Gulfstream™

G500/G600 GPS JAMMING/ SPOOFING PROCEDURES

Gulfstream Flight Operations| December, 2023

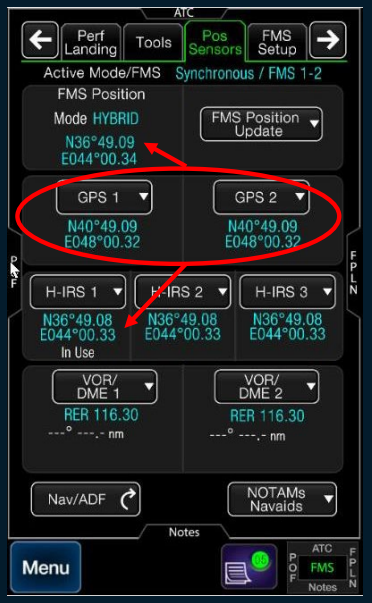
WHAT IS GPS SPOOFING?

- Occurs when a counterfeit GPS signal is used to replace the true GPS signal with a fake position that the system does not identify as being false
- When spoofing occurs, the avionics systems that use GPS are compromised, but their behaviors differ
- Due to variations in types of spoofing and which portions of GPS data are being spoofed, not all symptoms described in this presentation may be observed

WHAT IS GPS SPOOFING?

- When a spoofed GPS signal is received representing a non-moving GPS position, the following are commonly observed:

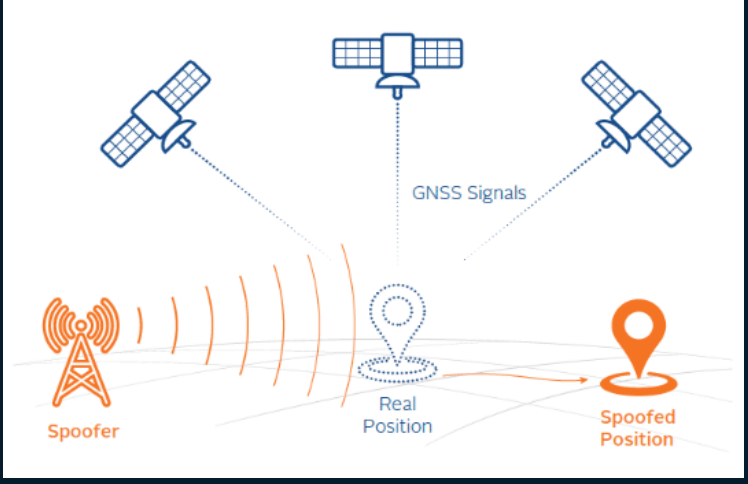
  - GPS Position appears at a different location, while Hybrid IRS and FMS position drifts towards it



Gulfstream

WHAT IS GPS SPOOFING?

- Spoofed position is likely a static position hundreds of miles away
- Key to fooling FMS is to intermix spoofing and jamming
- Jamming makes GPS invalid, then stability checks reinitialize which have no past data, therefore stability checks can't tell that the position is wrong
- UTC time may be wrong, but some spoofing may have the correct UTC time



Gulfstream

SOME AREAS OF CONCERN

- Iraq
- Iran
- Syria

Gulfstream

SIGNS OF GPS SPOOFING AND/OR JAMMING

- Loss of Synthetic Vision (blue over brown displayed)
- Amber DEGRADE on PFD

EPU rapidly increases to anywhere from 40-99 due to conflicting position between the Hybrid IRS/GPS and Nav Radios and Pure IRS.

Gulfstream

SIGNS OF GPS SPOOFING AND/OR JAMMING

- FMS 1-2-3 GPS Pos Miscomp Advisory CAS message posts when FMS position differs from GPS position > 10 miles
- Amber DEGRADE on MAP
- Unexpected movement of aircraft on MAP
- Flight guidance changes to steer to “new” position

Gulfstream

SIGNS OF GPS SPOOFING AND/OR JAMMING

FMS/Pos Sensors/GPS1-2

Inaccurate or frozen GPS time

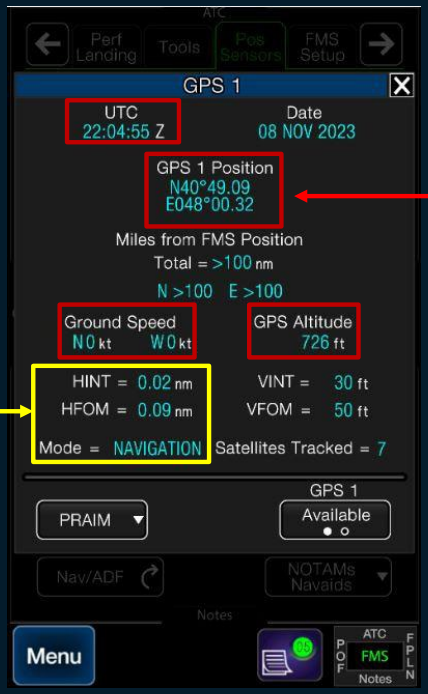
Large error between GPS and FMS position

SIGNS OF GPS SPOOFING AND/OR JAMMING

FMS/Pos Sensors/GPS1-2

GPS status Indicates incorrect time, position, ground speed (low or zero), and altitude

Horizontal Integrity, Figure of Merit, and Mode appear to be Correct



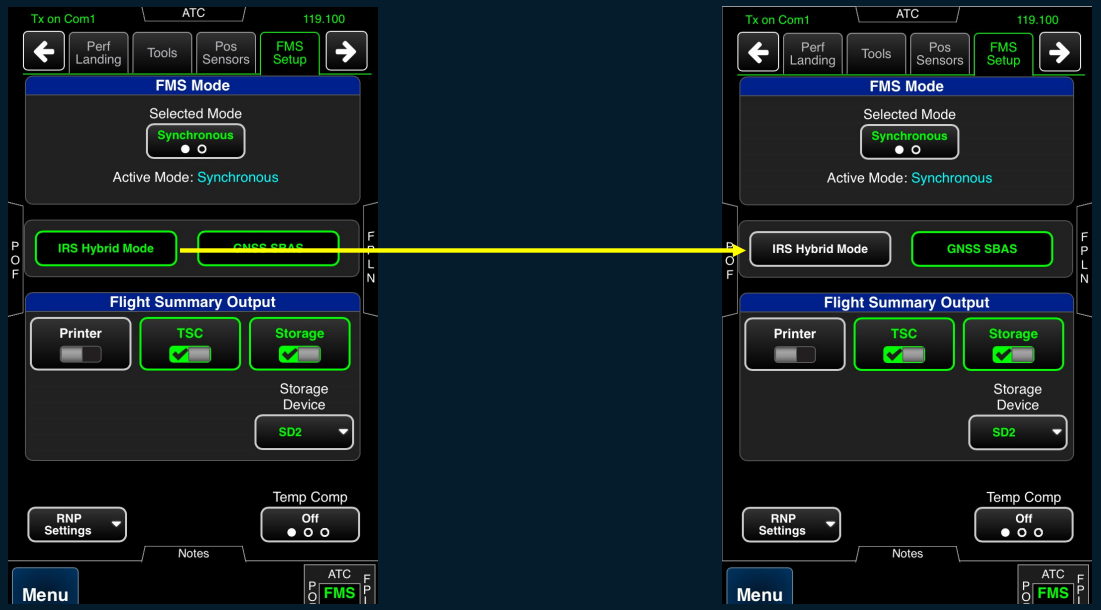
GPS Position is typically frozen

ACTIONS IN CASE OF GPS SPOOFING

1. Select heading/track lateral guidance
2. Report presence of spoofing and degraded nav capabilities to ATC, and request an initial vector
3. Deselect GPS 1 AND GPS 2 (FMS/Pos Sensors/GPS 1-2)

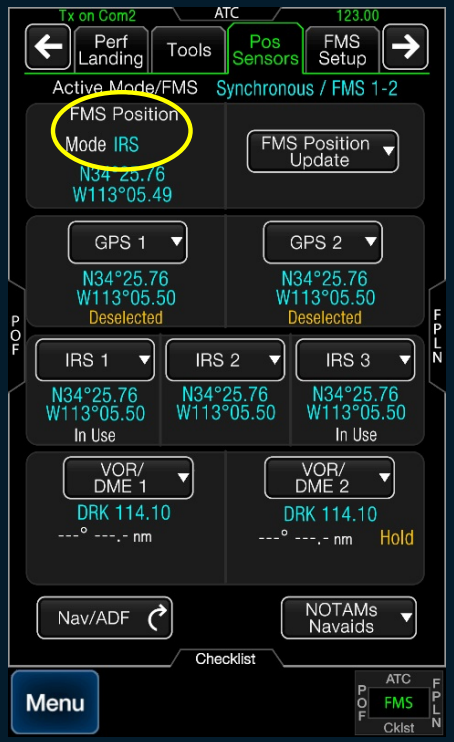
ACTIONS IN CASE OF GPS SPOOFING

4. Deselect IRS Hybrid Mode (FMS/FMS Setup)



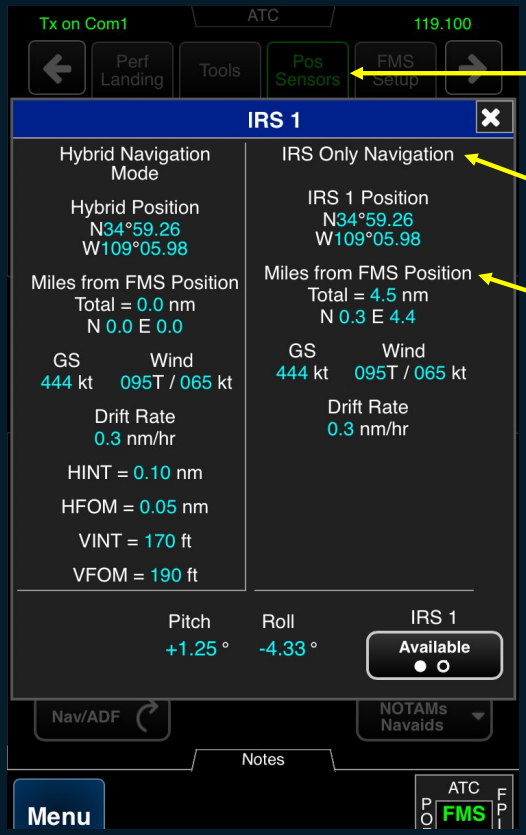
ACTIONS IN CASE OF GPS SPOOFING

FMS Position Mode will change to one of the following: IRS or VORDME or DMEDME



ACTIONS IN CASE OF GPS SPOOFING

5. Evaluate magnitude of “drift” which has occurred: distance between FMS and IRS position



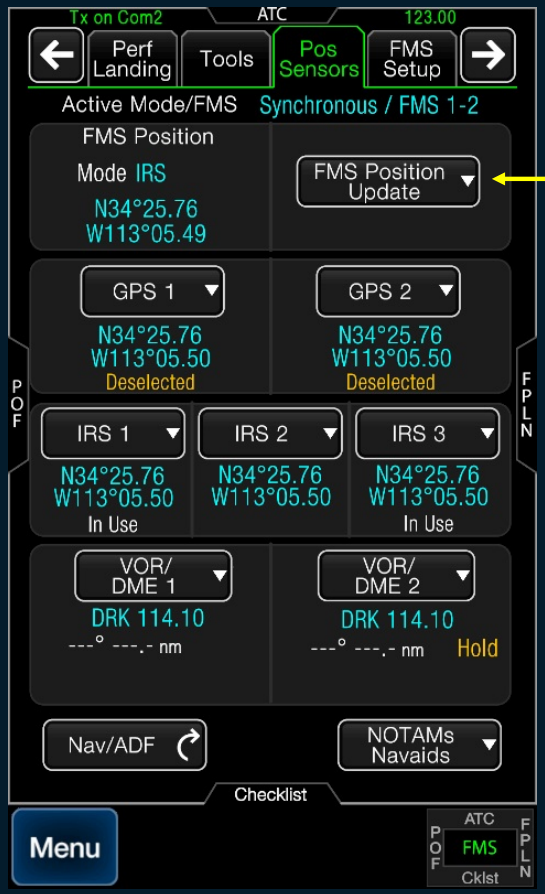
FMS/Pos Sensors/IRS 1

IRS Only Navigation

Miles from FMS Position

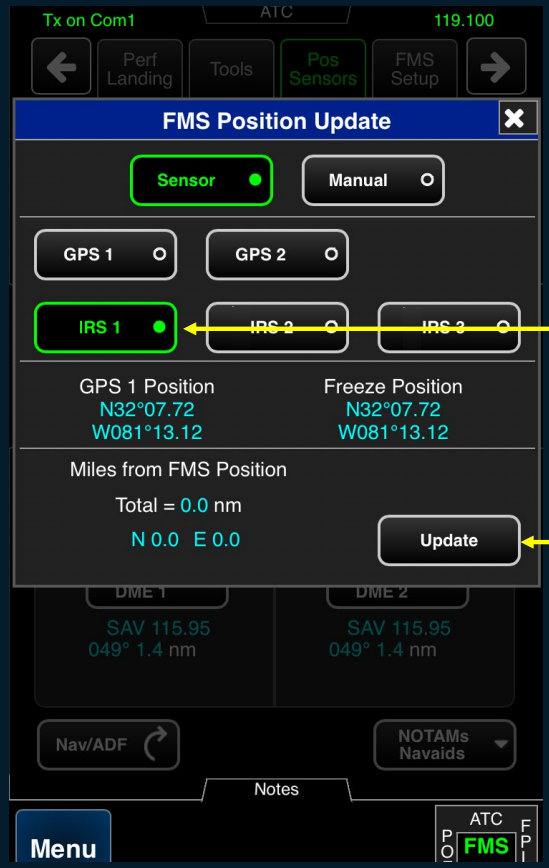
* *If greater than 5 NM: Perform a position update**

HOW TO PERFORM A POSITION UPDATE



FMS/Pos Sensors/FMS Position Update

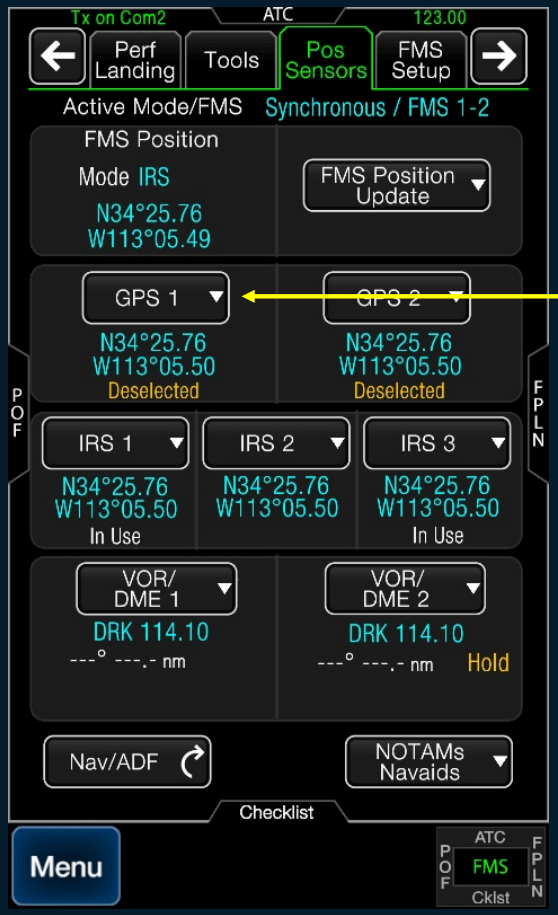
HOW TO PERFORM A POSITION UPDATE



Select IRS 1

Press Update, Continue flight

MONITOR GPS INFORMATION

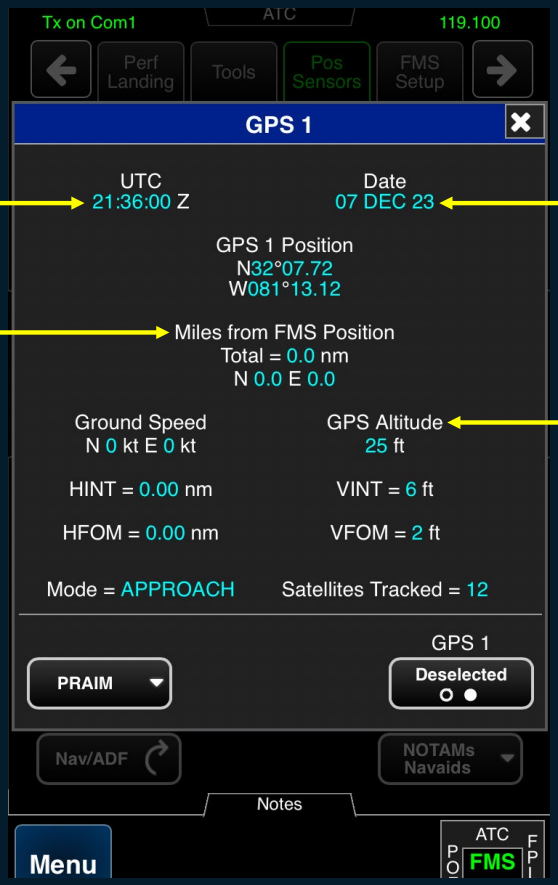


FMS/Pos Sensors/GPS 1

MONITOR GPS INFORMATION

GPS time

Miles from FMS position



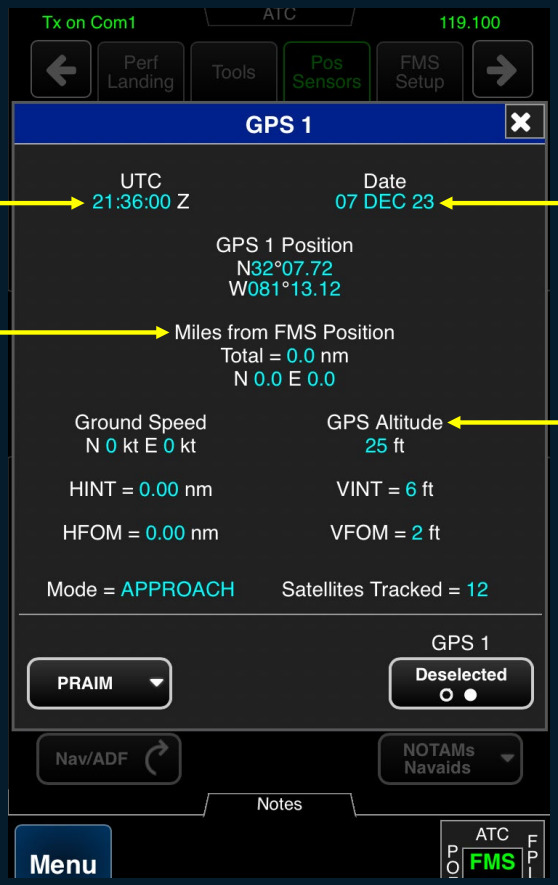
GPS date

GPS altitude

HOW TO KNOW WHEN SPOOFING HAS ENDED

GPS time returns to normal

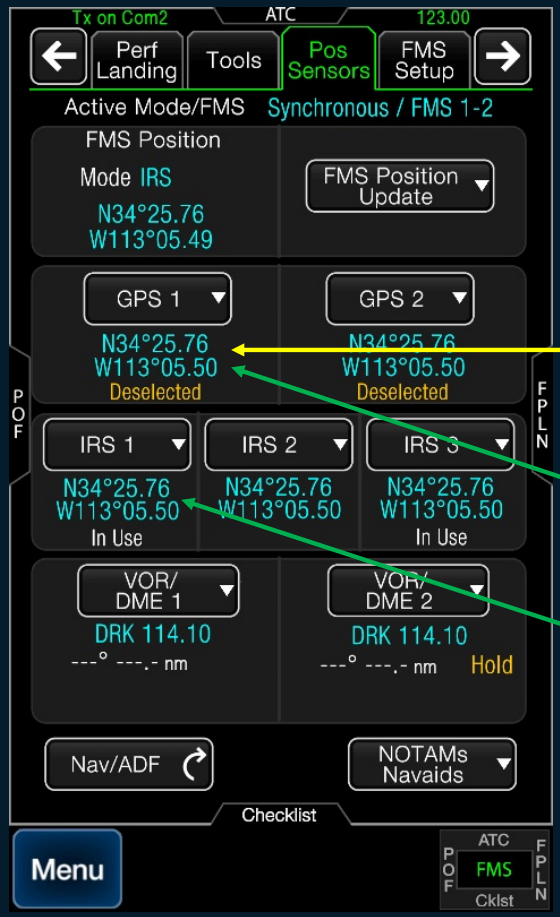
Only a small error from FMS position



GPS date returns to normal

GPS altitude returns to normal

HOW TO KNOW WHEN SPOOFING HAS ENDED



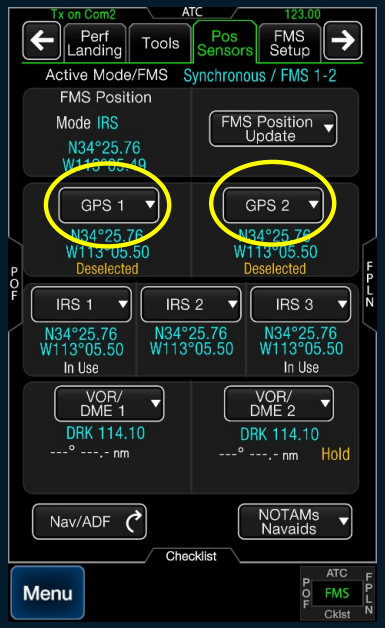
Normally GPS Spoofing causes GPS position to stop moving

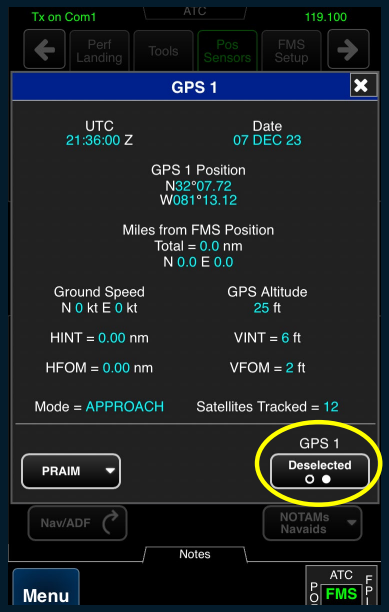
Once GPS position starts moving again, the spoof is probably over

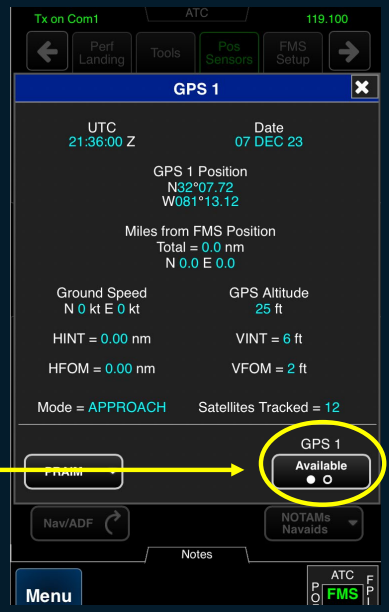
Once IRS position becomes close to the GPS position, the spoof is probably over

AFTER EXITING SPOOFING/JAMMING

Reselect GPS 1 AND GPS 2 (FMS/Pos Sensors/GPS 1-2)

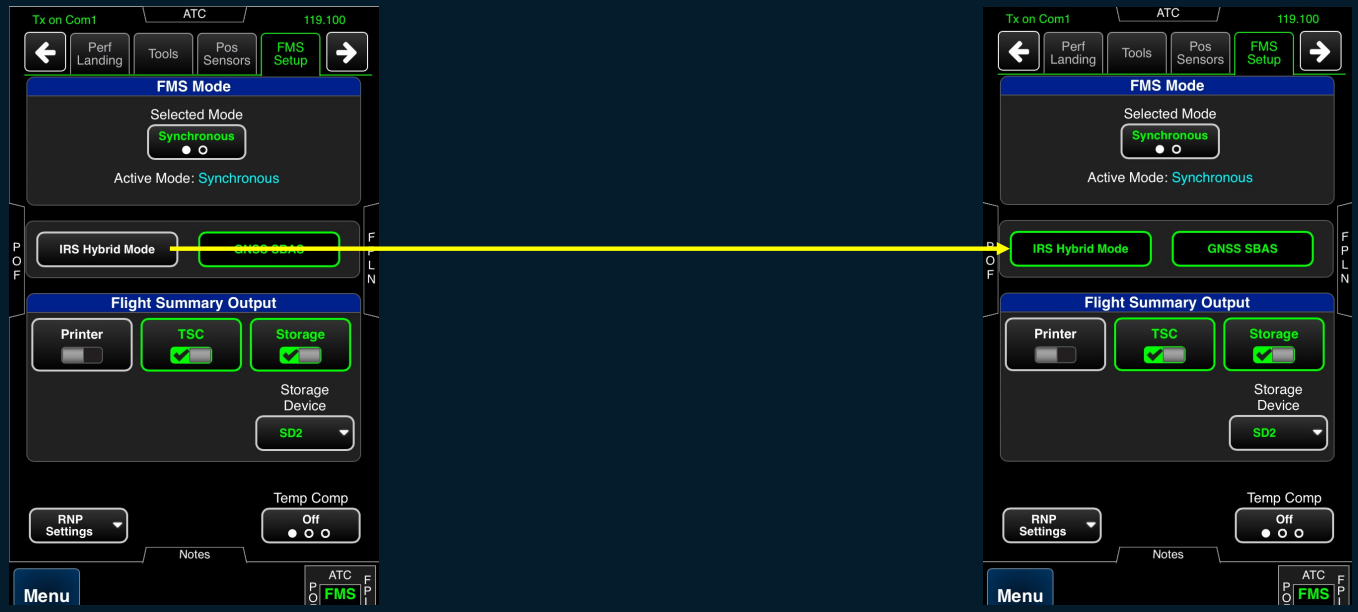






AFTER EXITING SPOOFING/JAMMING

Reselect IRS Hybrid Mode (FMS/FMS Setup)

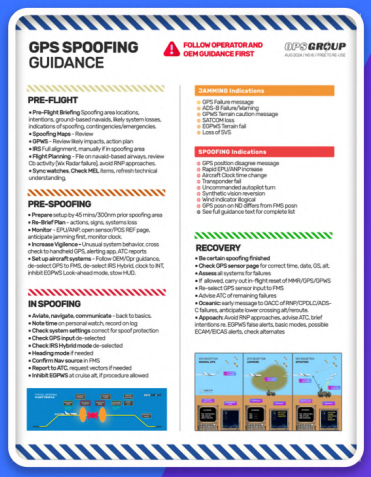


Transition back to normal FMS navigation operations

QUESTIONS

Crew Guidance

GPS SPOOFING



- Best practices for spoofing regions
- Actions before, during and after spoofing
- Typical spoofing flight profile

OPS GROUP

Extract from the report of the
GPS Spoofing WorkGroup 2024

GPS SPOOFING GUIDANCE

FOLLOW OPERATOR AND OEM GUIDANCE FIRST

OPS GROUP

AUG 2024 / NO © / FREE TO RE-USE

PRE-FLIGHT

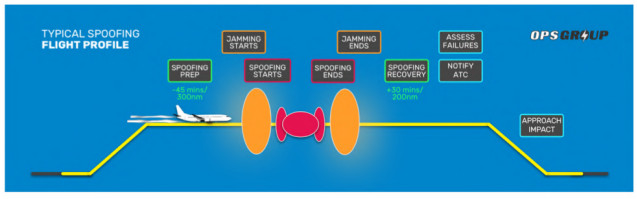
- **Pre-Flight Briefing** Spoofing area locations, intentions, ground-based navaids, likely system losses, indications of spoofing, contingencies/emergencies.
- **Spoofing Maps** - Review
- **GPWS** - Review likely impacts, action plan
- **IRS** Full alignment, manually if in spoofing area
- **Flight Planning** - File on navaid-based airways, review Cb activity (Wx Radar failure), avoid RNP approaches.
- **Sync watches, Check MEL** items, refresh technical understanding,

PRE-SPOOFING

- **Prepare** setup by **45 mins/300nm** prior spoofing area
- **Re-Brief Plan** - actions, signs, systems loss
- **Monitor** - EPU/ANP, open sensor/POS REF page, anticipate jamming first, monitor clock.
- **Increase Vigilence -** Unusual system behavior, cross check to handheld GPS, alerting app, ATC reports
- **Set up aircraft systems** - Follow OEM/Opr guidance, de-select GPS to FMS, de-select IRS Hybrid, clock to INT, inhibit EGPWS Look-ahead mode, stow HUD.

IN SPOOFING

- **Aviate, navigate, communicate** - back to basics.
- **Note time** on personal watch, record on log
- **Check system settings** correct for spoof protection
- **Check GPS input** de-selected
- **Check IRS Hybrid mode** de-selected
- **Heading mode** if needed
- **Confirm Nav source** in FMS
- **Report to ATC**, request vectors if needed
- **Inhibit EGPWS** at cruise alt, if procedure allowed



JAMMING Indications

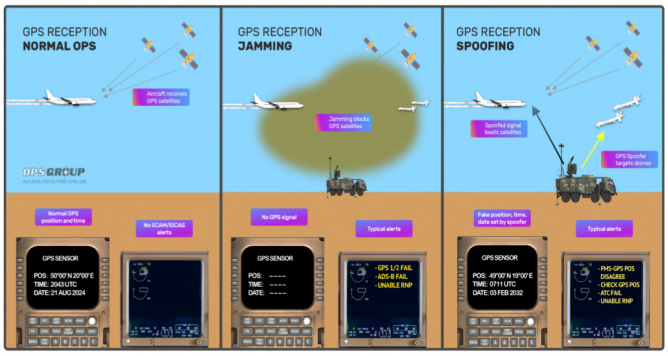
- GPS Failure message
- ADS-B Failure/Warning
- GPWS Terrain caution message
- SATCOM loss
- EGPWS Terrain fail
- Loss of SVS

SPOOFING Indications

- GPS position disagree message
- Rapid EPU/ANP increase
- Aircraft Clock time change
- Transponder fail
- Uncommanded autopilot turn
- Synthetic vision reversion
- Wind indicator illogical
- GPS posn on ND differs from FMS posn
- See full guidance text for complete list

RECOVERY

- **Be certain spoofing finished**
- **Check GPS sensor page** for correct time, date, GS, alt.
- **Assess** all systems for failures
- If allowed, carry out in-flight reset of MMR/GPS/GPWS
- Re-select GPS sensor input to FMS
- Advise ATC of remaining failures
- **Oceanic:** early message to OACC of RNP/CPDLC/ADS-C failures, anticipate lower crossing alt/reroute.
- **Appoach:** Avoid RNP approaches, advise ATC, brief intentions re. EGPWS false alerts, basic modes, possible ECAM/EICAS alerts, check alternates

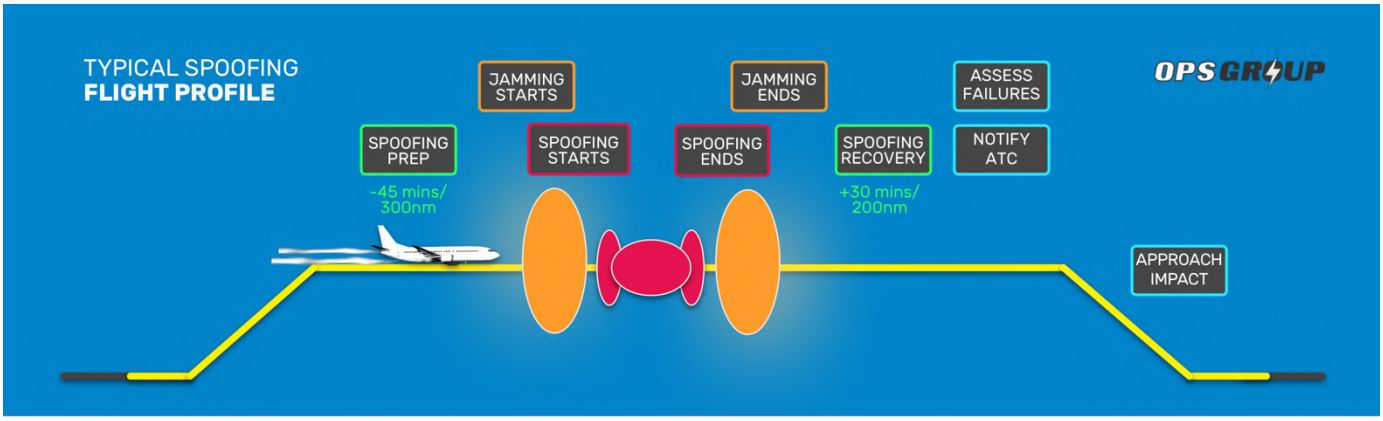


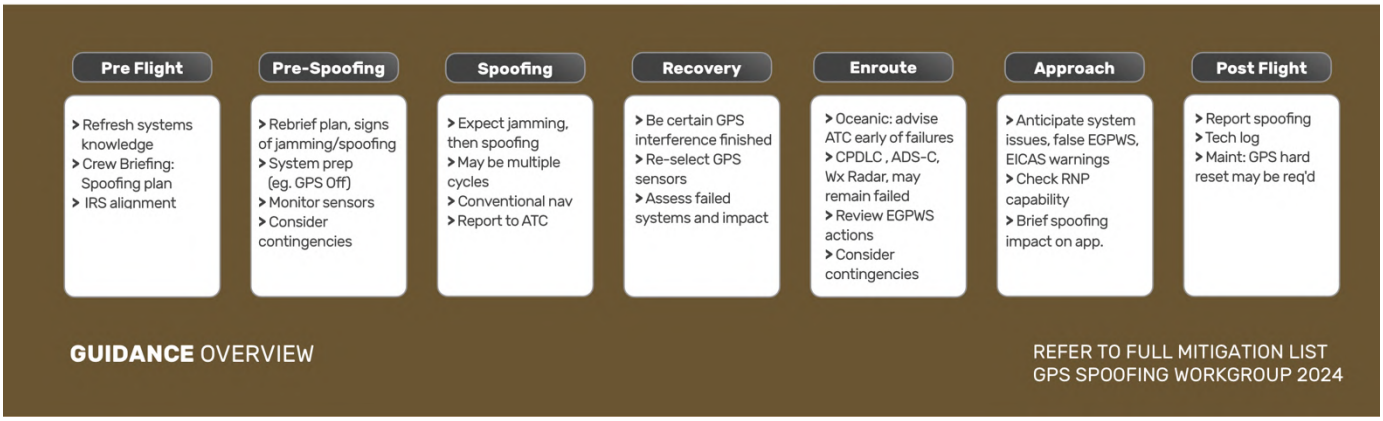
Crew Guidance

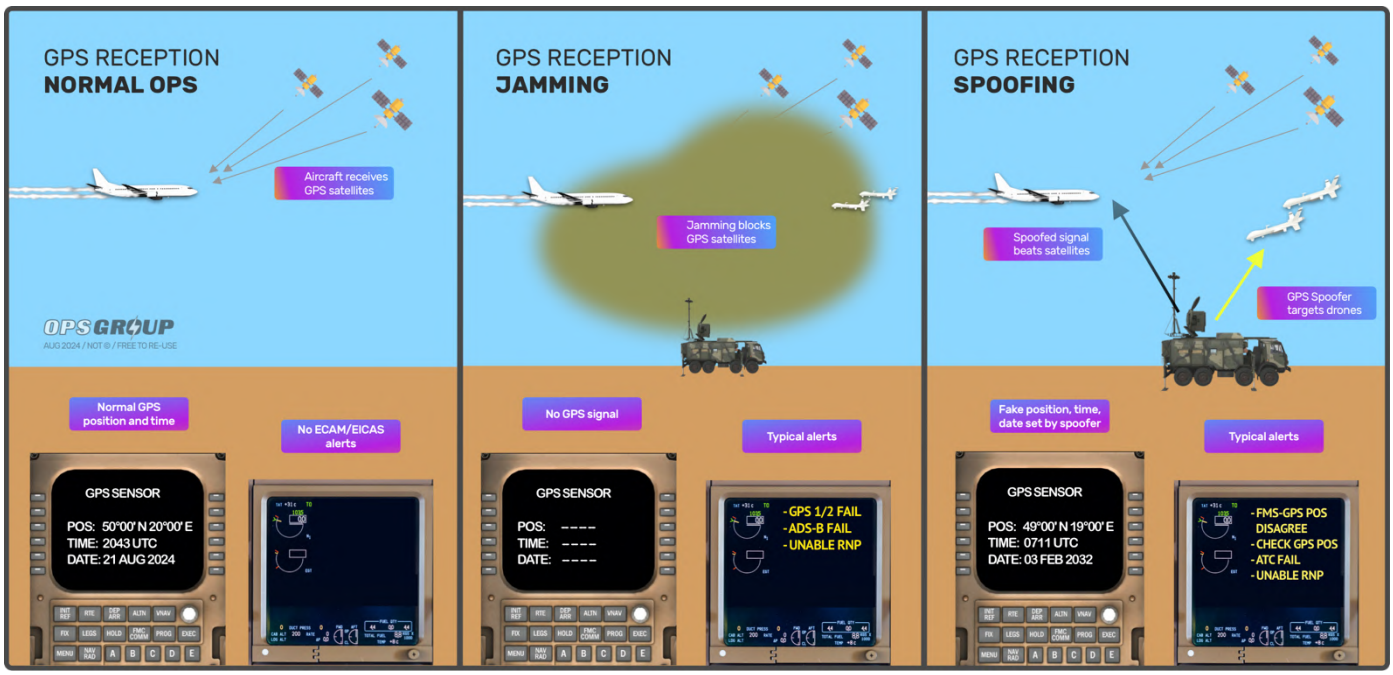
If you are operating a flight into a spoofing area **tomorrow**, this guidance will help to mitigate the impact of GPS Spoofing.

This is based on best practices collected from the flight crew participating in the GPS Spoofing Workgroup, as well as OEM and other expert input.

Nothing here is intended to replace or override company procedures, OEM advice, or legal requirements.


TYPICAL SPOOFING
FLIGHT PROFILE
OPSGROUP
JAMMING STARTS
JAMMING ENDS
ASSESS FAILURES
SPOOFING PREP
SPOOFING STARTS
SPOOFING ENDS
SPOOFING RECOVERY
NOTIFY ATC
-45 mins/ 300nm
+30 mins/ 200nm
APPROACH IMPACT


Pre Flight
> Refresh systems knowledge
> Crew Briefing: Spoofing plan
> IRS alignment
Pre-Spoofing
> Rebrief plan, signs of jamming/spoofing
> System prep (eg. GPS Off)
> Monitor sensors
> Consider contingencies
Spoofing
> Expect jamming, then spoofing
> May be multiple cycles
> Conventional nav
> Report to ATC
Recovery
> Be certain GPS interference finished
> Re-select GPS sensors
> Assess failed systems and impact
Enroute
> Oceanic: advise ATC early of failures
> CPDLC , ADS-C, Wx Radar, may remain failed
> Review EGPWS actions
> Consider contingencies
Approach
> Anticipate system issues, false EGPWS, EICAS warnings
> Check RNP capability
> Brief spoofing impact on app.
Post Flight
> Report spoofing
> Tech log
> Maint: GPS hard reset may be req'd
GUIDANCE OVERVIEW
REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024


GPS RECEPTION
NORMAL OPS
Aircraft receives GPS satellites
OPSGROUP
AUG 2024 / NOT © / FREE TO RE-USE
Normal GPS position and time
No ECAM/EICAS alerts
GPS SENSOR
POS: 50°00' N 20°00' E
TIME: 2043 UTC
DATE: 21 AUG 2024
GPS RECEPTION
JAMMING
Jamming blocks GPS satellites
No GPS signal
Typical alerts
GPS SENSOR
POS: ----
TIME: ----
DATE: ----
- GPS 1/2 FAIL
- ADS-B FAIL
- UNABLE RNP
GPS RECEPTION
SPOOFING
Spoofed signal beats satellites
GPS Spoofer targets drones
Fake position, time, date set by spoofer
Typical alerts
GPS SENSOR
POS: 49°00' N 19°00' E
TIME: 0711 UTC
DATE: 03 FEB 2032
- FMS-GPS POS DISAGREE
- CHECK GPS POS
- ATC FAIL
- UNABLE RNP

Pre Flight

Pre-Flight Briefing

For flights into known spoofing areas, include GPS Spoofing as a full briefing item. Consider:

- Likely entry and exit points of spoofing areas
- Intentions before, during, and after spoofing
- Availability of ground-based Navaids
- Likely system downgrades/losses (e.g. EGPWS, Weather radar, CPDLC, RNP)
- Expected indications of jamming, indications of spoofing
- Contingency planning (e.g. Engine failure, depressurization) in spoofing area
- Impact of spoofing on RNP requirements later in flight

Spoofing Maps

Check online spoofing map for latest locations of active spoofing. Knowing where the spoofing is happening is the best mitigation. (e.g. SkAI Live GPS Spoofing Tracker Map)

GPWS

Specifically review likely EGPWS impact, brief actions for EGPWS alerts in cruise, use of Terrain Override, EGPWS alerts on approach below MSA. Plan action in case of repeated EGPWS alerts on second approach in case of EGPWS response. Review difference between basic GPWS alerts and enhanced/Look-Ahead alerts. Be fully prepared for unusual EGPWS behavior.

IRS

Perform a full IRS Alignment for each flight into known spoofing areas. If departing from an airport within a spoofing area (e.g., LCLK, LLBG, OLBA), perform manual IRS alignment. Caution risk of IRS automatically taking GPS position.

Flight Planning

If practical, file airways associated with ground based navaids. Review GPS required routes, RNP-1 or -2 airways. Consider alternate routes further from the spoofing area. Review forecasted Cb activity, considering Weather Radar failure is possible. Consider if destination requires RNP approaches.

Contingencies/Emergencies

Consider the impact of spoofing on a diversion while in the spoofing area, or afterwards. Conventional arrival and approach / missed available or daylight VMC from MSA down. Review safe altitudes enroute (MEA/MORA) and at destination/alternate on approach (MSA).

Refresh Technical Understanding

Review difference between GPS Spoofing and GPS Jamming. Know which aircraft systems use GPS (long list!). Loss of ADS-B, SVS, GPWS etc. is not possible to be avoided. Refresh conventional navigation skills, be aware that most enroute airspace isn't actually RNP airspace. Spoofing takes place in areas with low Navaid coverage - may be many hundreds of miles between DMEs and VORs. Understand difference between Conventional/Standalone IRS and Hybrid IRS (B787, G650 etc.).

Synch watches

Synch mechanical watch to known source (e.g. iPhone) at dispatch, in preparation for aircraft clock failure.

NO-TAMS

Don't rely purely on NOTAMs to give comprehensive warnings of spoofing locations.

Crosscheck MEL items

Consider the impact of any MEL (Minimum Equipment List) items. Review impact of unserviceable system items in light of expected GPS Spoofing impacts, especially any inoperative radio navigation items.

Operations at airports WITHIN spoofing areas

- Expect on-ground spoofing, which creates greater risk of system impacts
- **IRS Alignment**: Turn off the GPS receiver via the FMC prior to aligning the IRS, and carry out a manual alignment. Be vigilant for automatic capturing of the spoofed GPS position during alignment.
- Do not plan GPS/RNP approaches, SIDs, STARs, into/out of known spoofing areas

Pre-Spoofing

Prepare for spoofing

Commence preparation and system setup well prior to first expected spoofing location. **Spoofing area ETA -45 minutes, or 300 nm is suggested**.

- Consider declining direct routings to remain on airway, especially if airway is based on Navaids.
- Evaluate emergency descent and diversion options with regard to spoofing impact on systems

Re-Brief plan

A quick re-brief of actions when spoofing is encountered. Intentions, and expected systems loss, e.g. ADS-B, CPDLC. Re-brief EGPWS actions in event of alert in cruise.

Monitor

Monitor EPU (Estimated Position Uncertainty) and ANP (Actual Navigation Performance) values. Open Sensor/Pos Ref page for GPS status. Anticipate jamming to commence before spoofing: the typical spoofing encounter now commences with a period of GPS jamming, which makes the GPS receiver more vulnerable to spoofing. Monitor aircraft clock for jumps or changes.

Increase vigilance

- Keep an eye on all aircraft systems for unusual behavior.
- Monitor aircraft position and navigation system status using all available means, including use of a handheld GPS e.g. Bad Elf, Garmin, iPad/iPhone, EFB. Keep the antenna of the external GPS system in sight of satellites but as shielded from the

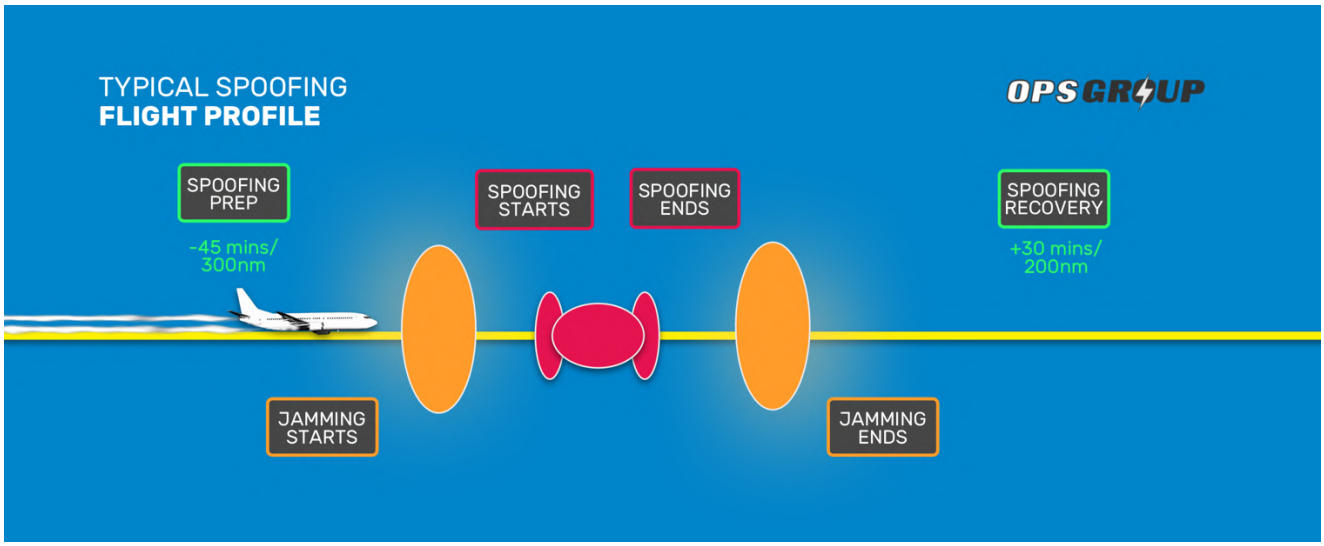
horizon as possible, using glareshield or aircraft frame. Any disagreement between aircraft GPS and external GPS will suggest spoofing.

- Use an alerting App such as APG's NaviGuard. Regularly cross-check aircraft system indications to standalone systems (e.g. Watch, VOR/DME position, EFB/External GPS) to detect spoofing early.
- Listen out for ATC or other aircraft reports of spoofing
- Be ready to apply systems setup as soon as typical initial warnings occur, in case of surprise/early spoofing encounter.
- Have Nav Log (OFP/CFP) tracks, times, distances ready to assist with manual/DR navigation.
- Keep an eye on GPS date (in sensors page). A date change is a strong indicator of likely problems recovering the GPS receiver post-spoofing.

Set up aircraft systems

- Always follow OEM and Operator Procedure as primary spoofing setup guidance.
- **De-select GPS input to FMS**. Note that this will only prevent the FMS position from including spoofed GPS values, but will not protect other systems e.g. EGPWS, Weather Radar.
- **Deselect** "**IRS HYBRID**" **mode** if applicable.
- **Set the aircraft clock to** "**Internal**" **(INT)** / manual, if possible, to protect CPDLC and other datalink functions.
- If procedure approved - **Inhibit EGPWS Look Ahead mode** to prevent false alerts at cruise altitude.
- Stow **Head Up Display** and do not use.

Within Spoofing Area



Typical indications of Jamming

It is common for jamming to precede spoofing. Jamming will result in the loss of GPS Signal only. The time from jamming to spoofing varies.

- **GPS Failure message**
- **ADS-B Failure/Warning**
- **GPWS Terrain caution message**
- **Loss of Ka SATCOM**
- **EGPWS Terrain fail**
- **Loss of SVS**

Typical indications of Spoofing

Unlike jamming, a GPS signal is present, but it has fake information. False GPS position, time, and date information will be processed by the GPS receiver as being valid. As soon as this is fed to other systems, failure messages will begin.

- **Rapid EPU or ANP increase**
- **GPS position** and IRS or FMS position disagree caution message
- **Aircraft Clock time changes**, or difference between Capt/FO clocks
- **Transponder failure**: EICAS/ECAM "ATC FAIL"
- **Autopilot turns aircraft unexpectedly**
- **ADS-B Failure/Warning**
- **Synthetic Vision** reverting to blue over brown
- **Loss of enhanced display**, such as display of terrain on PDI
- **Wind indication** on ND is illogical or has a major shift - erratic groundspeed
- **GPS position symbol** on ND drifts away from the FMS and the IRS symbols
- **Datalink** (CPDLC, ADS-C) failure warning
- **GPS information on sensor page** shows unusual values: altitude, etc.
- **Handheld GPS** (e.g. Garmin, iPad) **disagrees** with aircraft GPS position
- **EGPWS** audible warning ('Pull Up")
- **GPS 1 and 2 dramatically different** i.e. more than 100 meters, which may also give an ECAM/EICAS GPS miscompare warning.
- **Spoofing Alerting app** e.g. Naviguard gives alert
- **ACARS message** from ground/ops advises of spoofing (based on aircraft downlink message with unusual values).

Actions following confirmation of active spoofing

- **Aviate, navigate, communicate** – back to basics.
- Note the time on personal watch, record on log.
- Check system settings are correct for spoofing protection. Also applies to unexpected "surprise spoofing".
- **Check GPS input de-selected**
- **Check IRS Hybrid mode de-selected**
- **Heading mode**: Consider selecting heading mode to keep the aircraft on track during troubleshooting
- Confirm Nav Source in FMS: DME/DME, IRS, etc.
- **Report to ATC**. Advise ATC of spoofing encounter ASAP. Include position so that other crew on frequency are aware.
- **Request ATC vectors** or confirmation of correct position and track if required.

- If company procedures allow, **inhibit EGPWS at cruise altitude** (TERR OVRD). This avoids false "PULL UP" etc. warnings triggered by spoofed altitude data.
- Use **Conventional Navigation**
- Check Aircraft Clock Time and compare to current time.
- Check **GPS Date** on sensors page. A change of date, especially forward in time, is likely to create greater GPS receiver problems after spoofing.
- **FMS Auto-tune** may not function correctly (uses GPS to check Navaid position).
- **Set reminders** based on waypoint or coordinates (not time) to reverse all system settings changed for spoofing.

Recovery

Most spoofing encounters can be fully recovered from in flight. However, an increasing number of aircraft are left with severe impacts to navigation, communications, and safety systems (e.g. EGPWS) that are not recoverable before reaching destination.

Before beginning recovery, be certain that spoofing has finished. Double check known spoofing location map, and be alert to the possibility that another round of spoofing may occur. Allow a time period of normal GPS readings, e.g. 10 minutes.

Indications that spoofing is complete

The following items may be helpful to identify the end of GPS Spoofing:

On Sensors/Pos Ref page, GPS shows:

- Correct UTC time and date, **and**
- GS (Ground Speed) consistent with TAS, ND, **and**
- Consistent position and altitude

Actions after exiting spoofing area

- **Re-select GPS** sensor input to FMS
- **Assess** all systems for failures, especially Weather Radar, CPDLC/Datalink,
- If required, and if procedure exists/allows, carry out **in-flight reset of MMR/GPS Receiver**
- If required, and if procedure exists/allows, carry out **in-flight reset of GPWS computer**

ATC

- Advise ATC of any relevant systems remaining failed, e.g. Nav, CPDLC, ADS-C and impact on navigation (e.g. Unable RNP)
- Disregard any CPDLC mandate for domestic FIR's – airspace entry will not be denied.
- **If planning an oceanic crossing** with degraded RNP or Comms systems, advise the first oceanic ACC well before Oceanic Entry. For example, Shanwick requests a freetext remark in the RCL message at OEP -90, "RMK/RNP 10 ONLY DUE GPS INTERFERENCE / NO CPDLC"
- **For the NAT HLA**, note that RNP4 is required for PBCS tracks, as well as CPDLC and ADS-C for the RCP/RSP requirement. Elsewhere in the HLA, RNP 10 is the minimum, but RNP4 is often used for tactical separation outside the NAT PBCS Tracks. If you are RNP10 only, **expect lower crossing altitudes and reroutes**.
- Request to follow STARs (/SIDs) based on conventional navaids.
- Avoid/decline RNP approaches.

Destination/Alternate Approach considerations

- **Even if the GPS receiver appears normal** after spoofing, there is a risk of later failure or incorrect behavior. This is because the spoofing may have contaminated the receiver settings. In most cases, only a hard reset will guarantee receiver integrity.
- **Avoid RNP approaches** unless there is certainty that all systems are operating normally. Check missed approach for any RNP/RNAV requirement.
- **Advise ATC** of your earlier GPS interference, e.g. "Due to earlier GPS interference, unable xxx approach, request xxx approach". This will also give ATC a heads-up to monitor your tracking more closely.
- **Brief intentions re. GPWS responses.** Expect false EGPWS alerts, but re-brief to be clear on difference between GPWS basic mode alerts (Radio Altimeter based) and EGPWS alerts (GPS altitude based). Ensure all basic GPWS mode alerts are followed without delay, as these are not affected by spoofing. Brief intentions for different alert types.

- **Brief possible ECAM/EICAS alerts** on descent and approach, especially ones that may occur on final approach but can be disregarded, e.g. RNP related warnings.

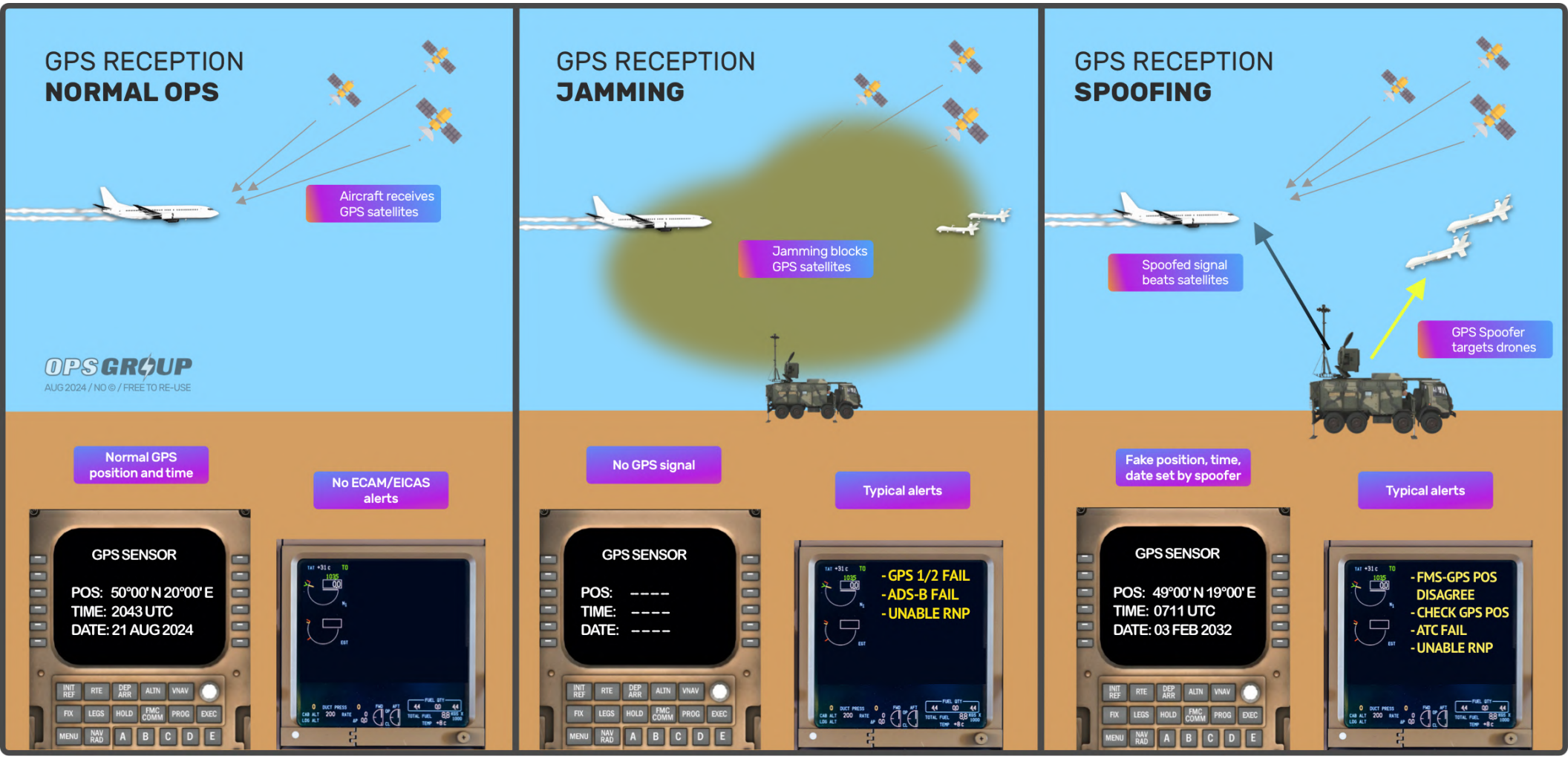
- **Check alternate** non-GPS approach availability.

Post Flight

- **File an Air Safety Report** for tracking of the GPS Spoofing problem.

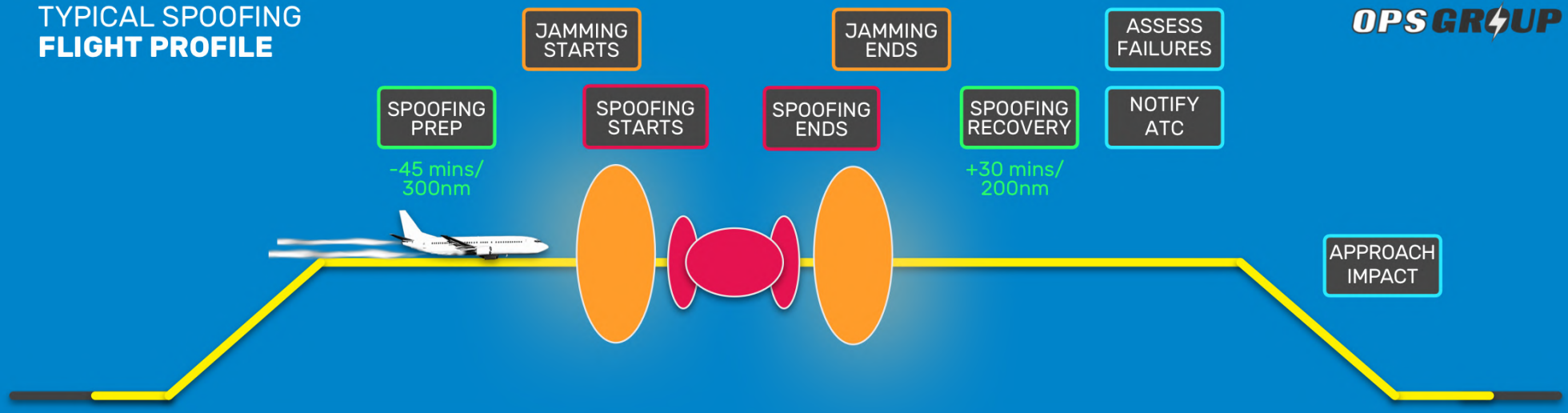
- **Tech Log:** Note any GPS Spoofing in the aircraft tech log each flight, to ensure a hard reset of the GPS / MMR is carried out

- For any unusual system impacts, send data to avionics manufacturers e.g. Honeywell, Collins.


GPS RECEPTION
NORMAL OPS
Aircraft receives GPS satellites
OPS GROUP
AUG 2024 / NO © / FREE TO RE-USE
Normal GPS position and time
No ECAM/EICAS alerts
GPS SENSOR
POS: 50°00' N 20°00' E
TIME: 2043 UTC
DATE: 21 AUG 2024
GPS RECEPTION
JAMMING
Jamming blocks GPS satellites
No GPS signal
Typical alerts
GPS SENSOR
POS: ----
TIME: ----
DATE: ----
- GPS 1/2 FAIL
- ADS-B FAIL
- UNABLE RNP
GPS RECEPTION
SPOOFING
Spoofed signal beats satellites
GPS Spoofer targets drones
Fake position, time, date set by spoofer
Typical alerts
GPS SENSOR
POS: 49°00' N 19°00' E
TIME: 0711 UTC
DATE: 03 FEB 2032
- FMS-GPS POS DISAGREE
- CHECK GPS POS
- ATC FAIL
- UNABLE RNP

TYPICAL SPOOFING **FLIGHT PROFILE**

OPSGROUP



Pre Flight

- Refresh systems knowledge
- Crew Briefing: Spoofing plan
- IRS alignment

Pre-Spoofing

- Rebrief plan, signs of jamming/spoofing
- System prep (eg. GPS Off)
- Monitor sensors
- Consider contingencies

Spoofing

- Expect jamming, then spoofing
- May be multiple cycles
- Conventional nav
- Report to ATC

Recovery

- Be certain GPS interference finished
- Re-select GPS sensors
- Assess failed systems and impact

Enroute

- Oceanic: advise ATC early of failures
- CPDLC , ADS-C, Wx Radar, may remain failed
- Review EGPWS actions
- Consider contingencies

Approach

- Anticipate system issues, false EGPWS, EICAS warnings
- Check RNP capability
- Brief spoofing impact on app.

Post Flight

- Report spoofing
- Tech log
- Maint: GPS hard reset may be req'd

GUIDANCE OVERVIEW

REFER TO FULL MITIGATION LIST
GPS SPOOFING WORKGROUP 2024