Inauguration laboratoire commun FAST-LAB

J.-M Friedt[1], P.-Y. Bourgeois[1], G. Goavec-Merou[1],
B. Legeard [2], A. Vernotte [2], F. Meyer[3]

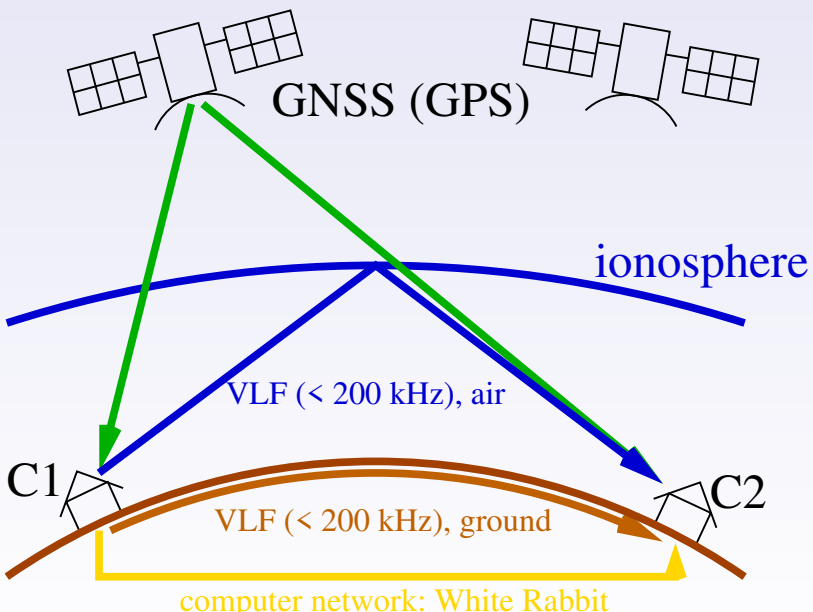
[1] FEMTO-ST/temps-fréquence & FAST-LAB, Besançon
[2] FEMTO-ST/DISC & FAST-LAB, Besançon
[3] OSU Théta/Observatoire de Besançon & FAST-LAB, Besançon

jmfriedt@femto-st.fr

July 9, 2019

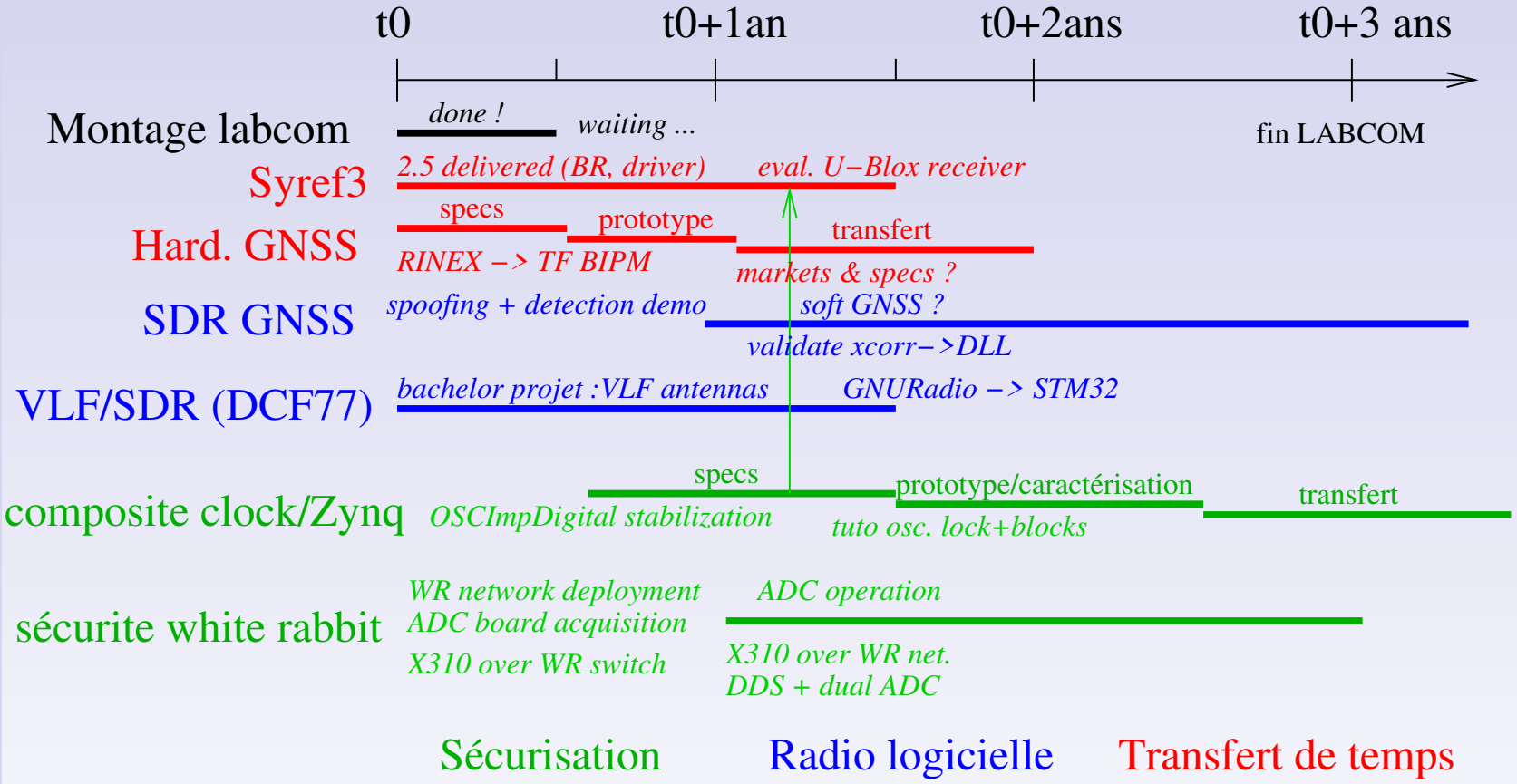
Introduction

- Deux interlocuteurs désirent comparer la base de temps de leurs horloges C1 et C2
- **Multiplier les canaux** de comparaison pour résister aux **brouillages et leurrages** de signaux de comparaison
- Une liaison radiofréquence ne peut se propager que d'une centaine de kilomètres tout au plus
- Une onde radiofréquence se propage à **300 m/μs** : comment sycnhroniser deux personnes à plus de 1000 km à mieux que la milliseconde ?
  - Observation d'un signal commun issu de GNSS
  - Observation d'un signal se propageant à très basse fréquence
  - Échange (bidirectionnel) de signaux informatiques (réseau fibré)

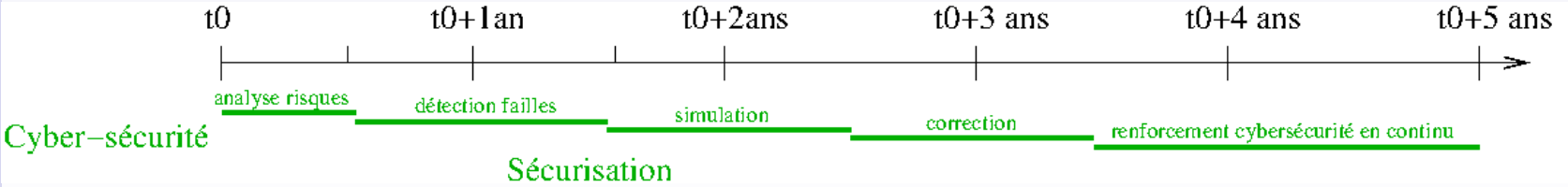


Projet LabCom FAST-LAB

Roadmap transfert de temps sécurisé

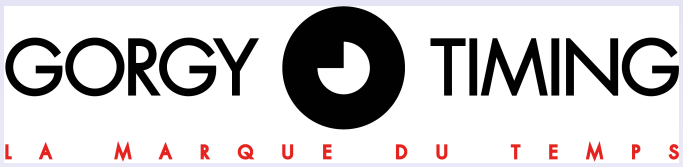


Roadmap cybersécurité



Résultats : montage administratif

- 9 mois pour réussir à s'accorder entre toutes les entitiés juridiques des tutelles de FEMTO-ST



- signature juste avant la limite de l'année, échéance de la signature
- maintenant : mi-chemin du projet (Mars 2018 + 18 mois)

$\Rightarrow$ 1 ingénieur de recherche financé à plein temps sur LabCom

Présentation des résultats obtenus jusqu'ici en cohérence avec roadmap

Résultats : Syref

- Le LNE-LTFB (Obs. Besançon) assume depuis 2000 la mission de diffusion de la référence nationale de fréquence en collaboration avec le LNE-Syrte (Obs. Paris)
- Certificats d'étalonnage estampillés du logo du BIPM $\longrightarrow$
- dernier matériel en date pour assumer cette mission : Syref 2.5 finalisée avec Gorgy Timing et livrée, planification de la Syref 3 (traçabilité **temps-réel** – 30 min – et récepteur multi-constellations) puis 4 (horloge composite)
- Évaluation des récepteurs GNSS multi-constellation U-Blox (Suisse), voir métrologiques dédíes au transfert de temps.

LNE-LTFB

Laboratoire Temps-Fréquence de Besançon
41bis, avenue de l'observatoire, B.P. 1615
25010 Besançon CEDEX
Tél : 03 81 66 69 31
Fax : 03 81 66 69 44
Mél : contact@ltfb.fr

Chaîne d'étalonnage temps-fréquences
Laboratoire Associé au LNE
n° 2.06

CIPM MRA

CERTIFICAT D'ÉTALONNAGE
N° 19G72.05

délivré à : OBSERVATOIRE DE BESANCON
41bis, avenue de l'Observatoire
BP1615
25010 BESANCON CEDEX

INSTRUMENT ÉTALONNÉ

Désignation : TA(OB)

Fabricant : HEWLETT-PACKARD

Type : 5071A N° de série : US49352985
N° d'identification : 1352985

Ce certificat comprend 5 pages et une annexe Date d'émission : 4 juin 2019

Le responsable du laboratoire
François MEYER

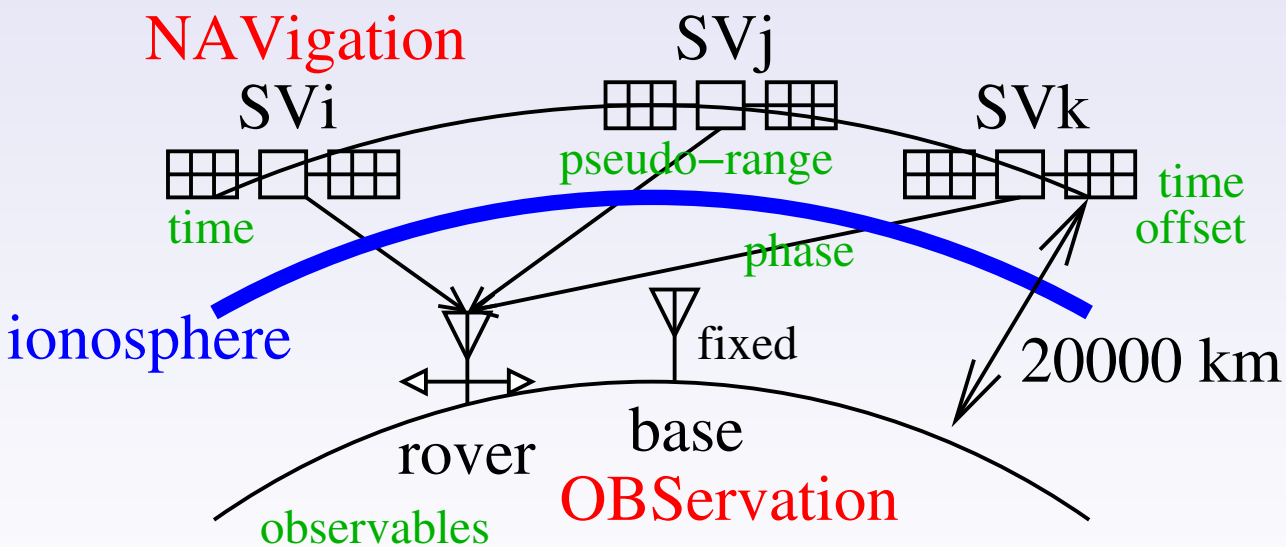
Les incertitudes élargies mentionnées sont celles correspondant à deux incertitudes types. Les incertitudes types ont été calculées en tenant compte des différentes composantes d'incertitudes, étalons de référence, moyens d'étalonnage, contribution de l'instrument étalonné, répétabilité... Ce certificat d'étalonnage garantit le raccordement des résultats d'étalonnage au système international d'unités (SI).
Le COFRAC est signataire de l'accord multilatéral de EA (European co-operation for Accreditation) et d'ILAC (International Laboratory Accreditation Cooperation) de reconnaissance de l'équivalence des documents d'étalonnage.

Accréditation n° 2.06
Liste des sites accrédités et portée disponible sur www.cofrac.fr

LA REPRODUCTION DE CE CERTIFICAT N'EST AUTORISÉE QUE SOUS LA FORME DE FAC-SIMILÉ PHOTOGRAPHIQUE INTÉGRAL

Résultats : GNSS matériel

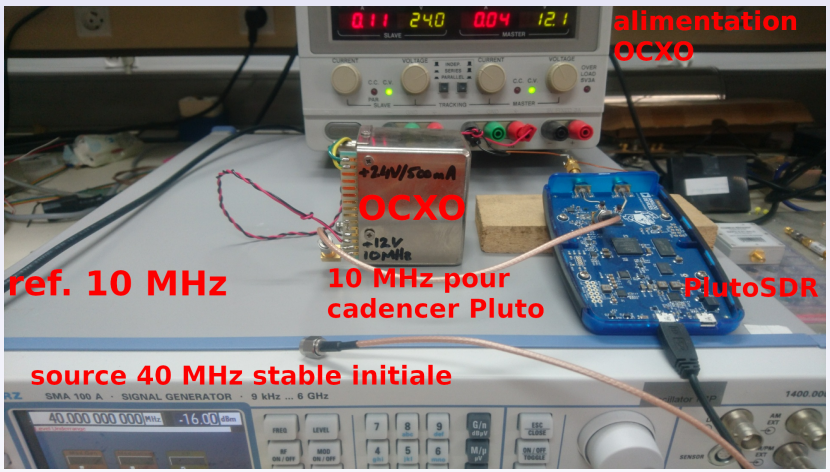
- **Multitude de récepteurs** arrivent sur le marché incluant de nouveaux circuits de réception (U-Blox, Qualcomm Snapdragon 855 dans les téléphones Xiaomi Mi{8,9})
- Exploitation des données brutes (pseudo-range dans fichiers RINEX et puissance) pour identifier tentative de leurrage
- Génération de fichiers de transfert de temps haute précision (récepteurs multiconstellations bifréquence)



Résultats : GNSS logiciel

- Un attaquant convenablement conçu [1] [2] [3] génère des puissances et des trames compatibles avec le récepteur ⇒ pseudo-range erronés ne peuvent être détectés
- adresser le problème du leurrage au plus près des signaux radiofréquences analogiques

- solution radio logicielle démontrant le leurrage et sa détection par une méthode sans décodage (*codeless*)
- solution d'acquisition de la constellation GPS par radio logicielle



[1] `www.bbc.com/news/technology-48786085`: "Russia denies ... GPS jamming"

[2] G. Goavec-Merou, J.-M Friedt, F. Meyer, *Leurrage du GPS par radio logicielle*, MISC HS (Feb. 2019) & *Spoofing GPS*, FOSDEM 2019

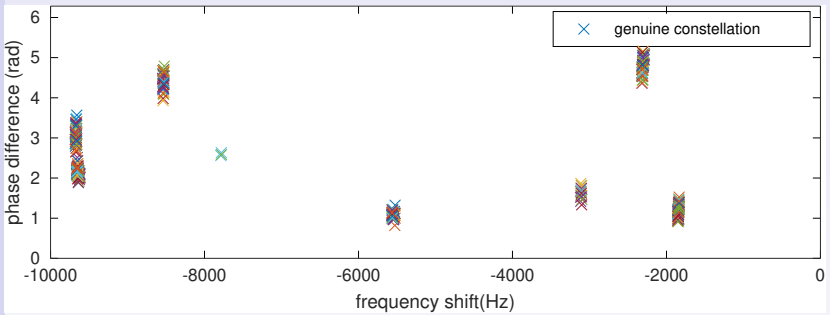
[3] `hackaday.com/2019/06/09/gps-and-ads-b-problems-cause-cancelled-flights/`

Résultats : GNSS logiciel

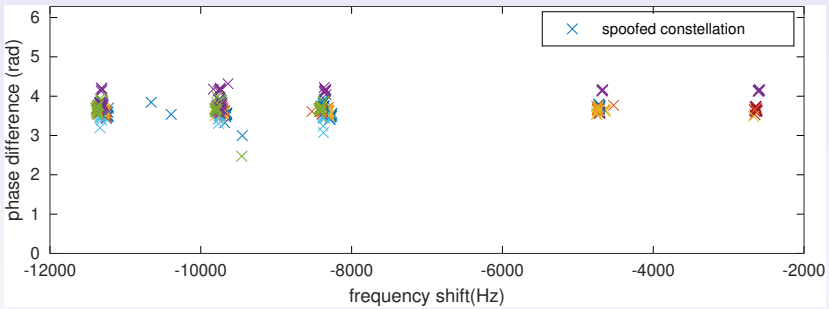
- Un attaquant convenablement conçu [1] [2] [3] génère des puissances et des trames compatibles avec le récepteur ⇒ pseudo-range erronés ne peuvent être détectés
- adresser le problème du leurrage au plus près des signaux radiofréquences analogiques

- solution radio logicielle démontrant le leurrage et sa détection par une méthode sans décodage (*codeless*)
- solution d'acquisition de la constellation GPS par radio logicielle
- Suite ? mise en œuvre du tracking ? adaptation de `gnss-sdr` ? [4]

Constellation GPS



Leurrage



Exploitation de la diversité spatiale des antennes de réception

[1] `www.bbc.com/news/technology-48786085`: "Russia denies ... GPS jamming"

[2] G. Goavec-Merou, J.-M Friedt, F. Meyer, *Leurrage du GPS par radio logicielle*, MISC HS (Feb. 2019) & *Spoofing GPS*, FOSDEM 2019

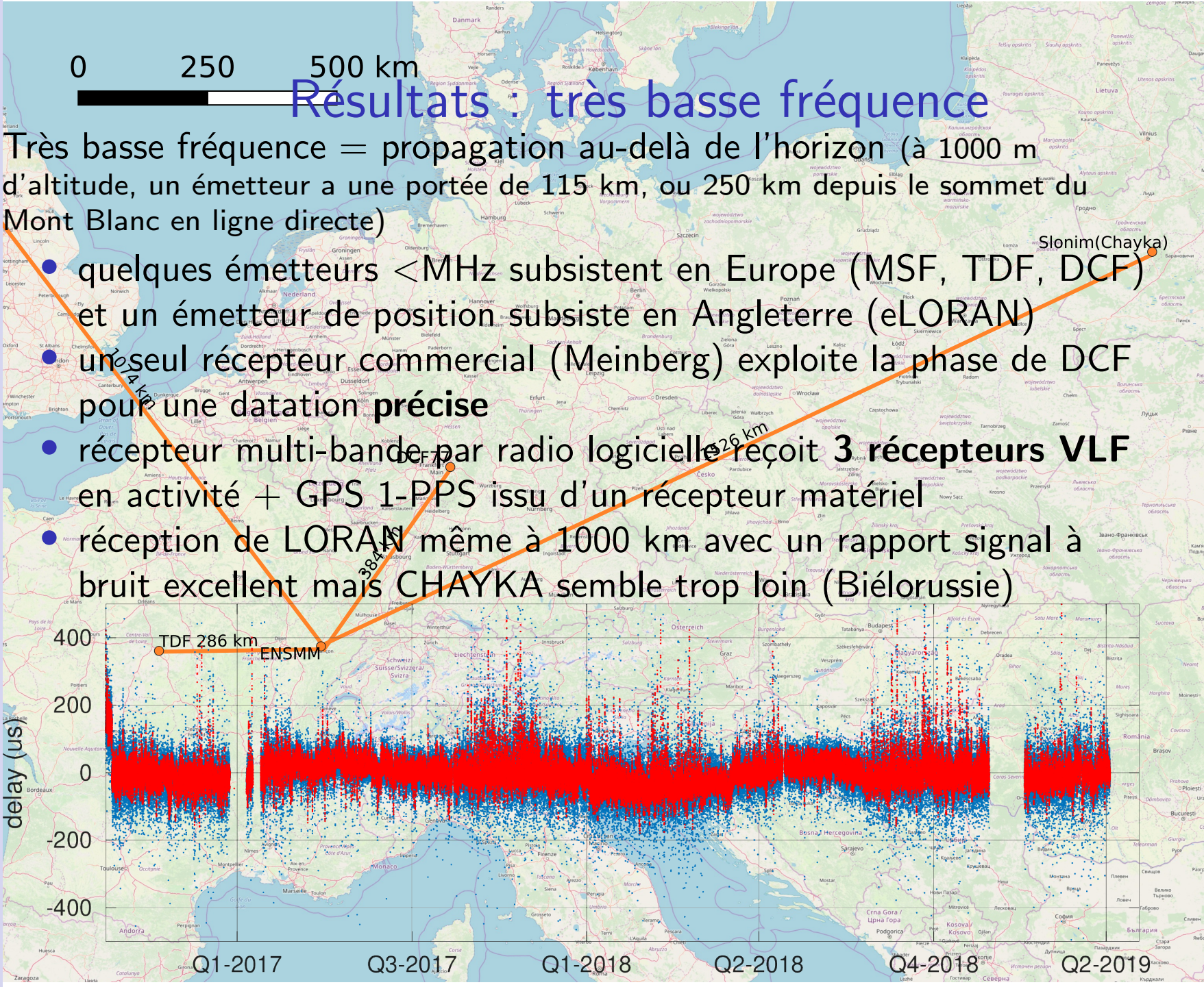
[3] `hackaday.com/2019/06/09/gps-and-ads-b-problems-cause-cancelled-flights/`

[4] `https://gnss-sdr.org/`

Résultats : très basse fréquence

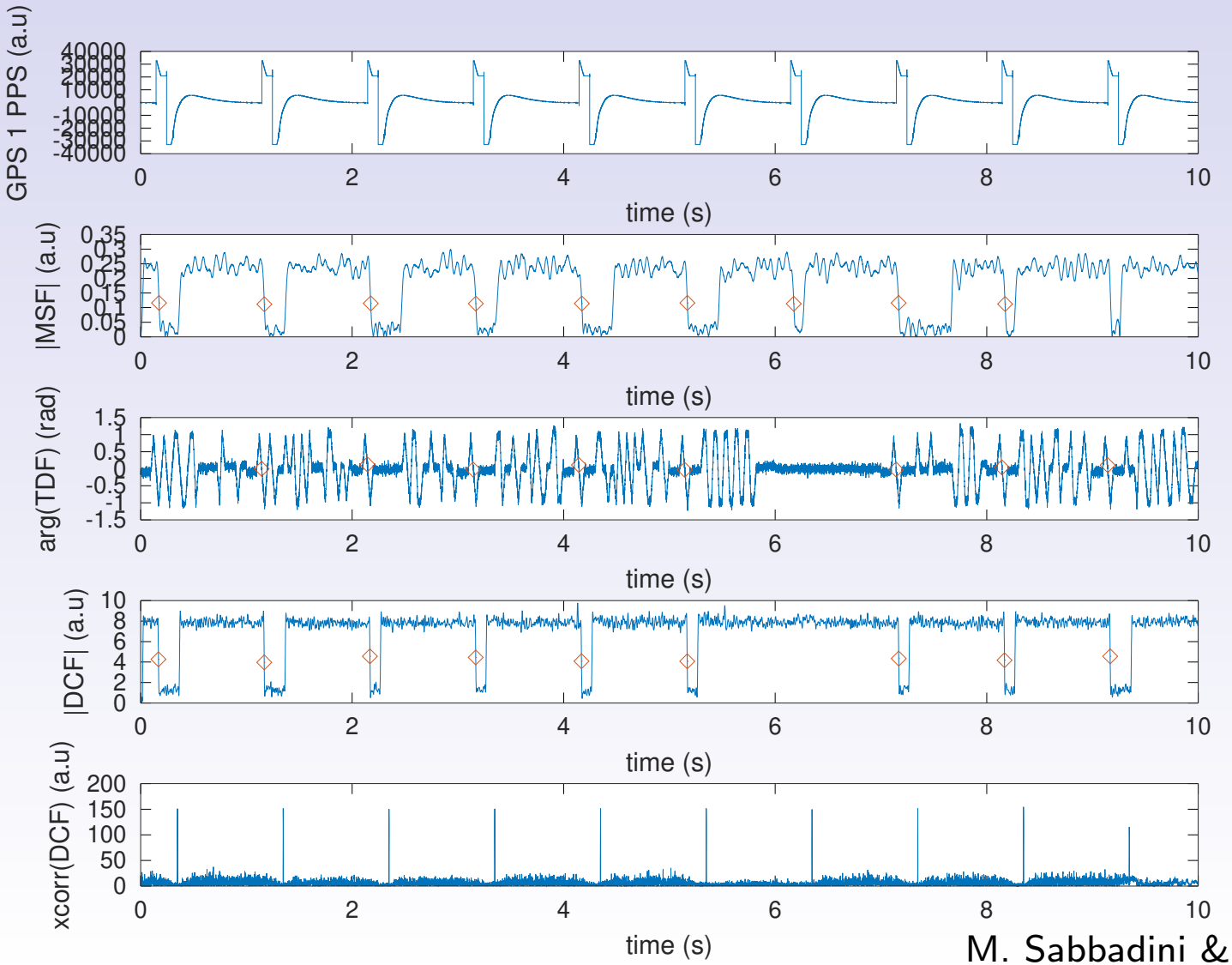
Très basse fréquence = propagation au-delà de l'horizon (à 1000 m d'altitude, un émetteur a une portée de 115 km, ou 250 km depuis le sommet du Mont Blanc en ligne directe)

- quelques émetteurs <MHz subsistent en Europe (MSF, TDF, DCF) et un émetteur de position subsiste en Angleterre (eLORAN)
- un seul récepteur commercial (Meinberg) exploite la phase de DCF pour une datation **précise**
- récepteur multi-bande par radio logicielle reçoit **3 récepteurs VLF** en activité + GPS 1-PPS issu d'un récepteur matériel
- réception de LORAN même à 1000 km avec un rapport signal à bruit excellent mais CHAYKA semble trop loin (Biélorussie)



Résultats : très basse fréquence

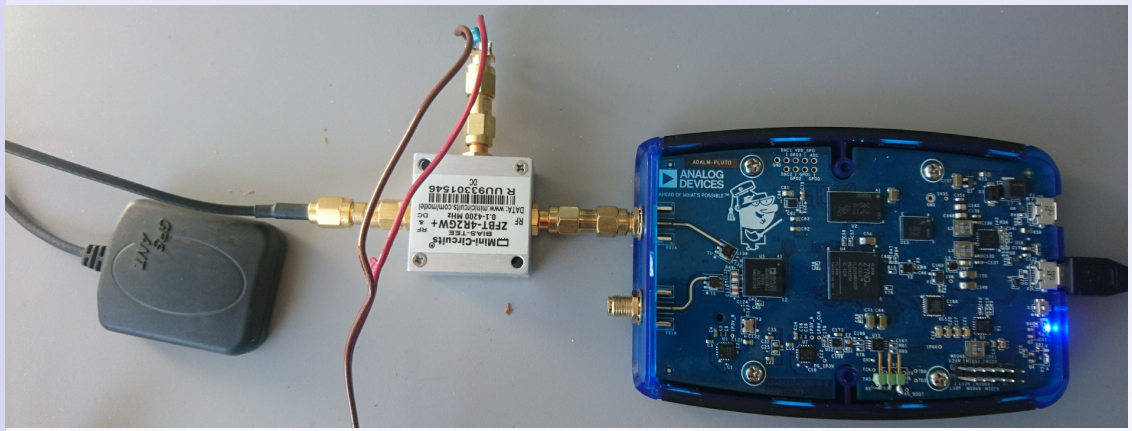
Solution totalement logicielle de réception de quatre émetteurs VLF (TDF, DCF φ et $|.|$, MSF, LORAN, référencés à GPS)

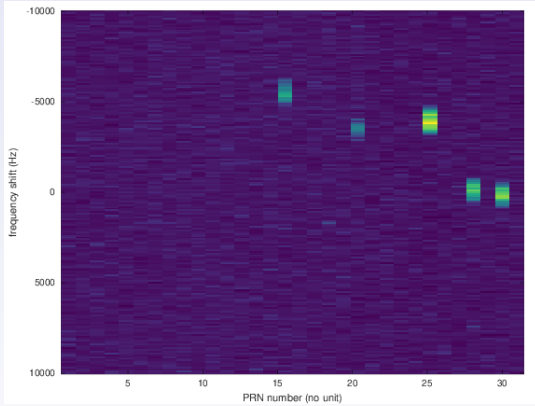


Résultats : horloge composite

Environnement de développement OscImpDigital stabilisé, étendu et documenté à `https://github.com/oscimp/oscimpDigital`

- indépendance de la plateforme (évolution rapide du matériel)
- indépendance du vendeur
- traitement en flux tendu (pipeline $\neq$ *batch processing*)



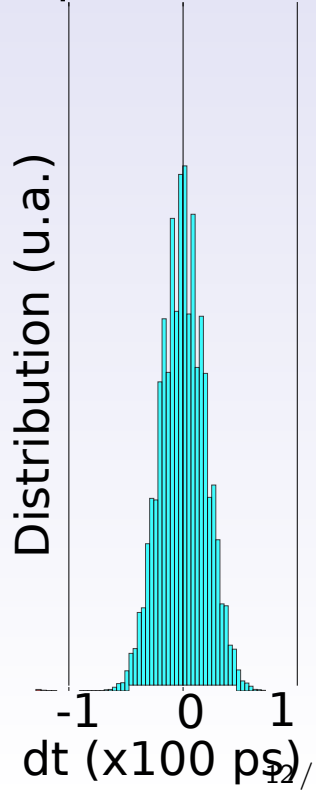


Récepteur GPS logiciel sur PlutoSDR développé sur l'environnement OscImpDigital [5]

[5] `https://github.com/oscimp/oscimpDigital/tree/master/doc/tutorials/plutosdr/2-PRN_on_PL`

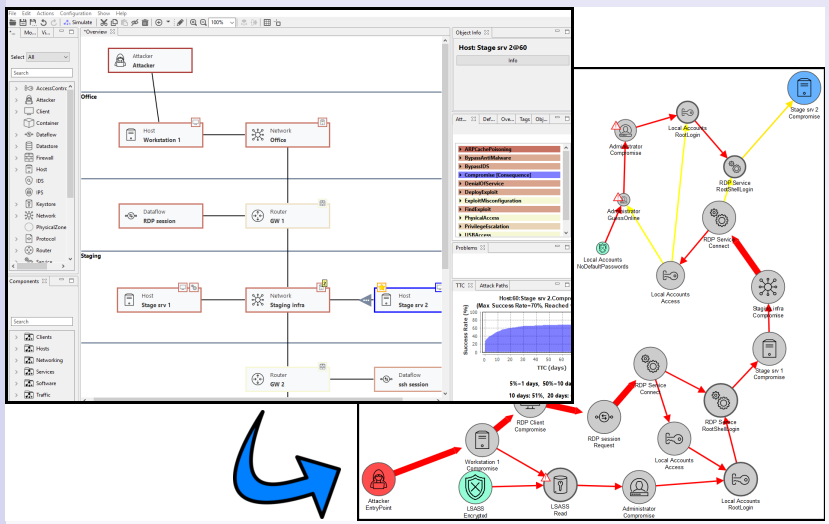
Résultats : White Rabbit et sécurité

- Prise en main du réseau existant liant masers de temps-fréquence de FEMTO-ST et Cs de l'Observatoire de Besancçon
- extension de ce réseau aux salles d'expériences de FEMTO-ST (hors ZRR) et vers les départements d'enseignement (électronique) et recherche (informatique) de l'Université
- disponibilité du réseau à côté du point d'arrivée de RENATER si un interlocuteur s'y intéresse un jour
- évaluation des fonctionnalités au-delà du transfert de temps et fréquence :
  - datation d'échantillons de signaux radiofréquences (RADAR distribué),
  - génération de signaux cohérents en phase (*distributed DDS*),
  - transport TCP/IP sur White Rabbit (non-implémenté à Noël 2018)



Résultats : cybersécurité (SCPTime)

- Analyse des risques de cybersécurité de transfert de temps sur réseau informatique (contexte de l'architecture SCPTime utilisée par Gorgy Timing)
- Étude bibliographique sur risques de leurrage sur White Rabbit [6] [7]
- Simulation d'attaques = analyse statistique pour estimer un temps (TTC) nécessaire à un attaquant pour atteindre son objectif (DoS, accès administrateur ...) en fonction de la nature de l'attaque



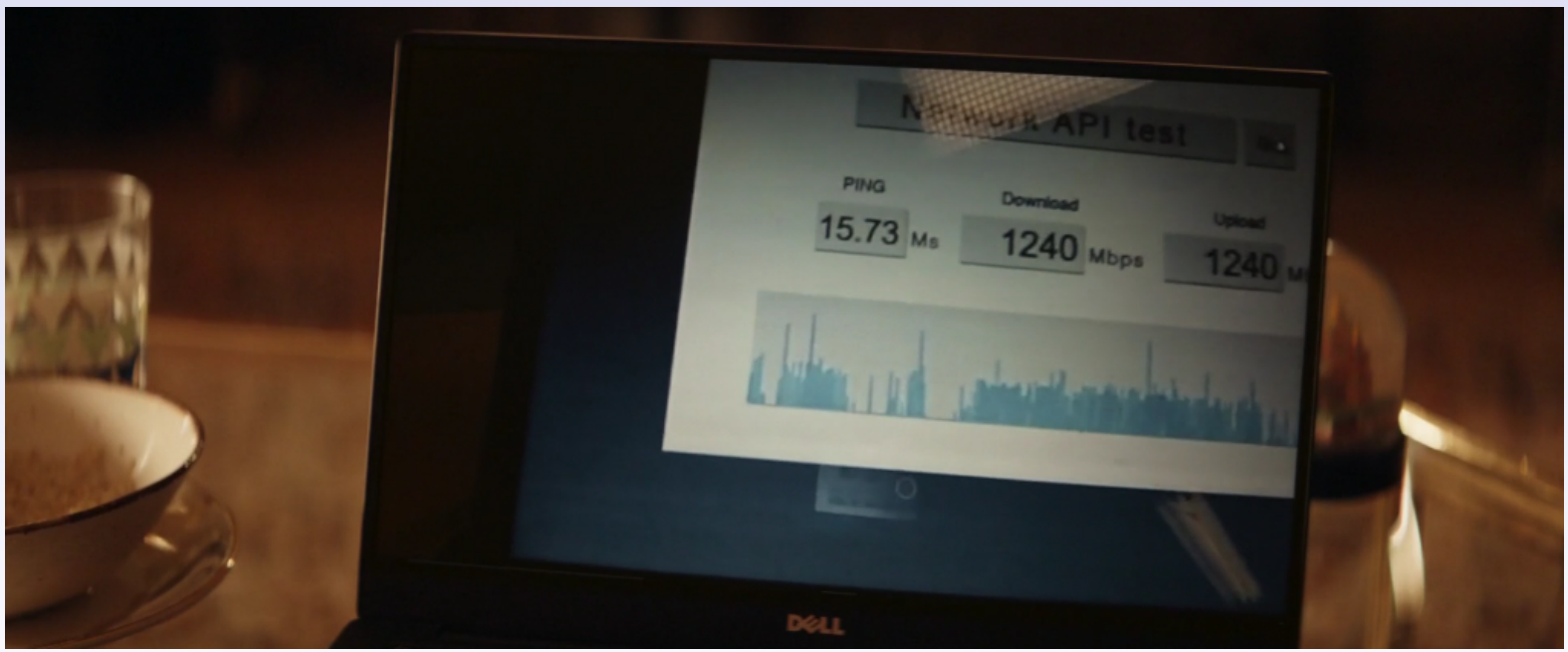
- Outil SecuriCAD pour la simulation d'attaques sur un modèle de réseau numérique
- Simulation d'attaques = identification des chemins critiques, i.e. maillon faible de l'infrastructure

[6] S. Barreto *& al.*, *Cyber-attack on Packet-Based Time Synchronization Protocols: the Undetectable Delay Box*, Proc. IEEE International Instrumentation and Measurement Technology Conference (2016)

[7] E. Itkin & A. Wool, *A security analysis and revised security extension for the precision time protocol*, IEEE Transactions on Dependable and Secure Computing (2017)

Conclusions et perspectives

- Toutes les lignes de la *roadmap* ont évolué et permis d'**améliorer nos connaissances** sur le transfert de temps et ses difficultés
- Sujet qui n'avait pas été abordé à FEMTO-ST avant ce projet qui a **stimulé l'étude**
- Absence de soutien financier en complément de l'ANR LabCom à corriger : CNES, ESA [8] ou DGA ? Ressources en personnel ?



The Hummingbird Project, Vincent @ 5820 s: "it's not the destination that's important, it's the people we meet and the lessons we learn".

[8] ESA, *NAVISP-EL1-037: PNT TIMING & SYNCHRONISATION FOR AVIATION SYSTEMS AND NETWORKS - EXPRO+*, Closing date 30/08/2019