

GNSS threats and fallback options

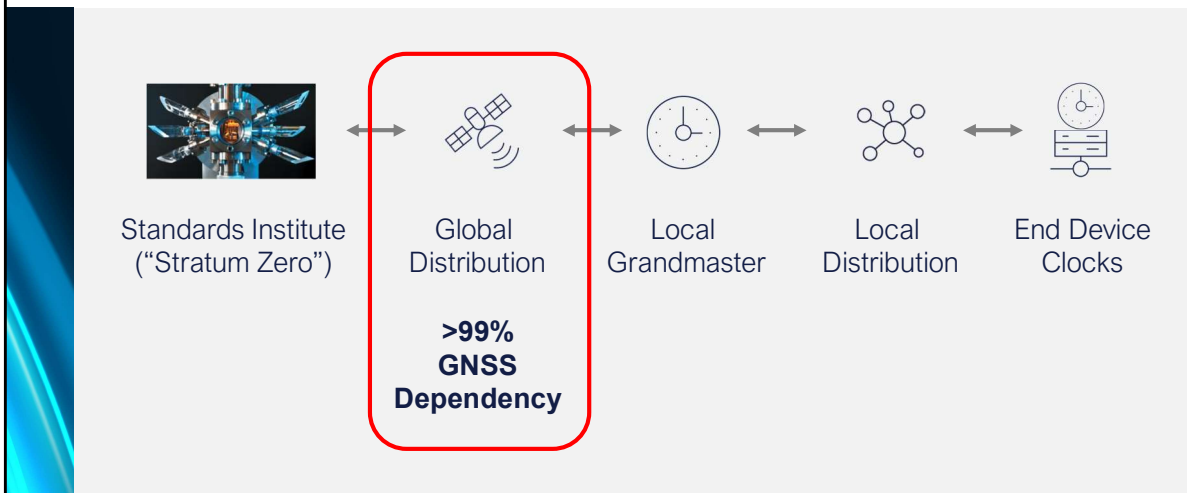
Richard Hoptroff, Chief Technology Officer, Hoptroff London Ltd

The lower half of the slide features a dark blue background with a white geometric shape on the left. The word "HOPTROFF" is written in white, bold, sans-serif capital letters. To the right, there are vibrant, abstract light streaks in shades of blue, cyan, and magenta, suggesting motion or data flow.

HOPTROFF

Good afternoon. My name is Richard Hoptroff and today we'll look at combining navigational satellite time with other timing sources for improved resilience and traceability.

The chain of comparisons



[CLICK] To ensure clocks agree, you need what is known as traceability to at least one standards institute, or Stratum Zero source as we call it.

Traceability is a continuous chain of comparisons which extends across the entire distribution chain all the way down to each clock in your environment.

[CLICK] In well over 99% of implementations today, global navigational satellites are in the chain of comparisons, and that fragility is what this whole ITSF session is about

Why GNSS is great for timing

- Free at the point of delivery
- Accurate to 10s of nanoseconds – far more accurate than most people need

[CLICK] The main reasons why GNSS is universally popular are that it is free, and it's so accurate that it meets everybody's' needs

Why GNSS is not that great for timing

- Subject to unintentional interference
- Subject to intentional interference
- Subject to logical interference
- Subject to meteorological interference
- Technically not traceable without Common View reference [1]

[CLICK] But the problem with it is it's a fragile system which is easily compromised, as you'll see in the slides that follow

[CLICK] And if get really picky, you could argue that it is not fully traceable without cross-checking using the Common View method

Local threats – Unintentional interference



[CLICK] Examples of unintentional interference include [CLICK] microwave ovens, [CLICK] truck drivers using signal jammers to cover their tracks and [CLICK] faulty active antennas in antenna farms that start transmitting rather than receiving

Local threats – Intentional interference

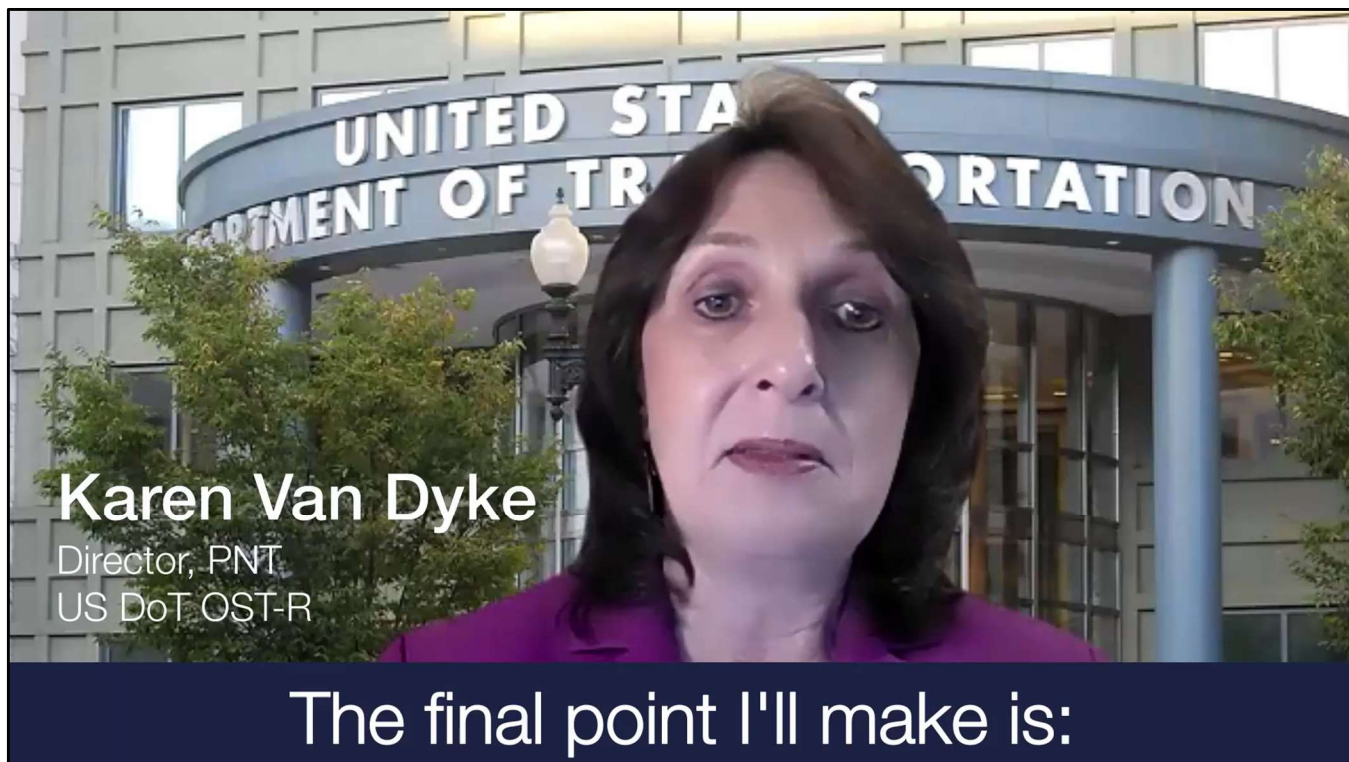


Source: EuroControl, Airbus

6

[CLICK] Examples of intentional interference include [CLICK] deliberate jamming and [CLICK] signal spoofing, either for defensive or offensive reasons.

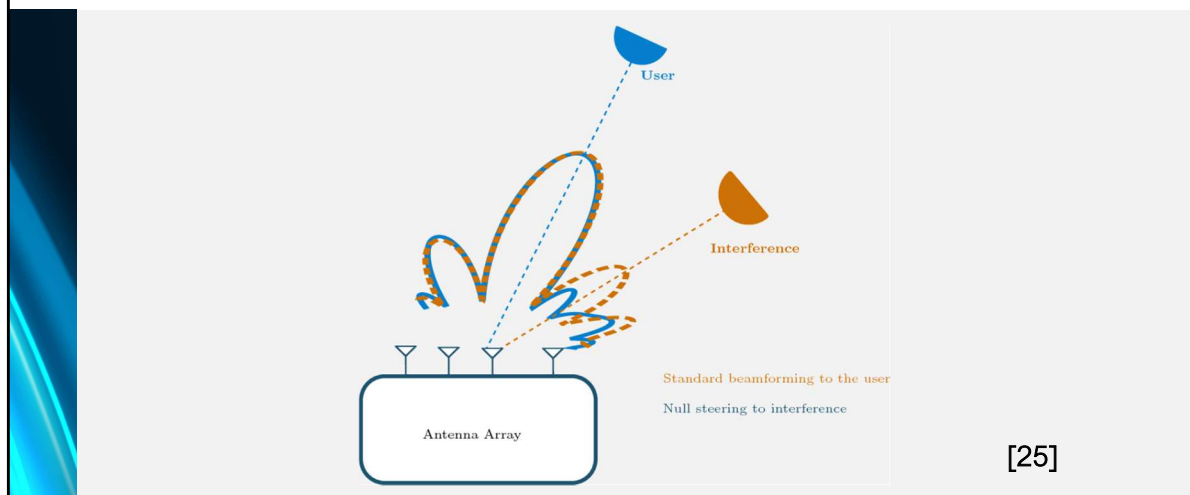
Spoofing is where an incorrect signal is generated to mislead the recipient. The map on the right shows recent areas of regular spoofing today as reported by Airbus



[VIDEO CLIP – 41 seconds] “The final point I’ll make is: This is so serious that last year the White House issued an executive order on strengthening national resilience through responsible use of Positioning, Navigation and Timing services. I’ve required NIST, the National Institute of Standards and Technology, to develop what’s known as a PNT profile to really assess your risk tolerance. That’s certainly something critical infrastructure is embracing and we want to have technology options available that can be adopted to ensure PNT resiliency.”

Mitigation

HOPTROFF



8

[CLICK] Mitigation of such interference has largely focused on antenna design to suppress suspicious signals. Their effectiveness depends on the nature of the interference. With jamming, at least you'll know if you have a problem because you'll have lost your signal, but with spoofing you won't know whether you've fixed the problem or not.

The only way to know if your time is right is if you have a second source to compare it to, which I'll discuss later.

Systemic threats – Logical interference



[8] [9] [10]



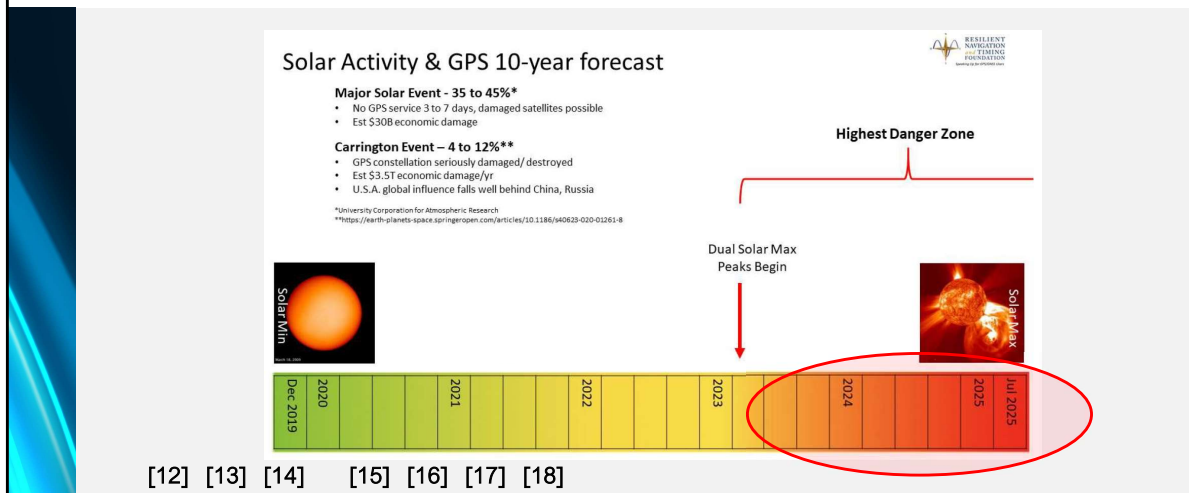
[11]

[CLICK] We also need to consider the potential for system-wide threats to navigational satellites.

[CLICK] Satellite programming errors happen on a regular basis,

[CLICK] and cyber-attacks are increasingly becoming a problem

Systemic threats – Meteorological interference



Graphic courtesy Resilient Navigation and Timing Foundation

10

[CLICK] And probably the least appreciated threats are the meteorological. Of course we need to protect against terrestrial weather such as lightning strikes and physical corrosion. [CLICK TO ZOOM UP] But coronal mass ejections are a serious systemic threat, with the potential to cripple entire satellite systems. Such flares are frequent but very directional, and have a prediction horizon of only minutes or hours. [CLICK TO ZOOM DOWN] When we next get an intense direct hit is potluck, but it will be catastrophic for satellite service. This problem will not go away while the sun still shines.

[CLICK] A severe peak in coronal activity is expected in 2025.

[CLICK] This is why major governments are paying serious attention to the problem.



[VIDEO CLIP – 25 seconds] “Is this something that boards should be aware of? Is this something that should be on peoples’ Risk Registers and something that companies should be thinking about? And as Richard joked before, timing is one of those subjects that people as a risk, and from a resilience perspective, just don’t really talk about on a daily basis. And I presume that a few years ago, nobody in the boardroom talked about pandemics either.”



[VIDEO CLIP – 12 seconds – Leon Lobo, NPL] “There was another report that was raised around the loss to the UK economy being of the order of £5bn over 5 days and there was a similar report in the US on this front as well.”

Fallback Options

- Fallback options : What is Plan B if GNSS is unavailable? [18]
- For traceable time, fallback options include:
 - NTPpool [19]
 - Radio services such as MSF [20]
 - Long Distance PTP [Next slide]
 - eLoran [21]
 - Satelles STL [22]
 - White Rabbit [23]
- Fallback options can be used to detect and alert for GNSS compromises

13

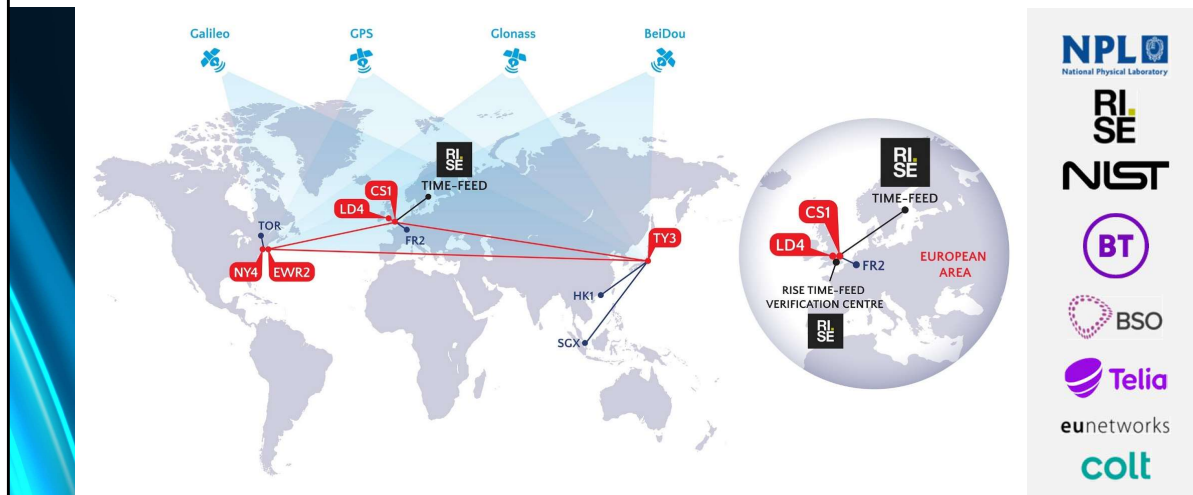
[CLICK] The best solution is to have a fallback option. A fallback option differs from mitigation in that it considers what to do if the primary service fails, for reasons anticipated or unexpected.

What is the Plan B until Plan A can be restored ?

For traceable time, there are a number of technology candidates, from NTPpool to White Rabbit each with their own trade-offs between accuracy, resilience and cost

As I mentioned earlier, without some kind of secondary reference, you don't know whether your time is traceably correct or not. The fallback option can function as this secondary reference and we have recently been developing tools to use this to generate alerts when the GNSS signal is compromised.

Long distance PTP

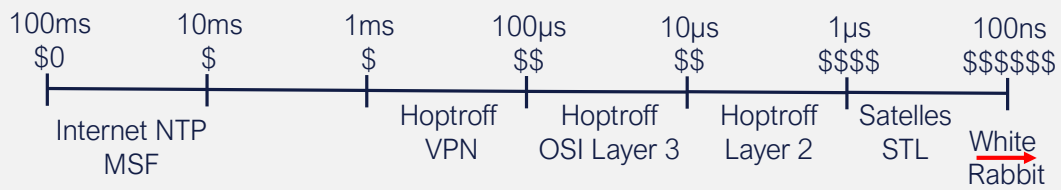


14

[CLICK] The Long Distance PTP network [CLICK TO ZOOM UP] we developed for financial services combines satellite sources and direct terrestrial connections to standards institutions including RISE, the Swedish standards institution, with NPL and NIST being added this quarter (Q4 2021).


[CLICK TO ZOOM DOWN] We achieve long distance time distribution by working closely with telecoms networks, and using client software specially designed to work with long distance PTP signals.

Fallback option accuracy vs cost tradeoff



[CLICK] Each fallback technology has different trade-offs between levels of accuracy and cost.

KPIs for Fallback Options



Accuracy	How wrong might my clocks be?
Cost	How much will it cost to achieve?
Continuity	What is the cost to me of an interruption in service?
Threats	What is the impact on society if service is disrupted?
Reliability	What is the expected uptime?
Scalability	How easy is it to deploy at scale?
Traceability	Can I prove my chain of comparisons back to UTC?
Ease-of-use	How easy is it to manage?

[CLICK] But in choosing a fallback technology, accuracy and cost are not the only factors that need to be considered.

[CLICK] Reliability, scalability and ease-of-use are also factors that need to be considered. Ease-of-use is particularly important, because the man-hours it takes to manage the system needs to be factored into the overall cost.

KPI sweetspots across market sectors

Sector	Accuracy	Continuity & Reliability	Threats	Scalability	Traceability	Ease-of-use	Cost
Power	1μs	***	***	1,000s	*	*	\$\$\$
Telecoms	1μs	***	***	10,000s	*	*	\$\$\$
Military	10μs	***	***	10,000s	*	*	\$\$\$
Finance	100μs	**	***	10,000s	***	**	\$\$\$
Gambling	1ms	*	*	10,000s	***	*	\$
Real-time bidding	1ms	*	*	10,000s	**	*	\$
Gaming	1ms	*	*	10,000s	**	*	\$
Media	1ms	**	***	10,000s	*	**	\$
GNSS Monitoring	1ms	**	***	10,000s	*	**	\$
Enterprise	1ms	*	***	100,000s	**	**	\$
Smart factories	1ms	***	***	1,000,000s	*	**	\$
Transport	1ms	**	***	1,000,000s	**	***	\$
Digital currencies	1ms	**	**	10,000,000s	***	*	\$
Insurance	100ms	**	*	10,000,000s	***	*	\$
Payments	10ms	**	***	10,000,000s	***	***	\$
Health	10ms	**	***	10,000,000s	***	***	\$
Emergency Services	10ms	**	***	10,000,000s	***	***	\$
Internet of things	1ms	*	***	100,000,000s	**	***	\$

[CLICK] The importance of these factors varies widely across industries, and to a large extent, you pay your money and make your choice. This slot is just 15 minutes and the font is quite small, so refer to your copy of the presentation if you want to spend more time on this slide.

This afternoon's session is all about the need for resilience if you need time synchronization for business continuity. We believe that incorporating fallback options is the only sure way forward, and there are a variety of technologies to choose from according to your needs.

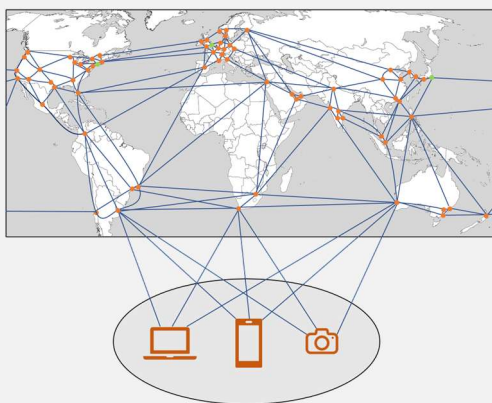
Collaboration with Innovate UK / NPL NTC [24]

HOPTROFF

Innovate UK



HOPTROFF



Mass-scale time dissemination to edge devices

18

[CLICK] We are currently extending this work further with three projects part funded by Innovate UK and NPL's National Timing Centre.

Our lead project is to achieve mass-scale traceable time dissemination of NPL's time standard, going all the way to edge devices such as payments systems, mobile devices, and so on.

Collaboration with Innovate UK / NPL NTC [24]

HOPTROFF

Innovate UK



Wireless last-mile time dissemination

19

[CLICK] We are also working with Spirent and Cranfield University on their project to extend Long Distance PTP to include a wireless last mile for devices in motion.

Collaboration with Innovate UK / NPL NTC [24]

HOPTROFF

Innovate UK



Secure time sync for airspace management

| 20

[CLICK] And we are working with Operational Solutions, along with Cranfield, to apply the technology to secure airspace management and security.

References

1. gssc.esa.int/navipedia/index.php/GPS_Time_and_Frequency_Transfer_Techniques
2. www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/
3. www.chronos.co.uk/files/pdfs/cs-an/chronos_detecting-rogue_gps_antenna.pdf
4. www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon
5. www.rtl-sdr.com/using-a-hackrf-for-gps-spoofing-on-windows
6. radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf
7. www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing
8. www.gpsworld.com/the-system-glonass-in-april-what-went-wrong
9. www.bbc.co.uk/news/technology-35463347
10. www.theregister.com/2019/11/08/galileo_satellites_outage
11. www.missionsecure.com/blog/the-cyber-attack-on-garmin-exposing-gps-vulnerabilities
12. en.wikipedia.org/wiki/List_of_solar_storms
13. www.theblackoutreport.co.uk/2019/08/06/quebec-blackout-1989-solar-storm
14. en.wikipedia.org/wiki/Solar_storm_of_2012
15. www.federalregister.gov/documents/2020/02/18/2020-03337/strengthening-national-resilience-through-responsible-use-of-positioning-navigation-and-timing
16. www.cisa.gov/publication/time-guidance-network-operators-cios-cisos
17. www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review
18. Apocalypse How? Oliver Letwin, 2020, ISBN 9781786496867
19. www.ntppool.org/en
20. www.npl.co.uk/msf-signal
21. www.gpsworld.com/innovation-enhanced-loran
22. satelles.com/technology/satellite-time-and-location-stl/overview-of-stl
23. white-rabbit.web.cern.ch
24. www.npl.co.uk/ntc
25. <https://scholarworks.montana.edu/xmlui/handle/1/3344>

[CLICK] You'll find a list of references at the end of your copy of this presentation.

Thank you

For a complimentary copy of the annual
Hoptroff Timing Report, email info@hoptroff.com*

hoptroff.com

* GDPR statement: By requesting to subscribe, you agree we may retain your email address
for Hoptroff marketing purposes, unless and until you ask us not to.
It will not be shared with other organizations.

[CLICK] I have no idea why my marketing people want to turn my face blue, but in any event, thank you very much for your time. We recently published our annual Hoptroff Timing Report, which reviews the timing industry in general. It's free, so just send us an email to subscribe.