TIME – THE INVISIBLE UTILITY

WHY IS TIME IMPORTANT?

Other It has been said that the world's most commonly asked question is "What time is it?" Accurate and resilient time is critical for sustaining nearly all modern organizations, yet many public and private sector organizations are unaware of their dependence on time. Without access to accurate and resilient time sources, critical functions (including cybersecurity, communications, and internet-connected devices) and critical services (including banking, utilities, and transportation) can become unreliable, inaccurate, or unavailable. Failure to properly manage time can have contractual or regulatory impacts.

SECTORS AND INDUSTRIES DEPENDENT ON TIME

Communications	Transportation	Power Grid	Finance	Security	IT
Telecommunication Cloud Operations Internet of Things (IoT)	Aviation Maritime Pipelines Rail	Frequency Monitoring Multi-rate Billing Fault Detection	Regulatory Requirements ATM Networks	Cryptography Access Control Forensics Surveillance	Smart Devices Incident Investigations

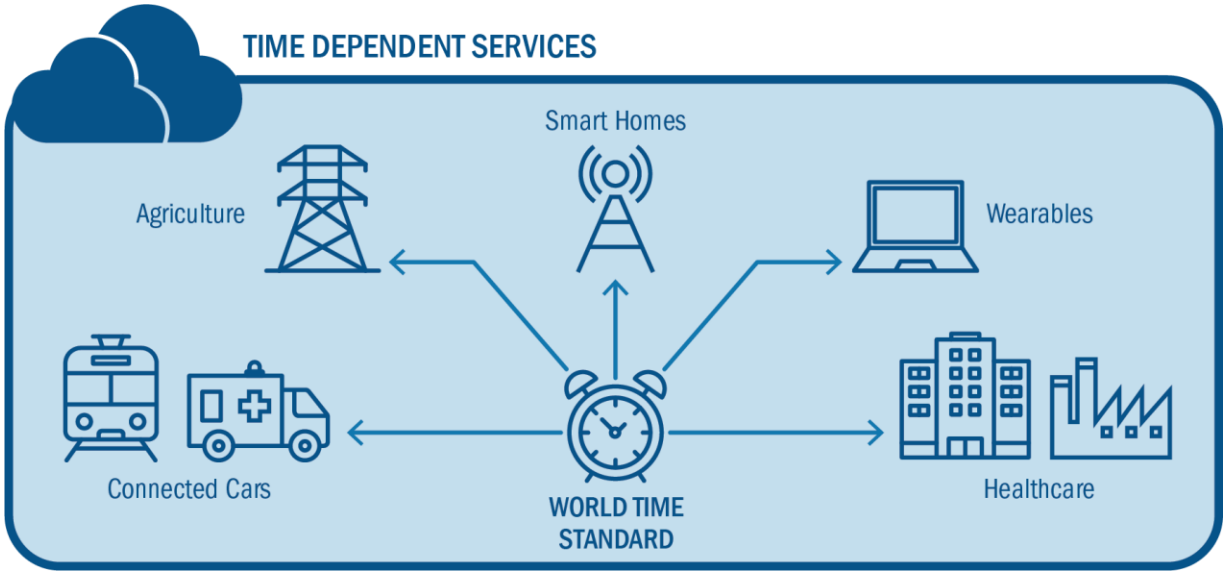
WHY IS IT "INVISIBLE"?

Organizations are typically unaware of who or what sets the time on their systems. They assume the time on their systems is correct, or perhaps "correct enough." They may have been right in the past, but as our systems grow in complexity, becoming global and mobile, proper timekeeping on our systems is becoming a necessity in both the private and public sectors worldwide. In the United States, the U.S. Naval Observatory (USNO) and the National Institute of Standards and Technology (NIST) are the principal sources of time.

WHY SHOULD YOU BE CONCERNED ABOUT TIME NOW?

GPS has become the de facto time standard for many commercial users because of its relatively low cost and ubiquitous availability. In 2017, 5.8 billion Global Navigation Satellite Systems (GNSS) devices, such as those using GPS, were in use. By 2020, this number is forecasted to increase to almost 8 billion—an estimate of more than one device per person on the planet.1 In 1997, the President's Commission on Critical Infrastructure Protection (PCCIP) identified dependence on the Global Positioning System (GPS) as a growing vulnerability within the United States Critical Infrastructure. Since that time, the use of GPS-dependent devices has grown significantly, increasing the risk to critical infrastructure.

[1] GNSS Market Report, Issue 5, copyright © European GNSS Agency, 2017, page 10. Retrieved from https://www.gsa.europa.eu/system/files/reports/gnss_mr_2017.pdf



Until recently, GPS devices were viewed simply as radio receivers. However, they are actually computers, with similar security risks. Threats include denial-of-service attacks (jamming) and the introduction of bad data into the system (spoofing). The advent of software-defined radios has increased the ease and lowered the cost with which these types of attacks can be launched. Efforts should be made to ensure accurate and resilient timing for your GPS devices.

Did you know?

- The week counter in GPS enables a system to supply the accurate date and time.
- Every 19 years, GPS's week counter must reset to zero? The next reset will occur on **April 6, 2019.**
- Guidance is available and you need to prepare **now** for the **April 6, 2019, GPS Week Number Rollover.**

WHAT CAN ORGANIZATIONAL LEADERS DO?

- Consider if your business would be impacted by inaccurate time.
- Determine how your business would be impacted by inaccurate time
- Determine level of time accuracy and resilience needed for your organization.
- Identify the source(s) of time used by your organization.
- Determine if your organization's time needs to be synchronized with external users.
- Based on your risk profile, assess if your current timing source, along with associated security and resiliency efforts, is appropriate
- If your organization depends on GPS as a time source, prepare for the upcoming GPS Week Number Rollover Event on April 6, 2019

GUIDANCE FOR THE GPS 2019 WEEK NUMBER ROLLOVER

- **Technical Slicksheet:** https://ics-cert.us-cert.gov/sites/default/files/documents/Technical-Level_Resilient_Timing_Overview-CISA_Fact_Sheet_508C.pdf
- https://ics-cert.us-cert.gov/Memorandum-US-Owners-and-Operators-Using-GPS-Obtain-UTC-Time

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to defend critical infrastructure against the threats of today, while working with partners across all levels of government and in the private sector to secure against the evolving risks of tomorrow.