Project: **DEFIS/2020/OP/0007-3 Alternative Positioning, Navigation and Timing (PNT) Services**	*File: Test Plan v2.1.docx*

D210 Technical Report

SCPTime®

Creation date	Creator	Editor	Approver
03/09/2021	Y. Jin	Y. Jin	J. Thimonier

Version	Creator	Date	Comments
v0.5	Y. Jin	29/09/2021	Draft test plan
v0.6	Y. Jin	28/10/2021	Final test plan
V1.0	Y. Jin	04/11/2021	Final test plan
V1.5	J. Thimonier	07/02/2022	T1-T4 tests results
V2.0	J.Thimonier	18/03/2022	Minor modifications
V2.1	J.Thimonier	24/03/2022	Minor modifications

I. Table of Contents

I.Introduction

This document describes the SCPTime technology offering an alternative timing service and the test plan that is related to the demonstration activities to be conducted at JRC and in France.

II.SCPTime technology

i. Description of the alternative Timing technologies

SCPTime® is the result of 5 years of R&D by bringing together knowhow, technologies, and expertise from the French Time/Frequency ecosystem.

SCPTime® is intended to make the legal time (UTC time, as defined by authorities of a country, a region, or an organization) available to the largest number of users, in a secured and traceable way from its source to the end user, to meet cybersecurity and regulatory requirements. It is in line with the trends towards a digital society by addressing the challenges of sovereignty and cybersecurity of time arising from the digital economy.

It is designed for the distribution and dissemination of secure, traced and certified "legal time" with target levels of accuracy, in TaaS (Time as A Service) mode

ii. SCPTime® architecture

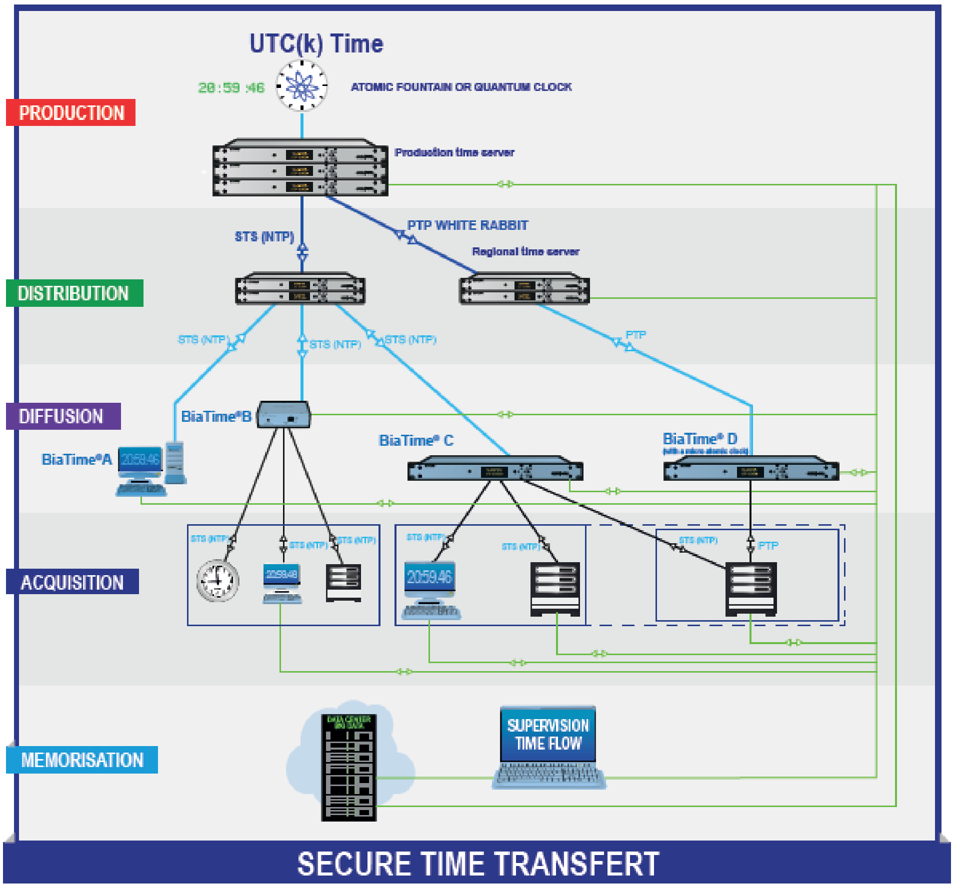
SCPTime® architecture is connected upstream to the legal time (UTC time) as its reference time source, and comprises Production, Distribution, Diffusion & Acquisition systems.

The time can be distributed over an IP network via standard time protocols such as NTP or PTP, or via a secure version of the NTP protocol called STS, which ensures the integrity of the time information between two systems if the transport infrastructure does not provide sufficient security.

SCPTrace, the built-in traceability system in SCPTime®, will provide evidence for administrative or legal process such as reconstitution of the events in logical order, delivery of certificates of conformity relating to legal or industrial requirements.

Through SCPTrace®, SCPTime® offers a total traceability of time and the related security to provide an accurate and certified time.

One complete entity of SCPTime® architecture is composed of the following components as a minimum:



Schema 1-1: SCPTime architecture

- **A reference time source:** Provided by legal time authority of a country, a region, … or high-performance atomic clock with good stability, or similar (quantum clock…)
- **A Time production system:** The production system is connected directly to the UTC reference time source and delivers time signal to Distribution system.
- **A Time distribution system:** The location of distribution sites shall be defined according to economic activities (close to the end users). The distribution site can be coupled with a datacenter.
- **A Time broadcasting system (Diffusion system):** Cloud or on-premise BiaTime Boxes.
- **A supervision system:** From production to acquisition, time data is monitored and reported through SCPTrace® supervision flow. The complete data is collected, analyzed and archived.
- **An acquisition system:** Software agents to be installed on devices which require time synchronization from time broadcasting system.

III.Test objectives

The main test objective is to demonstrate that the SCPTime timing service proposal answers the minimum technical requirements specified by EU Commission, which are listed as follows:

1. SCPTime timing service is resilient to GNSS failure
2. Timing accuracy provided by SCPTime timing service and delivered to user end is < 1µs compared with UTC
3. Timing service provided by SCPTime is traceable to UTC

4. SCPTime timing service is resilient and redundant to different modes of failure
5. The availability of SCPTime timing service is >99%

The demonstration activities have been conducted at JRC and in France, which have different objectives. Tests planned at JRC focus on the holdover accuracy measurement during the GNSS failure, while the objective of the demonstration in France (Paris and Grenoble) is to give an overview of the whole SCPTime France infrastructure as well as its network resilience capacity and the SCPTime timing service availability.

IV. Tests at JRC

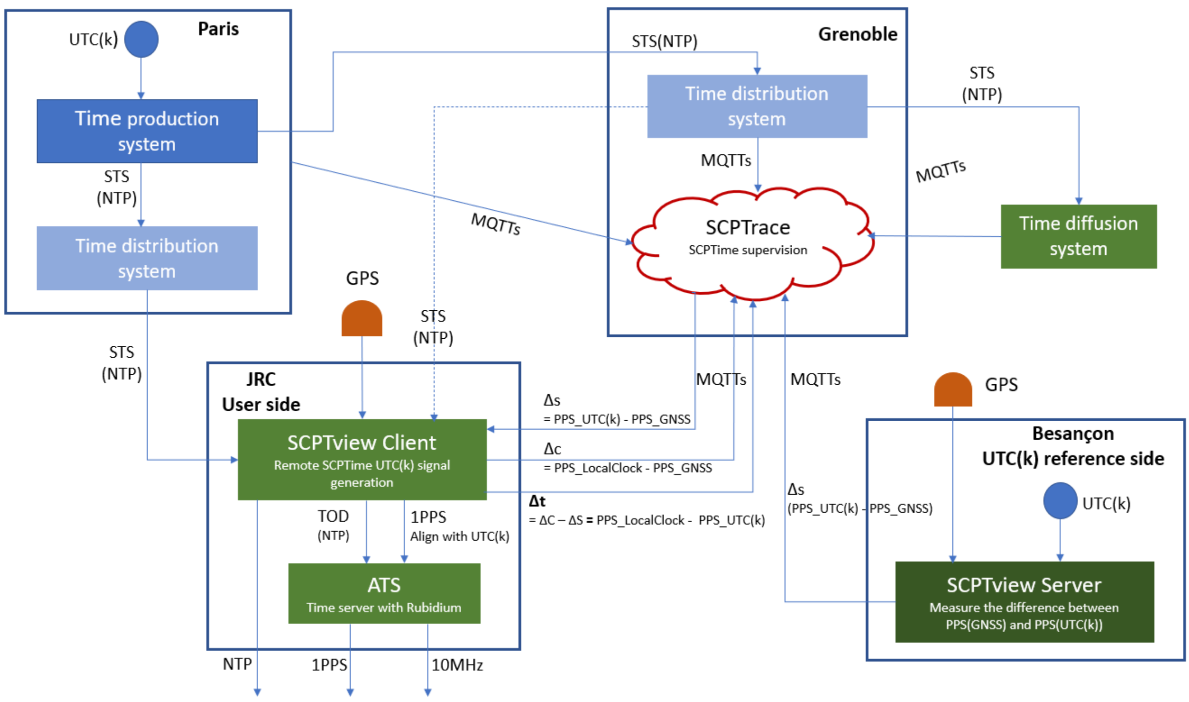
i. Test architecture

The test architecture for our "Alternative Positioning, Navigation and Timing (PNT) Services" project will be the SCPTime France architecture, which is a French national scale platform and is connected upstream to the UTC(OP) as its reference time source. It comprises Production, Distribution and Diffusion systems.

SCPTrace, the built-in traceability system in SCPTime, will provide evidence for administrative or legal process such as reconstitution of the events in logical order, delivery of certificates of conformity relating to legal or industrial requirements.

SCPTime implements the SCPTview technology by using GNSS signal to obtain an accuracy of a few tens of nano seconds compared with UTC(k) for SCPTime timing service that is delivered to user end.

The architecture diagram *Schema 1-1* shows the demo setup at JRC integrating SCPTView and its interconnection with SCPTime infrastructure in France.



Schema 2-1: SCPTime France infrastructure with SCPTview technology

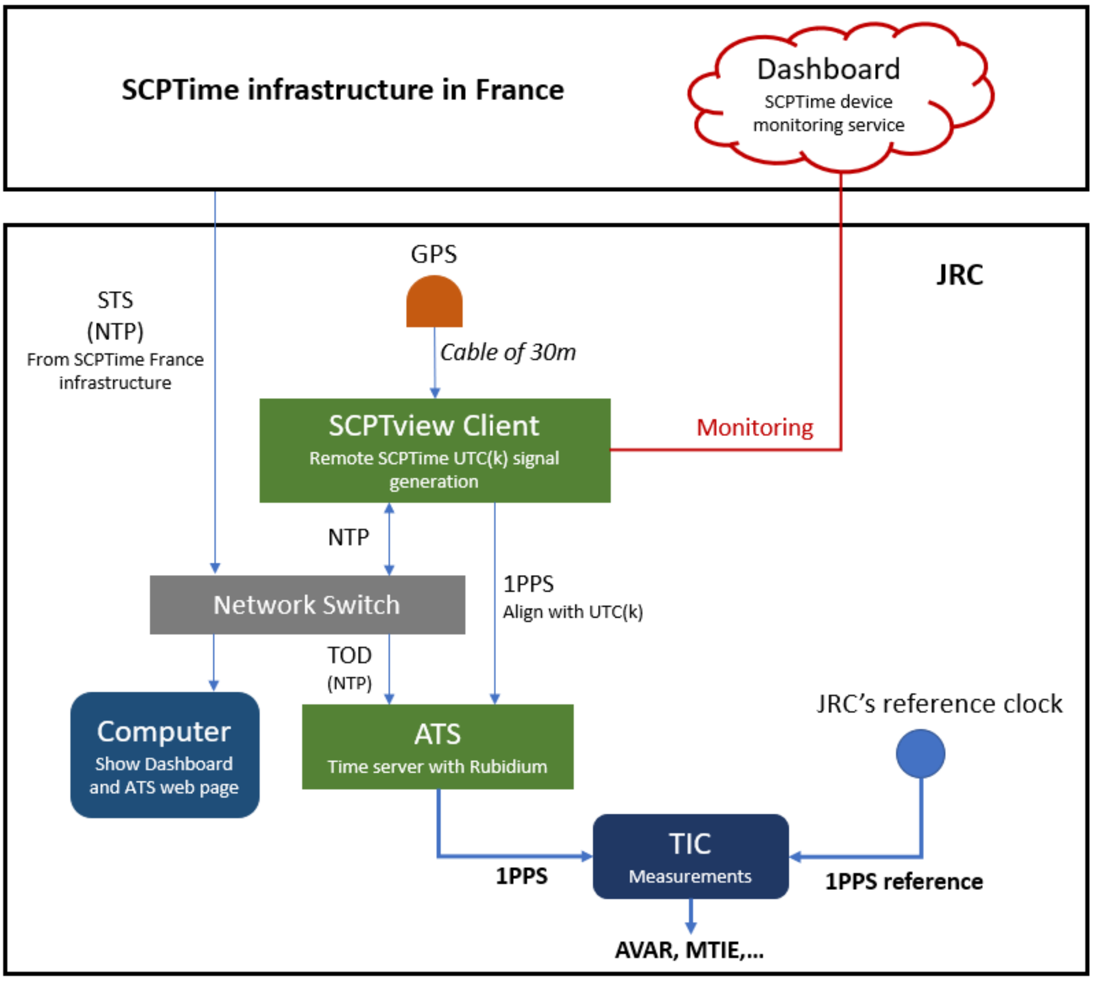
As shown in Schema 2-1:

- The SCPTview server is connected to the reference time UTC(k) and the GPS source.
- SCPTview server measures the PPS difference between the reference time UTC(k) and GPS time => " Δs = PPS_UTC(k) - PPS_GNSS".
- SCPTview server sends the Δs to SCPTime's supervision system SCPTrace.
- SCPTrace then transfers the Δs value got from SCPTview server to SCPTview Client
- SCPTview Client gets the Δs value from SCPTrace and meanwhile sends the PPS difference between GNSS and its local clock to SCPTrace => " Δc = PPS_LocalClock - PPS_GNSS".
- The PPS difference between local clock and reference time is thus calculated by SCPTview Client and sent to SCPTrace => " Δt= Δs – Δc= PPS_LocalClock – PPS_ UTC(k)".
- According to the calculated Δt, SCPTview Client phase shifts its 1PPS output signal from the Δt value to align with the PPS of reference time UTC(k) in distance.

Besides, an ATS (time server with rubidium) or similar device (other devices in development) at JRC will synchronize with SCPTview Client's 1PPS output signal which is aligned with the PPS signal of UTC(k). This ATS or similar device will deliver a 1PPS signal and a 10MHz signal as well as a timing service by NTP.

When the GNSS signal is lost, SCPTview Client will no longer calculate the offset between its local clock and UTC(k). Therefore, it will not be able to phase shift its 1PPS output signal to make it be aligned with the PPS of reference time UTC(k) in distance. It will stop delivering 1PPS signal to the ATS (or similar device). However, the ATS (or similar device) will ensure the holdover and continue to deliver timing service when maintaining accuracy based on its internal rubidium.

The tests at JRC will assess the SCPTview equipment's accuracy and holdover capacity to UTC(k) by taking the 1PPS output signal of the ATS or similar device and comparing it with JRC's reference clock in short term and medium term when the GNSS signal is lost. The *schema 1-2* shown below presents the tests set up at JRC:



Schema 2-2: Test set up at JRC

ii. Needed infrastructure at JRC

To realize the test setup at JRC, the following infrastructure is needed:

- Indoor room with stabilized temperature between 19°C and 23°C.
- A 19" rack cabinet with 4U available which can support 10Kg.
- Power supply: 230V AC up to 200W.
- A GNSS (GPS) signal brought by a coaxial cable with SMA connector.
- 2 IPv4 addresses on the same LAN.
- SCPTime equipment accepts DHCP or explicit configuration. In the latter case, JRC must provide the network configuration.
- If JRC has any DNS server, SCPTime can use it. If not, SCPTime will use theirs.
- Concerning internet access, one of the IP addresses should access internet on:
  - port TCP8883 (MQTTs)
  - Port UDP123 (NTP) (assuming the firewall is stateful)
  - Port UDP53 (if no DNS Server on LAN)
- A computer with Chrome/Firefox explorer for connection to SCPTime device monitoring web page "Dashboard" and to SCPTime time server web page.

iii. Tests description & result

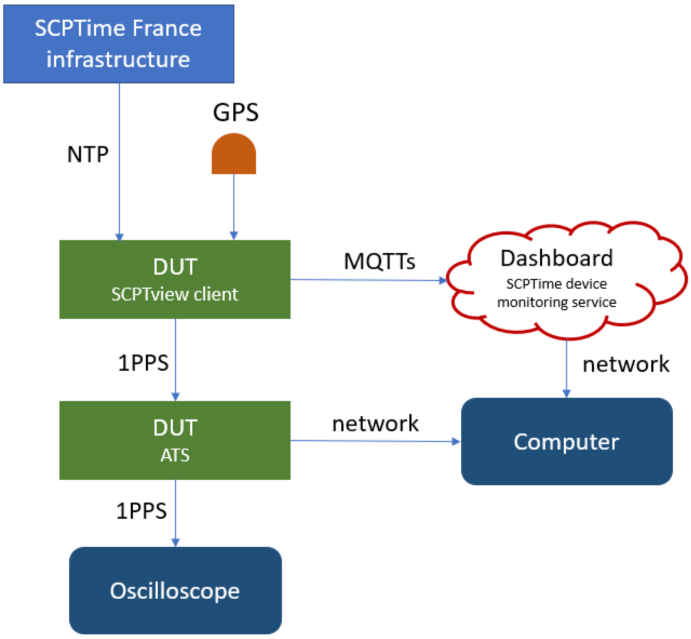
The table below shows the test scenarios that have been conducted at JRC.
The tests were conducted and validated by European Commission auditors, during the period between Nov. 2021 to Jan. 2022.

Test ID	Test name	Duration	Measurements	Metrics (if quantative)
T1F	System verification: Nominal operation	-	Dashboard, 1PPS	Fail/Pass, demo
T2H	Short term clock stability (with GNSS connected): Synchronization connection= 1day	24h	Dashboard, 1PPS	AVAR, MTIE
T2L	Short term clock stability: GNSS loss = 1day	24h	Dashboard, 1PPS	AVAR, MTIE
T3E	Medium term clock stability: GNSS loss = 14 days	14 days	Dashboard, 1PPS	AVAR

Table 1-1: Test scenarios at JRC

1. T1F: System verification

Test ID	T1F
Test name	System verification: Nominal operation
Test place / Date	JRC / 22-11-2021
Objective	Set up DUTs and verify that they are connected to SCPTime France infrastructure and UTC(OP) is delivered to the DUTs at JRC with some delay.
Output	1. DUTs ready to go (devices led and front interface) 2. Data - Dashboard 3. Data - 1PPS
Time to execute	-
Metrics	Pass/fail, descriptive, quantitative



Schema 2-3: System verification set up at JRC

Set up:

- Set up DUTs assembly according to the setup schema 2-2 and 2-3.
- Connect SCPTview Client and ATS to power supply (230VAC).
- Turn on SCPTview Client and ATS
  - *Devices are turned on*
- Connect SCPTview Client's GNSS input to the GPS antenna.
- Connect the network switch to internet to communicate with SCPTime France infrastructure.
- Connect the RJ45 connector of SCPTview Client to the network switch that is connected to SCPTime France infrastructure by internet.
- Connect the computer to the network switch that is connected to SCPTime France infrastructure by internet.
- Wait and check the led of SCPTview Client
  - *SCPTime client's led is set to green*
- Connect to SCPTime supervision's device monitoring service "Dashboard" on computer by internet (see Appendix 1)
  - *Connection to Dashboard OK*
- Verify the information of SCPTview Client on Dashboard => SCPTview is in synchronized state (see Appendix 1)
  - *Status: Synchronized*
  - *Sync.state: Synchronized*
- Connect the Ethernet input of ATS to the network switch to get the ToD (time of day) from SCPTime client with NTP.
- Connect the PPS input of ATS to 1PPS output of SCPTview Client which is aligned with UTC(k) to get the PPS source.
- Synchronize ATS with the PPS output of SCPTview Client.
- Connect the 1PPS output signal of ATS to oscilloscope and check the signal's characteristics
  - Voltage

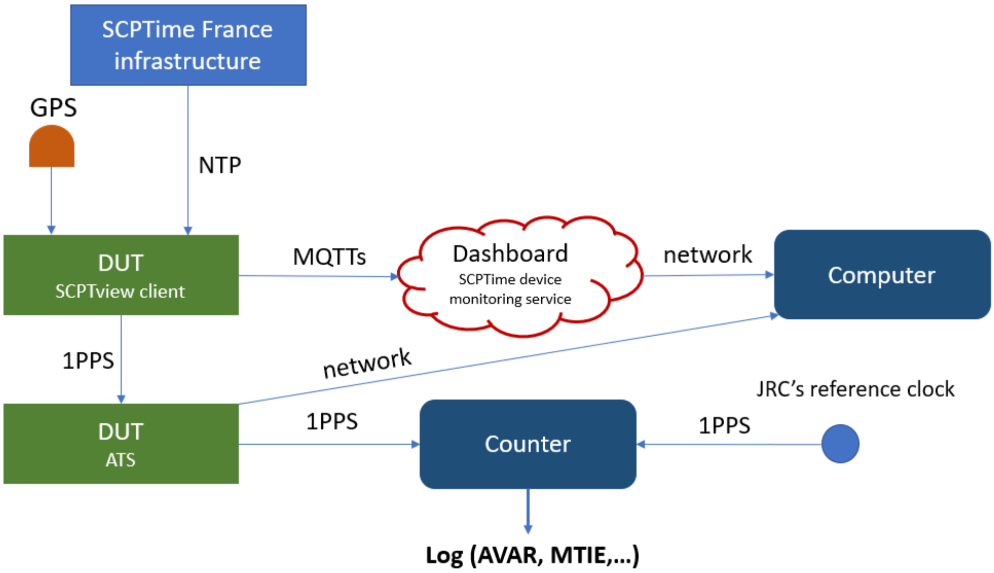
- Pulse width
- Rising edge velocity
- Falling edge velocity

Results		
Item	Expected result	Observed result
SCPTView Client front panel	LED is green	**Ok**
ATS front panel	External PPS locked LEDs are green	**Ok** **Ok**
ATS output	1PPS output is measured	**Ok**
SCPTime Dashboard	SCPTViewClient = gt__cvojrc Sync state = Synchronized	**Ok**

Comments / Metrics
Once the network configuration is done, the setup takes a couple of hours. We experiment a lack of strength with GNSS signal, resolved by adding a signal amplifier. We also correct the 1 PPS output for cable delay, the exact same value as it is corrected on UTC(IT) 1PPS signal : 300ns 1 PPS offset between SCPTime setup and UTC(IT) measure: ~250ns
Conclusion
Offset is less than 1 µs. **Test result: Success**

2. T2H: Short term clock stability with GNSS connection

Test ID	**T2H**
Test name	Short term clock stability with GNSS connection: Synchronization = 1 day
Test place / Date	JRC / from 11-12-2021 to 14-12-2021
Objective	To assess the short-term time stability when GNSS is connected and the server is synchronized for 1 day
Output	1. Devices led and front interface 2. Data - Dashboard 3. Data - 1PPS
Time to execute	24h
Metrics	Descriptive, quantitative, AVAR, MTIE vs UTC time



Schema 2-4: Short term stability set up (with GNSS)

Set up:

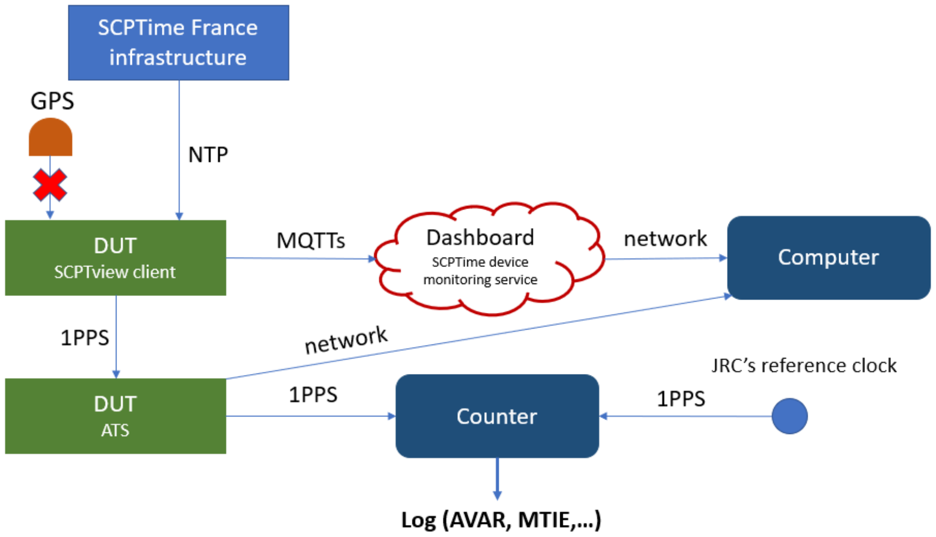
- Execute T1F.
- Connect the JRC's reference clock to the Counter as the reference 1PPS signal.
- Disconnect the 1PPS output of ATS from the oscilloscope and connect the output to the Counter to compare the signal with the reference signal.
- Run experiment for 24h, monitoring performance.

Results		
Item	Expected result	Obtained result
SCPTView Client front panel	LED is green	**Ok**
ATS front panel	External PPS locked LEDs are green	**Ok** **Ok**
ATS output	1PPS output is connected to counter	**Ok**
SCPTime Dashboard	SCPTViewClient = gt__cvojrc Sync state = Synchronized	**Ok**
Detailed result, metrics, and comments: see appendix 2		

Conclusion
Offset does not exceed 1µs for a period of 24 hours **Test result: Success**

3. T2L: Short term clock stability without GNSS

Test ID	T2L
Test name	Short term clock stability: GNSS loss = 1 day
Test place / Date	JRC / from 07-01-2022 to 10-01-2022
Objective	To assess the short-term time stability and synchronization when GNSS is lost for 1 day
Output	1. Devices led and front interface 2. Data - Dashboard 3. Data - 1PPS
Time to execute	Up to 24h
Metrics	Descriptive, quantitative, AVAR, MTIE vs UTC(IT) time



Schema 2-5: Short term stability set up without GNSS connection

Set up:

- Execute T2H.
- Unplug the GNSS input of SCPTview Client (after 24h of synchronization since SCPTview Client and ATS have been synchronized).
- Verify the device led of SCPTview Client after the GPS disconnection
    - *SCPTview Client's led is set to orange (holdover) and then quickly to red (freerunning)*
- Verify the SCPTview Client information on Dashboard => SCPTview Client is in freerunning (see Appendix 1):
    - *Status: Unsync*
    - *Sync.state: Freerunning*
- Verify the device's front interface of ATS
    - ATS is in "running with autonomy" state
- Run experiment for 24h, monitoring performance.

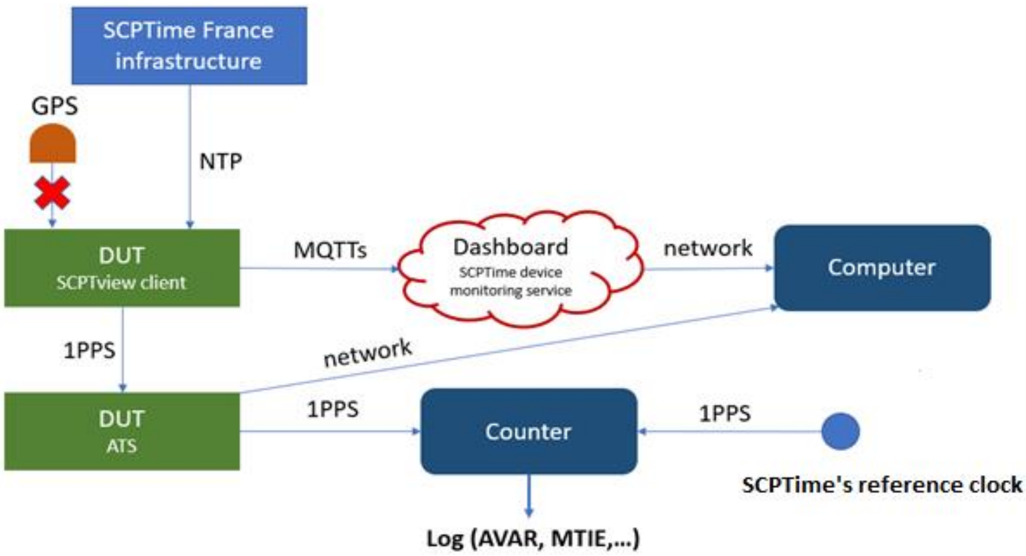
Results		
Item	Expected result	Obtained result
SCPTView Client	LED is red	**Ok**

front panel		
ATS front panel	Text: No Sync Sync LED is Off Alarm LED is blinking Red	**Ok** **Ok** **Ok**
ATS output	1PPS output is connected to counter	**Ok**
SCPTime Dashboard	SCPTViewClient = gt__cvojrc Sync state = Holdover for few seconds, then free running for 6 minutes, then unsync for the rest of the test	**Ok**
Detailed result, metrics, and comments: see appendix 3		

Conclusion
Drift does not exceed 1µs for a period of 24 hours **Test result: Success**

4. T3E: Medium term clock stability

Test ID	**T3E**
Test name	Medium term clock stability: GNSS loss = 14 days
Test place / Date	SCPTime Lab / from 24-12-2021 to 09-01-2022
Objective	To assess the medium-term time stability and synchronization when GNSS is lost for 14 days
Output	1. Devices led and front interface 2. Data - Dashboard 3. Data - 1PPS
Time to execute	14 days
Metrics	Descriptive, quantitative, AVAR, MTIE vs UTC(IT) time



Schema 2-6: Medium term stability set up without GNSS connection

Set up:

- Due to lack of time, the medium-term tests could not be carried out at JRC, Ispra.
- We reproduced as closely as possible the assembly in place at the JRC in our lab at La Mure.
- Endpoint measurements are conducted by SCPTime engineers and scientists with an HP53132A Universal Frequency Counter

Results		
Item	Expected result	Obtained result
SCPTView Client front panel	LED is red	**Ok**
ATS front panel	Text: No Sync Sync LED is Off Alarm LED is blinking Red	**Ok** **Ok** **Ok**
ATS output	1PPS output is connected to counter	**Ok**
SCPTime Dashboard	SCPTViewClient = gt__cvojrc Sync state = Holdover for few seconds, then free running for 6 minutes, then unsync for the rest of the test	**Ok**
Detailed result, metrics, and comments: see appendix 3		

Risks considered:

Risk	Probability	Severity	Action
Data recording fails	medium	high	monitor data frequently
Component fails	low	high	monitor data frequently

V.Tests in France

i.Test architecture

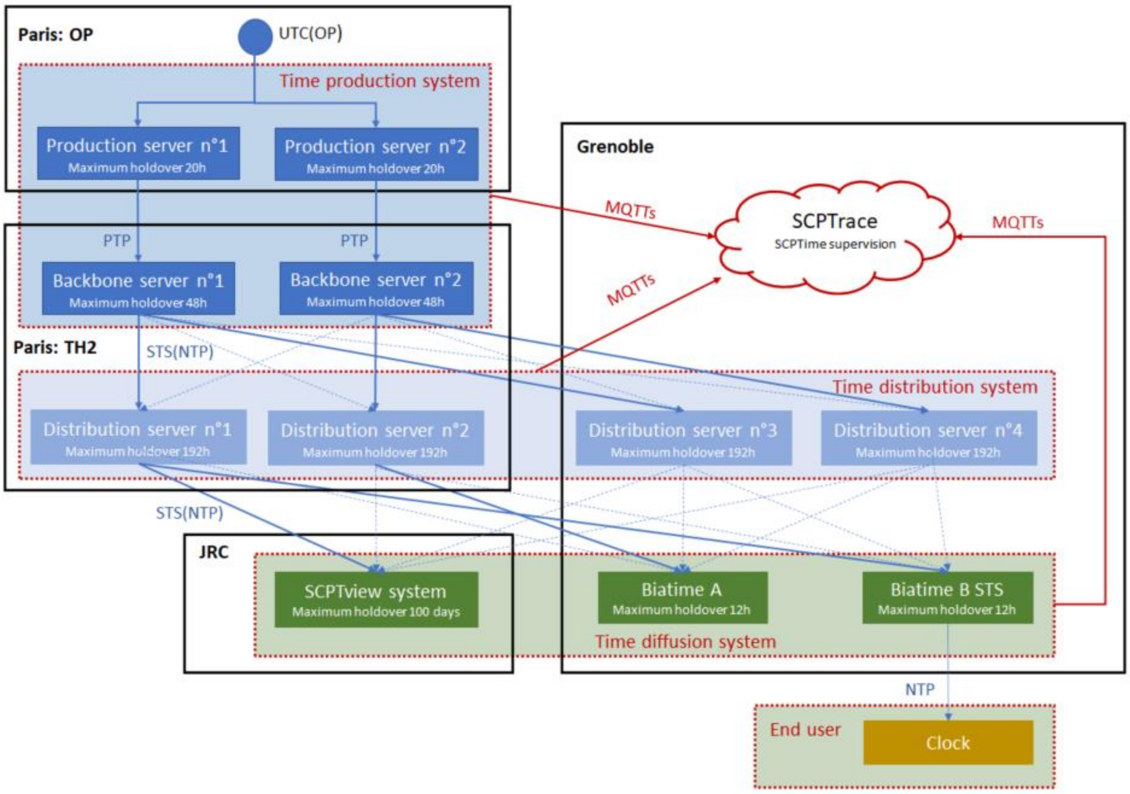
As shown in schema 3-1, the UTC(OP) can be distributed over an IP network via standard time protocols such as NTP or PTP, or via a secure version of the NTP protocol called STS, which ensures the integrity of the time information between two systems if the transport infrastructure does not provide sufficient security.

SCPTime devices are connected to SCPTrace via MQTTs. Through SCPTrace, SCPTime offers a total traceability of time and the related security to provide an accurate and certified time.

Every time system (production, distribution, diffusion) in SCPTime France infrastructure has multiple backup servers to ensure the continuity of service with very high resiliency both on hardware systems and software. Besides, every SCPTime time server has its own holdover capacity. The holdover capacity/duration of each SCPTime device is designed based on the requirement of ATTS Certification for each SCPTime infrastructure level.

The purpose is to ensure a holdover capacity of 5µs for production time system servers, 10ms for distribution time system servers and 150ms for diffusion time system devices. Thus, after calculation, production servers are configured with 20h’s maximum holdover time while backbone servers, distribution servers and diffusion devices are configured with 48h, 192h and 12h respectively. SCPTview system hasn't been defined yet in ATTS requirement, so for the moment, SCPTview system is configured with 100-day holdover which ensures a holdover capacity of 150µs.

Demonstration in France will show the SCPTime time service's resilience capacity and network monitoring by applying different kinds of failures, including device failure and network failure.



Schema 3-1: SCPTime France infrastructure

ii.Tests description & result

The table below shows the test scenarios that have been conducted during the demonstration activities in France.
The tests were conducted by SCPTime and validated by European Commission auditors.

Test ID	Test name	Duration	Measurements	Metrics (if quantative)
T4H	Resilience and network monitoring: Connection to SCPTime supervision loss	1h	SCPTime Dashboard	Demo
T4I	Resilience and network monitoring: SCPTime time distribution loss	1h	SCPTime Dashboard	Demo
T4J	Resilience and network monitoring: SCPTime network failure	1h	SCPTime Dashboard	Demo

Table 2-1: Test scenarios in France

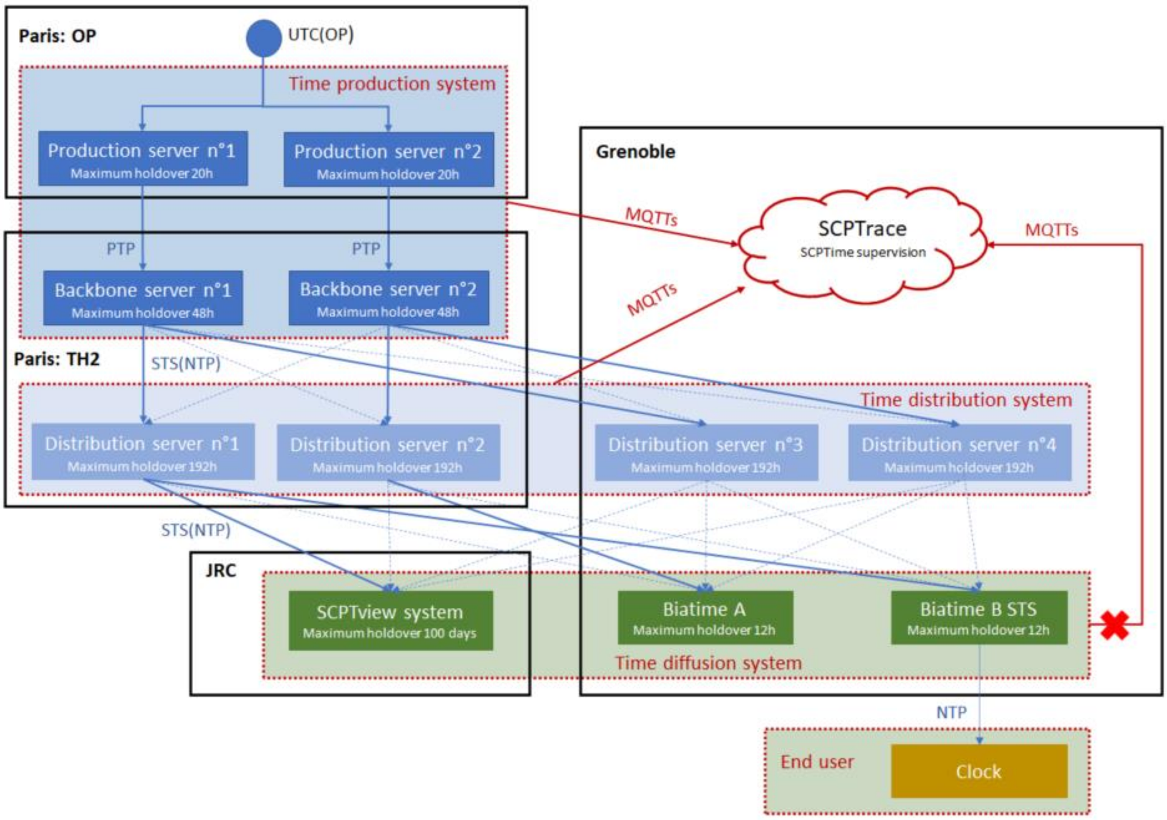
1. T4H: Resilience and network monitoring: Connection loss to SCPTime supervision

a) Description

Test ID	T4H
Test name	Resilience and network monitoring: Connection loss to SCPTime supervision at the diffusion point
Test place/ Date	France / 03-02-2022
Objective	Verify that the connection loss to SCPTime supervision system of Diffusion time device will not immediately disturb the delivery of SCPTime timing service to end user
Output	Data - Dashboard
Time to execute	1h
Metrics	Descriptive

Initial condition:

- All the SCPTime devices are connected to SCPTrace and SCPTime France infrastructure is working well.
- All the SCPTime devices are online and synchronized.
- The Biatime B STS is synchronized with the Distribution server (see schema 2-1).
- A clock is synchronized with Biatime B STS which is the only possible synchronization server for the clock (see schema 3-1).
- Biatime B STS is in "Synchronized" state on SCPTime supervision's device monitoring service "Dashboard".



Schema 3-2: Biatime B STS disconnected from SCPTrace in SCPTime France infrastructure

Actions:

- Disconnect the Biatime B STS from SCPTrace (disable its MQTTs port) without disconnecting it from network
    - *Connection loss to SCPTime supervision*
- Verify the Biatime B STS's synchronization information on SCPTime Dashboard => Biatime B STS is in Offline state (see Appendix 1)
    - *Biatime B STS's "Status" on Dashboard: Offline*
- Verify that the front panel LED of the Biatime B is Steady Orange, meaning being in holdover mode
- Verify that Biatime B STS continues to deliver time to the clock in Biatime B STS's holdover mode by checking the clock's synchronization state => Clock stays being synchronized with Biatime B STS
    - *Clock is in "Synchronized" state (multicolor display)*

b) Results

Output	Result expected	Observed
Biatime B STS's information on SCPTime Dashboard	Status: Offline	**Ok, status observed after 2s**
Biatime B STS LED on front panel	LED: Steady orange	**Ok, observed after 15s**
Clock's synchronization state	Clock's display is multicolour	**Ok, no impact**

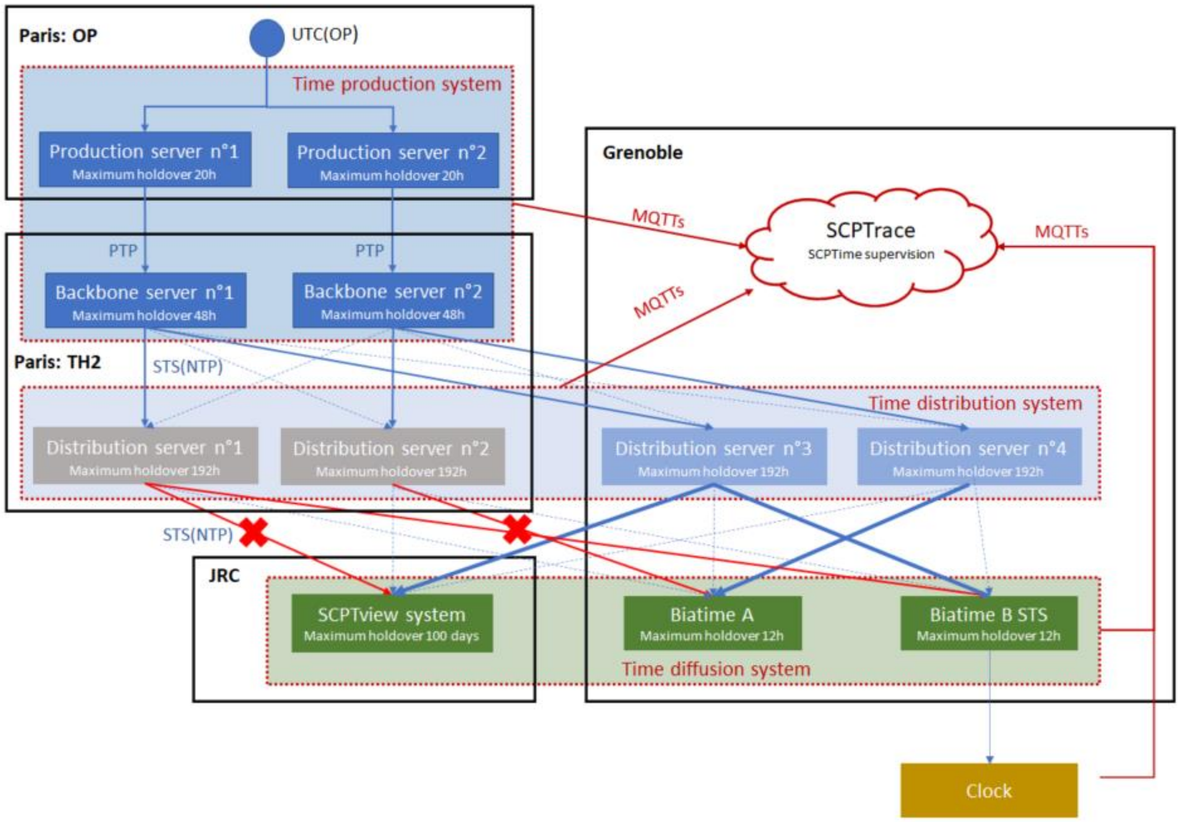
2. T4I: Resilience and network monitoring: SCPTime time distribution point loss

a) Description

Test ID	T4I
Test name	Resilience and network monitoring: SCPTime time distribution loss
Test Place / Date	France / 03-02-2022
Objective	Verify the changeover between different SCPTime distribution points to ensure the SCPTime timing service delivery to end user after a distribution point loss
Output	Data - Dashboard
Time to execute	1h
Metrics	Descriptive

Initial condition:

- All the SCPTime devices are connected to SCPTrace and SCPTime France infrastructure is working well.
- All the SCPTime devices are online and synchronized.
- The Biatime B STS is synchronized with a random Distribution server STS output.
- Biatime B STS is shown in "Synchronized" state and synchronized with a random Distribution server STS output on SCPTime Dashboard.



Schema 3-3: One SCPTime time distribution point loss

Actions:

- Downtime the Distribution server STS output to simulate the SCPTime time distribution point loss (inhibit the server NTP output).
- Verify the Distribution server STS output information on SCPTime Dashboard => Distribution server STS output is freerunning.
  - *Distribution server STS output "Status" on Dashboard: Freerunning*
- Verify the Biatime B STS's synchronization status and its sync server on SCPTime Dashboard
  - *Biatime B STS receives another upstream server and synchronizes with the new available Distribution server.*
  - *Biatime B STS continues to diffuse time to its downstream devices*
  - *Biatime B STS's "Status" on Dashboard: Synchronized*
  - *Biatime B STS's "Sync.state" on Dashboard: holdover then Synchronized*

b) Result

Item / Action	Expected result	Observed result
Get Synchronization server of Biatime gt__205890	Dashboard: Biatime B STS gt__205890 is synchronized with a distribution STS ouput = gt__xxxxxx Clock is synchronized with gt__205890	Biatime B is synchronized with gt__185430d Clock Ok
Switch off the Distribution STS output gt__185430d	Dashboard: Distribution STS output gt__185430d goes Freerunning	**Ok, observed after 3s**

	gt__205890 receive a new upstream server	New sync server is gt__185431a, observed after 2s
	gt__205890 goes holdover then synchronized	**Ok, synchronized after holdover of 60s**
	Clock desynchronizes for a few seconds then resynchronizes	**Ok, resynchronized after 40s**

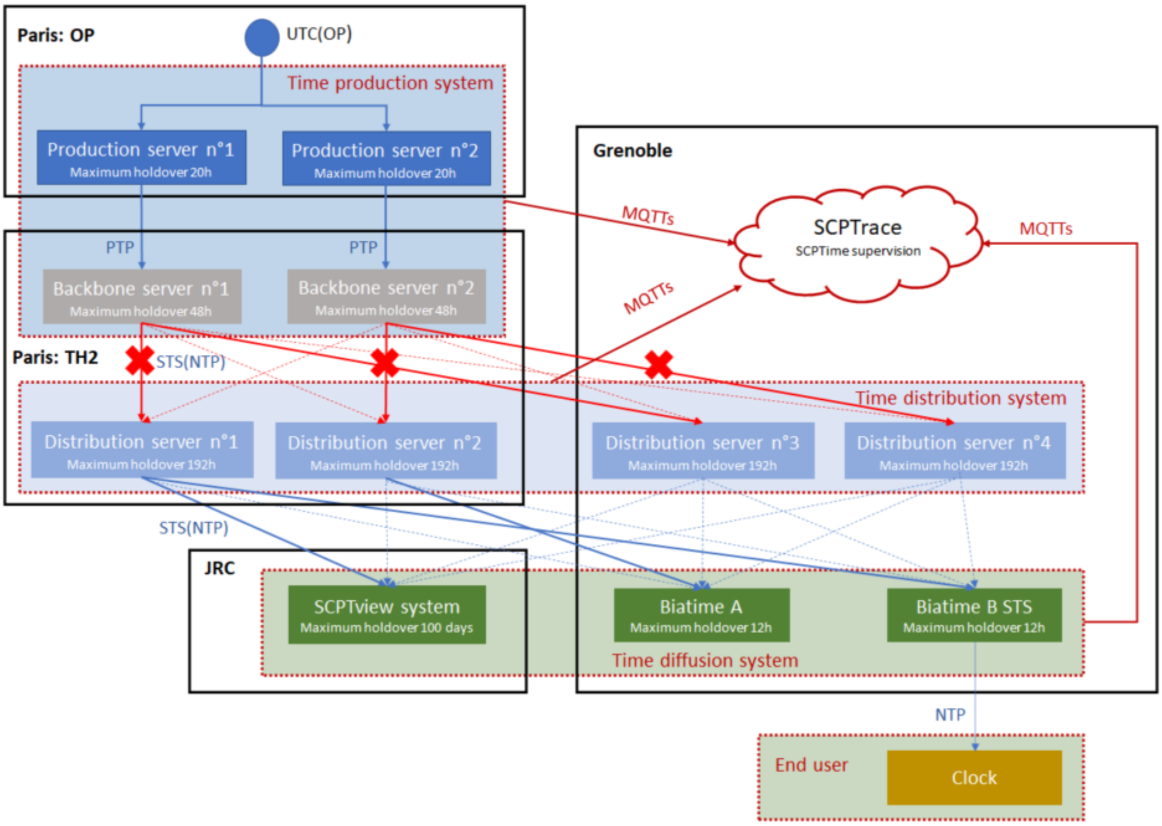
3. T4J: Resilience and network monitoring: SCPTime network loss

a) Description

Test ID	T4J
Test name	Resilience and network monitoring: SCPTime network failure
Test place / Date	France / 03-02-2022
Objective	Verify that SCPTime network failure will not disturb immediately the SCPTime timing service delivery to user end
Output	Data - Dashboard
Time to execute	1h
Metrics	Descriptive

Initial condition:

- All the SCPTime devices are connected to SCPTrace and SCPTime France infrastructure is working well.
- All the SCPTime devices are online and synchronized.
- The Distribution servers are synchronized with the Backbone servers.
- The Diffusion devices are synchronized with the Distribution servers.
- Backbone servers and Distribution servers are all shown in “Synchronized” status on SCPTime Dashboard.



Schema 3-3: SCPTime network failure

Actions:

- Disconnect all the Backbone servers' NTP output from network to simulate the network failure between Backbone servers and Distribution servers.
- Verify the Backbone servers' NTP output information on SCPTime Dashboard => Backbone server NTP outputs are in Critical_online and Freerunning state (see Appendix 1)
  - *Backbone server NTP output's "Status" on Dashboard: Critical_online*
  - *Backbone server NTP output's "Sync.state" on Dashboard: Freerunning*
- Verify the Distribution server's synchronization status on SCPTime Dashboard
  - Distribution server pass into "holdover" state (see Appendix 1) and continues to deliver time to diffusion servers during 192h
  - Distribution server's "Status" on Dashboard: Got_state_ip
  - Distribution server's "Sync.state" on Dashboard: Holdover
  - Distribution server's "Sync.server on Dashboard: -(Empty)
- Verify the Biatime B STS's synchronization state on SCPTime Dashboard
  - Biatime B STS stays in "Synchronized" Status and "Synchronized" Sync.state
  - Biatime B STS continues to diffuse time to its downstream devices

b) Result

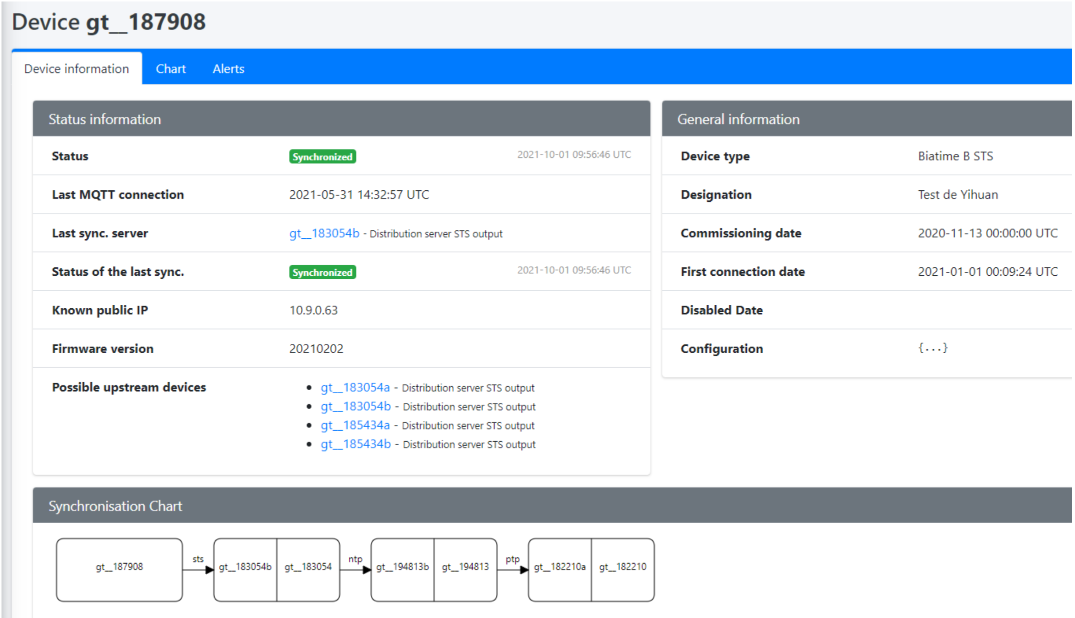
Output	Result expected	Observed
Backbone server NTP output's information on SCPTime Dashboard	Status: Critical_online Sync.state: Freerunning	**Ok, status observed after 2s**

Distribution server's information on SCPTime Dashboard	Status: Unsync Sync.state: Holdover	**Ok, status observed after 2s**
Biatime B STS's information on SCPTime Dashboard	Status: Synchronized Sync.state: Synchronized	**Ok, no impact**
Clock	Synchronized (multicolour)	**Ok, no impact**

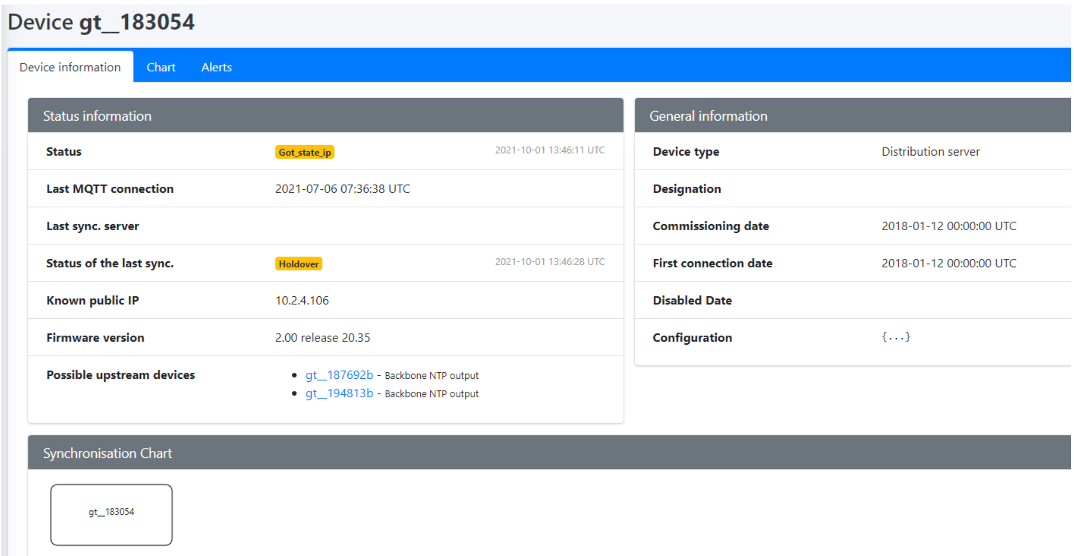
VI.Appendixes

i. Appendix 1: Examples of SCPTime's device monitoring service Dashboard and different synchronization state of device on Dashboard

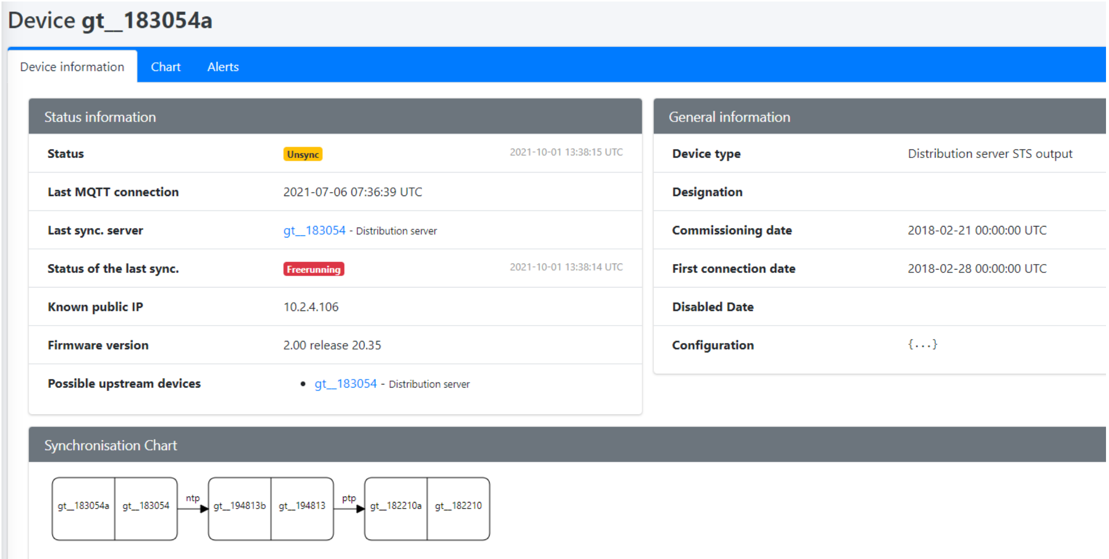
- Synchronized state:



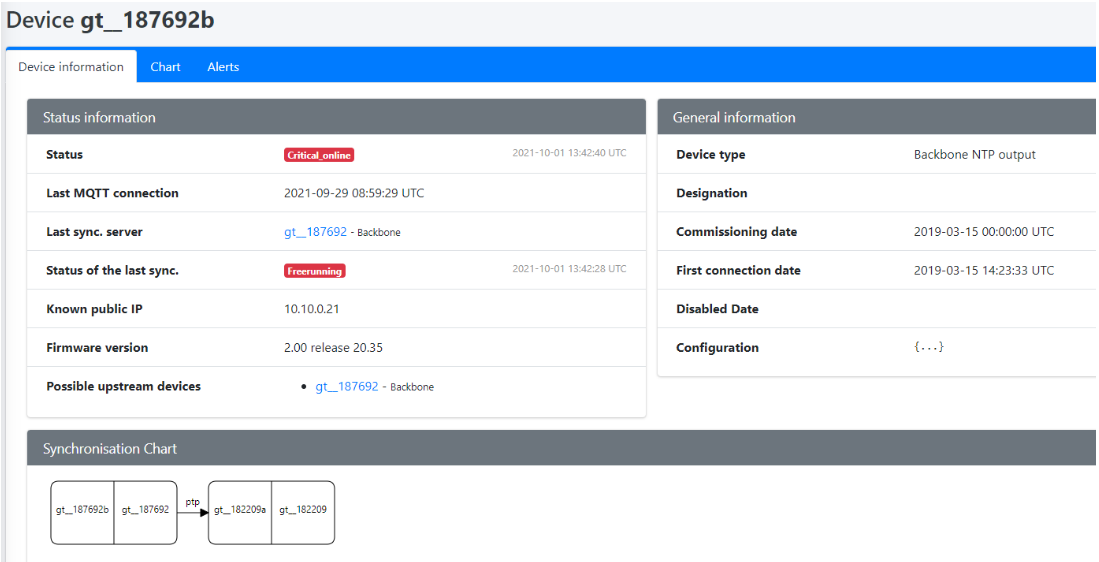
- Holdover state without available upstream server



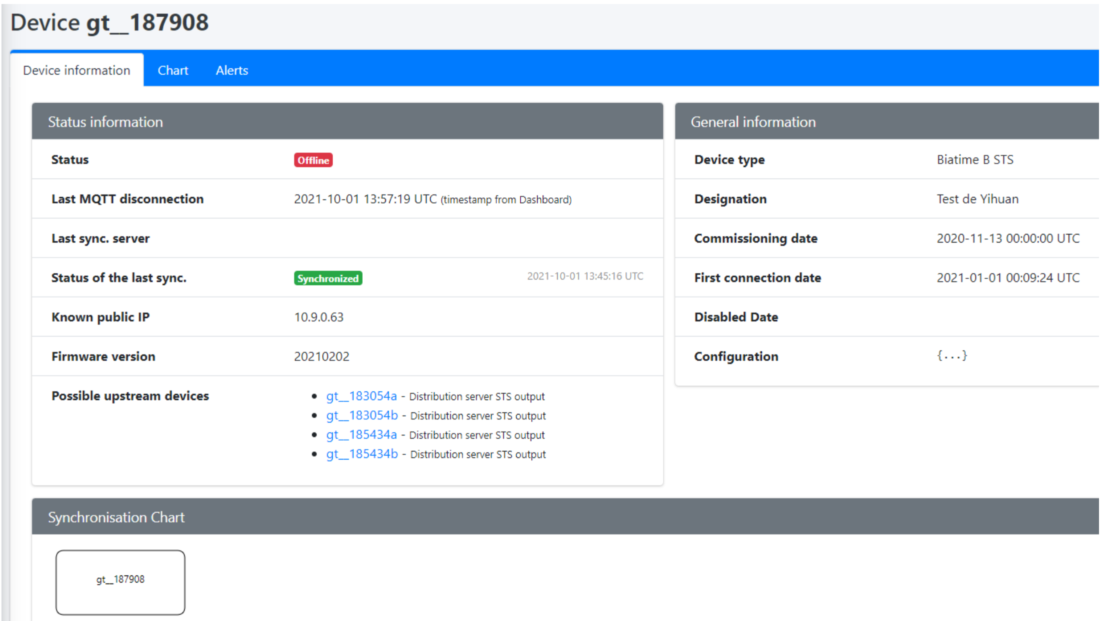
- Unsync and Freerunning state:



- Critical_online and Freerunning state:

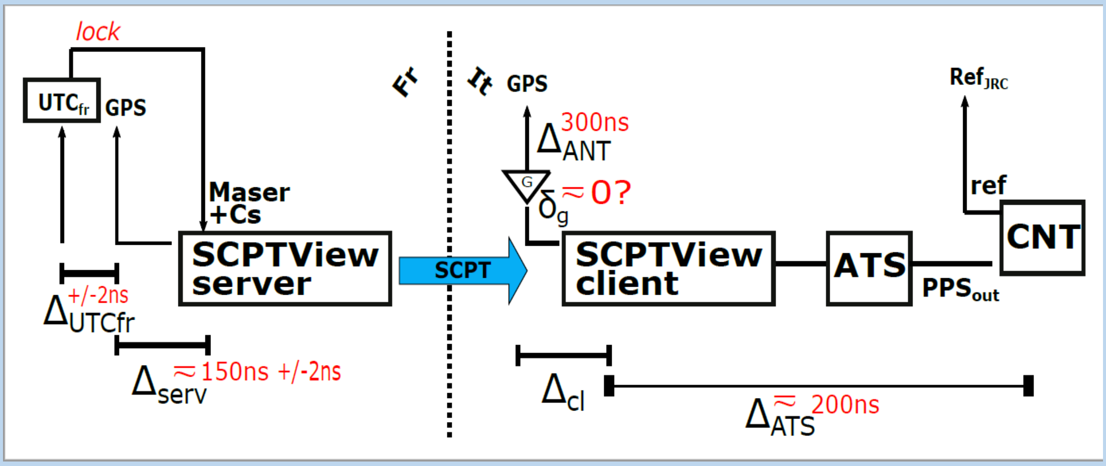


- Offline state:

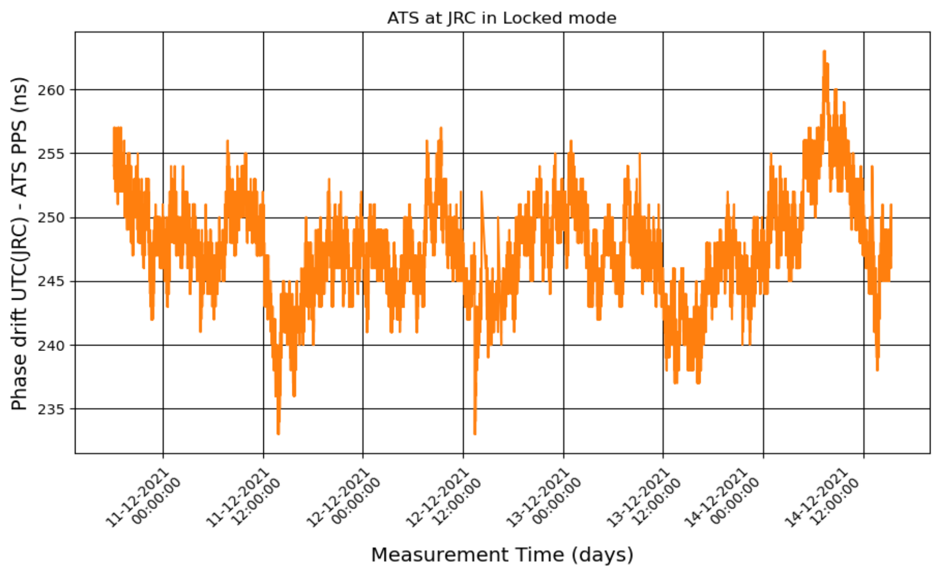


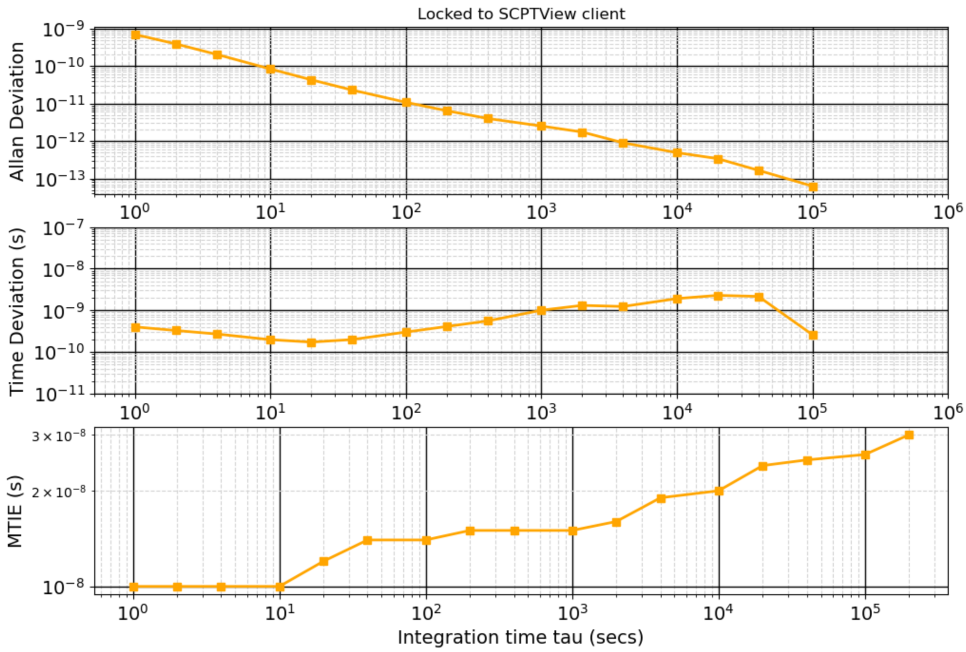
ii. Appendix 2: ADEV, TDEV and MTIE of ATS when synchronized with GPS connected

Comments / Metrics
When running in nominal state, with GNSS connected, the output of the 1PPS signal out of ATS will reflect the input signal of SCPTView server increase by the delay of the setup itself which is estimated between 100 and 200ns. The input signal on the server is set at 150ns +/- 4ns far from UTC(OP)



ATS output 1PPS is connected to a counter which reference is set to UTC(IT).
Measure is the difference in ns between the rising edge of the two signals
Data are provided by JRC.
We observed the behavior of our installation from December 11 to 14 and measured the offset between its output 1PPS signal and the reference 1PPS signal provided by JRC.
The peak to peak phase fluctuations are equal to 30 ns. The ADEV and TDEV at long term look good, with low values as 7.5e-14 and 360 ps @ 1day of integration time respectively.
MTIE shows maximum error of 27 ns @ 1 day of integration time (in good agreement with the observed peak to peak fluctuation value).



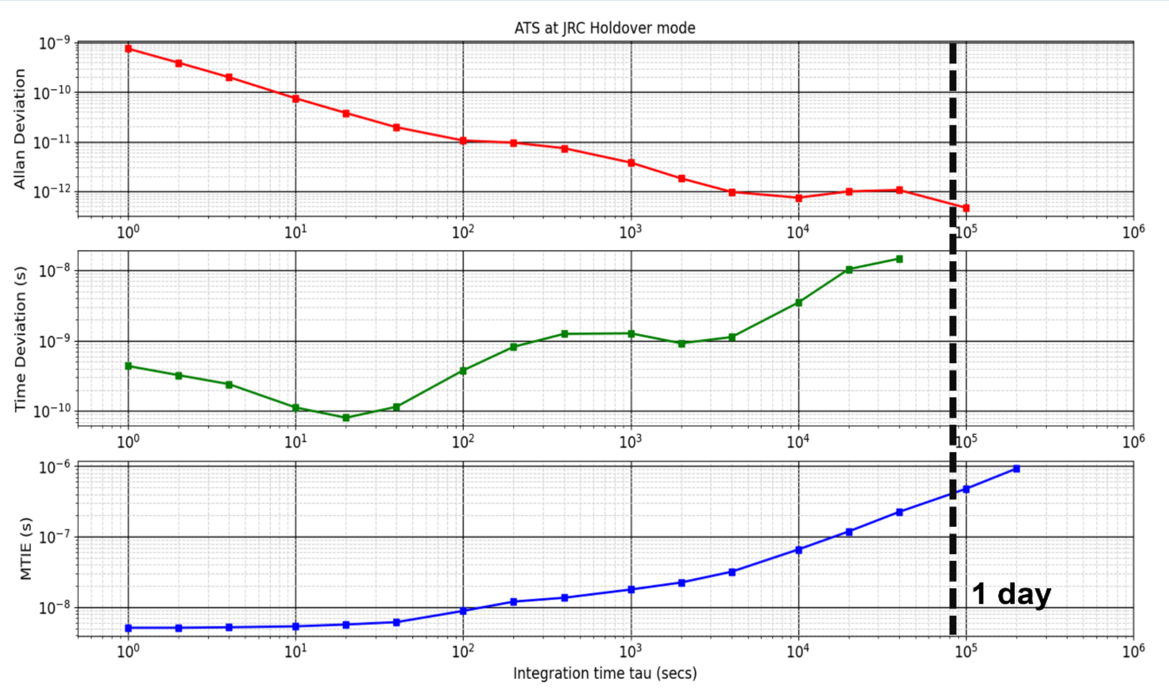


iii. Appendix 3: ADEV, TDEV and MTIE of ATS for its holdover mode with GPS unplugged for 24h

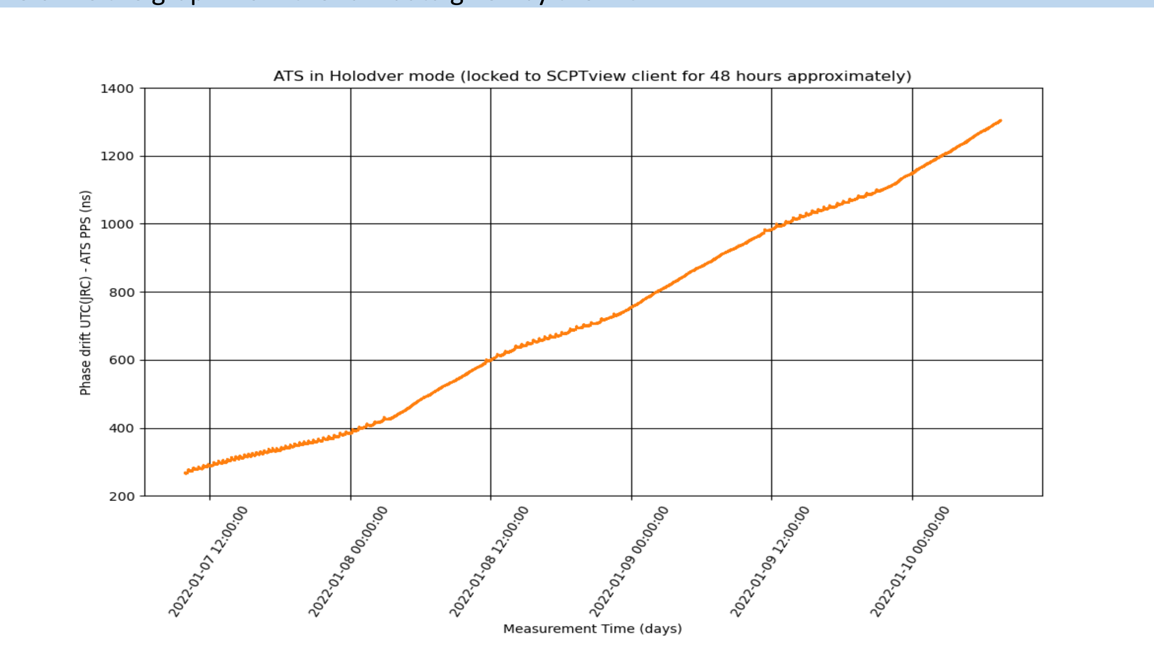
Comments / Metrics
Based on significant data provided by JRC for 24h with GNSS signal lost, here is the analysis from our scientific team: The holdover phase drift over the first day is 289 ns which increases to 387 ns and 401 ns for the second day and third day respectively. The Holdover Allan Deviation looks good at long term with a value in the low 1e-13 @ 1 day of integration time. It is expected that the short term (tau = 1 to 100 ns) Allan Deviation is limited due to the resolution of the Time Interval Counter (TIC). The Time Deviation reaches a value less than 50 ns @ half a day of integration time (there is not enough data for the 1 day point calculation). Following the trend of the time stability for the tau decade (from 10,000 to 100,000 seconds), it is expected that the Time Deviation will reach a value of 500 ns @ 1 day of integration time. But another quantity known as the Maximum Time Interval Error (MTIE) provides very useful information about the peak value of the time error over a certain period of integration time and is about 500 ns (< 1 µs) @ 1 day for the 3 day holdover dataset. Some oscillations with a magnitude of about 10 ns with periodicity ranging from 30 mins to an hour are observed which could be due to perturbation on signals or equipments. But even with these perturbations, the plots show overall good frequency and time stability performance.

Below is a plot comparing the JRC results with our lab tests. The comparison shows good agreement at long term for Allan and Time Deviation, and a bit better at JRC for MTIE.

Environmental conditions, in particular temperature variations, which have not been measured, can significantly influence the results



Below is the graph from the raw data given by the TIC:

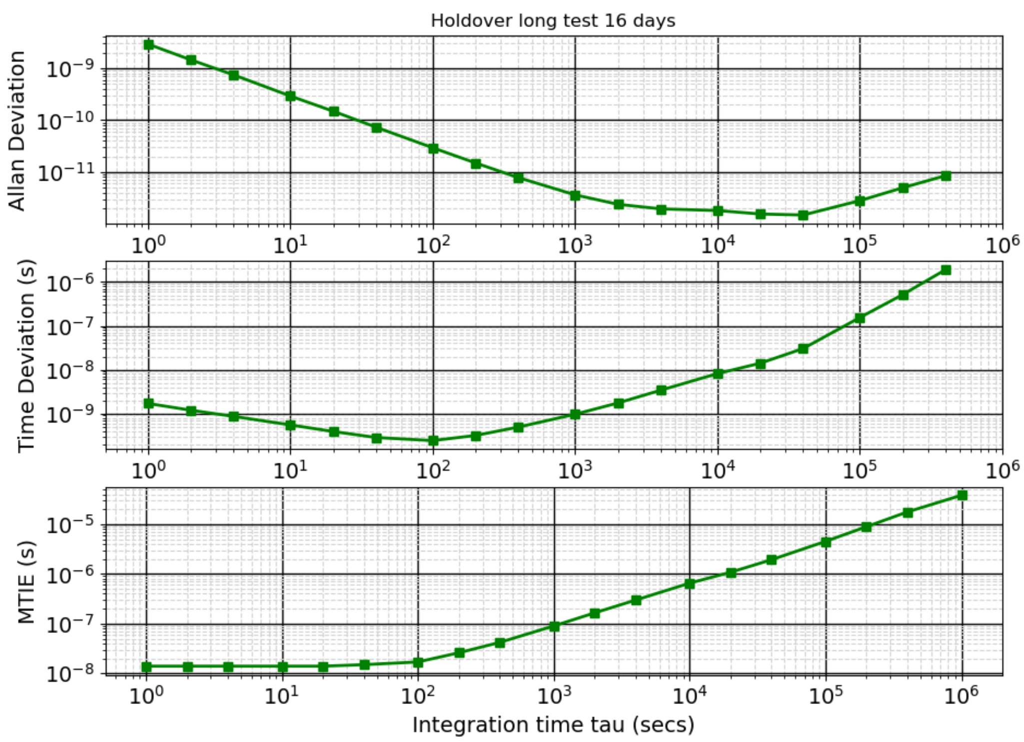


iv. Appendix 4: ADEV, TDEV and MTIE of ATS for its holdover mode with GPS unplugged for 14 days

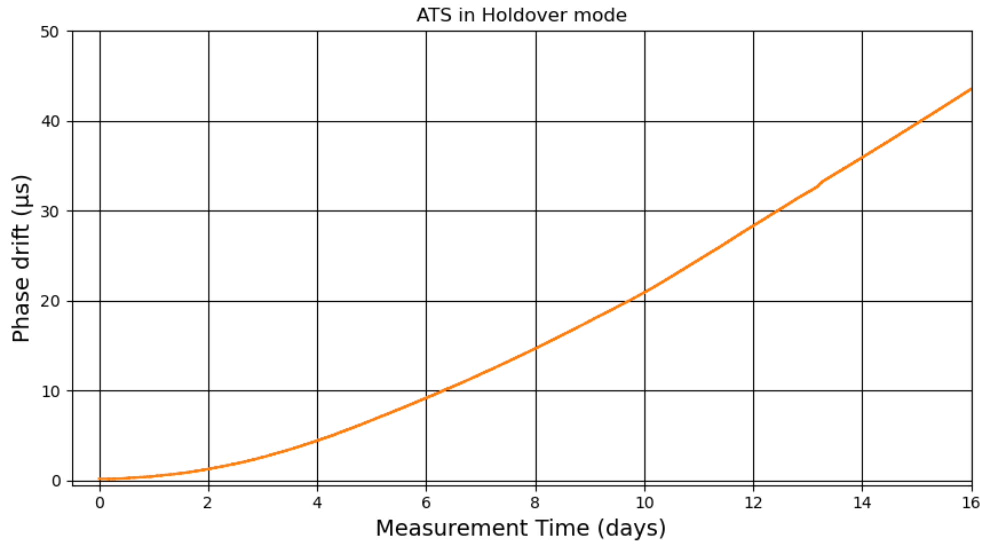
Comments / Metrics

Metric are based on significant data for 16 days with GNSS signal lost, permitting 5.5 days of integration time:
The holdover phase drift over 14 days is 35.9 µs
The Holdover Allan Deviation at long term has a value in the low 1e-11 @ 5.5 days of integration time.
It is expected that the short term (tau = 1 to 100 ns) Allan Deviation is limited due to the resolution of the Time Interval Counter (TIC).
The Time Deviation reaches a value just above 1µs @ 6 days of integration time (possible integration time with 16 days raw data).
The Maximum Time Interval Error (MTIE) provides very useful information about the peak value of the time error over a certain period of integration time and is about 50µs @ 10 days for the 16 days holdover dataset.

Environmental conditions, in particular temperature variations, which have not been measured, can significantly influence the results



Below is the graph from the raw data given by the TIC:


ATS in Holdover mode
Phase drift (µs)
Measurement Time (days)
0
10
20
30
40
50
0
2
4
6
8
10
12
14
16