable at the CORS.

Rover side

We build the networks side first. Rover-side comes later.

Danke
شكرا
Tack
ありがとうございます
Teşekkürler
Спасибо
Grazie
감사합니다
Obrigado
Thank you
Gracias
Tak
Merci
谢谢
Takk
Dziękujemy
Terima kasih
Dankjewel
धन्यवाद
Cảm ơn
Kiitos