

[WP-IC-004]

Certified Time As a Critical Infrastructure

By Bob Radvanovsky
CIFI, CISM, REM, CIPS
rsradvan@infracritical.com

Author of "Critical Infrastructure: Homeland Security and Emergency Preparedness"

Taylor and Francis Publishing, CRC Press
ISBN 0-84937398-0

Infracritical CC License Version 1.1

Attribution. The licensor (Bob Radvanovsky) permits others to copy, distribute, display, and perform the work. In return, licensees (you) must give credit to either Bob Radvanovsky or Infracritical, and the original author(s) of the material you use.

Non-Commercial. The licensor permits others to copy, distribute, display, and perform the work. In return, licensees may not use the work for commercial purposes – unless they get the licensor’s permission.

Share Alike. The licensor permits other to distribute original or derivative works, but only under a license identical to the one that governs the licensor’s work. Derivative works are Infracritical materials that have been edited, translated, combined with someone else’s

Exception. Certain elements (such as photos, graphs, text quotes) included within this document have been acquired from sources outside of Infracritical. Please contact the copyright owner to get permission for non-fair use purposes if you wish to copy, distribute, display, or perform an element that is not covered under the Infracritical CC License.

The Infracritical CC License follows licensing guidelines as outlined by Creative Commons standards: <http://www.creativecommons.org>.

Questions should be addressed to:
info@infracritical.com

Table of Contents

- Table of Contents..... 1
- Author’s Note about the Whitepaper 1
- Objective 1
- What is “Critical Infrastructure Protection” (CIP)?..... 2
 - Definition of “CIP” 2
 - How Does “CIP” Relate to “CIT”? 2
- What is “Critical Infrastructure Time” (CIT)?..... 3
 - Why NIST Cannot Deploy U.S. Time..... 3
 - Why Should CIT Be Used? 4
 - How is CIT Used?..... 5
 - Is GPS a Flawed Certified Time Source? 5
 - Alternative Certified Time Source in Lieu of GPS 6
 - Legal Reasons for a Certified Time Source 6
- Conclusion..... 7

Author’s Note about the Whitepaper

It is the intention of this whitepaper to convey to the general public the importance of properly defining and establishing the necessary infrastructure to support an accurate and timely available time-base for private and public sector us, both throughout and between the mentioned critical infrastructures (as outlined within the Homeland Security Presidential Directive No. 7, HSPD-7) within the United States. Without establishing such a crucial elemental piece to the overall puzzle, the validity, more importantly, the security of our critical infrastructures depends upon an accurate time source. This paper hopes to address several of those issues.

Objective

The objective of this document is to provide recommendations for creating and securing a certifiable time source that is relatively inexpensive, and is reliably and publicly available to the general public within the United States. The document defines and outlines the following definitions (“critical infrastructure protection” and “critical infrastructure time”) and reasons necessary for providing reliable, accurate, attestable and secured time sources for both public and private sectors, and their industries.

This document is by no means final or complete, but represents a conceptualization of a possible direction towards a securification methodology and practice model for an accurate and reliable time source, and is subject to review and discussion. Any and all questions, comments, critiques, et. al, are welcomed and should be directed to **Bob Radvanovsky** at Infracritical (email: rsradvan@infracritical.com).

What is “Critical Infrastructure Protection” (CIP)?

Much of what exists today is as a direct result from the catastrophic events following September 11, 2001. What U.S. policy makers consider to be “critical infrastructure” has been evolving and is often ambiguous. Twenty years ago, the word “infrastructure” was defined primarily with respect to the adequacy of the nation’s public works. In the mid-1990’s, however, the growing threat of international terrorism led policy makers to reconsider the definition of “infrastructure” in the context of national security. In May 1996, President Clinton created Presidential Decision Direction No. 63 further compartmentalizing functionalities of both military and industrial functions into distinct sectors, each one on par with another in terms of criticality, importance, and the level of impact.

Definition of “CIP”

The term “critical infrastructure protection” (CIP) pertains to the activities for protecting our critical infrastructures. This includes people, physical assets, and communication (cyber) systems that are indispensably necessary for national, state and urban security, economic stability, and public safety. CIP methods and resources deter or mitigate attacks against critical infrastructures caused by people (e.g., terrorists, other criminals, hackers, etc.), by nature (e.g., hurricanes, tornadoes, earthquakes, floods, etc.), and by hazardous materials accidents involving nuclear, radiological, biological, or chemical substances. It does entail some preventative measures and countermeasures, but usually are reactive by nature.¹

Defining, using and maintaining critical infrastructures are a process of themselves, such that it is an analytical model or template that guides the systematic protection of itself. More importantly, it is a reliable decision-making, sequential set of methodologies that assists decision makers in determining possible needs of what methods should be used for whatever is being safeguarded. The process ensures the protection of only those infrastructures upon which survivability, continuity of operations, and their mission successes depend upon. Thus, these methodologies safeguard only those infrastructures which are deemed important and vital for the continued operation of large scales of economies.²

How Does “CIP” Relate to “CIT”?

Critical infrastructures provide essential goods and services to corporations, governments, and its citizens and employees. Many of the infrastructures that exist are (predominately) service-oriented, providing “just in-time servicing”, which works (in theory) similar to “just in-time manufacturing”. The premise is that services are provided when they are needed, to where they are needed or requested. Ad-hoc servicing sometimes requires distribution of goods or services to their customers, thus requiring an elaborate mechanism put into place that is highly-defined and precise. Precision requires calibration periodically, and some services rely on timing services to synchronize with one another, either within the same sector, or between other sectors. The best prime example would be the distribution of water and wastewater services, and its treatment, as well as electrical power distribution. Both services are separate sectors, but rely heavily on accurate time sources for the distribution of their “products”, in this case, water and electricity. Time needs to be viewed as a critical infrastructure, certainly as a critical resource, by which these two services can remain operable.

¹ “Critical Infrastructure: Homeland Security and Emergency Preparedness”, Bob Radvanovsky, Taylor and Francis, 2006.

² Ibid.

What is “Critical Infrastructure Time” (CIT)?

The definition of “critical infrastructure time” represents a type designation of source time telemetry data or information that is representative of not only a critical infrastructure, and its sector, but might be useful for business clients who depend on accurate and reliable timed business functions, both from a legal as well as financial responsibility. The criticality of necessitating a valid certified time source is justified through several reasons that are becoming increasingly important every year. Our society (as a whole) is becoming more and more interconnected, with a significantly growing dependency towards automated venues. These venues provide everything from simple systems, such as vending services of goods and products, to counters at turnstiles for mass transit entrance and exit points, to extremely complex systems, such as water flow control or interconnecting electrical transmission systems. These systems are indicative of environments that require industry-acceptable standards pertaining to redundancy and resiliency. Redundancy levels specify areas of criticality or importance for a specified set of event triggers, whereas resiliency levels specify to what degree they are considered redundant.³

Methods of communication include intra- and inter-connecting communication networks (both within and throughout) the enterprise; areas that these mechanisms rely upon. One of the keystones that are required by these systems are optimal capabilities, is the reliance upon a stable, valid and certifiable time source. This time source is vital in ensuring that the enterprise remains at acceptable operational levels, that customers are being serviced correctly, and that the enterprise is capable of switching to alternative pathways (should one or more of any given node within the enterprise fail) seamlessly and without flaw. Timing is crucial, esp. when dealing with critical functions pertaining to human life.

Such functions, such as water/wastewater services, energy production and transmission, life support systems, and other lesser-known systems, such as traffic flow control – all rely upon a systematic approach that is performed automatically, quietly and without any intervention from a human. Without a sustained time source, human intervention is required, either to correct the date/time flaw, or corrective functions carried through resulting from a date/time flaw.

Why NIST Cannot Deploy U.S. Time

The National Institute of Standards and Technology (NIST) was not chartered to operate nor maintain time for the United States, outside of the federal government, and even that, is limited in its capacity. Unlike most federal laboratories that derive their missions from those of their parent agencies, NIST is chartered by Congress in broad and comprehensive legislation. First written in 1900 and signed into law in 1901, the NIST authorizing legislation is periodically updated, and in 1988, in a sweeping rewrite of the authorization, Congress placed NIST in the forefront of federal efforts to improve the use of technology in the competition for global markets.⁴

³ <http://www.spirit.com/Network/net0701.html>.

⁴ “An Assessment of the National Institute of Standards and Technology Measurement and Standards Laboratories: Fiscal Year 2001 (2001)”, http://books.nap.edu/openbook.php?record_id=10204&page=297.

The Omnibus Trade and Competitiveness Act of 1988 augmented NIST’s functions and capabilities, specifically receiving new orders to carry out its mandate to assist the private-sectored firms that capitalize on advanced technology; the act reconfirmed importance of NIST’s existing capabilities asserting that NIST’s measurements, calibrations, and quality assurance techniques were the underpinning of U.S. commerce, technological progress, improved product reliability, improved manufacturing processes, and public safety.⁵ NIST continues to have a unique responsibility to promote economic growth by working with industry to develop and apply technology, measurements, and standards.⁶

For the most part, neither NIST nor the federal government is really chartered to provide accurate, reliable time to the United States for non-military applications. That means that, legally, companies and citizens that are accessing the U.S. time source are accessing a service that was not designed for large-scaled deployments. In fact, if 100 million “servers” accessed the NIST time source servers at once, this would (quite literally) *shutdown* the NIST U.S. time base. From a deployment perspective, NIST wasn’t designed to handle large amounts of individuals, corporations and government organizations simultaneously to access its time source for time resynchronization and calibration.

Simply put, NIST was not built for distribution of the U.S. time base to top-tier time service providers.

Why Should CIT Be Used?

The premise is to provide a suitable, logical infrastructure that deploys the U.S. time base, accurately, efficiently, and reliably, and has resiliency safeguards built into its architecture. The reason for this is simple: not everyone would be capable of accessing a unitary time source, and should rely upon a distributed time source. The question is, how reliable and accurate would it be?

If implemented, the reliability factors would be handled by commercial businesses, operated by corporations, but audited by the federal government, say through the Department of Commerce or the Department of Interior, which have extensive background (and interests) in a reliable U.S. time base. The Department of Commerce might be interested from the simple fact that it controls our weather telemetry data and information obtained through the National Oceanic and Atmospheric Administration (NOAA), as well as the National Weather Service (NWS), which is used by just about everyone, and relied heavily by government and volunteer first responders and emergency management organization and agencies under natural disaster weather conditions. Accurate time means accurate telemetry data and information, which might mean that lives and property might be saved. If a crisis, resulting from a natural disaster occurrence can be averted, would save local and county governments thousands, if not millions of taxpayer dollars. Additionally, this would save state and federal governments from necessarily having to deploy rescue and disaster fund relief programs if disasters could be averted. Much of this depends on one and only one factor: accurate time. If the date/time stamps are off, weather telemetry data and information is equally as off, which means that a storm cell or cyclonic system could be much further ahead than originally predicted. A few seconds might equally translate to a few minutes. Fifteen minutes in some portions of the United States can make significance in whether lives and property are lost or recoverable.

⁵ Ibid.
⁶ Ibid.

How is CIT Used?

Creating a practice model that incorporates non-Internet-based remote time servers would not disrupt NIST's time network. More importantly, NIST's time servers would not be subject to attack through the Internet, further laying claim that the U.S. time base is reliable and accurate. The model would incorporate a method of a centralized distributed mechanism by which each region would transmit time accordingly from a valid, non-relayed time source, such as from NIST, but not through public networks. This would allow the servers to remain as pristine as possible, thereby reducing any risk of attack, data corruption, time manipulation, etc. from occurring at the time source itself, as well as unnecessary overhead from clients simply wanting to recalibrate their time services.

Regional distribution would provide accurate time to local sources, and from there, would be distributed to each client requiring an accurate, reliable time source. More and more corporate organizations are requiring their time to be valid. One significant argument is that time can be obtained through Global Positioning Systems (GPS), but are willing to accept whatever risks are inherent to utilizing GPS-based time sources. The most significant risk is that the U.S. government can remove the GPS service *at any time*. The more significant reasons are war and terrorism. That being said, corporations cannot reliably use GPS-based time sources, esp. today in a time of war.

CIT can be used from either any type of network, considering that resiliency factors are built into the network; that being, if a node that a client or group of clients were to access, were to fail or shutdown, clients would have alternative locations to synchronize from that are very local to their region of the United States. Much to the same regards that zip codes were designated based on locale, so too should time sources be defined based on location within the United States. This increases the accuracy of the time data being received from the time source through a reduction in "time lag", or the amount of time that it takes for a client to receive accurate time from its time source. Another term might be "time drift", but would prefer "time lag" as networks become increasingly/decreasingly congested based on usage.

Is GPS a Flawed Certified Time Source?

Some might think so. The system is flawed by inaccurate timing signals from the satellites -- errors that were deliberately introduced. The positioning system was designed to have two tiers of service: the Precise Positioning Service and the Standard Positioning Service. If you were part of the military of the United States or of one of our Nation's allies, or were in an approved government agency, and if you had expensive cryptographic decoders and passkeys, you could take advantage of the more accurate GPS data from the Precise Positioning Service that could pinpoint your latitude and longitude to within roughly 72 feet (22 meters) -- or less than half that in some cases -- and your elevation, relative to sea level, to within roughly 90 feet.⁷

⁷ <http://tech2.nytimes.com/mem/technology/techreview.html?res=9506EEDC133EF936A25755C0A9669C8B63>.

Since GPS receivers need signals from four satellites to calculate their position precisely, accuracy will suffer if signals from one or two satellites are lost. In many cases, the algorithms built into GPS receivers can cope with short interruptions. However, an even greater source of error is atmospheric conditions, which can degrade the microwave carrier signals that GPS satellites transmit and introduce errors. Any error is most definitively likely to be compounded, creating larger positioning errors, because the GPS uses calculations that are based on signals sent from as many as four satellites. And even small signal errors can result in large positioning errors because position calculations are based on minute time differences; the problem becomes worse if more than one satellite's signals contain errors.⁸

Alternative Certified Time Source in Lieu of GPS

Governments (federal, state and local governments) utilize an alternative to the Global Positioning System (GPS) as a means of triangulating positions of personnel, and thereby synchronize their time of arrival. Although GPS technology involves the use of transmission of at least three radio signals from a "constellation" of 24 satellites to a hand held receiving unit, the receiving unit can use a triangulation method to calculate almost extremely accurate measurements of the user's position, velocity, and time. This method of time differentiation -- via cellular telephone technology -- is another indoor/outdoor location identification method known as the "time difference of arrival" technique, and is used similarly to that of the GPS technology. Rather than calculate of location based on time difference of arrival from three or more satellites, this method depends on at least three cellular antennas.⁹ Although the method is only accurate to a range of 80-120 meters, it does meet E911 requirements, and is more cost effective than the use of assisted GPS.

Legal Reasons for a Certified Time Source

Actually, there are several, one of which was recently brought to my attention in that time should be viewed in terms of "legal standards in time" as opposed to "accurate standards in time". What this means is that time sources that we do not have prove as being accurate as defined accurate by the federal government and approved as being "accurate". Circular as this may sound, this means that time telemetry data needs to come from a higher authority that can be attested by a third-party auditing firm under a court of law. That means, simply put, that time will need to be certified, using U.S. government approval mechanism, sort of like having a "USDA" stamp on that side of beef, only it deals with guaranteeing time itself.

From a treaty perspective, time is very important. If you had a treaty with another country, or if your corporation that was based out of the United States, had a treaty with another corporation that was based from another country outside of the control or influence of the United States, say The Netherlands, every second might determine if your corporation had to spend money or not when it came time to the renewal of the treaty. Treaty protocols are reliant on measurement mechanisms that are exceedingly complicated and complex, and the science and implementation of these mechanisms is called "metrology".¹⁰ Implementing these types of treaties involves interests between corporations and governments between the U.S. and foreign interests (corporations and governments alike), making them legal; thus, enabling our international export of commerce. Metrology is the basis for the existence of international treaties of exportation. Without an accurate time source, these treaties would become null and void.

⁸ <http://tech2.nytimes.com/mem/technology/techreview.html?res=9506EEDC133EF936A25755C0A9669C8B63>.

⁹ http://grothserver.princeton.edu/~groth/frs142s04/Presentations/Nick_Presentation.ppt.

¹⁰ The term "metrology" (from Greek 'metron' (measure), and -logy) is the science of measurement. Metrology includes all theoretical and practical aspects of measurement. It is a field of study which has been highly politicized and nationalized with sharp even severe rhetoric as the field progressed; <http://en.wikipedia.org/wiki/Metrology>.

Conclusion

The growing importance and dependencies on our critical infrastructures (and their resources) is evident that resiliency and reliability factors play an increasingly important role. As our society grows more and more dependent upon machines to assist us with our daily lives, it becomes crucial to ensure that the flow of goods and services isn't interrupted, damaged, or destroyed. Such endeavors require an even greater importance as to how these systems are executed in an accurate and timely manner. Thus, stressing the importance to the reliable and accurate time source becomes a critical element, not simply a necessary one.

Time, therefore, needs to be considered as a "critical infrastructure", and not, certainly as a "critical resource" that is responsible for ensuring that our critical infrastructures do not fail.