Limitations in timing and time transfer
-
lessons from Statnett COSECTIME pilot project

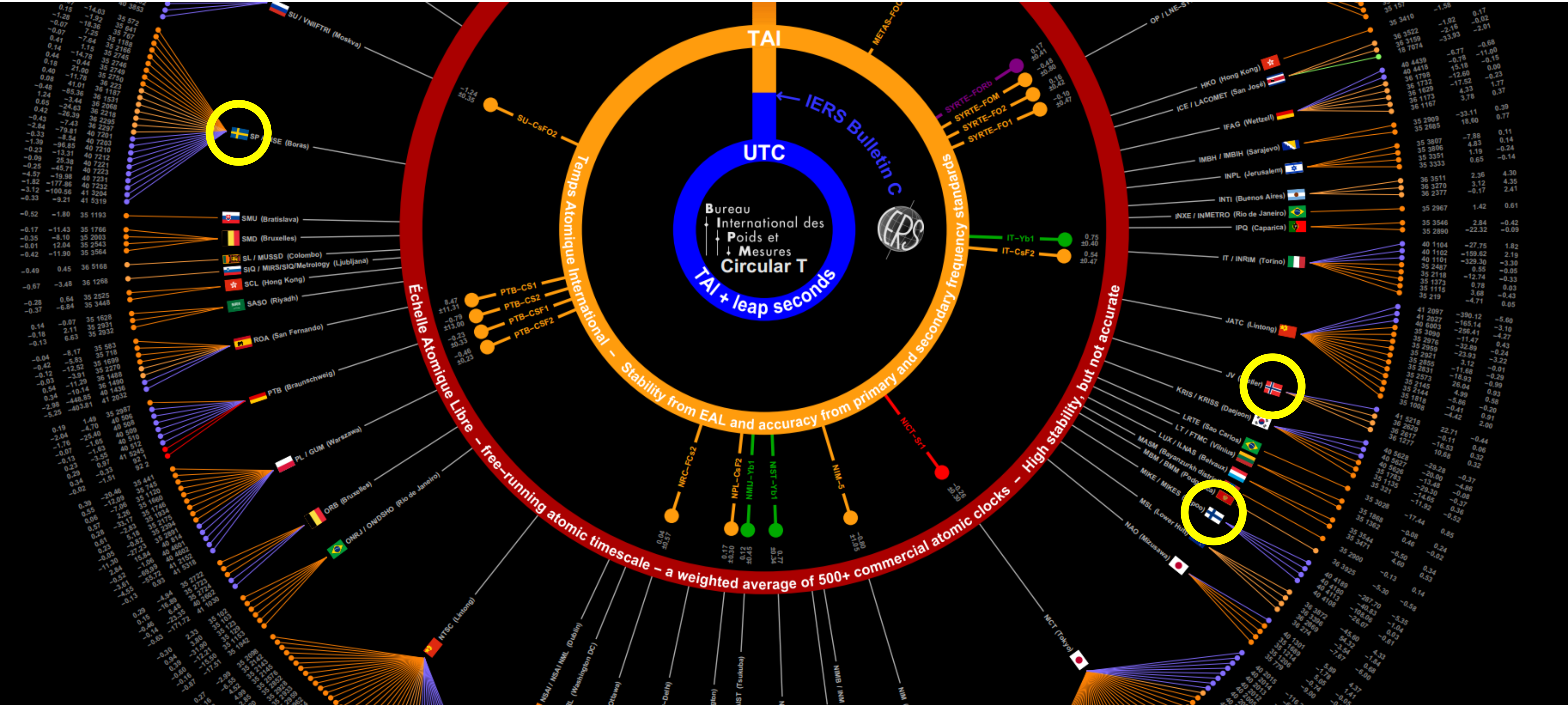
Seminar on
Safety and Security Issues in Positioning, Navigation and Timing
June 14 2023

Harald Hauglin

Chief engineer, time and frequency metrology
Justervesenet – Norwegian Metrology Service
hha@justervesenet.no

Justervesenet

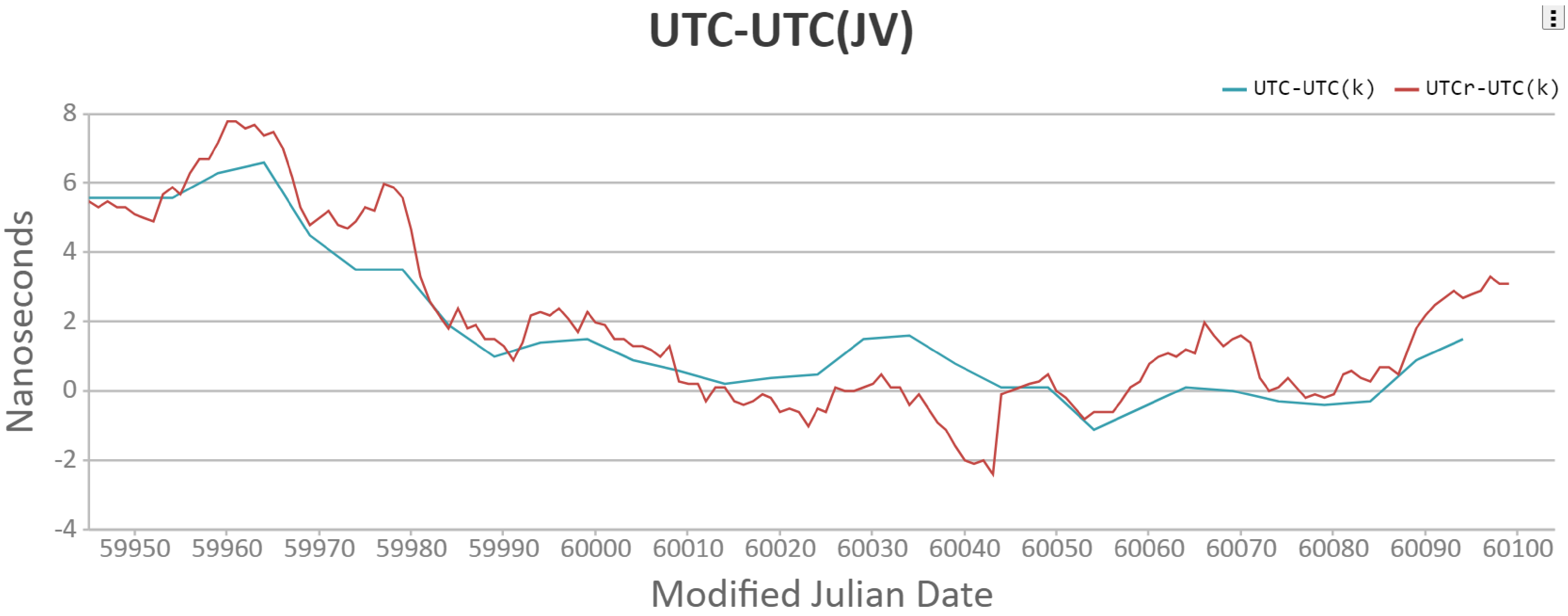
Nordic timing labs contribute 30+ clocks to TAI/UTC



https://www.justervesenet.no/wp-content/uploads/2021/03/UTC-illustrasjon-mars-21.pdf

Justervesenet

UTC(JV) during 2023. Target << 10 ns offset and increased redundancy



https://webtai.bipm.org/database/canvas.html?lab=JV&utclab=ok&utcrlab=ok&mjd1=59945&mjd2=60104

Justervesenet timing lab R&D on PNT security

In collaboration with Norwegian Space Centre:

- Tests of Galileo OSNMA.
- GNSS-signal generator for generating tests of GNSS jamming and spoofing

In collaboration with Statnett:

- COSECTIME 1-3 2016 –
- 2022-25 EU-project EPM ‘Digital-IT’ on timing and sampled values at digital substations

Redundant secure timing sources and timing distribution to digital power protection and control applications

H. HAUGLIN*, T. DUNKER*, A. WALLIN+, O. TUNGLAND*, N. HURZUK*, R. LØKEN*
*JUSTERVESENET, +VTT MIKES,*STATNETT,
** Norway, *Finland

Summary

The power transmission system is increasingly dependent on accurate time-stamping of digitally sampled values used for protection and control. In particular, real-time streaming of data from networked Phasor Measurement Units (PMUs) for wide area ‘closed loop’ automated control applications implies a critical dependence of accurate, available, and reliable microsecond-level timing.

While microsecond accuracy is easily met by GNSS timing receivers, GNSS signals for open civilian use are weak and also lack effective authentication mechanisms. GNSS timing receivers are therefore vulnerable to interference from malicious or inadvertent radio noise (jamming) and susceptible to ‘spoofing’ with generated GNSS-signals containing misleading timing and navigation data.

The overall goal of the COSECTIME project funded by Statnett is to demonstrate the applicability of state-of-the art fiber-optic time transfer techniques for traceable, secure and redundant synchronization of digital power transmission protection and control applications. In full deployment , the transmission system operator (TSO) will generate redundant autonomous UTC-traceable atomic timescales and distribute timing through redundant fiber optic networks also under TSO control. Here we present results from a pilot demonstration of timing distribution to the Statnett R&D project pilot IEC 61850 digital substation.

1. Introduction – timing requirements in the power system

The power transmission system is increasingly dependent on accurate time-stamping of digitally sampled values used in protection and control. Power system uses of timing and associated accuracy requirements are summarized in figure 1. For a comprehensive overview of power sector timing issues, see references [NASPI2017] and [GSA2018].

The IEC 61850 requirement of microsecond accuracy with respect to UTC can be met by properly installed and characterized GNSS timing receivers [EURAMET2016] in combination with timing distribution using the IEEE 1588 PTP precision timing protocol on the substation process bus. However, GNSS signals for open civilian use are weak and also lack effective authentication mechanisms. GNSS timing receivers may therefore be vulnerable to interference from malicious or inadvertent radio noise (jamming) and susceptible to ‘spoofing’ with generated GNSS-signals containing misleading timing and navigation data [Shepard2012]. Malicious timing attacks or simply inadvertent timing errors may have adverse impact on monitoring and control applications [Almas2018]. Applications studied in [Almas2018] illustrate the role of precision timing as a valuable cyber-asset in power sector control systems. For critical applications timing accuracy requirements need to be complemented by requirements on availability and integrity.

URL: https://e-cigre.org/publication/CSE017-cse-017

Spoof proof GPS timing

A detection and mitigation system for GPS time spoofing

Aril Johannes Schultzen

Thesis submitted for the degree of
Master in Informatikk: programmering og nettverk
60 credits

Spoof proof GPS timing
Faculty of mathematics and natural sciences

UNIVERSITY OF OSLO

Autumn 2016

Justervesenet
Institutt for Informatikk, UiO

https://www.duo.uio.no/handle/10852/53770?show=full

GPS timing interference

Building a setup for evaluating the effect of jamming and spoofing on GPS based timing devices

Thomas Rødningen

Thesis submitted for the degree of
Master in Robotics and Intelligent Systems: Cybernetics and Autonomous Systems
60 credits

Department of Informatics
Faculty of mathematics and natural sciences

UNIVERSITY OF OSLO

Spring 2022

Justervesenet
Forsvarets Forskningsinstitutt og ITS/UiO
Statnett

Norwegian policy process update 2023:

Recommendations to establish a national timing service

NSM sikkerhetsfaglig råd (2023):

NSM

Sikkerhetsfaglig råd

Et motstandsdyktig Norge

8 Romsikkerhet

Det bør etableres en nasjonal tidstjeneste

Tilgang til nøyaktig tid er avgjørende for både stats- og samfunnssikkerheten. Formålet med å opprette en slik tjeneste er å redusere avhengigheten av GNSS-tid og sikre tilgang på nøyaktig tid ved redusert tilgang eller forstyrrelser av GNSS-signaler. En slik nasjonal evne kan være basert på et antall sikrede bakke-baserte atomklokker og distribusjon av nøyaktig tid i ekom-nettene.

https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglig-rad-et-motstandsdyktig-norge#Sikkerhetsfaglig%20r%C3%A5d%20-%20et%20motstandsdyktig%20Norge

Totalberedskapskommisjonen (2023):

NOU Norges offentlige utredninger 2023: 17

Nå er det alvor

Rustet for en usikker fremtid

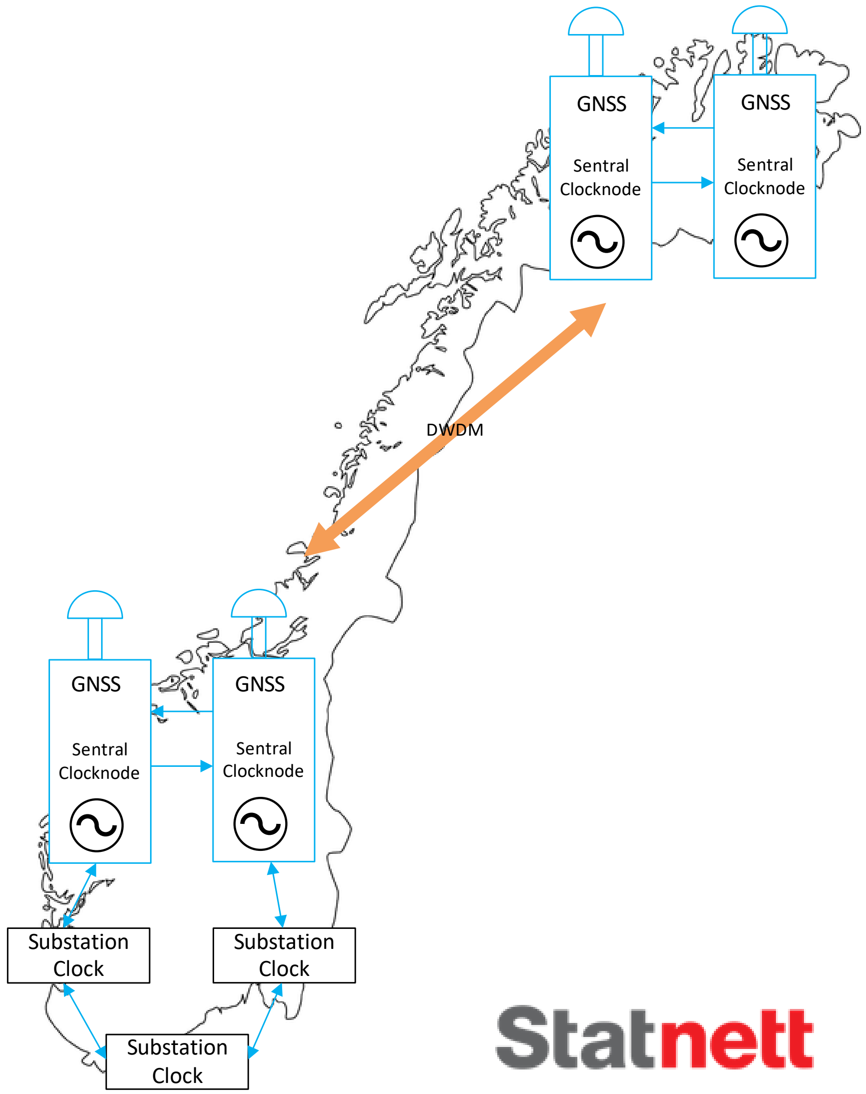
21.5.1 Tydeliggjøre et myndighetsansvar for norsk romvirksomhet

Kommisjonen vil særlig påpeke at de fleste satellittbaserte tjenestene tjener både sivile og militære formål, uten at det synes som om roller, ansvar og myndighet på området i tilstrekkelig grad er avklart. Kommisjonen har videre merket seg at svært mange samfunnsfunksjoner er avhengige av nøyaktig tid fra satellitter som er utenfor nasjonal kontroll. En nasjonal tidstjeneste som sikrer nasjonal egenevne med tanke på nøyaktig tid vil være et viktig virkemiddel for å redusere denne sårbarheten.

https://www.regjeringen.no/no/dokumenter/nou-2023-17/id2982767

Statnett is developing a nation-wide timing service for power sector needs

COSECTIME3 goals



Statnett

BfK § 7-14 **j) Sikker tidsreferanse** *Driftskontrollsystem som er* ***avhengig*** *av* ***eksakt*** *tidsreferanse,* *skal ha* ***sikre kilder*** *for tidsangivelse.*

- Statnett generates its own autonomous atomic timescales referenced to UTC
- No direct dependence of global navigation satellite systems
- Redundant clock systems and sync networks
- Deliver accurate timing (1µs) to transmission network substations via optical fibers for:
  - Protection relays (over IP)
  - Phase Measuring Unit

Why power sector reliance on accurate timing?

2003 North East USA blackout a wake-up call

Justervesenet

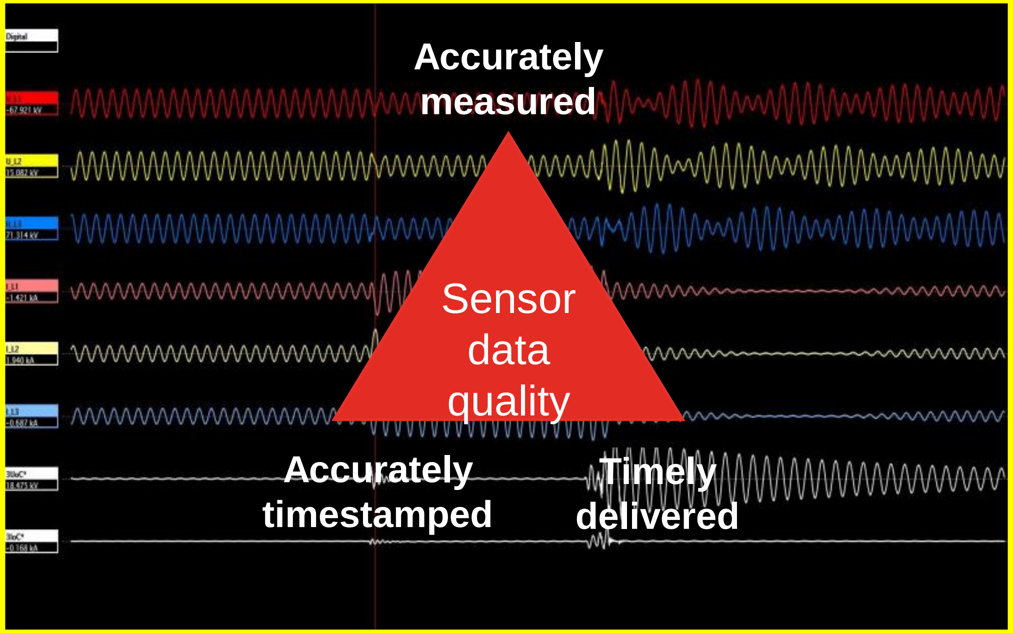
Digital networked control systems require tight synchronization

Wikipedia

Analog control systems, manual processes, wide operating margins

↓

Digital control systems, timestamped sensor data over networks, automated processes for rapid response



Sensor timestamps need microsecond accuracy: GPS/GNSS disciplined clocks.

Incorrect timestamps may give wrong estimates of grid power flows.

Justervesenet

How secure/resilient?

Timing threats

- GNSS jamming
- GNSS spoofing
- Network timing attacks

Other timing mishaps

- Failing clocks
- Sync network failures
- GNSS equipment failures

Level*	Minimum Requirements
Level 1	**Ensures recoverability after removal of the threat.** 1. Must verify that stored data from external inputs adheres to values and formats of established standards. 2. Must support full system recovery by manual means, making all memory clearable or resettable, enabling return to a proper working state, and returning the system to the defined performance after removal of the threat. 3. Must include the ability to securely reload or update firmware.
Level 2**	**Provides a solution (possibly with unbounded*** degradation) during threat.** Includes capabilities enumerated in Level 1 plus: 4. Must identify compromised PNT sources and prevent them from contributing to erroneous PNT solutions. 5. Must support automatic recovery of individual PNT sources and system, without disrupting system PNT output.
Level 3	**Provides a solution (with bounded degradation) during threat.** Includes capabilities enumerated in Levels 1 and 2 plus: 6. Must ensure that corrupted data from one PNT source cannot corrupt data from another PNT source. 7. Must cross-verify between PNT solutions from all PNT sources.
Level 4	**Provides a solution without degradation during threat.** Includes capabilities enumerated in Levels 1, 2 and 3 plus: 8. Must have diversity of PNT source technology to mitigate common mode threats.

https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework

Lessons from COSECTIME pilot demos:

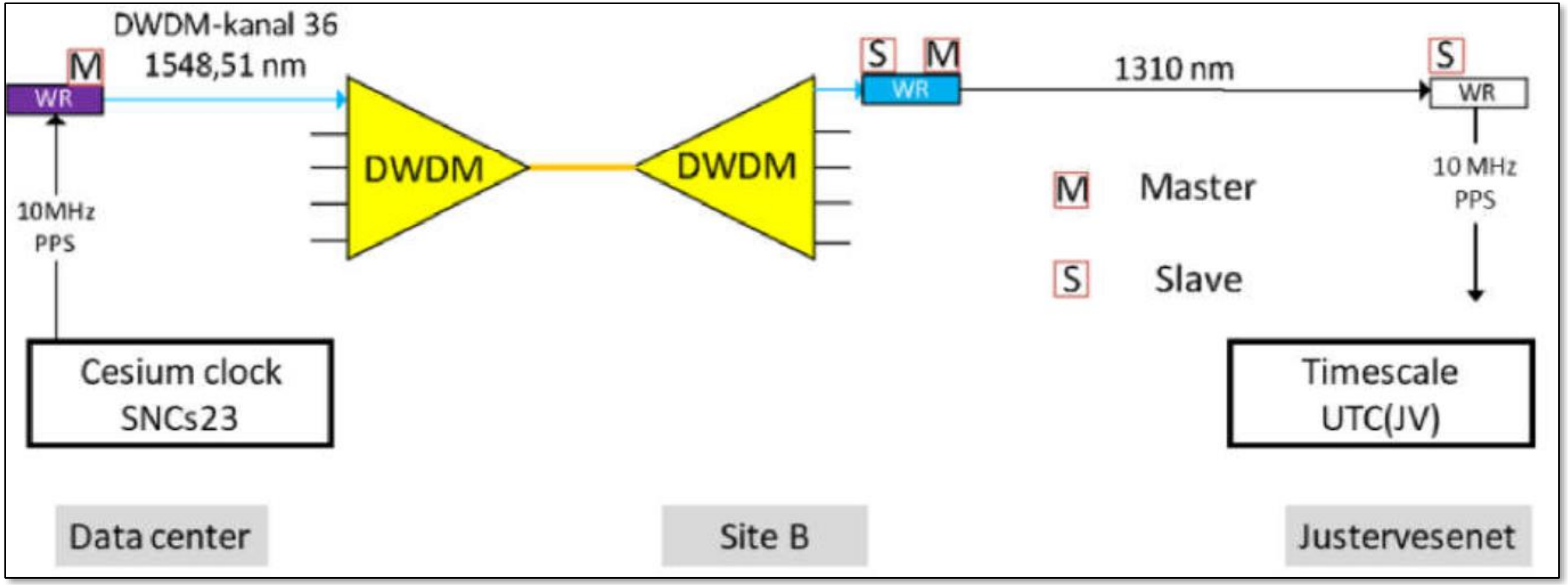
#1: Timing networks may have intermittent glitches

#2: Timing networks are asymmetric and need calibration

#3: Asymmetries may change due to network reconfiguration

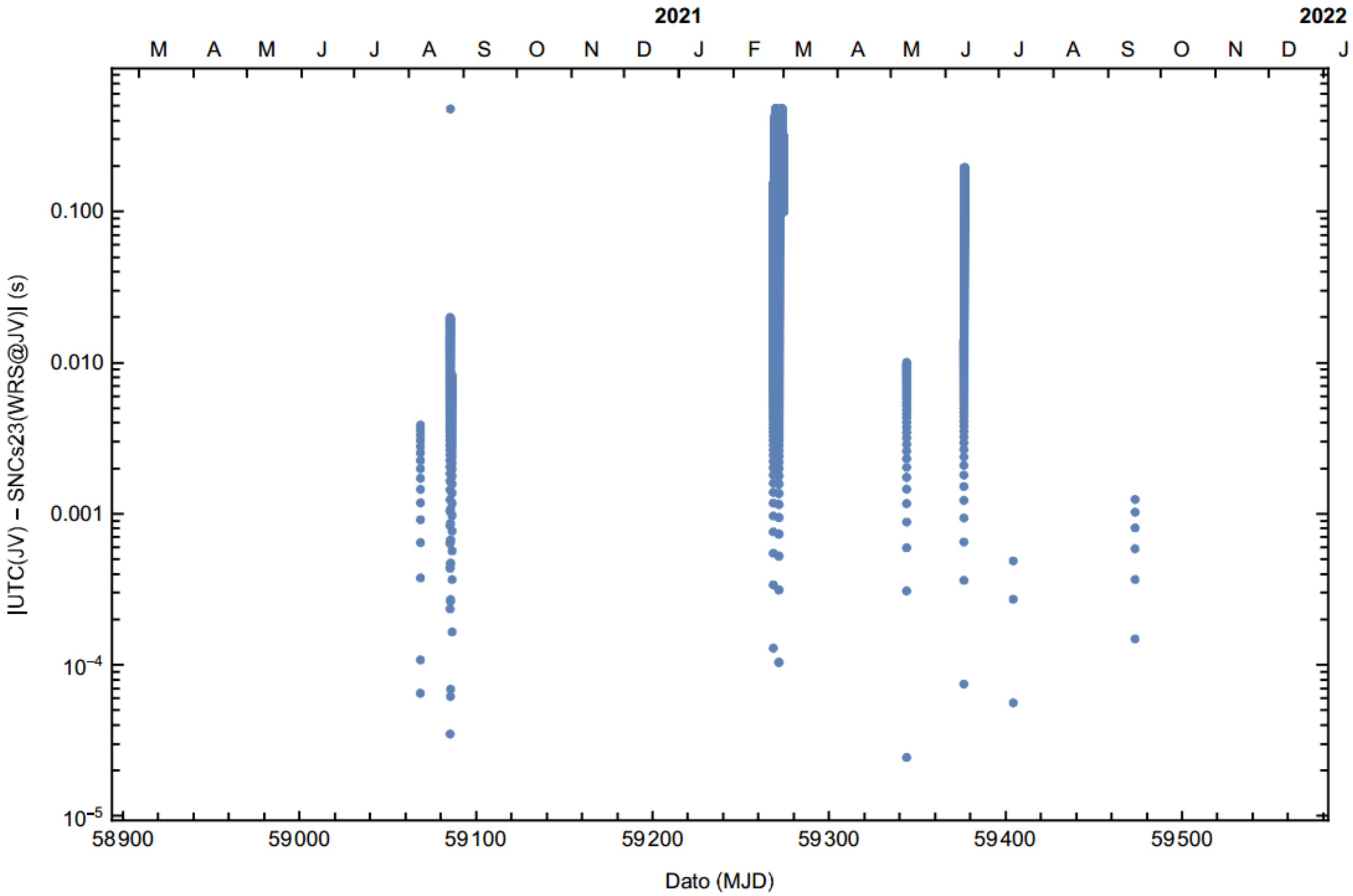
#4: Cs clocks may autonomously provide <1 μs timing over years

Time transfer over high accuracy network



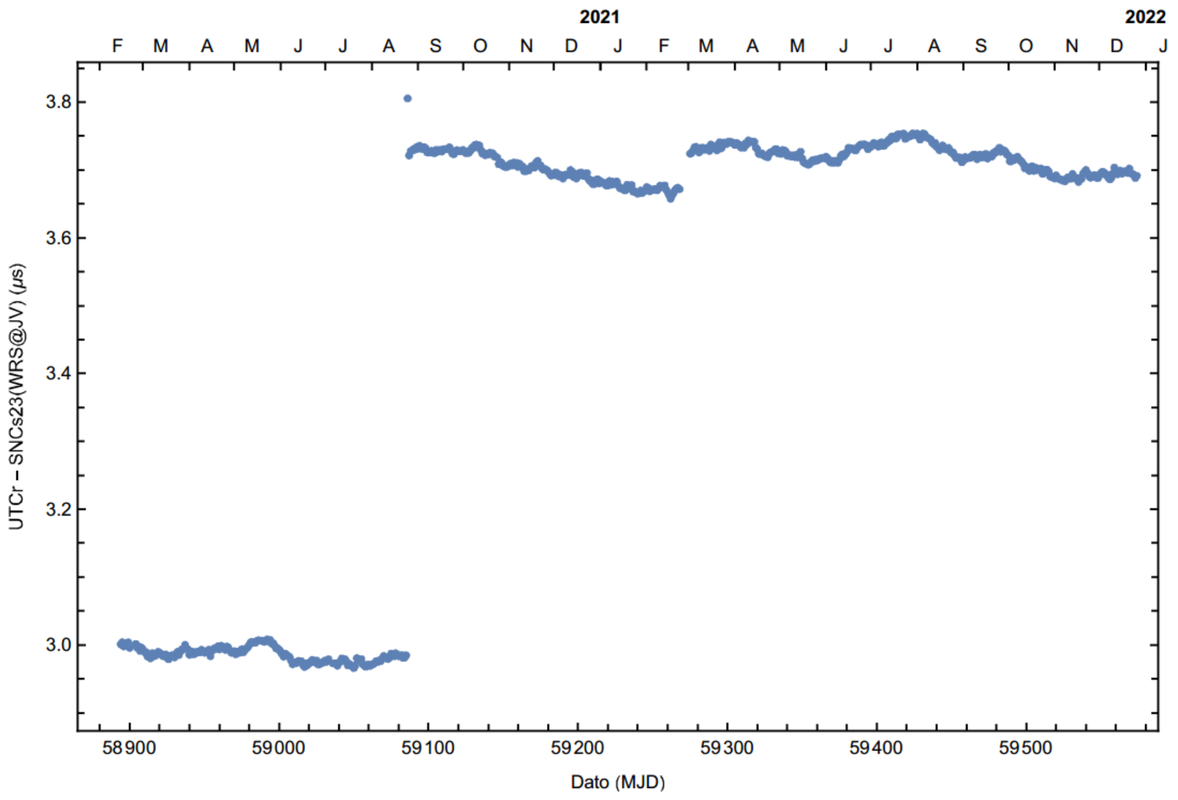
Justervesenet

Statnett time scale measured against UTC(JV)



- Two years of continuous operation
- Outliers 1 % of the time
- Some are planned outages, other intermittent glitches

Statnett time scale measured against UTC(JV)



- 3 microsecond asymmetry needs calibration to compensate
- Changes in asymmetry due to network reconfiguration
- Statnett time scale is stable to +/- 100 ns over 2 years of autonomous operation

Justervesenet

Lessons from COSECTIME pilot demos:

#5: Clocks may/will fail

#6: Alternative timing sources need to be combined and selected using robust logic for actual resilience

Robust sync? 2 x belts + 2 x suspenders

Sync demo at digital substation pilot – Statnett-prosjekt COSECTIME

Cesium clock#1

3. priority

GNSS timing

1. priority

Timing over optical network (PTP)

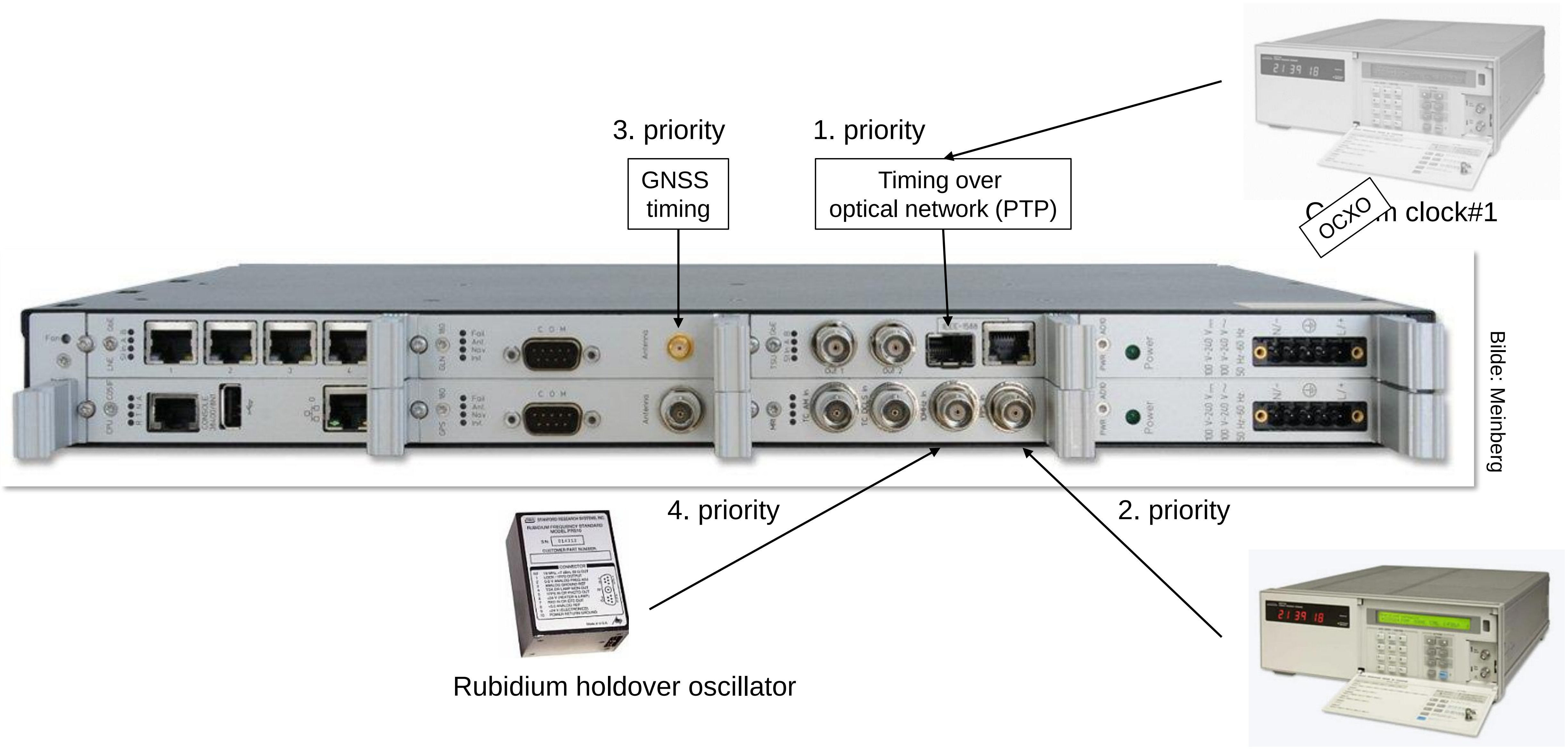
Bilde: Meinberg

4. priority

2. priority

Rubidium holdover oscillator

Cesium clock#2

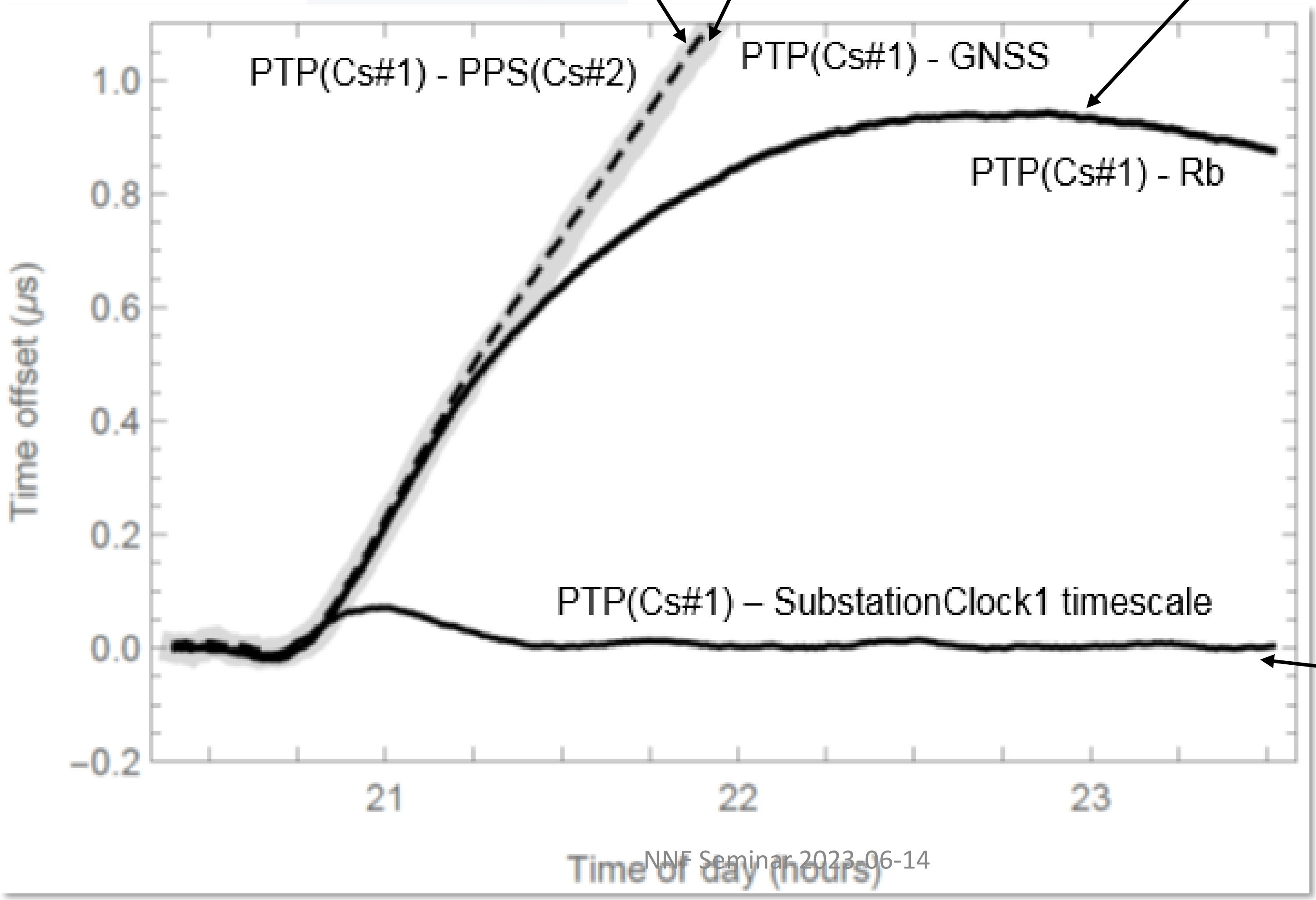


3. priority
1. priority
GNSS timing
Timing over optical network (PTP)
OCXO
Bilde: Meinberg
4. priority
2. priority
Rubidium holdover oscillator
Cesium clock#2

2. priority

3. priority
GNSS timing

4. priority



1. priority

Justervesenet

Conclusions

- Engineering challenge: National timing service keeping the performance of GNSS and reducing direct dependence
  - Robust multi-source systems (‘zero trust’)
  - Core timing network
  - Accurate clock nodes
- Distributing resilient timing over 5G may enable also alternative GNSS independent position and navgation

Extras

PNT security ∈ cyber security

https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=GPS

Name	Description
CVE-2022-36779	PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection Proscend M330-w / M33-W5 / M350-5G / M350-W5G / M350-6 / M350-W6 / M301-G / M301-GW ADVICE ICR 111WG / https://www.proscend.com/en/category/industrial-Cellular-Router/industrial-Cellular-Router.html https://cdn.shopify.com/s/files/1/0036/9413/3297/files/ADVICE_Industrial_4G_LTE_Cellular_Router_ICR1
CVE-2022-34769	PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection Proscend M330-w / M33-W5 / M350-5G / M350-W5G / M350-6 / M350-W6 / M301-G / M301-GW ADVICE ICR 111WG / https://www.proscend.com/en/category/industrial-Cellular-Router/industrial-Cellular-Router.html https://cdn.shopify.com/s/files/1/0036/9413/3297/files/ADVICE_Industrial_4G_LTE_Cellular_Router_ICR1
CVE-2022-34150	The main MiCODUS MV720 GPS tracker web server has an authenticated insecure direct object reference vulnerability on endpoint and parameter device IDs, which accept arbitrary device IDs without further verification.
CVE-2022-33944	The main MiCODUS MV720 GPS tracker web server has an authenticated insecure direct object references vulnerability on endpoint and POST parameter “Device ID,” which accepts arbitrary device IDs.
CVE-2022-27224	An issue was discovered in Galleon NTS-6002-GPS 4.14.103-Galleon-NTS-6002.V12 4. An authenticated attacker can perform command injection as root via shell metacharacters within the Network Tools section of the web-management interface. All three networking tools are affected (Ping, Traceroute, and DNS Lookup) and their respective input fields (ping_address, trace_address, nslookup_address).
CVE-2022-26019	Improper access control vulnerability in pfSense CE and pfSense Plus (pfSense CE software versions prior to 2.6.0 and pfSense Plus software versions prior to 22.01) allows a remote attacker with the privilege to change NTP GPS settings to rewrite existing files on the file system, which may result in arbitrary command execution.
CVE-2022-2199	The main MiCODUS MV720 GPS tracker web server has a reflected cross-site scripting vulnerability that could allow an attacker to gain control by tricking a user into making a request.
CVE-2022-2141	SMS-based GPS commands can be executed by MiCODUS MV720 GPS tracker without authentication.
CVE-2022-2107	The MiCODUS MV720 GPS tracker API server has an authentication mechanism that allows devices to use a hard-coded master password. This may allow an attacker to send SMS commands directly to the GPS tracker as if they were coming from the GPS owner’s mobile number.
CVE-2022-20081	In A-GPS, there is a possible man in the middle attack due to improper certificate validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06461919; Issue ID: ALPS06461919.
CVE-2021-37778	There is a buffer overflow in gps-sdr-sim v1.0 when parsing long command line parameters, which can lead to DoS or code execution.
CVE-2021-3720	An information disclosure vulnerability was reported in the Time Weather system widget on Legion Phone Pro (L79031) and Legion Phone2 Pro (L70081) that could allow other applications to access device GPS data.
CVE-2021-32929	All versions of Uffizio GPS Tracker may allow an attacker to perform unintended actions on behalf of a user.
CVE-2021-32927	An attacker may be able to inject client-side JavaScript code on multiple instances within all versions of Uffizio GPS Tracker.
CVE-2021-21292	Traccar is an open source GPS tracking system. In Traccar before version 4.12 there is an unquoted Windows binary path vulnerability. Only Windows versions are impacted. Attacker needs write access to the filesystem on the host machine. If Java path includes a space, then attacker can lift their privilege to the same as Traccar service (system). This is fixed in version 4.12.
CVE-2021-0547	In onReceive of NetInitiatedActivity.java, there is a possible way to supply an attacker-controlled value to a GPS HAL handler due to a missing permission check. This could lead to local escalation of privilege that may result in undefined behavior in some HAL implementations with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174151048
CVE-2020-5246	Traccar GPS Tracking System before version 4.9 has a LDAP injection vulnerability. It occurs when user input is being used in LDAP search filter. By providing specially crafted input, an attacker can modify the logic of the LDAP query and get admin privileges. The issue only impacts instances with LDAP configuration and where users can craft their own names. This has been patched in version 4.9.
CVE-2020-35552	An issue was discovered in the GPS daemon on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) (non-Qualcomm chipsets) software. Attackers can obtain sensitive location information because the configuration file is incorrect. The Samsung ID is SVE-2020-18678 (December 2020).
CVE-2020-11445	TP-Link cloud cameras through 2020-02-09 allow remote attackers to bypass authentication and obtain sensitive information via vectors involving a Wi-Fi session with GPS enabled, aka CNVD-2020-04855.
CVE-2020-0133	In MockLocationAppPreferenceController.java, it is possible to mock the GPS location of the device due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-145136060
CVE-2019-9534	The Cobham EXPLORER 710, firmware version 1.07, does not validate its firmware image. Development scripts left in the firmware can be used to upload a custom firmware image that the device runs. This could allow an unauthenticated, local attacker to upload their own firmware that could be used to intercept or modify traffic, spoof or intercept GPS traffic, exfiltrate private data, hide a backdoor, or cause a denial-of-service.
CVE-2019-20784	An issue was discovered on LG mobile devices with Android OS 7.0, 7.1, 7.2, 8.0, and 8.1 (MTK chipsets) software. Interaction of GPS with 911 emergency calls is mishandled. The LG ID is LVE-SMP-180012 (January 2019).
CVE-2019-20473	An i
CVE-2019-20471	An i
CVE-2019-20470	An i
CVE-2019-20468	An i
CVE-2019-15340	The
CVE-2019-15304	Lier app
CVE-2019-14951	The
CVE-2018-4851	A vu
CVE-2018-16554	The
CVE-2017-5239	Due
CVE-2017-5238	Due
CVE-2017-5237	Due
CVE-2017-17098	The
CVE-2017-17097	gps-
CVE-2017-14918	In A
CVE-2016-6727	The
CVE-2016-6544	getg
CVE-2016-6543	A ca d MAC/device ID of an iTrack Easy can be registered under multiple user accounts allowing access to getgps GPS data, which can allow unauthenticated parties to track the device.
CVE-2016-6540	U cated access to the cloud-based service maintained by TrackR Bravo is allowed for querying or sending GPS data for any Trackr device by using the tracker ID number which can be discovered as described in CVE-2016-6539. Updated apps, version 5.1.6 for iOS and 2.2.5 for Android, have been released by the vendor to address the vulnerabilities in CVE-2016-6538, CVE-2016-6539, CVE-2016-6540 and CVE-2016-6541.
CVE-2016-5348	The component in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-10-01, and 7.0 before 2016-10-01 allows man-in-the-middle attackers to cause a denial of service (memory consumption, and device hang or reboot) via a large xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 29555864.
CVE-2016-5341	Th PS component in Android before 2016-12-05 allows man-in-the-middle attackers to cause a denial of service (GPS signal-acquisition delay) via an incorrect xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 31470303 and external bug 211602 (and AndroidID-7225554).
CVE-2016-3801	T MediaTek GPS driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28174914 and MediaTek internal bug ALPS02688853.
CVE-2016-10135	ssue was discovered on LG devices using the MTK chipset with L(5.0/5.1), M(6.0/6.0.1), and N(7.0) software, and RCA Voyager Tablet, BLU Advance 5.0, and BLU R1 HD devices. The MTKLogger app with a package name of com.mediatek.mtklogger has application components that are accessible to any application that resides on the device. Namely, the com.mediatek.mtklogger.framework.LogReceiver and com.mediatek.mtklogger.framework.M orted since they contain an intent filter, are not protected by a custom permission, and do not explicitly set the android:exported attribute to false. Therefore, these components are exported by default and are thus accessible to any third party application by using android.content.Intent object for communication. These application components can be used to start and stop the logs using Intent objects with embedded data. The available logs ar obile log. The base directory that contains the directories for the 4 types of logs is /sdcard/mtklog which makes them accessible to apps that require the READ_EXTERNAL_STORAGE permission. The GPS log contains the GPS coordinates of the user as well as a timestamp for the coordinates. The modem log contains AT commands and their parameters which allow the user's outgoing and incoming calls and text messages to be obtained. The netw obile log contains the Android log, which is not available to third-party apps as of Android 4.1. The LG ID is LVE-SMP-160019.
CVE-2014-996	n all Qualcomm products with Android releases from CAF using the Linux kernel, the GPS client may use an insecure cryptographic algorithm.
CVE-2014-9194	Arbiter 1094B GPS Substation Clock allows remote attackers to cause a denial of service (disruption) via crafted radio transmissions that spoof GPS satellite broadcasts.
CVE-2014-8321	Stack-based buffer overflow in the gps_tracker function in airodump-ng.c in Aircrack-ng before 1.2 RC 1 allows local users to execute arbitrary code or gain privileges via unspecified vectors.
CVE-2014-5982	The RunKeeper - GPS Track Run Walk (aka com.fitnesskeeper.runkeeper.pro) application 4.7 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2014-5968	The iGolf - Golf GPS (aka com.igolf) application 20 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2013-2038	The NMEA0183 driver in gpsd before 3.9 allows remote attackers to cause a denial of service (daemon termination) and possibly execute arbitrary code via a GPS packet with a malformed $GPGGA interpreted sentence that lacks certain fields and a terminator. NOTE: a separate issue in the AIS driver was also reported, but it might not be a vulnerability.
CVE-2012-6336	The Missing Device feature in Lookout allows physically proximate attackers to provide arbitrary location data via a "commonly available simple GPS location spoofer."
CVE-2012-6335	The Anti-theft service in AVG AntiVirus for Android allows physically proximate attackers to provide arbitrary location data via a "commonly available simple GPS location spoofer."
CVE-2012-6334	The Track My Mobile feature in the SamsungDive subsystem for Android on Samsung Galaxy devices does not properly implement Location APIs, which allows physically proximate attackers to provide arbitrary location data via a "commonly available simple GPS location spoofer."
CVE-2012-6042	GPSMapEdit 1.1.73.2 allows user-assisted remote attackers to cause a denial of service (crash) via a long string in a lst file.
CVE-2012-1288	The UTC Fire & Security GE-MC100-NTP/GPS-ZB Master Clock device uses hardcoded credentials for an administrative account, which makes it easier for remote attackers to obtain access via an HTTP session.
CVE-2009-2204	Unspecified vulnerability in the CoreTelephony component in Apple iPhone OS before 3.0.1 allows remote attackers to execute arbitrary code, obtain GPS coordinates, or enable the microphone via an SMS message that triggers memory corruption, as demonstrated by Charlie Miller at SyScan '09 Singapore.
CVE-2009-0194	The domain-locking implementation in the GARMINAXCONTROL.GarminAxControl_t.1 ActiveX control in npGarmin.dll in the Garmin Communicator Plug-In 2.6.4.0 does not properly enforce the restrictions that (1) download and (2) upload requests come from a web site specified by the user, which allows remote attackers to obtain sensitive information or reconfigure Garmin GPS devices via unspecified vectors related to a "synchronisation error."
CVE-2008-5704	src/unit_test.c in gpsdrive (aka gpsdrive-scripts) 2.10~pre4 might allow local users to overwrite arbitrary files via a symlink attack on the /tmp/gpsdrive-unit-test/proc temporary file, a different vector than CVE-2008-4959 and CVE-2008-5380.
CVE-2008-5703	gpsdrive (aka gpsdrive-scripts) 2.10~pre4 allows local users to overwrite arbitrary files via a symlink attack on the (a) /tmp/.smswatch or (b) /tmp/gpsdrivepos temporary file, related to (1) examples/gpssmswatch and (2) src/splash.c, different vectors than CVE-2008-4959 and CVE-2008-5380.
CVE-2008-4959	geo-code in gpsdrive-scripts 2.10~pre4 allows local users to overwrite arbitrary files via a symlink attack on (1) /tmp/geo.google, (2) /tmp/geo.yahoo, (3) /tmp/geo.coords, and (4) /tmp/geo#####.coords temporary files.
CVE-2007-0554	SQL injection vulnerability in print.asp in Guo Xu Guos Posting System (GPS) 1.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2005-3523	Format string vulnerability in friendsd2 in GpsDrive allows remote attackers to execute arbitrary code via the dir (direction) field.
CVE-2004-1388	Format string vulnerability in the gpsd_report function for BerliOS GPD daemon (gpsd, formerly pygps) 1.9.0 through 2.7 allows remote attackers to execute arbitrary code via certain GPS requests containing format string specifiers that are not properly handled in syslog calls.
CVE-2003-0362	Buffer overflow in gPS before 0.10.2 may allow local users to cause a denial of service (SIGSEGV) in rgpsp via long command lines.
CVE-2003-0361	gPS before 1.1.0 does not properly follow the rgpsp connection source acceptation policy as specified in the rgpsp.conf file, which could allow unauthorized remote attackers to connect to rgpsp.
CVE-2003-0360	Multiple buffer overflows in gPS before 1.0.0 allow attackers to cause a denial of service and possibly execute arbitrary code.

CVE-ID	
CVE-2014-9194	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Arbiter 1094B GPS Substation Clock allows remote attackers to cause a denial of service (disruption) via crafted radio transmissions that spoof GPS satellite broadcasts.	

Effects of incoherent spoofing – Skibotn 2021

GNS Clock [CLK1 - checking time]:

Enable Outputs | Miscellaneous | Initialize Receiver

Priority	Source	Status	Offset
01	GNSS Receiver	Signal available, Is master, Is locked	- 66h 58m
02	PPS in	Signal available	-145.6ms [+150.0ns]
03	Fixed Freq. in	Signal available	-41.60ms
-	IRIG	Not prioritized	N/A
-	NTP	Not prioritized	N/A
-	PTP (IEEE1588)	Not prioritized	N/A
-	PPS plus string	Not prioritized	N/A

Information

GNS Clock [CLK1]:

Common Information

Name	Value
GNSS Status:	NORMAL OPERATION
GPS Position LLA:	LAT: 70.0000 LON: 10.0000 ALT: 89m
GPS Position LLA Degree:	LAT: 70° 00' 0" N LON: 10° 00' 0" E ALT: 89m
GPS Position XYZ:	X:2154718m Y: 379935m Z:5971124m

Justervesenet

How dependent on accurate timing?

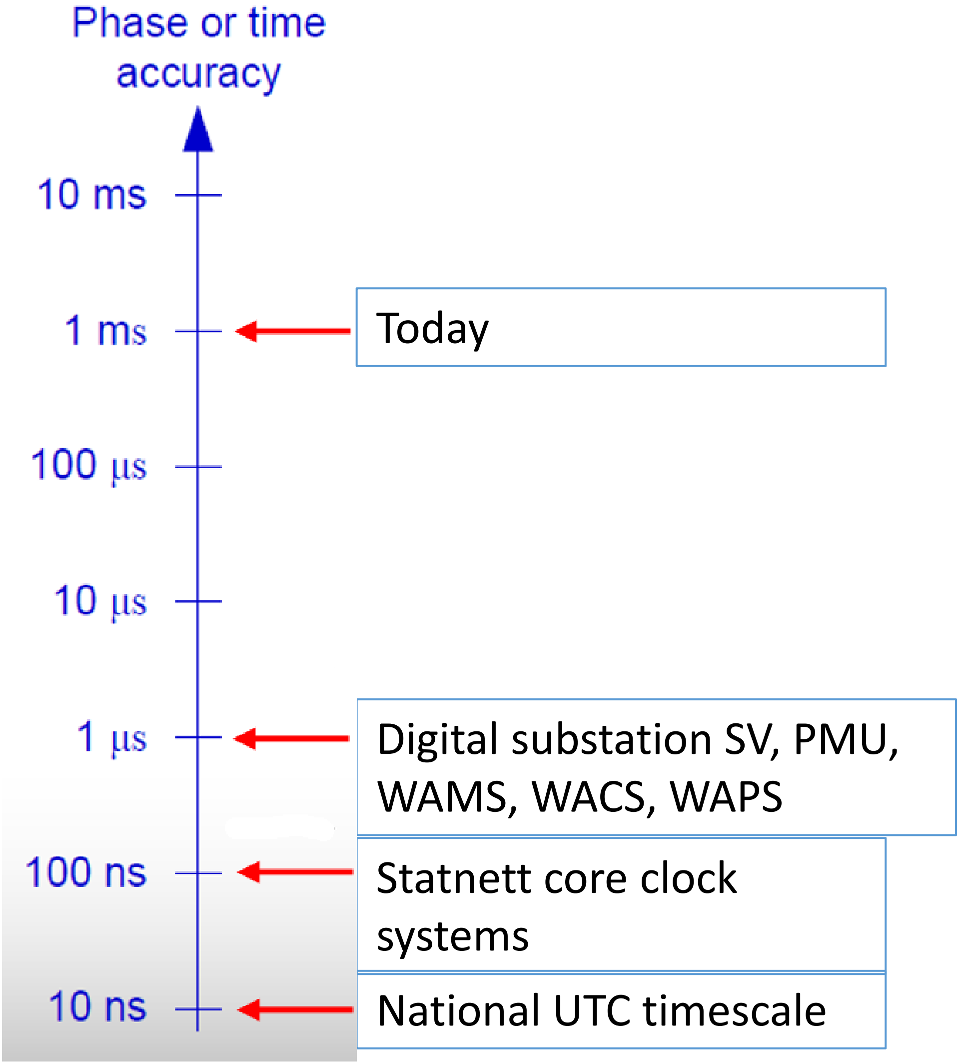
Nice to have

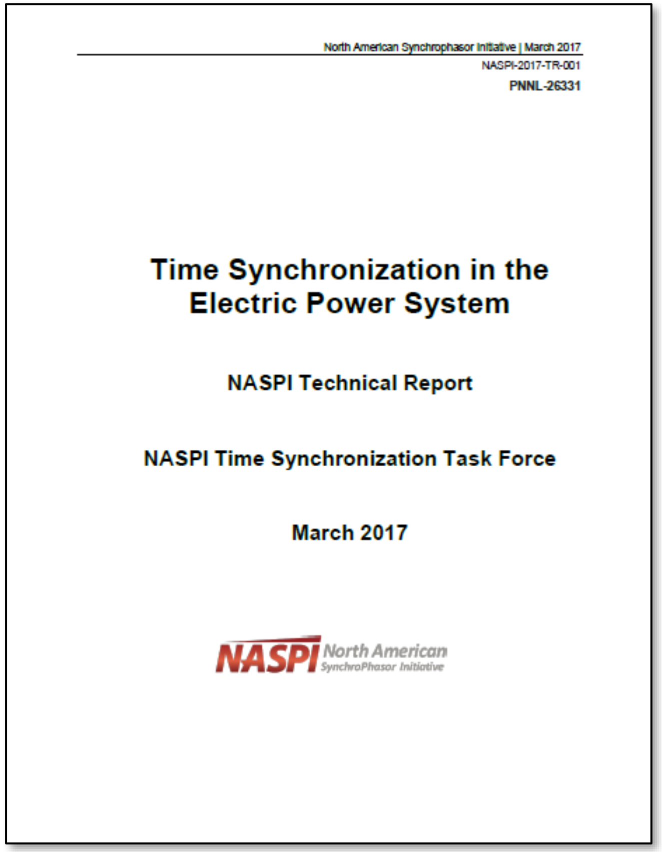
- Better real-time system modelling
- Better fault analysis
- Faster fault localization
- Leaner substations
- Better wide-area monitoring (WAMS)

Need to have

- Synchronized sampled values within substations
- Wide-area synchronized data for protection (WAPS)
- Wide-area synchronized data for control (WACS)

How accurate?




North American Synchrophasor Initiative | March 2017
NASPI-2017-TR-001
PNNL-26331

Time Synchronization in the Electric Power System

NASPI Technical Report

NASPI Time Synchronization Task Force

March 2017

NASPI North American SynchroPhasor Initiative

https://www.naspi.org/node/608