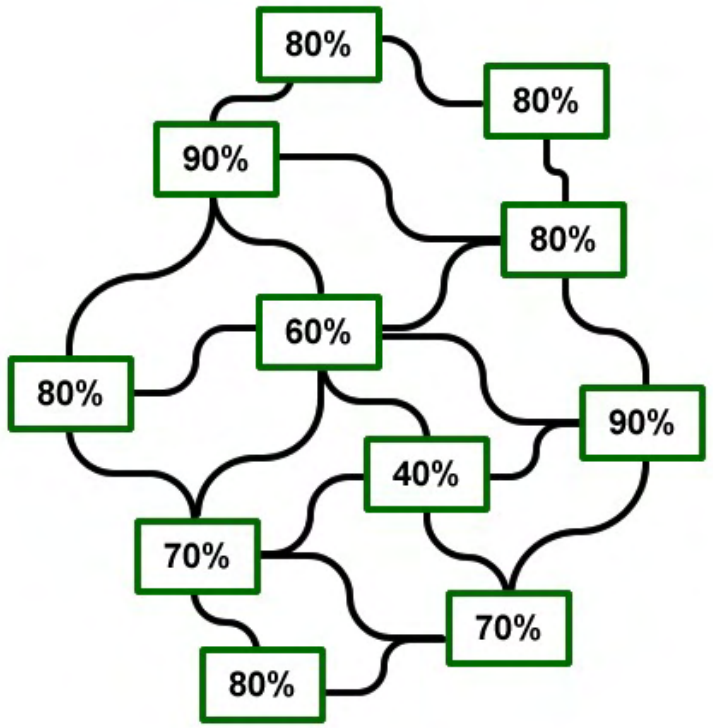
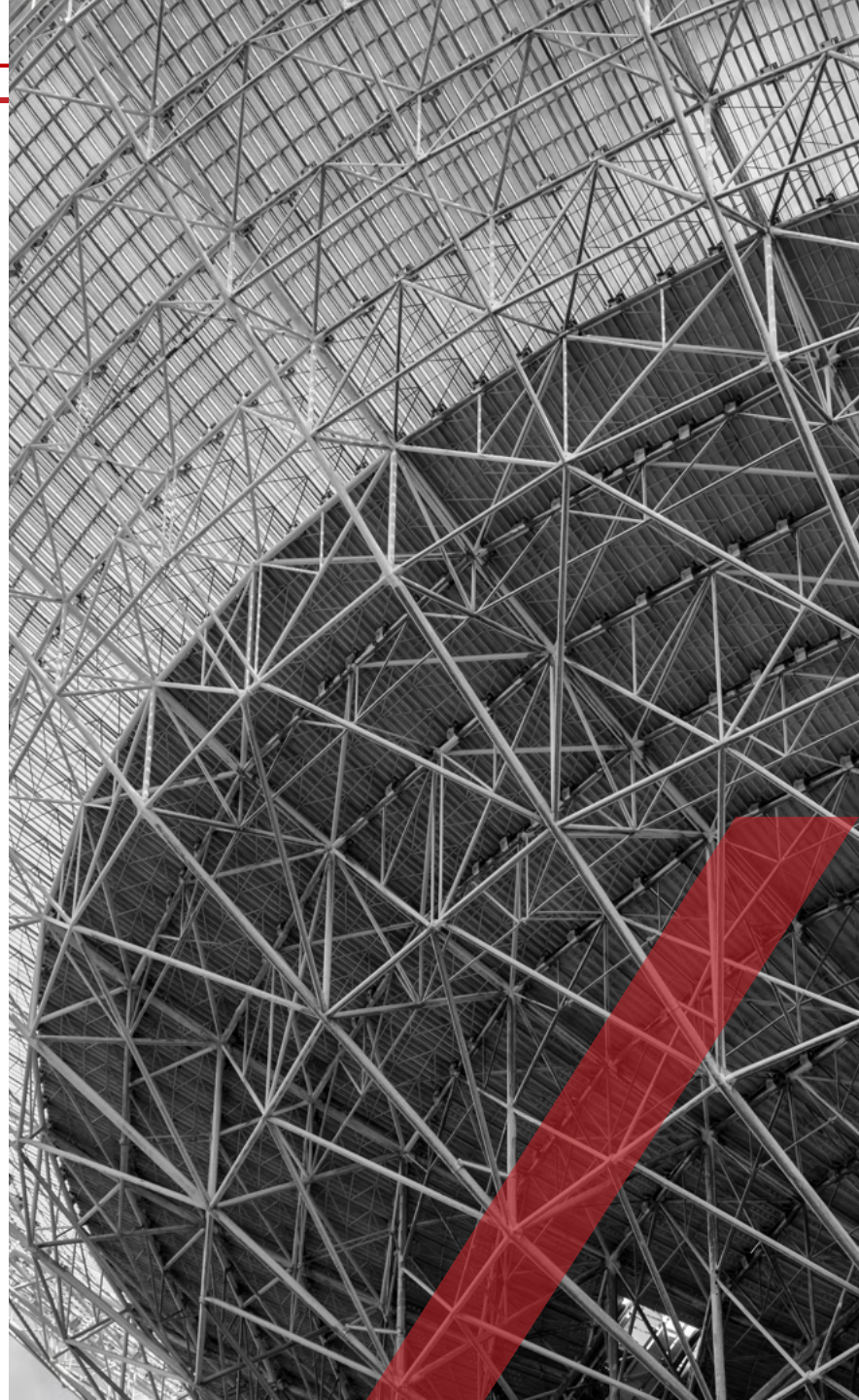
ELPROMA PIK TIME SYSTEMS®

Why do the Critical Infrastructures of Industry 4.0 Misunderstand the Modern Cybersecurity Paradigm of Synchronization?

Tomasz Widomski
www.elpromatime.com



Network running normally

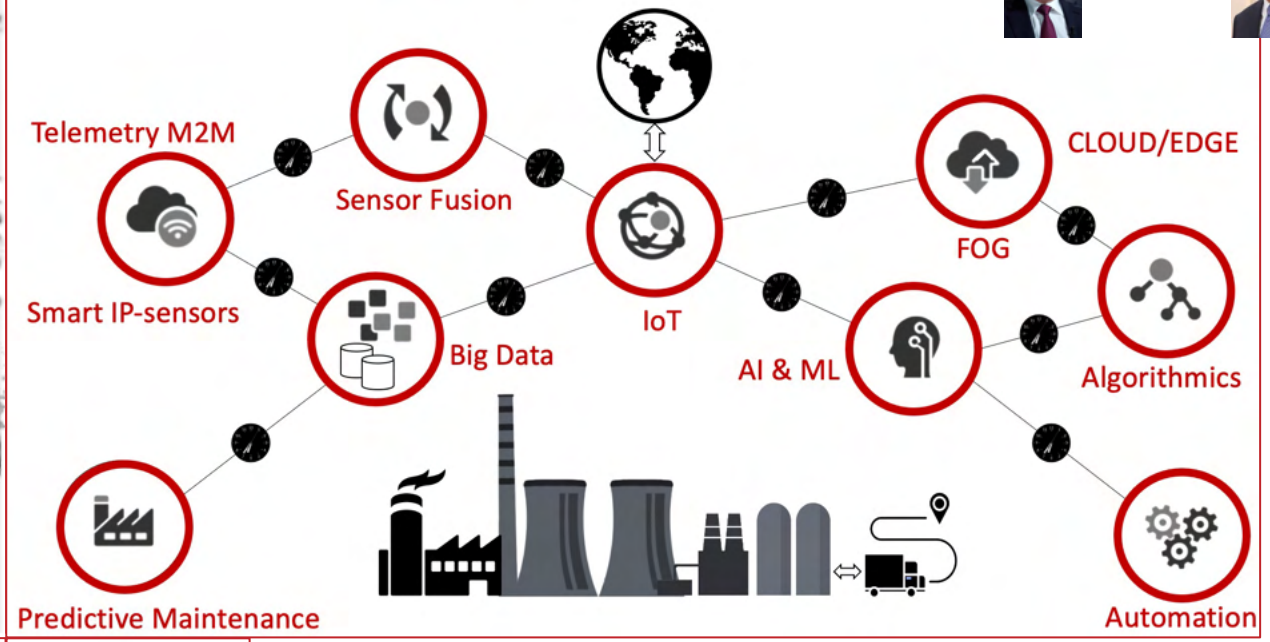


Retrospective vs. Predictive Maintenance

Mongolian Empire of Genghis Khan AD 1200

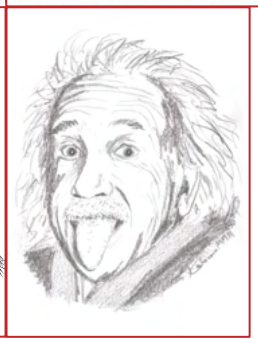
Retrospective Maintenance

Global Industry 4.0 "Empire" Today



Predictive Maintenance

Isaac Newton
Absolute TIME concept



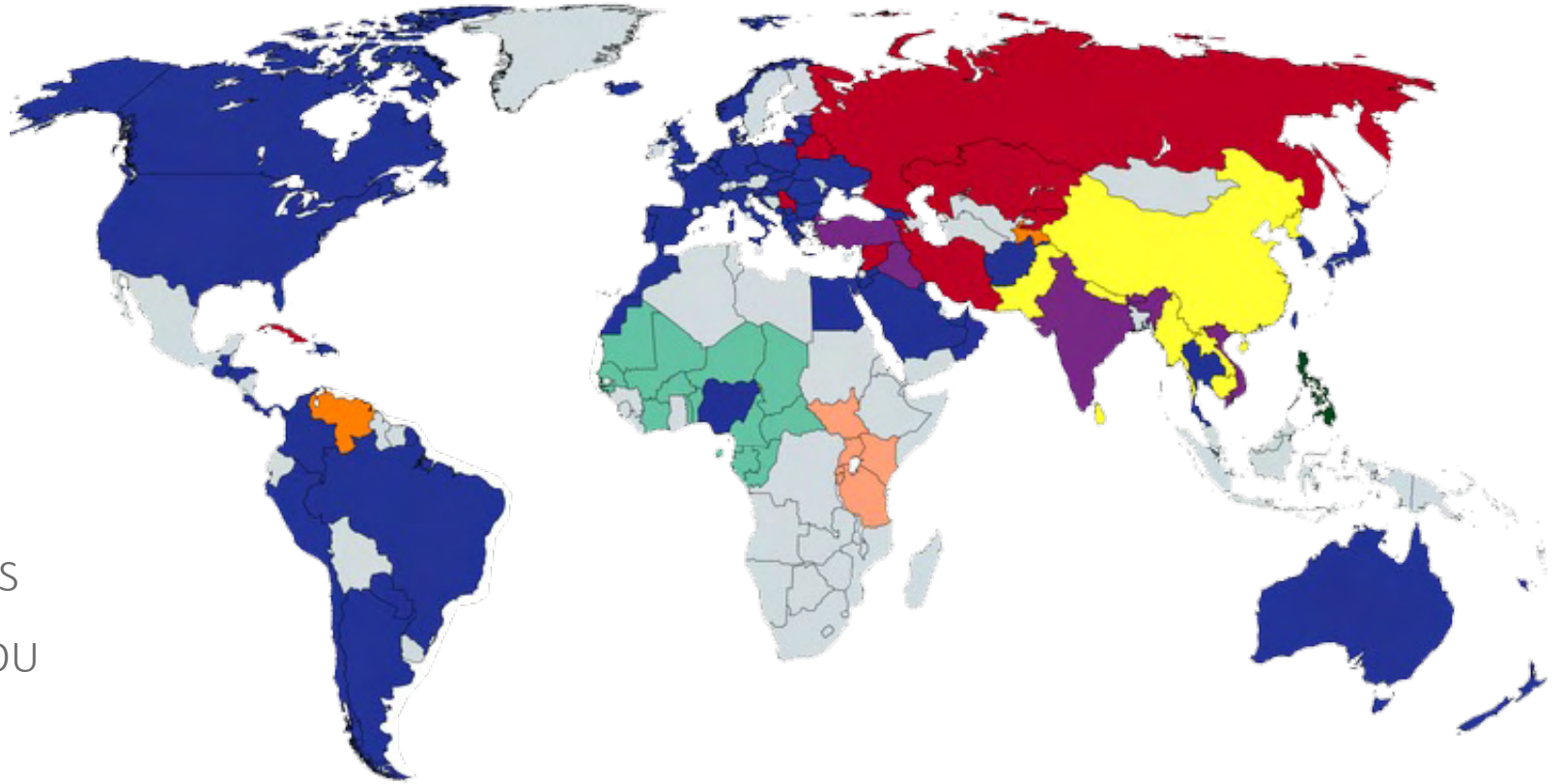
Albert Einstein
Relative TIME concept

YouTube
ITFS2020

GNSS Sync vs. Geopolitics

US Directive EO 13905 (02/2020)

GPS, GLONASS, NEIDOU, IRNSS are millitary
GALILEO is civil



The sensitivity of GNSS geopolitics :

- US friendly => GPS + GALIEO
- CN friendly => BEIDOU
- RU friendly => GLONASS
- US & RU friendly => IRNSS+GPS+GLONASS
- US & CN friendly => GPS+GALILEO+BEIDOU
- all others => any GNSS (neutral)

What Is a Real UTC Output From GNSS Receiver ?

GNSS Errors

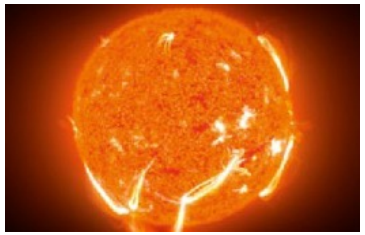
GPS SVN23 causes 13 microsecond 26/01/2016
GLONASS causes 200km problem on 01/04/2014

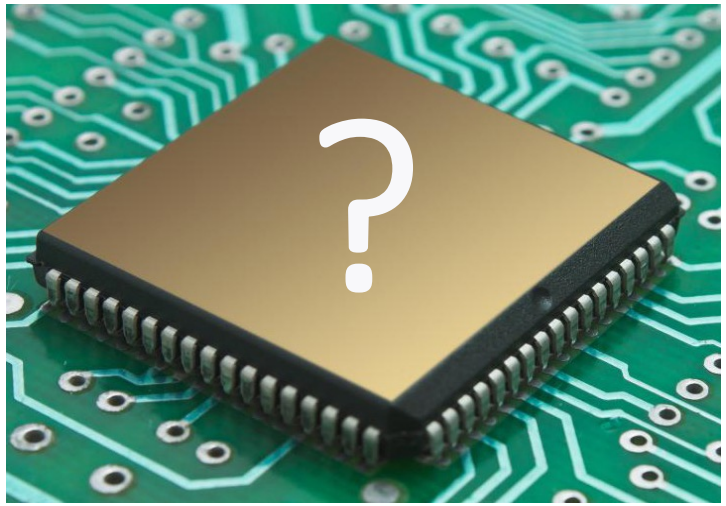
Numeric Overlows

caused by miniaturization and challenge of computing the time
GPSd 24/10/2021, WNRO 06/04/19, … UTC Leap Second etc.

Solar storms

Disturbancies of magetic field
by streams of charged particles





Urban canyon

Dense of cityscapes create
urban canyon eefects

A thought experiment

- *Assuming the GNSS company is US,*
- *and it's r&d in Russia,*
- *and production in China,*

What is the target UTC it produce ?
GPST, GLONASST, BEIDOUT … or MIX ?

Spoofing

Signals can be spoofed with a false
signals creating false timing

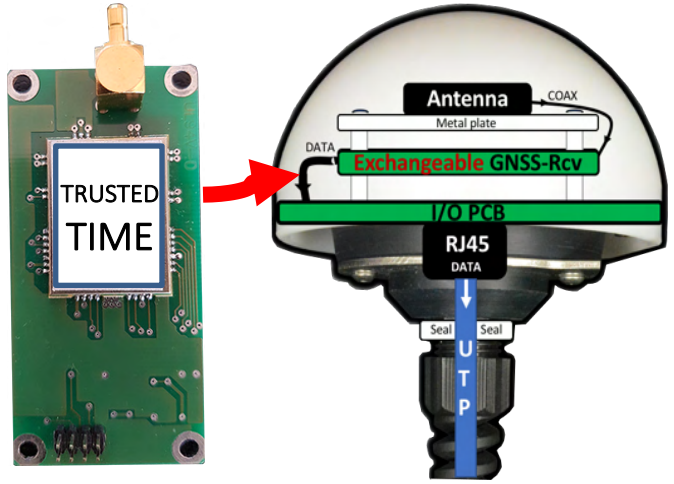
Jamming

Signals can be deliberately jammed by drivers
dodging emloyers attemps to track then.

YouTube link Security Trough Flexibility

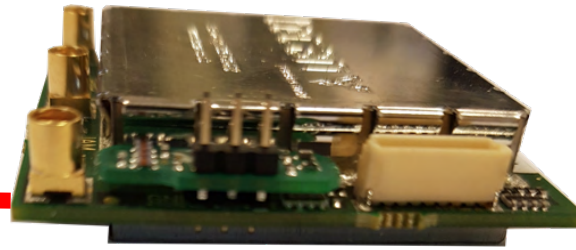
1) The replaceable GNSS-receivers supports different vendors

- makes time-server independent on volatile security of GNSS
- best world leading CHIP suppliers, only well tested, calibrated etc.
- quick replacement to next CHIP module (e.g. if firmware bug detected)
- smart gain sensing (no signal to weak or signal to strong like an “overdrive”)
- multi-path mitigation for urban canyon reflected signals
- geopolitics settings => exclusive: GPS, GALIELO, GLONASS, BEIDOU, IRNSS
- single band L1 or multiband L1 + L2 + L5 for improving robust synchronization
- UTC with robust LEAP-SECOND support supported independently on GNSS



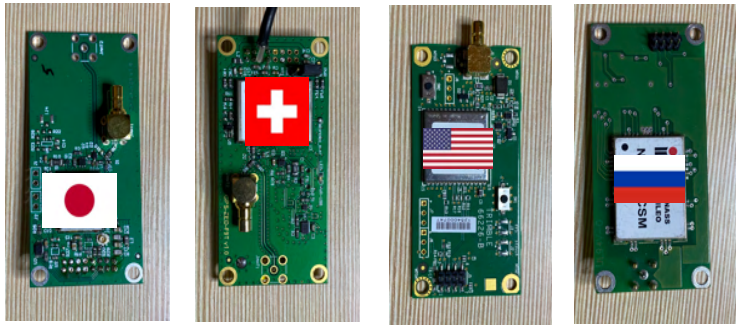
2) Built-in anti-jamming/spoofing detection and active anti-jamming filter

- alarm generated down to server – it switches early to holdover
- jamming filtering GPS L1 with upgrade to anti-spoofing GNSS L1/L2/L5



2) Real physical redundancy of GNSS receivers – each operating as CLOCK

- introduces the natura geographical anti-jamming if distance high enough



4) Extremely Easy installation. No taught mounting coax. Ethernet cable in use

Thales Alenia Space GIANO Project - Tests In Poland
The 1st Galileo Anti-Spoofing Receiver w/ T-RAIM Authentication

- ***Multi-GNSS*** *GPS/Galileo/EGNOS,*
- ***Multi-frequency*** *L1/E1, L5/E5a, E6*
- ***Direct-Sampling*** *digital down-conversion approach*
- *Resilience against* ***Jamming & Spoofing***
- *Galileo OS authentication* ***T-RAIM algorithm***
- ***Digital Time-Steering*** *and* ***Holdover mode***

TTS-5/OSTT-4

Cs fountain

5071A w/ NTS-5000

Advanced Jamming Tests In Poland

ELPROMA in cooperation with

iTTi e-technologie i biznes

Łukasiewicz
Przemysłowy Instytut Automatyki i Pomiarów PIAP

ZKR-1 Jamme

- ✓ Modes of operation:
  - Continuous jamming
  - Responsive jamming
  - Spectrum scanning
- ✓ Frequency range:
  - 25-5900 MHz
- ✓ Total RF output power:
  - 150 W

Tests hosted in dedicated specialized areas under special state & telco acknowledgments

Missing The Standardisation For Oscillator Holdover

AIR FORCE OFFICIAL PRESS RELEASE - GPS GROUND SYSTEM ANOMALY

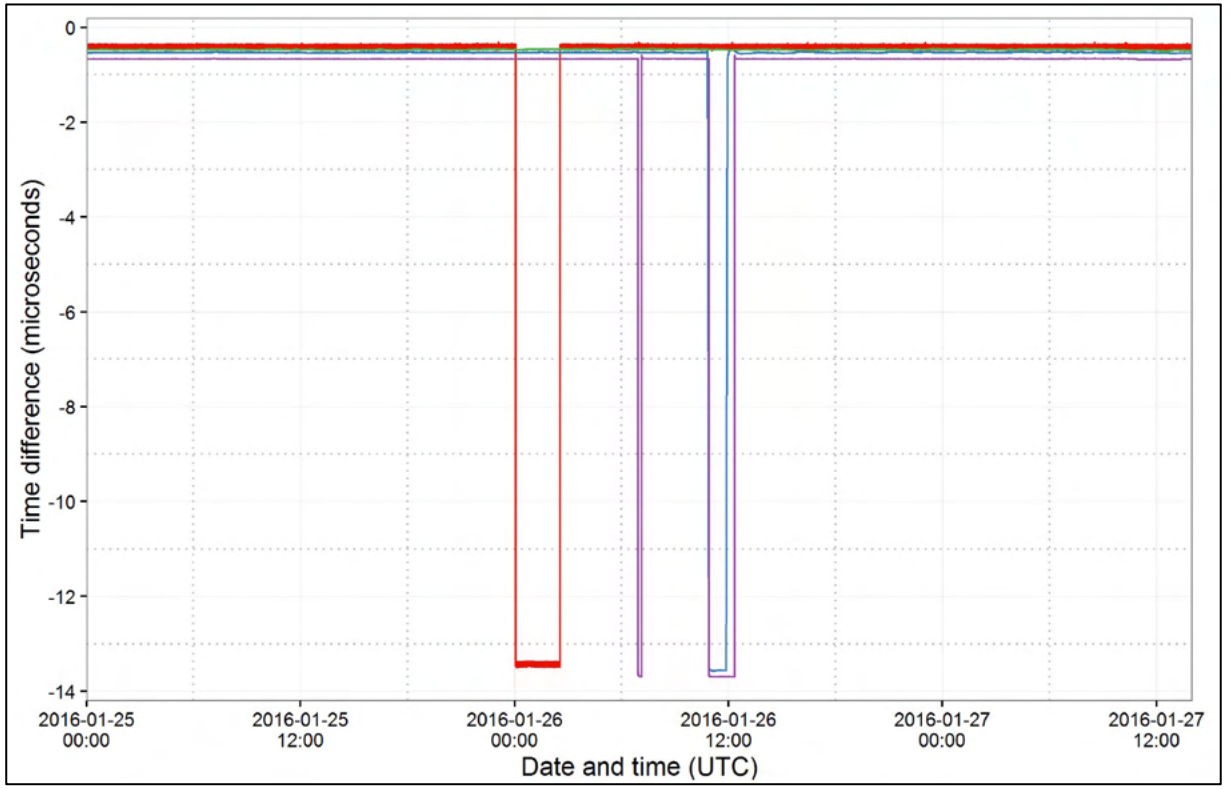
JAN 27, 2016

On 26 January at 12:49 a.m. MST, the 2nd Space Operations Squadron at the 50th Space Wing, Schriever Air Force Base, Colo., verified users were experiencing GPS timing issues. Further investigation revealed an issue in the Global Positioning System ground software which only affected the time on legacy L-band signals. This change occurred when the oldest vehicle, SVN 23, was removed from the constellation. While the core navigation systems were working normally, the coordinated universal time timing signal was off by 13 microseconds which exceeded the design specifications. The issue was resolved at 6:10 a.m. MST, however global users may have experienced GPS timing issues for several hours. U.S. Strategic Command's Commercial Integration Cell, operating out of the Joint Space Operations Center, effectively served as the portal to determine the scope of commercial user impacts. Additionally, the Joint Space Operations Center at Vandenberg AFB has not received any reports of issues with GPS-aided munitions, and has determined that the timing error is not attributable to any type of outside interference such as jamming or spoofing. Operator procedures were modified to preclude a repeat of this issue until the ground system software is corrected, and the 50th Space Wing will conduct an Operational Review Board to review procedures and impacts on users. Commercial and civil users who experienced impacts can contact the U.S. Coast Guard Navigation Center at (703) 313-5900.

Reference US AIR FORCE

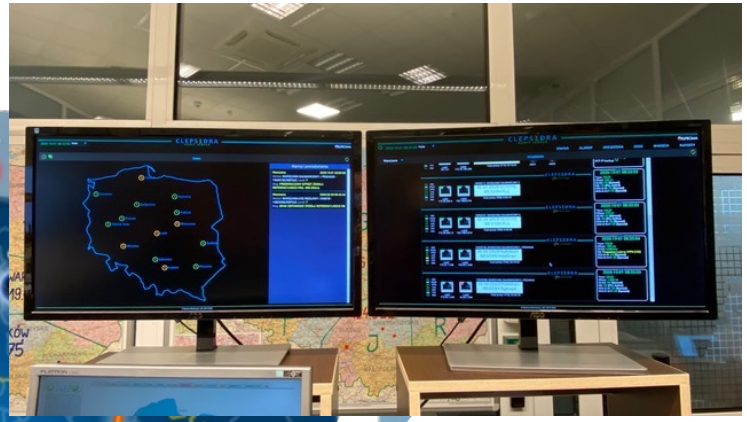
Anomalies:

- GPS SVN23 problem => 5 tested product gives 5 different results
- Depends on holdover algorithm the same effect can be observed too …



Reference Metsähovi Radio Observatory

Time & Frequency Domain At NLPQT Project (Poland)
The National Laboratory of Photonics & Quantum Technology



- *Supercomputer network*
- *Protected by QKD*
- *UTC(PL) T&F domain*
- *Single photon technology*
- *Picosecond synchronization*
- *Cesium fountain frequency ref.*
- *OSTT-4, NTS-5000 ePRTC 1PPS/10MHz transfer*
- *Considering ref. time for 5G backbone Poland*
- *Considering PNT in Poland*
- *Considering Quantum Internet in Poland*

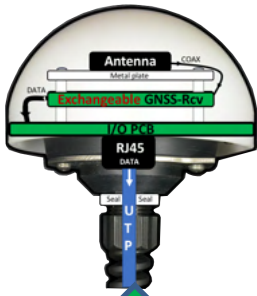
ELPROMA PIK TIME SYSTEMS®

GNSS ALARMING

LEVEL 1

NMI

CLOUD TaaS



NMI

TIME and/or GNSS robust info telemetry

FILETERED ANT 1

UNFILTERED ANT 2

RF INPUT

ANT-1 PRIMARY

ANT-1 SECONDARY

ANT-2 UNITARY

FILETRING

LEVEL 2

INPUT ANT

SIMULATED OUTPUT

IRIG-B IN

IRIG-B OUT

10MHz

1PPS IN

1PPS OUT

BNC T1 E1

SIMULATION

LEVEL 3

LAN 1

EXPANDER #1

EXPANDER #2

1PPS OUT

LAN 5 LAN 6

EXPANDER #3

SERVER

NTS-345

EXPANDER #4

1PPS OUT

LAN 9 LAN 10

EXPANDER #5

#2 IRIG-B OUT

#3 IRIG-B OUT

#4 IRIG-B OUT

#5 IRIG-B OUT

PE

ANT 1

ANT 2

IRIG-B IN

IRIG-B OUT

10MHz IN

10MHz OUT

1PPS IN

1PPS OUT

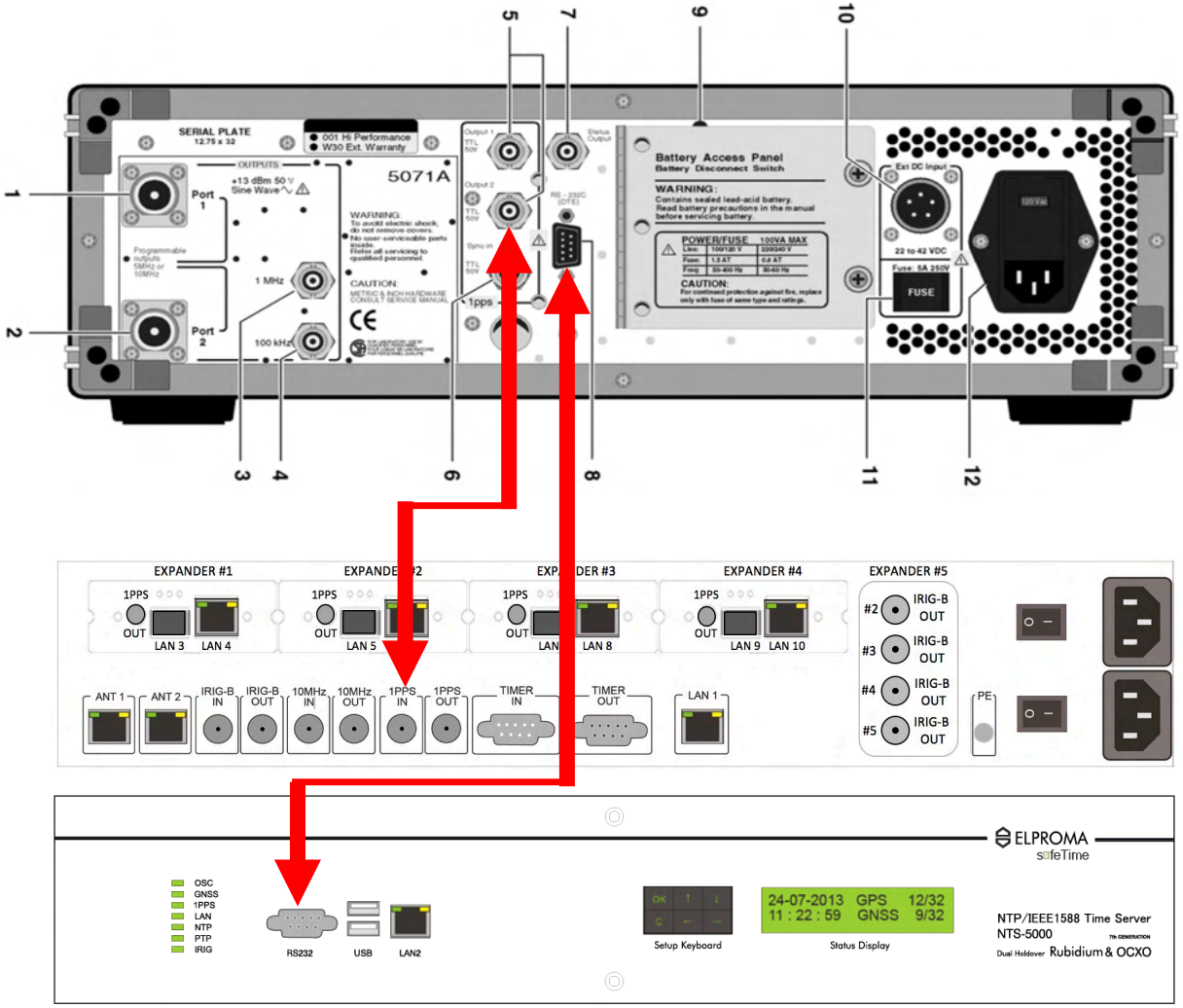
TIMER IN

TIMER OUT

LAN 1

UTC Directly From Cs Atomic Clock 5071A

YouTube link



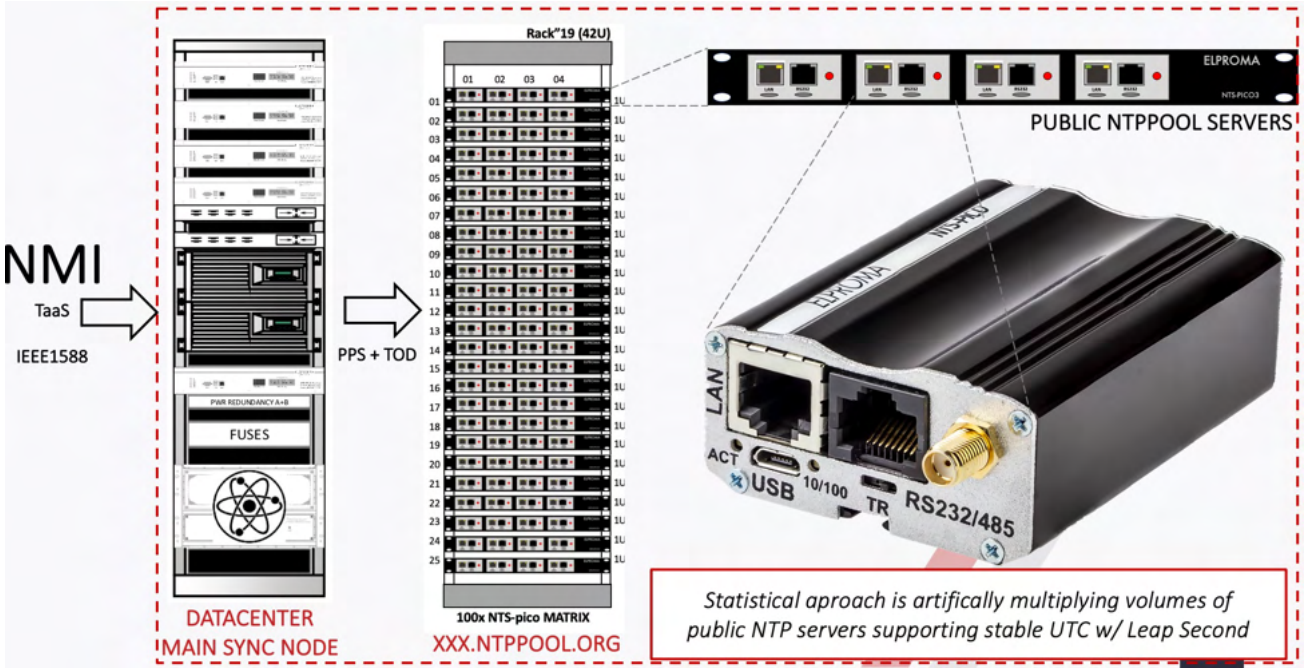
- ✓ No GNSS antennas
- ✓ UTC for IEEE15888 & NTP hosted only from 5071A
- ✓ Note! TAI is not basing on a physical clocks

IoT & Public NTP Servers

NTP Pool Project

https://www.ntppool.org

- Hundrets of milions IoT devices world wide
- Enterprises using LINUX servers
- Risk of getting “in touch” to darknet servers
- Trusted UTC incl. leap second s can not be ensured by POOL



5’ Bulgaria — bg.pool.ntp.org (43)
Belarus — by.pool.ntp.org (6)
Switzerland — ch.pool.ntp.org (178)
Cyprus — cy.pool.ntp.org (7)
Czech Republic — cz.pool.ntp.org (50)
1 Germany — de.pool.ntp.org (776)
Denmark — dk.pool.ntp.org (59)
Estonia — ee.pool.ntp.org (11)
Spain — es.pool.ntp.org (16)
Finland — fi.pool.ntp.org (76)
Faroe Islands — fo.pool.ntp.org (0)
2 France — fr.pool.ntp.org (331)
Guernsey — gg.pool.ntp.org (0)
Gibraltar — gi.pool.ntp.org (2)
Greece — gr.pool.ntp.org (20)
Croatia — hr.pool.ntp.org (8)
Hungary — hu.pool.ntp.org (51)
Ireland — ie.pool.ntp.org (16)
Isle of Man — im.pool.ntp.org (1)
Iceland — is.pool.ntp.org (16)
Italy — it.pool.ntp.org (41)
Jersey — je.pool.ntp.org (0)
Liechtenstein — li.pool.ntp.org (2)
Lithuania — lt.pool.ntp.org (16)
Luxembourg — lu.pool.ntp.org (14)
Latvia — lv.pool.ntp.org (21)
Monaco — mc.pool.ntp.org (1)
Moldova — md.pool.ntp.org (15)
Republic of Montenegro — me.pool.ntp.org (0)
Macedonia — mk.pool.ntp.org (6)
Malta — mt.pool.ntp.org (0)
4 Netherlands — nl.pool.ntp.org (259)
Norway — no.pool.ntp.org (41)
Poland — pl.pool.ntp.org (47)
Portugal — pt.pool.ntp.org (11)
Romania — ro.pool.ntp.org (18)
Republic of Serbia — rs.pool.ntp.org (13)
5” Russian Federation — ru.pool.ntp.org (150)
Sweden — se.pool.ntp.org (83)
Slovenia — si.pool.ntp.org (16)
Svalbard and Jan Mayen — sj.pool.ntp.org (0)
Slovakia — sk.pool.ntp.org (20)
San Marino — sm.pool.ntp.org (0)
Turkey — tr.pool.ntp.org (25)
Ukraine — ua.pool.ntp.org (60)
3 United Kingdom — uk.pool.ntp.org (299)

Active Servers

Africa	49
Asia	323
Europe	2773
North America	979
Oceania	145
South America	60
Global	4056
All Pool Servers	4309

As of 2021-10-30

ITU-R WP7A – contribution. Freezing UTC Leap Seconds

https://www.itu.int/md/R19-WP7A.AR-C/en => Document #15

ELPROMA ELECTRONICS

Date: the 12th of Apr 2021

PL 05-152 Czosnow, ul Dunska 2A, Poland www.elpromatime.com

The expert recommendation of activities regarding future UTC leap-second support

To Whom it may concern,

Further continuation of handling *UTC leap second* introduces a high risk of failure for IT and Industry4.0 (OT). Although the leap-second problem has always existed, currently with exponentially growing automation and the close interdependence of entire Industry4.0 systems, there is recommendation for immediate suspension of the *UTC leap-second*. Currently considered the first in history negative leap-second makes us especially worry.

The global economy is strongly dependent on GNSS, which provides the UTC reference to all modern critical infrastructures, such as distributed smart grids, telecom 5G, financial markets and broadcasting. Moreover, the observed strong migration of smaller IT/OT systems to CLOUD makes it a 5th critical infrastructure. The following problem affects all countries and all segments of each individual economy. It is complicated by the lack of leap-second servicing standard, the poor dialogue between the IT and time metrology community, the diversity of implementation of GNSS receivers, as well as different approach of serving UTC between GLONASS vs. GPS/GALILEO/BEIDOU/IRNSS.

The leap-second makes UTC time scale discrete, hence appearance of problems such as:

1) Time discrepancies in distributed system, where the validity of the data is determined by difference between *remote sensor timestamp* and receiving local timestamp of central server. This may lead to the acceptance of invalid data (wrongly computed DELAY) and, consequently, to the wrong predictive management. Such risk will increase with the growing popularity of TSN (Time Sensitive Networking) and TCC (autonomous Time Coordinated Computing) at Industry4.0

2) Failures of software and firmware of IoT devices based on the Windows or Linux/Unix kernels. Please note, that every modern IT / IoT device produced as of today has a firmware based on one of the operating systems listed above. The unexpected peaks in time introduced by the UTC leap second are dangerous for stability of the OS-kernel. They disturb the low-level event chronology, according to which concurrency management and the low-level utilization of system processes take place. Disturbing the chronology results in the "kernel panic" – risk causing crash of the operating system (OS), firmware or even a part of CLOUD.

The UTC leap second can trigger a large-scale domino effect, leading to a blackout: in telecom, power systems and Industry 4.0 automation. Sooner or later, such failures must begin to occur, unless a leap-second suspension remains effective. We consider a negative leap second, which has never been put into practice before, to be particularly very dangerous experiment on a working active production environment.

on behalf of Elproma

Tomasz Widomski
Member of Supervisory Board

Radiocommunication Study Groups

Received:

Subject: Working document towards a preliminary draft new Report ITU-R TF.[UTC]

Document 7A/xx-E
26 August 2021
English only

Poland

PROPOSED ADDITION TO WORKING DOCUMENT TOWARDS A PRELIMINARY DRAFT NEW REPORT ITU-R TF.[UTC]

As part of the preparation by WP 7A of a draft new report on UTC responding to Resolution 655 (WRC-15), Poland proposes additions to chapter 6:

- *Chapter 6 on* Impact of a possible change in the definition of UTC on radiocommunication services and other applications;
- *creating new section* 6.12 *on* Impact on other applications - IT and Industry 4.0, containing proposed text given below;
- *creating new section* 6.13 *on* Impact on other applications – not technical, containing the original text of section 6.12 without modification.

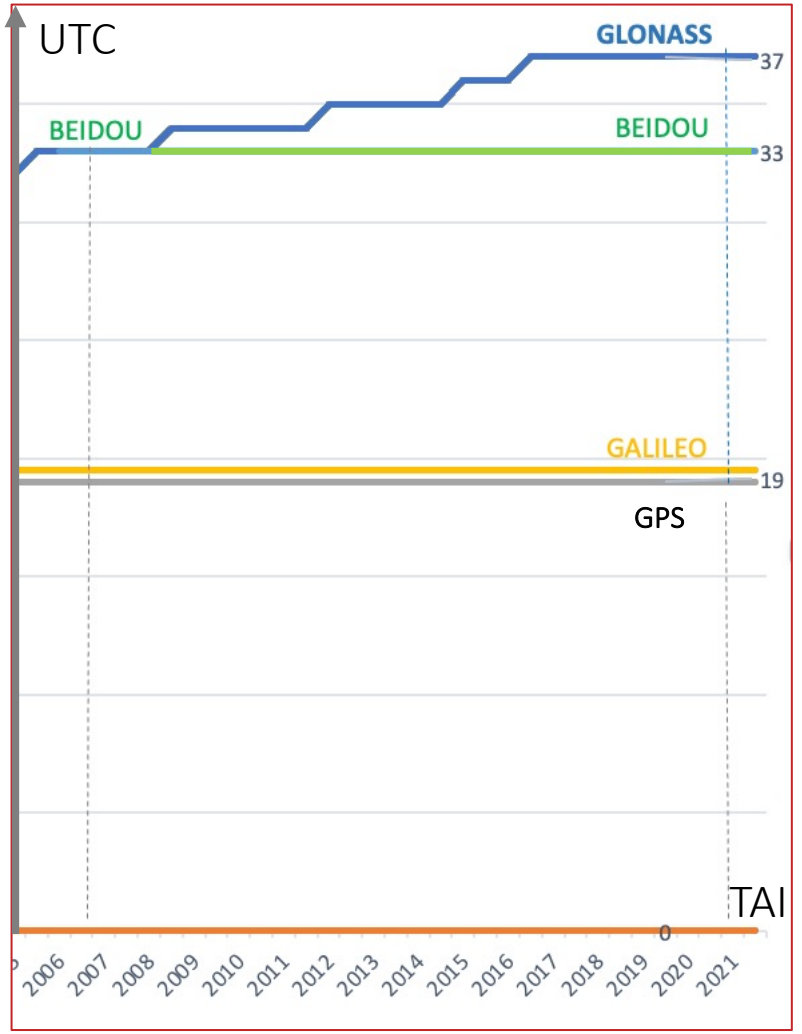
The global economy is strongly dependent on GNSS, which provides the UTC reference to all modern critical infrastructures, such as distributed smart grids, telecom 5G, financial markets and broadcasting. Moreover, the observed strong migration of smaller IT and Industry 4.0 (OT) systems to CLOUD makes it a 5th critical infrastructure. The following problem affects all countries and all segments of each individual economy. It is complicated by the lack of leap-second servicing standard, the poor dialogue between the IT and time metrology community, the diversity of implementation of GNSS receivers, as well as different approach of serving UTC between GLONASS vs. GPS / GALILEO / BEIDOU / IRNSS.

Further continuation of handling *UTC leap second* introduces a high risk of failure for IT and OT. Although the leap-second problem has always existed, currently with exponentially growing automation and the close interdependence of entire Industry 4.0 systems, there is a need for urgent suspension of the *UTC leap-second*. Currently considered the first in history negative leap-second makes users especially worry.

The leap-second makes UTC time scale discrete, hence appearance of problems such as:

1) Time discrepancies in distributed system, where the validity of the data is determined by difference between *remote sensor timestamp* and receiving local timestamp of central server. This may lead to the acceptance of invalid data (wrongly computed DELAY) and, consequently, to the wrong predictive management. Such risk will increase with the growing popularity of TSN (Time Sensitive Networking) and TCC (autonomous Time Coordinated Computing) at Industry 4.0;

2) Failures of software and firmware of IoT devices based on the Windows or Linux/Unix kernels. It is to be noticed, that every modern IT / IoT device produced as of today has a firmware based on one of the operating systems listed above. The unexpected peaks in time introduced by the UTC leap second are dangerous for stability of the OS-kernel. They disturb the low-level event chronology, according to which concurrency management and the low-level utilization of system



Our Contribution

- **ITU (International Telecom Union)** removing UTC leap-second link (doc #15) — 2021-2022
  - ITFS2020 importance of time for Industry 4.0 (You Tube link)
  - G2 Forum Geo-political TV discussion with 3M, Elproma (You Tube link)
- **TAP Project (OCP)** – replaceable GNSS modules GM PCIe from Facebook/NVIDIA — 2020
  - Elproma contribution to Facebook & NVIDIA video (You Tube link)
  - OCP Project Page listing ELPROMA as participant (7th Oct 2020 link)
- **GIANO Project** (Thales Alenia Space) – the 1st professional GALILEO Timing Rcv with Anti-Spoofing Authentication Facility (together with PIK-Time) — 2019-2022
- **DEMETRA Project H2020** TSI#2 "*Trusted Time Distr. w/ Audit & Verif. Facility*" — 2015-2017
  - Horizon2020 Demetra GSA web page (link)
  - PTTI/ION 2016 Demetra TSI#2 PDF paper (link)
  - Success Story in Asia Smart-Grids (link)
- **CERN White Rabbit** co-developer (today's High Accuracy IEEE1588:2019 stack) — 2009-2014
  - PTTI/ION 2011 very first introduction PDF paper (link)
  - CERN original team list 2009-2014 (link)

ITU Radiocommunication Study Groups WP-7A

OPEN Compute Project®

European Commission Innovation and Networks Executive Agency

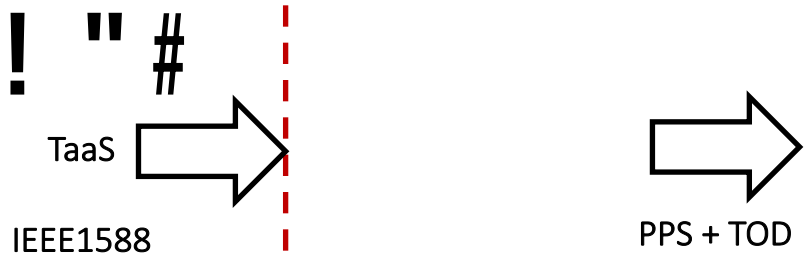
HORIZON 2020

CERN

Thank You

t.widomski@elpromatime.com
www.elpromatime.com

Apendix



PUBLIC NTPPOOL SERVERS

DATACENTER
MAIN SYNC NODE

XXX.NTPPOOL.ORG

Statistical aproach is multiplying volumes of public NTP servers, supporting stable UTC w/ Leap Second