CHRONOSec™ Cyber Security Audits

GNSS is a Critical part of your Cyber Security Strategy

DATASHEET

Disruption of GNSS signals can have a significant impact on synchronisation and timing within Operational Technology (OT). It is therefore critical that organisations have in place, within an overall Cyber Security strategy, monitoring and mitigation plans to ensure continued operation under accidental or deliberate GNSS disruption.

Chronos has developed our CHRONOSec™ services to help organisations build such strategies and plans. The principles of CHRONOSec™ are based on our understanding of the complexities of a wide range of technologies and an appreciation of the impact of OT disruption on individual organisations

The service is based on the following framework:

- Detailed design audit looking at accuracy requirements, how time is obtained, distributed and consumed in the user's application, focusing on all diverse and independent sources of time for redundancy and resilience
- Threat modelling looking at possible attack vectors or scenarios that may be used to disrupt the timing infrastructure of the user's networks. This can also include monitoring and recording the GPS signals received.
- Stress-testing using state of the art GNSS simulation & test equipment both live and lab-based
- Full report of test results, recommendations on securing and protecting time sources and designing and provisioning backup

The details of how these stages are delivered will vary with the environment and technologies in place and the availability of offline test units. These stages could be combined with network-based attempts to access GNSS management systems and/or combined with physical attack on the RF cabling to the GNSS antenna. In more details these stages include:

CHRONOSec™ Cyber Security Audit

GNSS is a Critical part of your Cyber Security Strategy

1. Planning and reconnaissance

- Define the scope and goals of the test, including the systems to be addressed and the testing methods to be used
- Gather intelligence (e.g. GNSS/PTP/NTP time servers etc.) to better understand how the target system has been designed and its potential vulnerabilities

2. Gaining Access and/or Trust

For timing systems this stage includes jamming and/or spoofing a GNSS signal that is used as a reference to control the clocks within the system.

The jamming and spoofing can be combined with optional network-based attacks to exploit vulnerabilities in the management systems used to control the network.

3. Maintaining access and or Trust

The goal of this stage is to see if the vulnerability can be used to achieve a persistent control of the time reference in the exploited system— long enough for an attacker to cause failure or prolonged outage.

4. Analysis

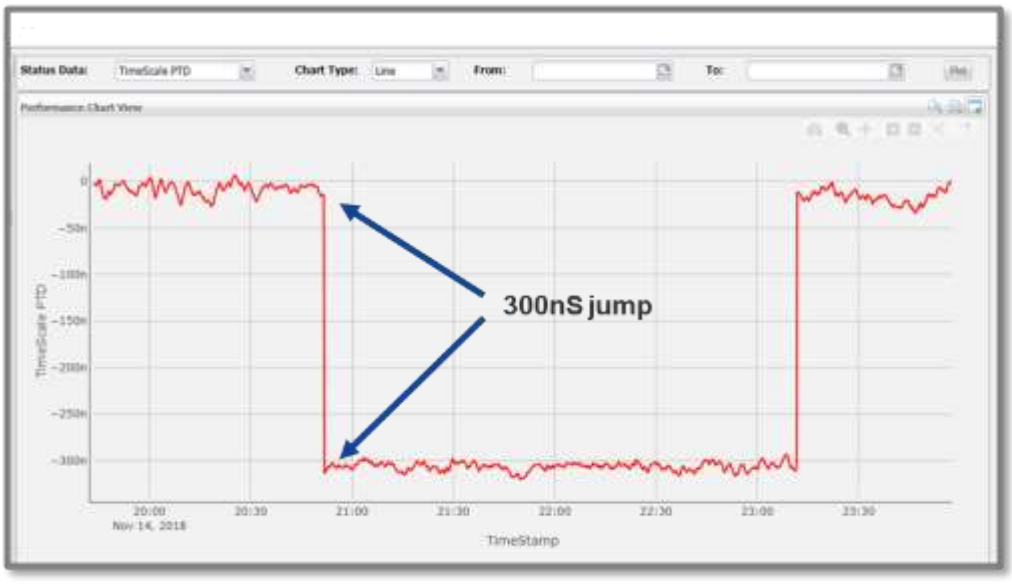
The results of the active tests are then compiled into a report which details:

- Specific vulnerabilities that were exposed and exploited
- Impact assessment on the user's application
- The amount of time the tester was able to remain in the system undetected

This information is analysed by security staff to help improve the user's resilience to attack and reliance on GNSS and other application security solutions to mitigate vulnerabilities and protect against possible future attacks.

These stages cannot be completed by our team in isolation. The OT owning organisation has to be actively involved throughout the process to ensure we understand the implications of any test or activity and both sides have a clear picture of results and threats. The final report will fully describe the state of either vulnerability or robustness of the sync and timing dependant systems within the overall OT infrastructure.

For more information please contact our Team who will be happy to help.



Live tracking shows a significant time deviation on the GPS signal – accidental or deliberate?

DATASHEET