GNSS and your Cyber Security Strategy

GNSS is a Critical part of Cyber Security Strategy

APPLICATION NOTE

Operational Technology (OT) across all sectors is increasingly complex and reliant on accurate timing and synchronisation to operate. This synchronisation can be either within a single site or across a wide network of equipment regionally or nationally. Most time and synchronisation systems rely on signals from Global Navigation Satellite Systems (GNSS) such as GPS or GLONASS. Disruption of these signals either deliberately or accidently can have a significant impact on OT. The protection and hardening of OT infrastructures should therefore be part of an organisation's overall Cyber Security strategy.

Chronos has unrivalled industry experience gathered over more than 30 years of designing, supplying, installing, commissioning & supporting GNSS systems for timing & navigation applications. We are trusted as experts by our customers across Finance, Power, Broadcasting, Aerospace, Telecom, Defence & Security and Manufacturing. We have used this experience to design a range of audit services that focus on the vulnerabilities of OT to GNSS denial or interference. By using these services and hardening the synchronisation and timing elements of an OT system an organisation will ensure this element of the operation is secure even under accidental or deliberate attack.

GNSS signals are very low power by design. The satellites have to run on minimal power and are in orbit 20,000 km from the earth. The signals from the constellations are based on a timing pulse taken from atomic clocks on board the satellites and co-ordinated by an earth-based control infrastructure. These signals are directly traceable to UTC – the world's reference timescale. The power levels of the signals and open nature of the communication leaves them susceptible to disruption through spoofing and jamming.

Benefits:

- Fully understand your organisations use of time and synchronisation
- Define the critical applications that use time and the accuracy they need and impact of disruption
- Complete active testing to identify any vulnerabilities
- Implement mitigation strategies based on the results from active testing

GNSS jamming is somewhat easier to detect than spoofing as it results in the complete loss or absence of the original radio signal and is relatively easy to detect in the GNSS receiver itself. Spoofing however can be much more troublesome to identify. The intention of spoofing the GNSS signal is to create a copy or a clone of the signal that appears authentic to a GNSS receiver. Depending on the level of sophistication employed by the attacker some spoofed signals can be almost impossible to differentiate from the original. Having complete

GNSS is a Critical part of Cyber Security Strategy

APPLICATION NOTE

control over the spoofing of a signal an adversary could very subtlety alter timing or location information which could over time be enough to cause failures and malfunctions in those systems reliant on GNSS.

If an attacker intends to cause disruption to OT systems then small & subtle timing errors could be slowly introduced in way that could defeat spoofing-detection algorithms and introduce possible points of failure in those networks. A coordinated attack over multiple geographic locations could cause catastrophic failures due to timing differences between multiple sites exceeding design limits.

OT infrastructures should be capable of monitoring GNSS signals, identifying disrupted data and responding with mitigating actions that ensures the OT environment continues to operate with a level of timing and synchronisation accuracy suitable for its guaranteed operation. Mitigation strategies will depend on the OT environment, requirements for sync and timing, how long the OT will function without the required sync and timing and the level of risk the organisation is prepared to take on continued operation.

Infrastructure Suitability

Any OT infrastructure that uses timing and synchronisation could be a target for GNSS disruption. Chronos services are suitable for any such environment with maybe particular relevance to:

- Critical National Infrastructure such as Power, Broadcast, Finance, Telecoms, Government
- Industrial infrastructures where timing and sync distortion could lead to expensive and lengthy outages
- Infrastructures where Safety of life risks increase due to failure

The technologies involved in these examples are likely to include GNSS receivers, grandmasters, PTP and NTP clocks, IP networking and probably multi-site (or multinational) operations