American Petroleum Institute

Suzanne Lemieux
Manager, Operations Security & Emergency Response Policy
Corporate Policy

200 Massachusetts Ave NW
Washington, DC 20001
USA
Telephone 202-682-8453
Email lemieuxs@api.org
www.api.org

July 13, 2020
Profile of Responsible Use of PNT Services
National Institute of Standards and Technology

Subject: The National Institute of Standards and Technology's Request for Information*, Profile of Responsible Use of Positioning, Navigation, and Timing Services*, Docket Number 200429-0124

The American Petroleum Institute (API) and its members offer the following comments on the National Institute of Standards and Technology's Request for Information, "Profile of Responsible Use of Positioning, Navigation, and Timing Services", Docket Number 200429-0124. API is the only national trade association representing all facets of the natural gas and oil industry, which supports 10.3 million U.S. jobs and nearly 8 percent of the U.S. economy. API's 600 members include large integrated oil and natural gas companies, as well as pipeline, exploration and production, refining, marketing, marine businesses, and service and supply firms. They provide most of the nation's energy and are interested in how positioning, navigation, and timing services can continue to be used to improve safety, efficiency, and environmental protection efforts while ensuring the safety and security of communities, employees, and operations.

NIST is seeking the following information from PNT technology vendors, users of PNT services and other key stakeholders for the purpose of gathering information to foster the responsible use of PNT services:

1. Describe any public or private sector need for and/or dependency on the use of positioning, navigation, and timing, or any combination of these, services.

Aviation, shipping, deep water drilling, pipeline and computing systems use PNT for location, heading, speed, and other critical calculations.   Drones, depending on the model, can make use of all aspects of PNT, requiring GPS to enforce no fly zones within the United States.

Offshore drilling rigs, vessels and MODU's (mobile offshore drilling unit) with Dynamic Positioning (DP) systems require reliable PNT services.   Deepwater drilling depends on GPS to ensure accurate placement of the drillship over the correct location for drilling. Once drilling has commenced, there is a dependence on GPS and other navigational aids to maintain location with data fed to the dynamic positioning system (DPS) to ensure the drillship does not drift while connected to the sea floor.

Deepwater drilling also depends on GPS and NTP to maintain accurate time stamping of real-time drilling data on both land and offshore operations.

Trucks use GPS tablets for navigation.

Centrally controlled pipelines tend to use NTP for time. Remote SCADA and other field sites will use GPS for time.

GPS time servers are deployed in the majority of process control network environments and utilize the clock systems of the GPS network of satellites to synchronize of stratum-1 time to control systems, power systems, network devices, domain controllers, virtual machines, etc. Not all process controls systems, though, rely on GPS for time; some instead leverage NTP across the internal corporate network.

Health, environment, and safety lone worker protection systems use GPS to identify the location of field personnel in emergency situations.

In the maritime sector, the International Maritime Organization (IMO) International Convention for Saving Lives at Sea (SOLAS) requires vessels constructed after 2002 to carry a "receiver for a global navigation satellite system or a terrestrial radio navigation system, or other means, suitable for use at all times throughout the intended voyage to establish and update the ship's position by automatic means" (Regulation 19, 2.1.6). In practice, this usually takes the form of a Global Positioning System (GPS) receiver.

2. Identify and describe any impacts to public or private sector operations if PNT services are disrupted or manipulated.

Disruption or manipulation of PNT services within aviation, shipping, or trucking could cause vehicles to veer off course at a minimum or crash. There is potential with the former to cause a ship to navigate into territorial waters where it may be seized. The United States Maritime Administration Advisory "2019-012-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea-Threats to Commercial Vessels by Iran and its Proxies" noted that GPS interference was present in two of six maritime incidents within the region, which is frequented by oil tankers. Advisory "2020-001-Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea, Gulf of Aden, and Indian Ocean-Threats to Commercial Vessels by Iran and its Proxies" which supersedes 2019-012 reiterates the threat to GPS.

Offshore drilling rigs, support vessels and MODU's with Dynamic Positioning (DP) systems could be disrupted if the level of redundancy does not include diversity of technology within the PNT.

Within process control networks, it is important all devices/systems are synchronized to an accurate common time source. As noted above, some process control systems will use GPS for time while others may rely on NTP across the internal network. If PNT (GPS) time were changed or redirected, then the applications/systems using GPS would have a different time than those using NTP and this may cause disruptions. Some data may be invalid if the times do not match and the time gap is more than a certain threshold.

Jamming GPS would not typically result in an immediate impact but over time a rig could slowly drift and would be an issue over an extended time.

GPS attacks would affect communications between safety controllers within the process control safety system. Most systems use a time stamp on the inter-trip communications to determine how old the message is as part of the determination of whether the message is valid. If the message is too old the communications is considered failed and the signal goes to the fault stated which is usually trip. The "age" is usually set for 3 to 6 seconds. In the case of a hack where the time is abruptly changed, the change could cause all of the inter-trips to fail causing a shutdown. Where the time is unavailable, there would probably be little effect as the Safety Controllers all sync to a master controller so if they drifted, they would drift together.

Loss of time synchronization could cripple root cause analyses after an incident as it might not be possible to properly synchronize the sequence of events from the various components on the process control network.

Remote SCADA and other field sites which use GPS for time could be impacted by GPS jamming or spoofing.

Consensus appears that at most, PNT disruption might cause a shutdown of the process; a health, environmental, or safety event is not likely from such an attack.

3. Identify any standards, guidance, industry practices and sector specific requirements referenced in association with managing public or private sector cybersecurity risk to PNT services.

Marine Technology Society Dynamic Positioning Committee – DP vessel Design Philosophy Guidelines which the USCG uses as reference and [USCG–2011–1106] Mobile Offshore Drilling Unit Dynamic Positioning Guidance are two marine standards on PNT.

Department of Homeland Security has published guidance ("Best Practices for Improved Robustness of Time and Frequency Sources in Fixed Locations" January 6, 2015 https://www.us-cert.gov/sites/default/files/documents/Best%20Practices%20-%20Time%20and%20Frequency%20Sources%20in%20Fixed%20Locations_S508C.pdf and "Improving the Operation and Development of Global Positioning System (GPS) Equipment Used by Critical Infrastructure" 2017? https://www.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf) although a speaker at RSA Conference 2018 argued that the DHS recommendations in the latter were either ineffective, unimplementable, or too costly.

4. Identify and describe any processes or procedures employed by the public or private sector to manage cybersecurity risks to PNT services.

API companies utilize many well-known standards and frameworks, including the NIST Cybersecurity Framework, NIST.SP.800-30r1 - Guide for Conducting Risk Assessments, NIST.SP.800-37r2 - Risk Management Framework for IT & OT and NIST.SP.800-82 rev2 - Guide to Industrial Control System -ICS-Security and ISO 27000 to manage risk.

High level risk assessments of PNT cybersecurity risks have been conducted. Personnel have attended presentations at the RSA Conference, International Information Integrity Institute (I-4), and other venues and have done research regarding potential PNT cybersecurity issues and risks.

Some of the assessments cover controls and mitigations of risks.

5. Identify and describe any approaches or technologies employed by the public or private sector to detect disruption or manipulation of PNT services.

On drilling ships, Dynamic Positioning (DP) systems designed with diversity and redundancy e.g IMU positioning and HydroAcoustic Positioning Systems are used.

We are aware of research conducted at Los Alamos National Laboratory in 2003 (Warner, Jon & Johnston, Roger. "GPS Spoofing Countermeasures https://pdfs.semanticscholar.org/36e1/7f723bff8d429aca4714abe54500a9edaa49.pdf?_ga=2.190821090.893877736.1574372109-2126968739.1574200464) which identified seven actions to identify suspicious GPS signals. The recommendations involve looking at signal strength, timing, and satellite identifications and identifying signals which are "too perfect" or "too strong" as these may be coming from a terrestrial GPS generator. Research a year later (Emy Rivera, Robert Baykov, and Guofei Gu; "A Study On Unmanned Vehicles and Cyber Security"; https://pdfs.semanticscholar.org/521c/2dd41bd7de10cb514f4e9d537fd434699cb7.pdf) cautioned that anti-spoofing techniques such as checking signal thresholds are not always reliable and a quick review of the Los Alamos controls finds them most effective against an unsophisticated attack.

While we are aware of the GPS countermeasures highlighted by Los Alamos and other research, we are unaware of these actually being deployed within the public or private sector.

6. Identify any processes or procedures employed in the public or private sector to manage the risk that disruption or manipulation to PNT services pose.

The risk has mostly been accepted to date as impacts are muted in most environments. This is not the case with drones, ships, and other vehicles which may crash or be intercepted if they rely on GPS and it is intercepted.

7. Identify and describe any approaches, practices, and/or technologies used by the public or private sector to recover or respond to PNT disruptions.

Incident response processes would handle manipulation of PNT in the process control environment. NIST.SP.800-184 - Guide for Cybersecurity Event Recovery is among the standards/processes used. There are manual navigational means which could be used on ships. Drones might be steered manually by humans watching video if GPS signals were jammed. As controls are problematic, the solution is resilience, allowing by video camera, for example, if GPS were off-line.

8. Any other comments or suggestions related to the responsible use of PNT services.

The Oil and Natural Gas industry makes significant use of PNT services and API is pleased that NIST has initiated this effort to better identify risks and countermeasures. API is open to continued engagement with NIST on this topic and looks forward to the published report. API and its members encourage NIST to continue engaging stakeholders and users, as they continue to explore PNT uses, criticality, and resilience.

Regards,

Suzanne Lemieux
Manager, Operations Security & Emergency Response Policy
Corporate Policy
American Petroleum Institute