INL/RPT-22-69090-Revision-0

The Role of Timing in Industrial Control Systems: A Primer

October 2022

Megan Mincemoyer Egan

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/RPT-22-69090-Revision-0

The Role of Timing in Industrial Control Systems: A Primer

Megan Mincemoyer Egan

October 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

The Role of Timing in Industrial Control Systems

A Primer

Summary

Accurate and synchronized time is an important dependency within an industrial control system. Manipulation or degradation of timing can result in varying impacts based on the critical infrastructure sector. As control systems continue to be digitized and automated, they require more precise timing elements which increases the potential impact of a cyber-attack on timing elements.

Timing Implementations

Network Time Protocol (NTP) is the most prevalent way to meet timing needs in an industrial network since its introduction in 1985. NTP can provide nominal accuracies within tens of milliseconds on wide area networks (WANs) or within sub milliseconds on local area networks (LANs).[1] NTP can be implemented using a client-server model or a peer-to-peer model for propagation through the network. Some industrial processes require Precision Time Protocol (PTP) for more precise timing; however, PTP is often derived from another time source such as NTP or Global Positioning System (GPS) before being converted into PTP.[2] PTP can provide accuracy to one microsecond. Although GPS timing is more precise, it is substantially more expensive to give each network node its own GPS receiver than it is to integrate one GPS receiver and use PTP to propagate the time through the network.[3]

Time requirements for industrial control systems (ICS) can be classified as either absolute, meaning devices require the exact time and date, or relative, meaning the exact time may or may not be accurate but must be consistent across all devices. Timing in ICS can be derived from several sources, including GPS or an atomic clock, such as those maintained by the U.S. National Institute of Standards and Technology (NIST). NTP requires network time servers established by organizations and companies across the world to ingest

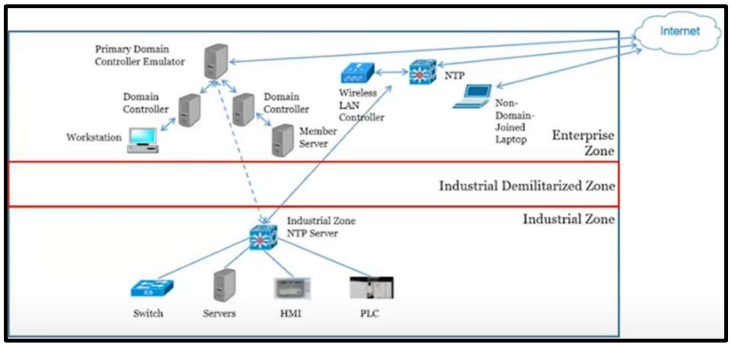

Figure 1- Typical Industrial Zone Time Architecture according to Jeff Shearer during the SANS ICS Security Summit talk "Killing Time" [2]

time from these original sources and make it available for systems requiring timing through requests. As of 2016, NIST received more than 16 billion time requests per day to its Internet Time Service.[4] Microsoft Windows also offers Windows Time Service which uses NTP algorithms to "select the best time source from the configured sources based on the computer's ability to synchronize with that time source."[5] Industrial environments can integrate time from any of these services to centralize at one or more NTP servers, which then propagate the time throughout the network. For segmented ICS networks, time is required to pass from the enterprise network through the industrial demilitarized zone for use in the industrial zone.[6]

Timing Impacts

According to a report from the U.S. Department of Homeland Security, the four critical infrastructure sectors with the most stringent timing requirements are the electric sector, the communications sector, the emergency services sector, and the financial sector.[7] This product will look at the first two, as they have the tightest requirements. In the electric sector, timing is used for log file coordination in control rooms as well as grid-wide monitoring and control in the supervisory control and data acquisition (SCADA) system. Loss of timing synchronization can result in the loss of energy management system workstations and therefore loss of visibility into the SCADA system; this exact incident occurred in 2014 and an electric sector organization temporarily lost visibility into their bulk power system assets.[8] Timing is also a critical dependency for phasor measurement units, which are sophisticated monitoring devices used to measure voltage, current, and frequency at multiple locations in the grid, allowing for increased efficiency in monitoring and control to maintain grid stability and predict faults.[9,10] Phasor measurement units require a timing accuracy of better than 1 microsecond, a standard that can be met by PTP, but not NTP.[11,12] Lack of precision timing capability will degrade or deny the use of certain advanced monitoring tools, which could result in less efficient operations due to increased margins of error from the reduced precision of real-time analyses.

Wireless communications in the telecommunications sector also require specific timing requirements, particularly as generations of cellular networks continue to evolve. 4G networks require a timing accuracy of 1.5 microseconds but this decreases to approximately 240 nanoseconds for 5G networks. According to the Ericsson Technology Review, "The two main types of synchronization requirements that are relevant for 5G networks are those that depend on the radio network operation and those that depend on the supported services (application-driven requirements)."[13] Radio network operation requirements include maintaining time domain isolation to prevent radio frequency interferences between base-stations and implementing communication features that rely on coordinated transmission or reception from multiple transmission reception points. The application-driven requirements for 5G networks are

other time-sensitive industrial processes such as smart manufacturing, autonomous transportation, and positioning for emergency services.[14] Disruption or manipulation of the timing components in telecommunications networks could result in a significant outage, impacting other dependent sectors such as emergency services, transportation systems, and financial services.[15]

Timing Vulnerabilities

The U.S. Government has recognized the critical role timing services play in functions across the 16 critical infrastructure sectors. In February 2020, Executive Order 13905, Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services, mandated U.S. Government agencies identify significant risks to critical infrastructure resulting from unmitigated PNT vulnerabilities. The Cybersecurity and Infrastructure Security Agency (CISA) is working on these issues through the development of PNT Profiles to "provide a common framework for assessing and mitigating PNT-related risk."[16]

Multiple vulnerabilities have been discovered in NTP over the last 20 years and in PTP in the last 5 years. Some of these have been due to vulnerabilities or inherent insecure design in the protocols themselves and others result from vendor or equipment implementations of the protocols. For example, in 2018, CVE-2018-7183 stated there was a buffer overflow vulnerability in a function of NPT called ntpq. This vulnerability could allow remote attackers to execute arbitrary code through a query response with specifically crafted data.[17] An earlier disclosure, released in 2014, included several vulnerabilities that would allow a remote attacker to send a specifically crafted packet and either crash the NTP daemon or execute arbitrary code with the privileges of the NTP user. This vulnerability was reportedly "easily exploited remotely by a low skilled attacker" with publicly available exploits.[18] In 2019, CVE-2018-0378 revealed a vulnerability in the PTP feature of several Cisco switches which, if exploited, would cause a denial of service (DoS) condition and impact traffic needing to pass through the device on the network.[19]

Conclusion

Despite widespread awareness of time as a critical dependency in ICS and across critical infrastructure, especially within the U.S. government, most public efforts are focused on decreasing reliance on GPS as a time source and the "responsible use of PNT."[20] As the trend of automation in industrial processes grows, the need for precise, accurate timing and the dependency on this timing also grows. Electric and telecommunications companies, as well as those in other critical infrastructure sectors, will rely more on the precision and accuracy of time within their systems. This increases the risk to control systems and critical infrastructure from malicious manipulation, degradation, or denial of timing sources and processes.

[1] D. Mills. "Network Time Protocol (NTP) General Overview." University of Delaware. https://www.eecis.udel.edu/~mills/database/brief/overview/overview.pdf (Accessed May 27, 2022)
[2] J. Shearer. "Killing Time". SANS ICS Security Summit 2021. https://youtu.be/2iV-KuGQtgU?t=1029 (Accessed May 27, 2022)
[3] J. Laird. "PTP Background and Overview". University of New Hampshire InterOperability Laboratory. https://www.iol.unh.edu/sites/default/files/knowledgebase/1588/ptp_overview.pdf (Accessed May 27, 2022)
[4] J. Sherman and J. Levine. "Usage Analysis of the NIST Internet Time Service". Journal of Research of the National Institute of Standards and Technology. https://tf.nist.gov/general/pdf/2818.pdf (Accessed May 27, 2022)
[5] "How the Windows Time Service Works". Microsoft. https://docs.microsoft.com/en-us/windows-server/networking/windows-time-service/how-the-windows-time-service-works (Accessed May 27, 2022)
[6] J. Shearer. "Killing Time". SANS ICS Security Summit 2021. https://youtu.be/2iV-KuGQtgU?t=1029 (Accessed May 27, 2022)
[7] "Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)." United States Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508_0.pdf (Accessed May 27, 2022)
[8] "Lesson Learned: Loss of EMS/Dispatch Workstation Functionality due to NTP Time Synchronization Device Misconfiguration." North American Electric Reliability Corporation. https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/LL20140902_%20Loss_of_EMS_Dispatch_workstation_functionality.pdf (Accessed August 19, 2022)
[9] D. Arnold. "Timing in Industry: Power, Finance, Broadcast." Meinberg, WSTS 2019. https://wsts.atis.org/wp-content/uploads/sites/9/2019/03/0_08_Meinberg_Arnold_Timing_Power_Finance_Broadcast.pdf (Accessed May 27, 2022)
[10] P Hoffman. "How Synchrophasors are Bringing the Grid into the 21st Century". U.S. Department of Energy. https://www.energy.gov/articles/how-synchrophasors-are-bringing-grid-21st-century. (Accessed May 27, 2022)
[11] D. Arnold. "Timing in Industry: Power, Finance, Broadcast." Meinberg, WSTS 2019. https://wsts.atis.org/wp-content/uploads/sites/9/2019/03/0_08_Meinberg_Arnold_Timing_Power_Finance_Broadcast.pdf (Accessed May 27, 2022)
[12] "Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS)." United States Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508_0.pdf (Accessed May 27, 2022)
[13] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren. "5G synchronization requirements and solutions". Ericsson Technology Review. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-synchronization-requirements-and-solutions (Accessed June 6, 2022)
[14] S. Ruffini, M. Johansson, B. Pohlman, and M. Sandgren. "5G synchronization requirements and solutions". Ericsson Technology Review. https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-synchronization-requirements-and-solutions (Accessed June 6, 2022)
[15] "Communications Sector". U.S. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/communications-sector (Accessed June 6, 2022)
[16] "Understanding Vulnerabilities of Positioning, Navigation and Timing". United States Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/fact_sheet_pnt_vulnerabilities_508.pdf (Accessed May 27, 2022)

[17] "NTP BUG 3414: ntpq: decodearr() can write beyond its buf limits". Network Time Foundation. https://doc.ntp.org/support/securitynotice/ntpbug3414/ (Accessed June 6, 2022)
[18] M. Lennon. "Easily Exploitable NTP Vulnerabilities Put ICS Operators at Risk". Security Week. https://www.securityweek.com/easily-exploitable-ntp-vulnerabilities-put-ics-operators-risk (Accessed June 6, 2022)
[19] National Vulnerability Database. "CVE-2018-0378 Detail". National Institute of Standards and Technology. https://nvd.nist.gov/vuln/detail/CVE-2018-0378 (Accessed June 6, 2022)
[20] "Understanding Vulnerabilities of Positioning, Navigation and Timing". United States Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/sites/default/files/publications/fact_sheet_pnt_vulnerabilities_508.pdf (Accessed May 27, 2022)