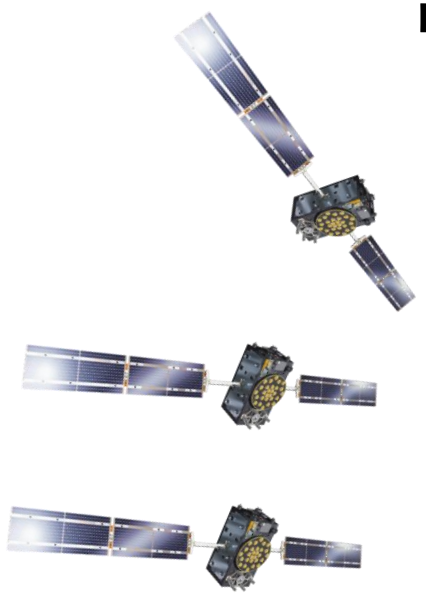
高精度測位補強サービスの将来展望について



QBIC第2回海外展開WG

廣川　類　（三菱電機株式会社）

2023年6月22日 13:35-14:05

MITSUBISHI ELECTRIC CORPORATION

Contents

1. 高精度測位補強サービスの現状
2. QZSS CLAS機能向上の構想
3. PPP-RTK/PPP認証機能に関する研究

1 高精度測位補強サービスの現状

高精度測位における相互運用性と標準化

- オープンな高精度補強サービス、低コストGNSS受信機が普及し、高精度測位を利用するアプリケーションが普及する
- 複数のプロバイダ（GNSS,補強サービス業者）、複数の受信機が混在して使用される
- 課題：組み合わせの数は非常に多く、開発・試験に多くのリソースが必要となる
- このため、プロバイダ・受信機間、受信機・アプリ間におけるインターフェイスの定義・標準化が必要

1-2 オープンな高精度補強サービスの普及

- 衛星配信によるオープンなPPP/PPP-RTK補強サービスが利用可能となっている
- UN-ICGの枠組みでPPPの相互運用性に関するタスクフォースを開始（2019-）：11団体
  - ✓ 2nd Workshopを実施（2023/3 at JRC）
  - ✓ パラメータ（性能指標等）の定義明確化、参照モデル等について議論、RTCMと連携
- 主要パラメータをまとめ、「PPP Service Providers Report」を作成(rev.2 draft)
- 伝送フォーマットについては日本発のCompact SSR (CSSR)（派生含む）でまとまりつつある

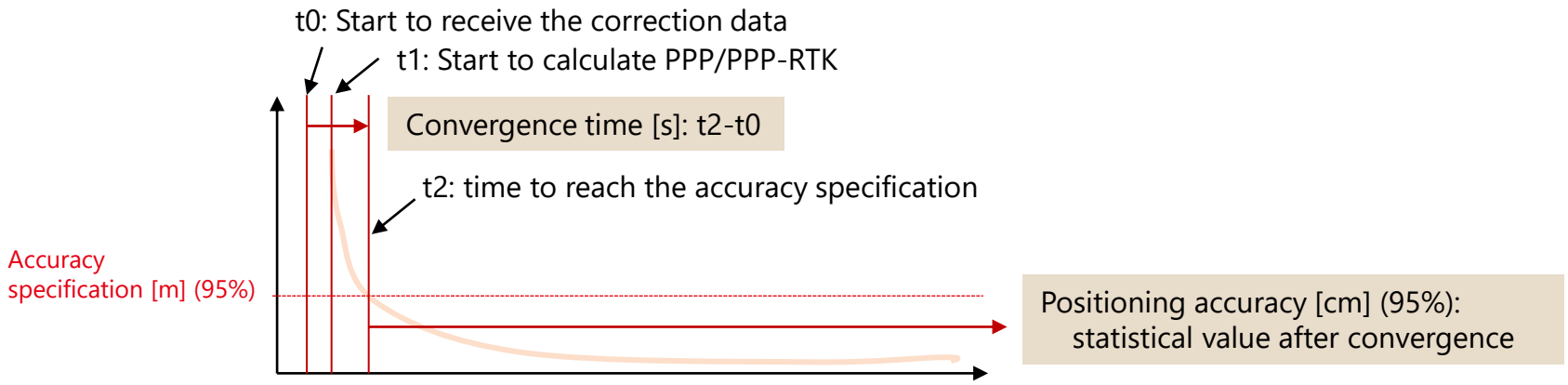
List of Open Satellite-Based High-Accuracy GNSS Correction Service

System	Country	Service Area	Service	Satellite	Status	Signal	Data Rate	Format in SIS
QZSS CLAS	Japan	Japan	PPP-RTK	IGSO/GEO	Operational (2018-)	1.278GHz (L6D)	1,695bps	**CSSR**
QZSS MADOCA	Japan	Asia/Oceania	PPP	IGSO/GEO	Trial service (*1)	1.278GHz (L6E)	1,695bps	**CSSR**
Galileo HAS	EU	Global	PPP	MEO	Operational (2023-)	1.278GHz (E6b)	448bps	Similar to **CSSR**
BeiDou 3	China	China+	PPP	GEO	Operational (2020-)	1.207GHz (B2b)	456bps	Customized **CSSR**
PPP via SouthPAN	AU/NZ	Oceania	PPP	GEO	Early Service (2022-)	1.207GHz (E5b)	500bps?	(TBD)
GLONASS	Russia	Russia	PPP	MEO/IGSO	Development (2030-)	1.202GHz (L3SVI)	3,155bps	**CSSR**
KPS	Korea	(TBD)	(TBD)	GEO	Development (2035-)	1.278GHz (L6)	(TBD)	(TBD)

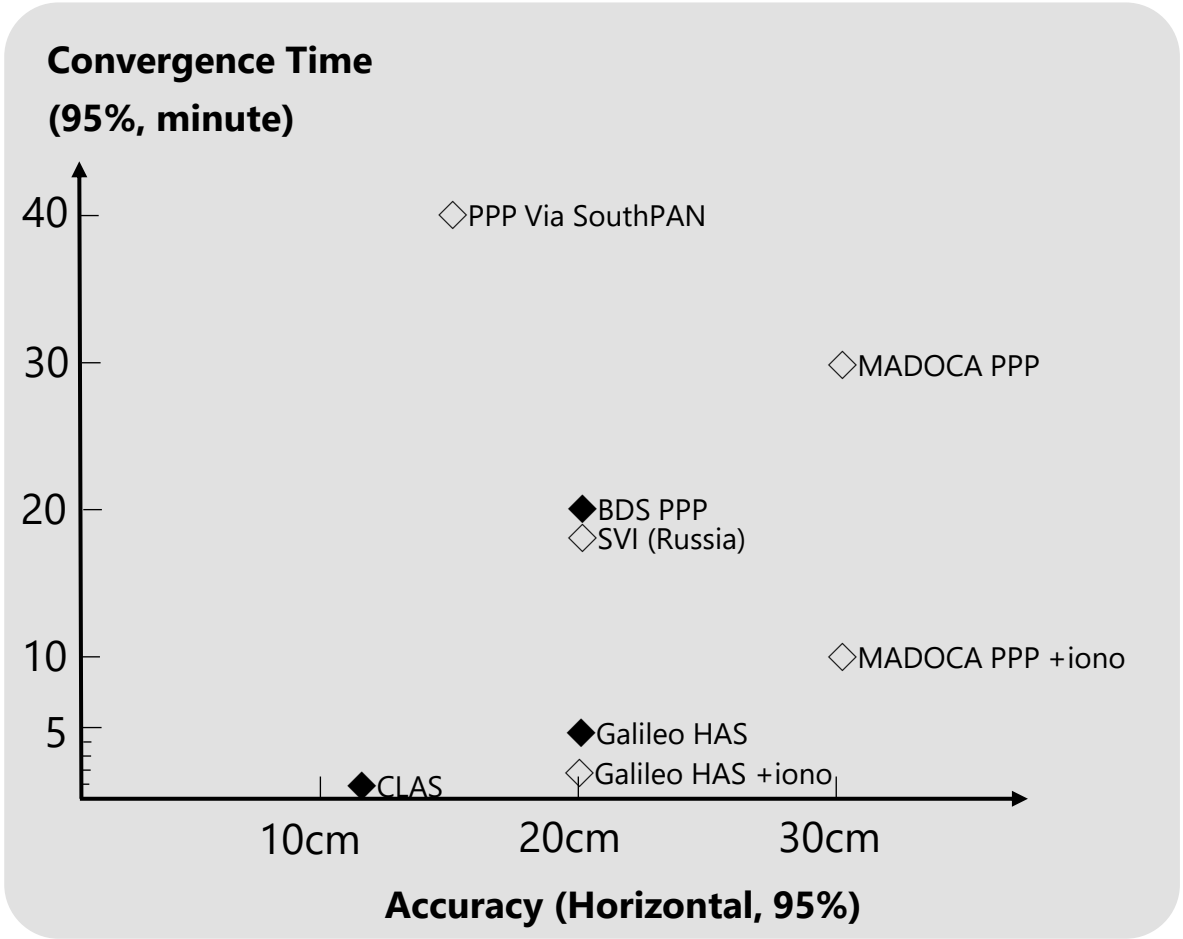
*1 Operational from 2024

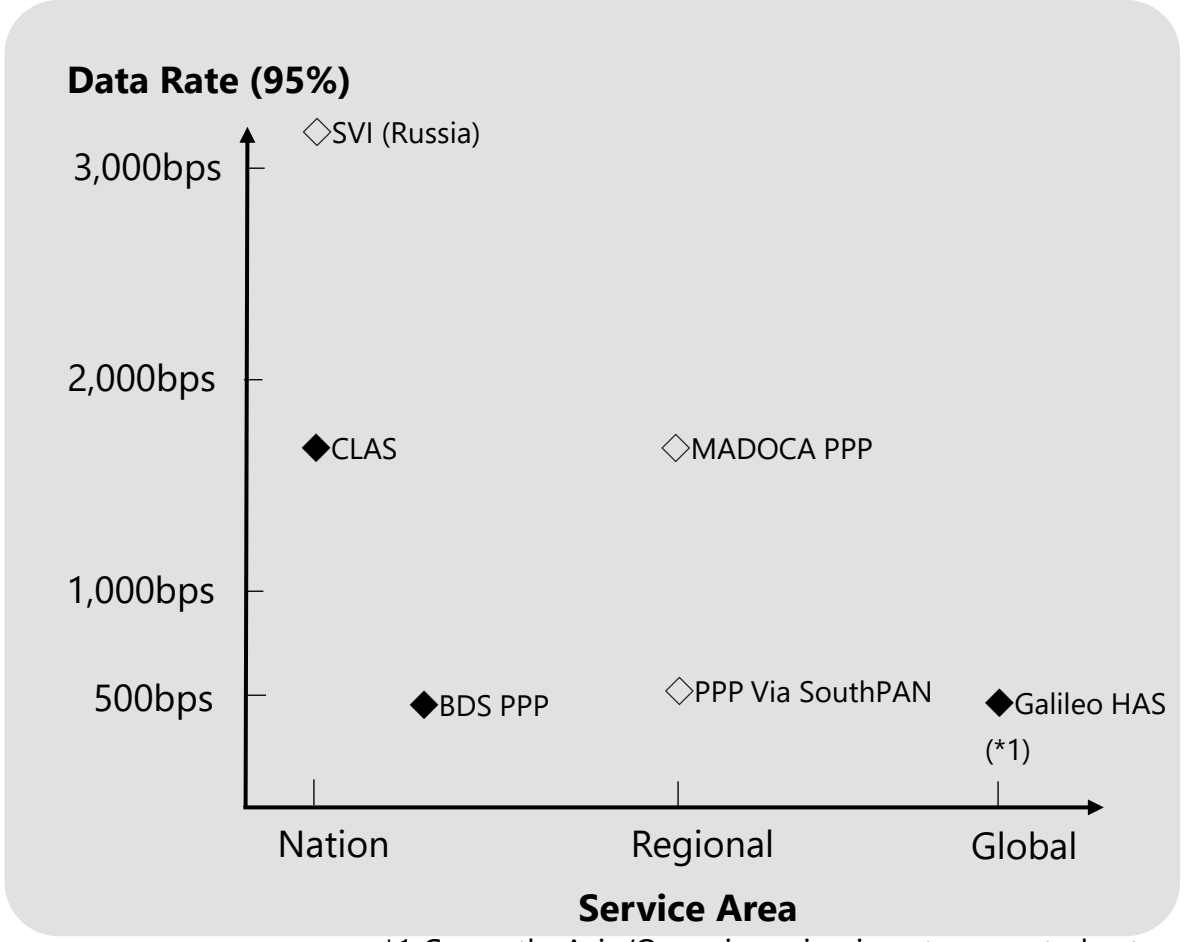
ICG 3PITF における議論

- 追加: “reference time system”, “reference coordinates”
- 定義があいまい:
  - ✓ 測位精度:
    - ➢ Statics value after convergence? If so what is the definition of convergence?
  - ✓ 収束時間:
    - ➢ It is including time-to-receive correction data?
    - ➢ Time to reach specification or time to convergence?
    - ➢ If specification, what if error increases later?
  - ✓ 用語の定義：PPP, PPP-float, PPP-AR, PPP-RTK, PPP with iono
- Standardized algorithm for PPP:　Galileo HAS reference algorithm
- OSS Toolkit: RTKLIB, PPPLIB, CLASLIB, MADOCALIB, cssrlib



（参考）PPP/PPP-RTK performance map





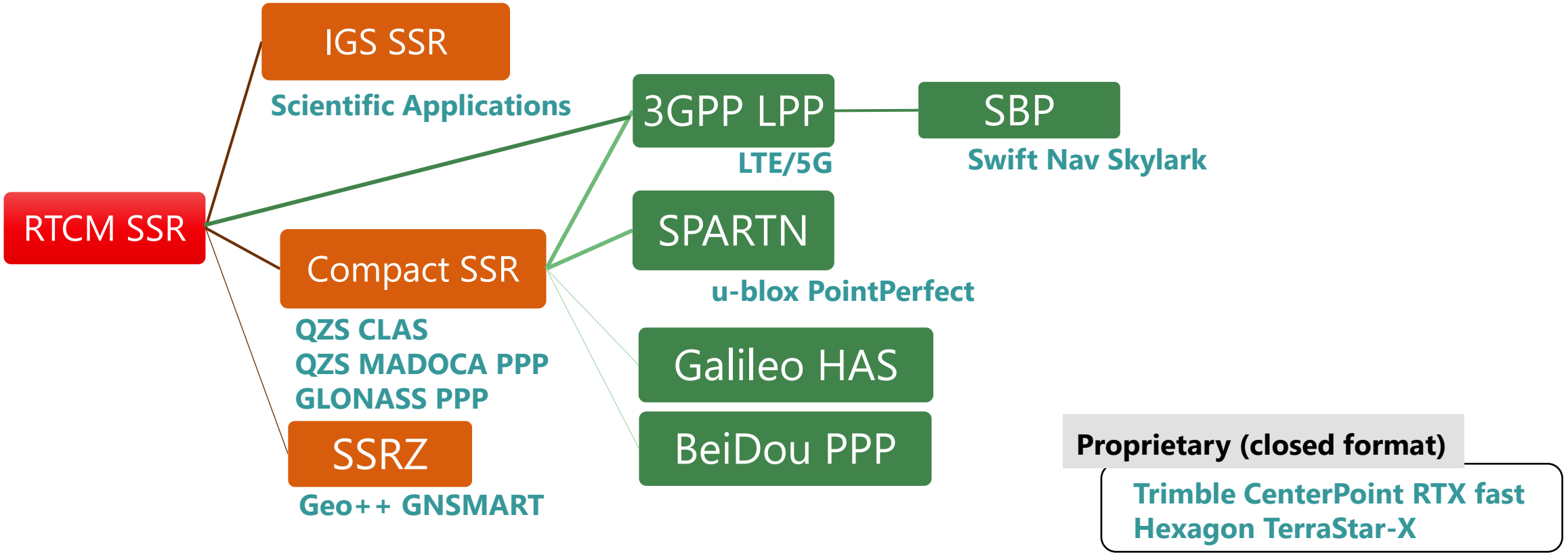
*1 Currently, Asia/Oceania region is not supported yet

◆ Operational ◇Development or Trial Service

From PPP Service Providers Report, 2nd

PPP/PPP-RTKのオープンフォーマット

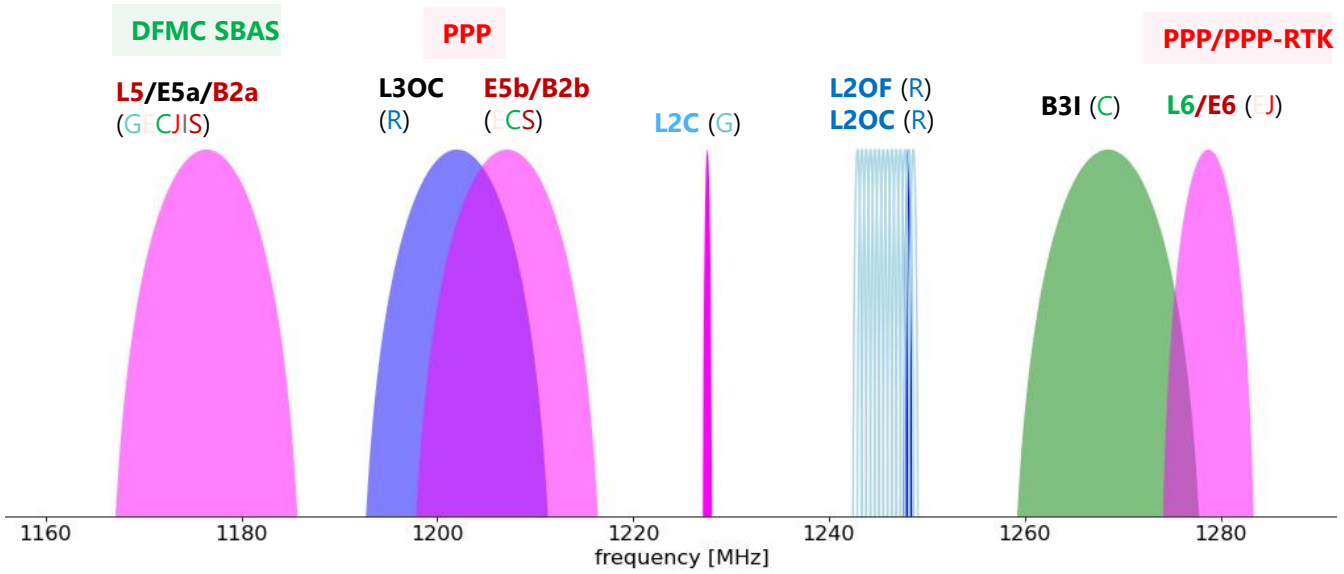
- RTCM SC-104 委員会でSSR標準（RTCM-SSR）を2011年に定義（ステージ1：PPP）
- RTCM SSR互換のPPP/PPP-RTK用高効率オープンフォーマットCompact SSRが2015年に提案されQZSS CLASに採用。3GPP、Galileo HAS、GLONASS PPPにも適用。
- RTCM SSRは標準化が長らく滞っていたが、SSR TaskForceにより標準化提案をまとめ中。

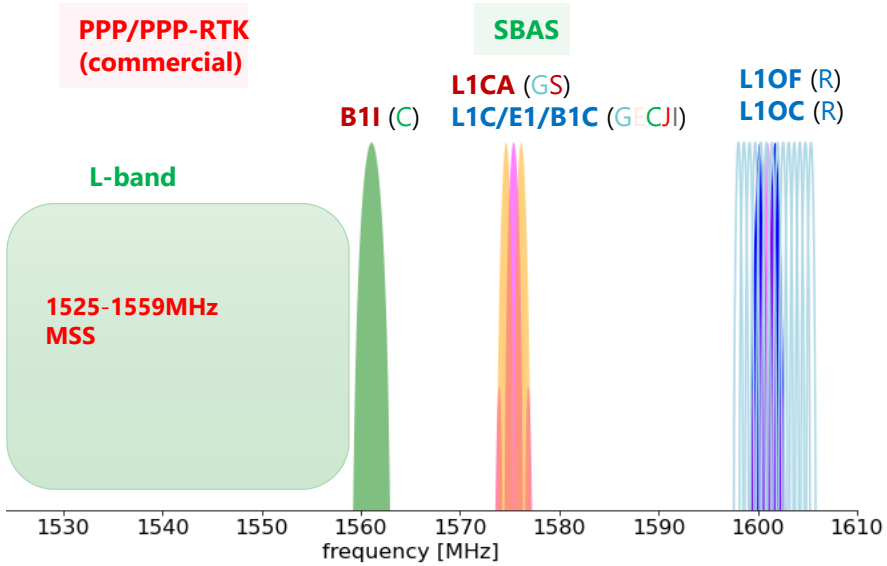


GNSSオープン信号周波数と補強信号

■ PPP/PPP-RTK補強信号がRNSSバンド (1.2GHz および 1.5GHz)で衛星から放送されている

- 4 種類の補強信号に分類できる:
  1. 1.575GHz (L1), 1.176GHz (L5): SBAS
  2. **1.278GHz(L6/E6): QZSS PPP/PPP-RTK, Galileo PPP, (KPS)**
  3. **1.202-1.207GHz(E5b/B2b/L3SVI): Beidou PPP, PPP via SouthPAN, Glonass PPP**
  4. 1.525-1.559GHz (L-band): commercial PPP/PPP-RTK service





Ranging or Correction

Ranging　Correction

lower L-band (1.2GHz)

upper L-band (1.5GHz)

1-7 RTCMにおける議論：L1C/Bの相互運用性に関する議論など

- SSRメッセージの標準化：SSRタスクフォースに参画、議論中。コンテンツ定義フェーズの後、圧縮メッセージについて議論予定（詳細後述）。
- LNAVメッセージの最新化：次版に反映予定（現在はJAXA時代のICDを参照）
- CNAV, CNAV2 メッセージ提案：GPSと連携して実施中
- NRTK マルチGNSS対応： Galileo, BDSは相互運用性テスト完了、QZSについては２社目の参加待ち
- MSMメッセージのL1C/B対応：内閣府と連携して、改訂案を提示。
- 受信機メーカーから相互運用性に関する指摘があり、定義を詳細化
  - ✓ 問題：L1C/BとL1C/Aの位相が厳密に一致する保障はなく、タイミングは受信機の実装に依存。
  - ✓ 対策：全世代のQZSで送信するL1Cをピボットとして、L1C-L1C/A、L1C-L1C/Bを90deg位相で定義することにより、互換性を確保する。「90deg位相」の符号はGPSの実装に合わせる。
  - ✓ L1C/B運用開始後に相互運用性試験を実施、フォーマット改訂を提案する方向で合意
- Network RTKのマルチGNSS対応に関する議論が行われている。現状のGPS/GLONASSに加えて、Galileo/BDS/QZSSを追加する提案。Galileo/BDSは相互運用性テストまで完了、規格化の予定。QZSSは相互運用性テストに参加する企業が１社のみで進んでいない状況。

3.1.7. Phase Relationship within Signals

3.1.7.1. L1

For L1 signals, the phase relationships between L1CD, L1CP, and L1C/A (or L1C/B) are shown in Table 3.1.7-1 and Figure 3.1.7-1:

Table 3.1.7-1 Phase relationships

	Carrier wave	Phase lag	accuracy
Block I	L1CD and L1C/A	same phase	± 5°
	L1CP and L1C/A	90° phase lag	± 5°
	L1CP and L1CD	90° phase lag	± 5°
Block II and III	L1CD and L1C/A (or L1C/B)	90° phase lag	± 5°
	L1CP and L1C/A (or L1C/B)	90° phase lag	± 5°
	L1CP and L1CD	same phase	± 5°

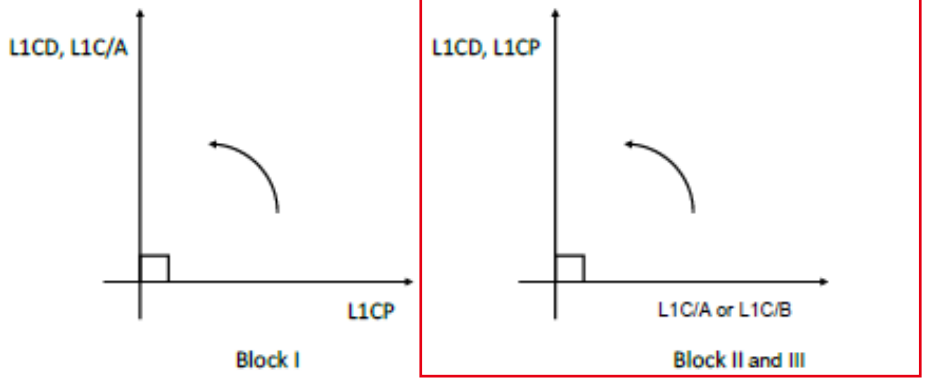


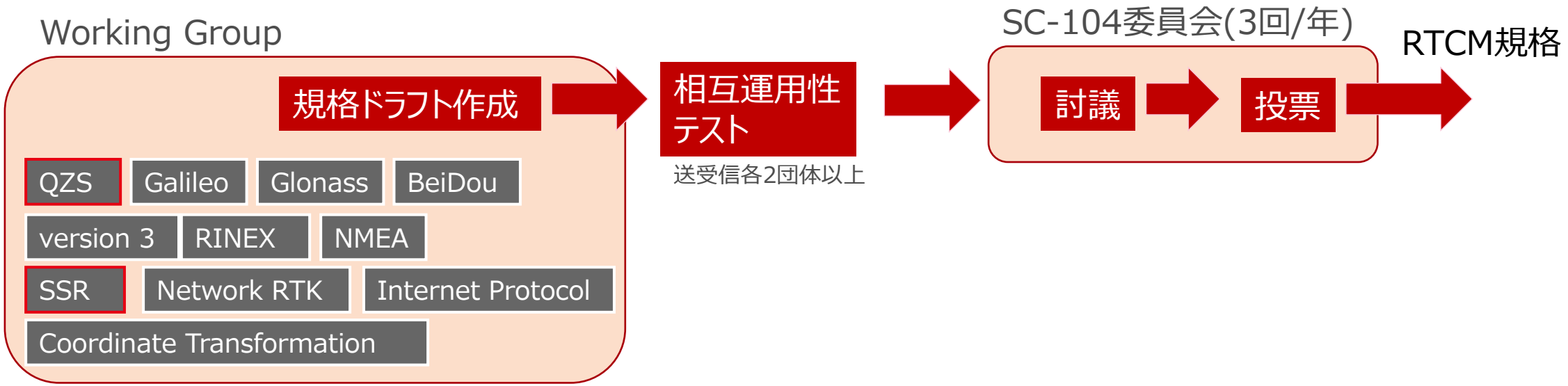
Figure 3.1.7-1 Phase Relationship of L1

（参考）RTCM 標準化委員会について

補強情報配信形式の業界標準：RTCM SC-104委員会で定義されるRTCM 規格

・主要受信機メーカ、補強サービス業者、研究機関等が参加
・国内からJAXA、三菱電機、ALESが参加

三菱電機はQZS WGのチェアを務めており、CLASで使用する圧縮方式SSR (Compact SSR)の標準化、QZS関連規格化を推進



*** RTCM SC-104: The Radio Technical Commission for Maritime Service, Special Committee 104**

1-9 RTCM SSR Taskforce における議論

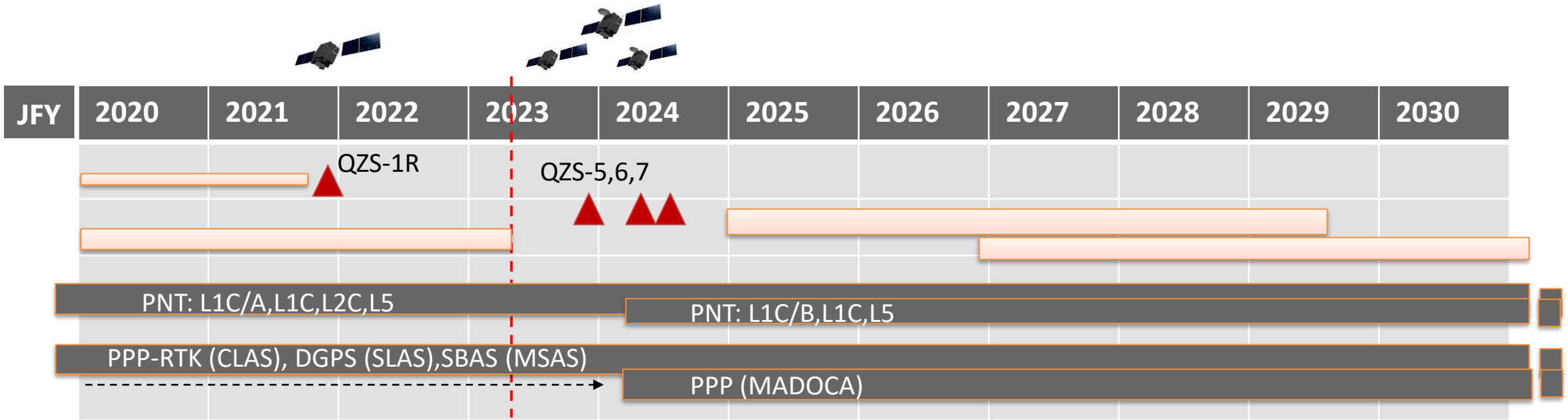
- TFメンバーにより隔週ペースで議論を継続、TFドラフト提案段階までまとまってきた。
- PPPのみならずPPP-RTKを包含、トータルパッケージとして議論
- 受信機メーカー、プロバイダにより積極的な議論が行われている：Hexagon, Geo++, Swift, Trimble
- Interoperability testに関する議論も開始
- 1年程度でTF提案まで到達できると思われる。
- コンテンツを規格化後、圧縮メッセージ等を定義

#	Item	TF Proposal
1	Satellite Orbit, Clock	As previously defined
2	Code Bias	As previously defined
3	Phase bias	RTCM SSR Phase Bias Message – Draft v6
4	Ionosphere message	RTCM SSR Ionospheric Correction Message – Draft v2
5	Tropospheric Correction Message	RTCM SSR Tropospheric Correction Message – Draft v2
6	Grid Definition Message	RTCM SSR Grid Definition Message – Draft v5
7	Satellite Antenna Message (PCV/GDV)	RTCM SSR Satellite Antenna Message – Draft v6
8	Metadata message	RTCM SSR Metadata Message - Draft v2

2 QZSS CLAS機能向上の構想

2-1 QZSS Project status

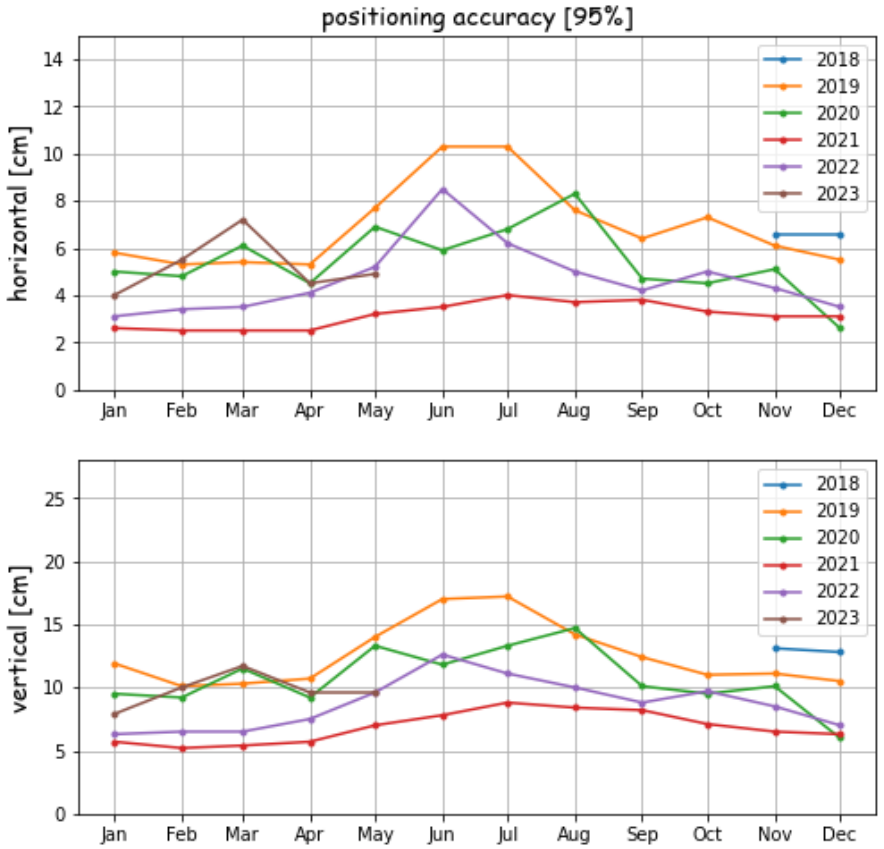
- QZSS 4 satellite constellation is in continuously operation with Q1R, Q2, Q4 and Q3.
- Development of QZS 5,6,7 is underway, they are planned to be launched in JFY2023-2024.
- Trial service of MADOCA-PPP with Compact SSR has started in Sep 2022, regional PPP service plans to be operational by JFY2024.
- L1C/B signal is planned to be operational in JFY2024 after QZS-5 is launched.
- QZNMA will be operational in JFY2024, draft ICD for QZNMA (IS-QZSS-SAS) was published on Jan 24, 2023.

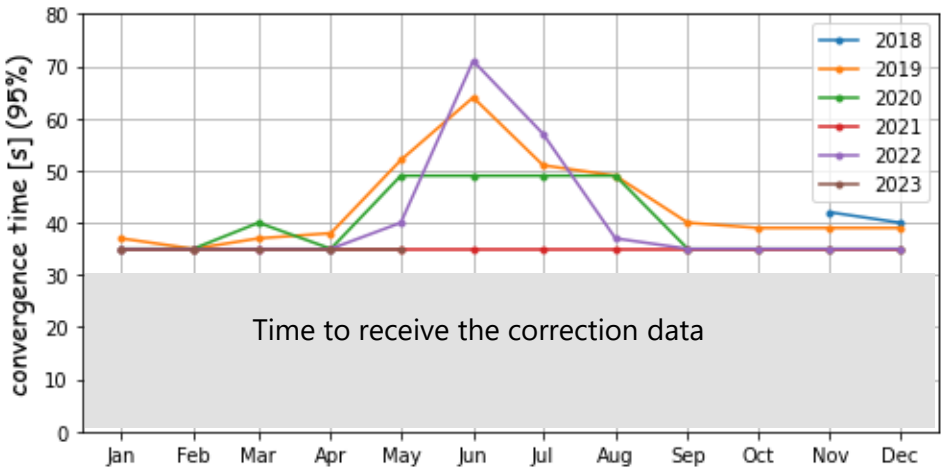


2-2 Performance of QZSS CLAS

- QZSS CLAS is operational since Nov. 2018, it proves quite good performance and the reliability.
- High-accuracy positioning solution can be obtained in 5 seconds after receiving correction data.

Kinematic mode



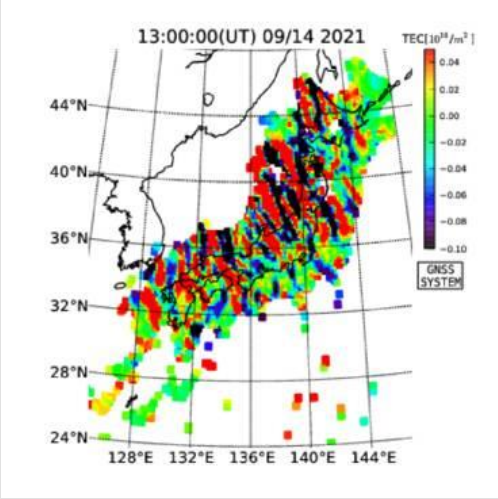


* Analyzed by CLASLIB, based on the daily solution of 72 CORS stations in Japan

2-3 Events and feedback during operation of CLAS

Atmospheric disturbance

- Ionospheric disturbance degrades the positioning performance



From: https://aer-nc-web.nict.go.jp/GPS/QR_GEONET/MAP15/

Natural disaster and System events

- Power outage on reference stations because of earthquake or typhoon.
- Failure event on internal network and equipment.
- System outage of Galileo in July 2019.

From https://qzss.go.jp

Positioning in Non-open sky condition

- The availability of high-accuracy position is limited on non-open-sky condition

CLAS改善の方向 (ION Pacific PNT 2022)

- More satellites by combining multiple channels of multiple QZSS satellites.

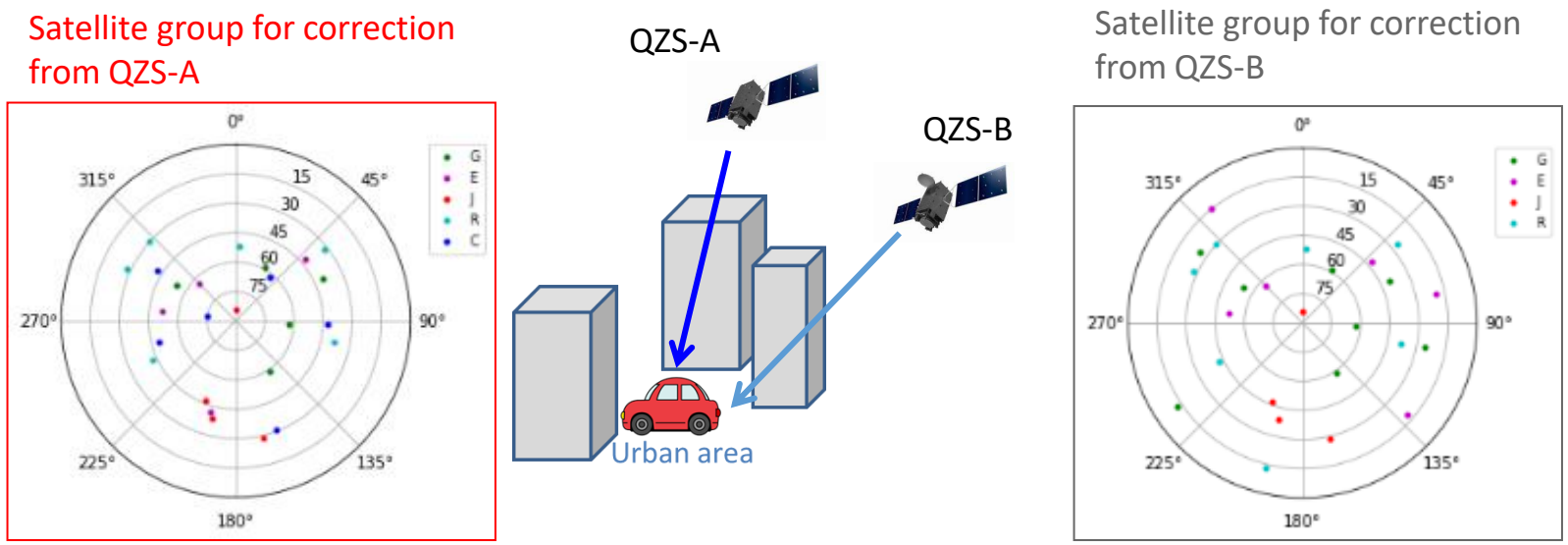
- Correction Message Authentication (CMA) for PPP/PPP-RTK.

- Localized heavy rainfall prediction by estimating IPWV.

- Applying the standardized message in RTCM SC-134 and 3GPP.

CLAS性能向上計画（2023年5月 受信機WG）

1. QZS 5号機L6Dチャネルからの CLAS補強配信
2. 補強衛星数を増やすための更新（下位互換性を確保）
3. CLAS補強メッセージへの認証機能の付与

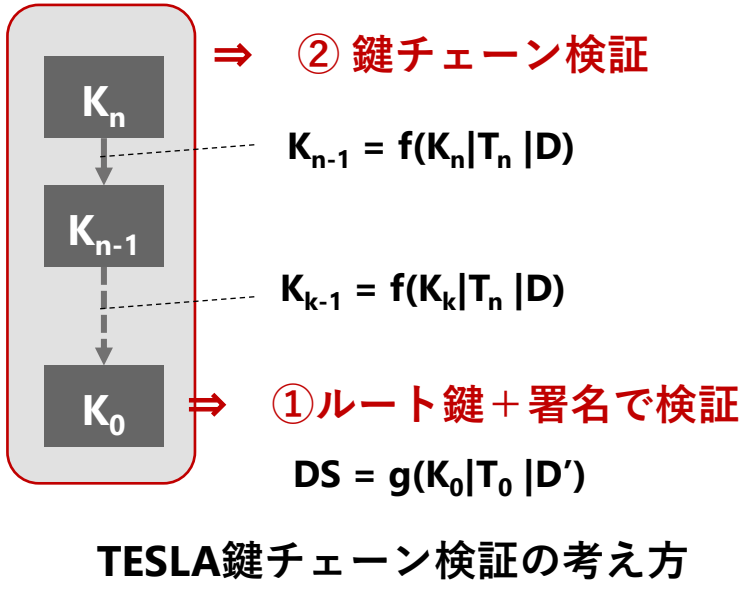


補強衛星数を増やすための方式例：号機別配信

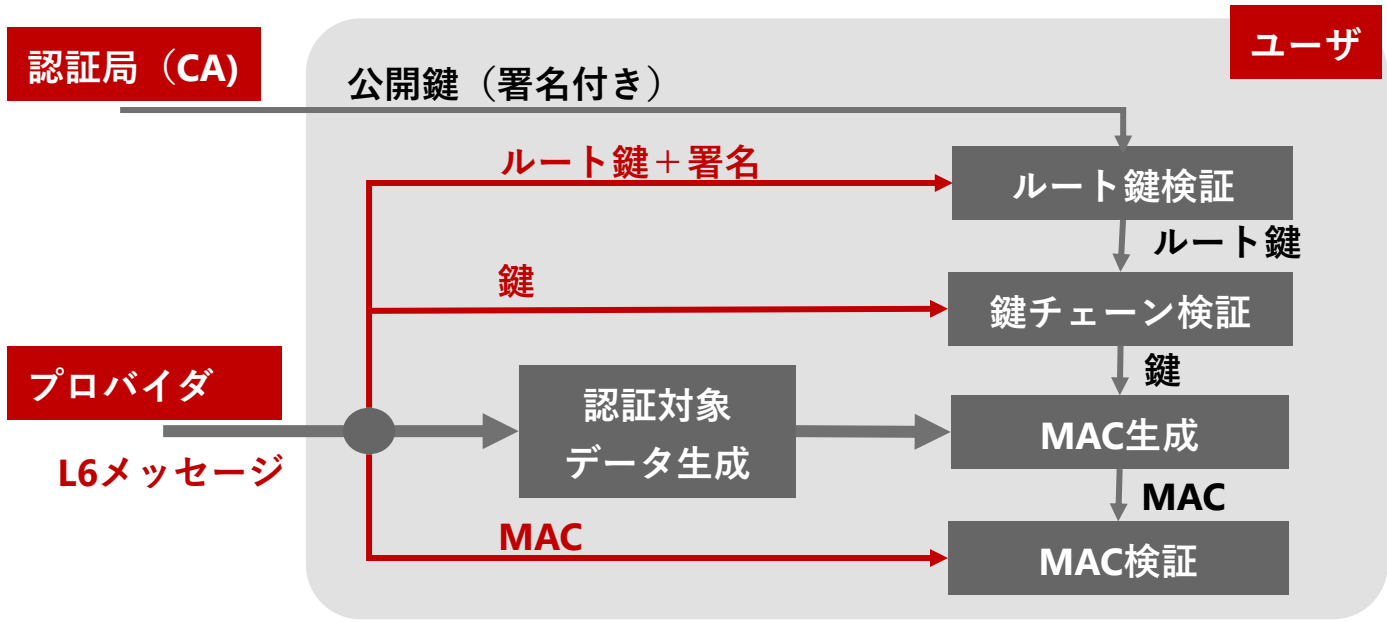
2-6 QZSS CLAS認証機能付与について(2023年5月 受信機WG)

- CLAS補強メッセージに認証機能を付与（～JFY2026）
- 認証メッセージの送信方法： L6DまたはL6E をユーザ利便性等に基づき判断
- 認証方式として、伝送効率・計算効率に優れるTESLA方式の採用を検討

（参考） TESLA方式：遅延鍵公開により秘密鍵を共有する認証方式（Galileo OSNMAで採用）
- ✓ デジタル署名（DS）伝送方式に比べてデータ伝送効率、計算負荷が約２倍優れる
- ✓ 前提条件：プロバイダ・ユーザ間で時刻がある程度（例：約1秒）整合している
- ✓ 検証手順
  - ① ルート鍵検証： 公開鍵を用いてルート鍵署名を検証
  - ② 鍵チェーン検証： 鍵チェーンをハッシュで順次計算、ルート鍵(K_0)の整合性を確認
  - ③ MAC検証：L6メッセージから鍵を用いてMACを生成、送信されたMACと比較・検証



TESLA鍵チェーン検証の考え方

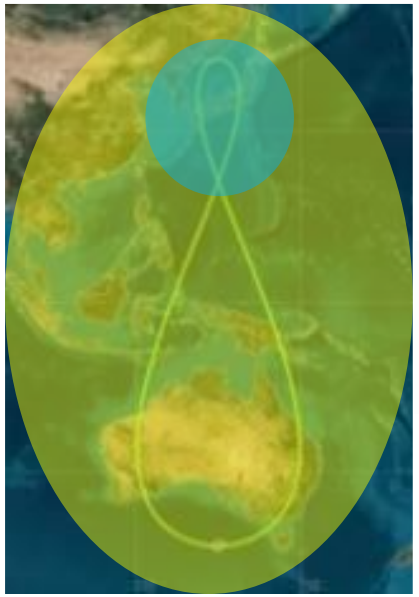


3 PPP-RTK/PPP認証機能に関する研究

高精度補強認証関連の研究成果紹介　（注：CLAS高度化契約における仕様設計は別途検討中）

a. A Message Authentication Proposal for Satellite Based Nation-wide PPP-RTK Correction Service (ION GNSS+ 2019)
b. PPP/PPP-RTK Message Authentication (ION GNSS+ 2021, NAVIGATION)

A Message Authentication Proposal for Satellite Based Nation-wide PPP-RTK Correction Service



ION GNSS+ 2019

September 20, 2019 at Miami, Florida

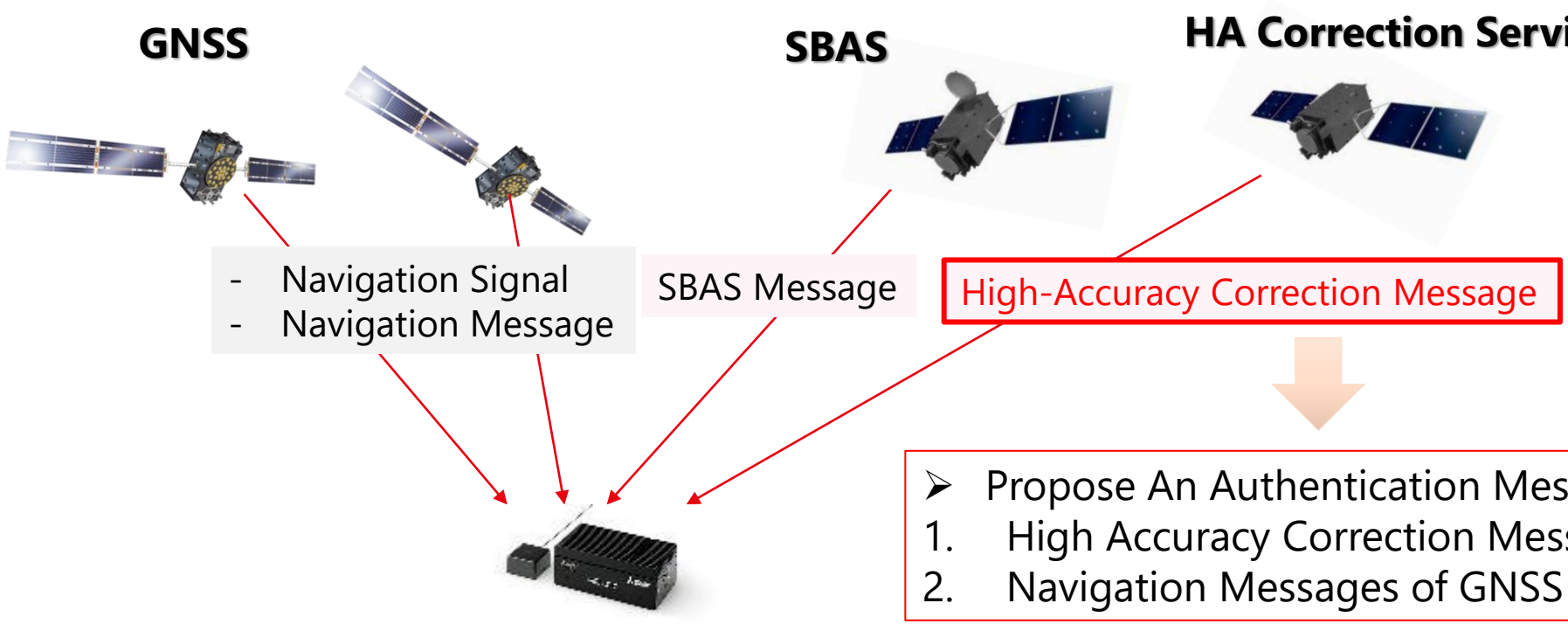
Dr. Rui Hirokawa, Dr. Seigo Fujita

MITSUBISHI ELECTRIC CORPORATION

Authentication of Navigation Message and Correction Service

- ✓ GNSS open signal can easily attacked by low-cost GNSS signal spoofer.
- ✓ GNSS providers such as Galileo, GPS, QZS are working to provide the authentication information for their navigation signals and messages.
- ✓ In this paper, we present a fundamental study to add the authentication information for satellite based high-accuracy (HA) correction service.

LimeSDR-mini
+GPS-SDR-sim



➢ Propose An Authentication Message for,

1. High Accuracy Correction Messages for PPP/PPP-RTK
2. Navigation Messages of GNSS Satellites (option)

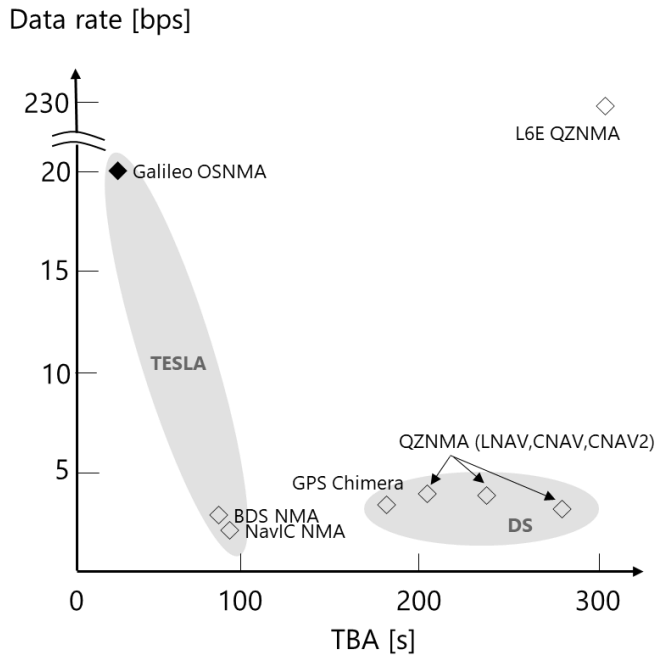
Example of Other GNSS/SBAS

- ✓ For the variable length stream, the message occupation rate depends on the number of available satellites and signals. The priority control of messages will be necessary.
- ✓ HA correction should be high priority, NMA could be low priority.

	Navigation Message	Navigation Signal	SBAS Message	HA Correction Message
Application	Galileo E1B OS-NMA	GPS L1C Chimera	- SBAS, DFMC SBAS	CLAS/Compact SSR
Frame Coding	fixed	fixed	fixed	variable (RTCM stream)
Data Rate	125bps	50bps	250bps	1,695bps
Update Interval	10 minute	2 hour	30-216sec	5sec clock, 30sec other
Data Rate	16.6% (20bps)	6% (3bps)	22% (55bps)	3-5% (50-85bps)
TBA	10sec	6sec,3min	6sec	5sec (correction) 30sec or more(NMA)
Encryption	TESLA	ECDSA P224	TESLA	TESLA

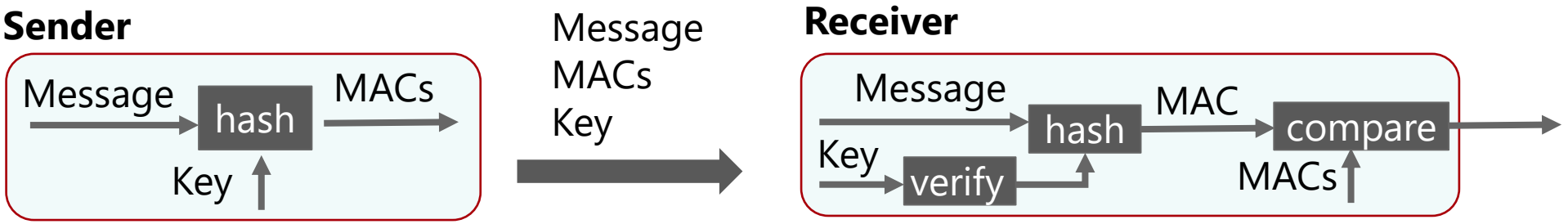
（参考）NMAパラメータ比較

	Galileo E1B OSNMA	BDS B1C NMA	NavIC NMA	GPS L1C Chimera	QZNMA LNAV	QZNMA CNAV	QZNMA CNAV2	QZNMA L6E
Auth-Type	TESLA	TESLA	TESLA	DS	DS	DS	DS	DS
Authentication Delay	30sec	90sec	96sec	180sec	240sec	216sec	288sec	300sec
Time to First Authentication	<150sec	?	144sec	180sec	240sec	216sec	288sec	300sec
Time between Authentication	30sec (432sec)	90 or 36sec	96sec	180sec	240sec	216sec	288sec	300sec
Security Level	128bits *1	128bits	116bits	112bits	128bits	128bits	128bits	128bits
Size of Key	128bits *1	128bits	116bits	-	-	-	-	-
Size of MAC	40bits *2	?	30bits	-	-	-	-	-
Size of DS	512bits	512bits	?	448bits	512bits	512bits	512bits	512bits
Data rate	20bps	2.5 or 6.3bps	2.3bps	3.0bps	3.8bps	4.2bps	2.9bps	230bps
Hash Algorithm	SHA-256 *3	SM3	?	SHA-512	SHA-256	SHA-256	SHA-256	SHA-256
MAC Function	HMAC-SHA256*4	HMAC-SM3	?	-	-	-	-	-
DS Algorithm	ECDSA P-256 *5	SM2	?	ECDSA P-224	ECDSA P-256	ECDSA P-256	ECDSA P-256	ECDSA P-256
Self Auth	Y	Y	Y	Y	Y	Y	Y	-
Cross Auth	Galileo	-	-	-	-	-	-	GPS+Galileo
UTC Auth	Y	-	-	-	-	-	-	-
Signal	E1B	B1C	?	L1C	L1C/B (C/A)	L5	L1C	L6E



Type of Key for Authentication

- ✓ The message is authenticated by the digital signature (symmetric/asymmetric).
- ✓ We should care about the authentication performance (security level, time between authentication) and the resource limitation (band-width, computational).



technique	Key handling	Advantage	Drawback
Symmetric key	the key is shared by transmitter and receivers	• Lower computational resource • Shorter key length	• Difficulty to share the private key
Asymmetric key	a private key known only to transmitter, a public key can be distributed publicly	• Non-disclosure of secret key (*1)	• High computational resource • Longer key length

*1 the authentication of public key is still needed.

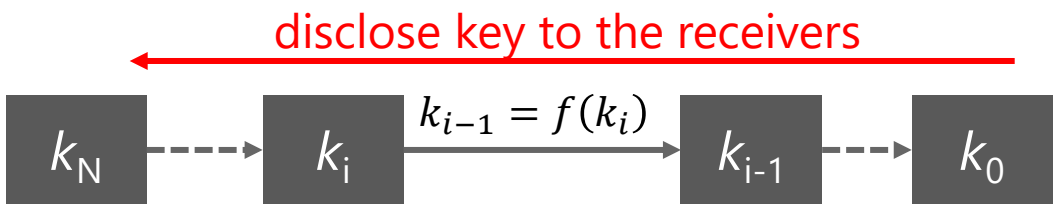
LPC1768 ARM Cortex-M3 96MHz: ECDSA P-256 458msec ⇔ SHA-256 0.6msec
Performance of State-of-the-Art Cryptography on ARM-based Microprocessors (nist.gov)

TESLA: Timed Efficient Stream Loss-tolerant Algorithm

- TESLA provides delayed per-packet data authentication, defined in RFC4082, ISO/IEC 29192-7:2019(E).
  - Efficient and robust protocol
  - Requirement:
    1. Loose time synchronization.
    2. Initial commitment to the key chain: the last key of chain (k_0) with signature

Sender

1. Generate key chain with non-reversible function f
2. Disclose key with reverse order $(k_0, \ldots, k_N)$ with delay



$$k_{i-1} = f(k_i) = trunc(hash(k_i||salt))$$

"salt" can prevent pre-computational attacks

m_i , MAC_i
k_{i-1}

k_0
Sign of k_0

Receiver

1. Receive message m_i and MAC_i
2. Receive key k_i with delay
3. Verify k_i with key-chaining
   - k_0 is verified with signature of sender
   - Signature is verified by certification of sender
4. Calculate MAC for m_i using k_i ,compare with MAC_i :

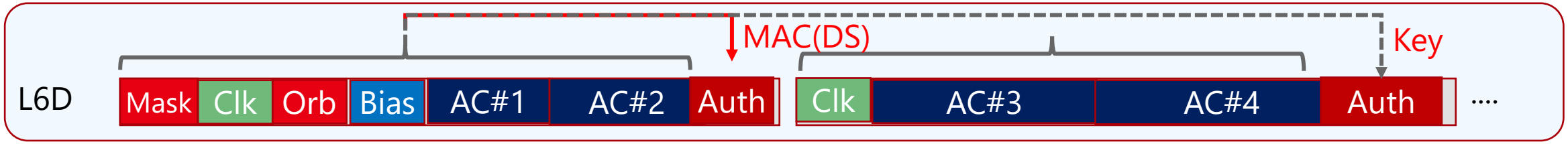
$$MAC = trunc(hash(m_i, k_i||salt))$$

Certification (public-key) of sender

Messaging Design for QZS L6

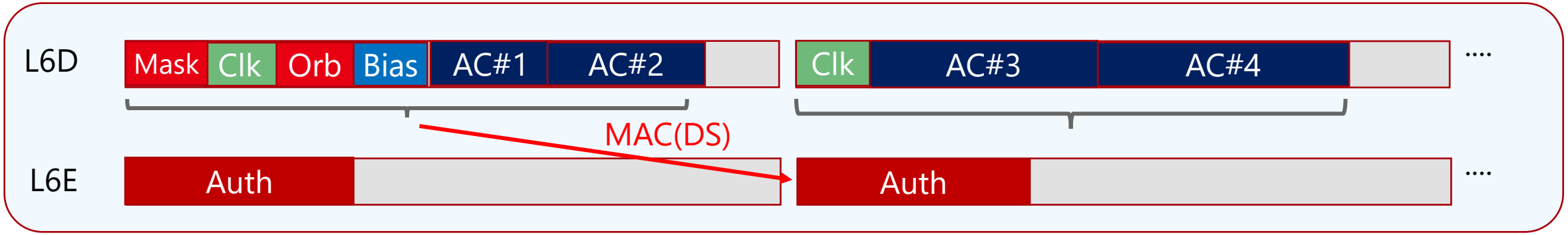
(1) Same channel (L6D)

- Independency of Service
- Slower TTFAF, TBA
- TESLA



(2) Separate channel (L6E)

- Faster TTFAF, TBA
- Need additional channel
- Asymmetric Encryption (like ECDSA) can be applied



Message data rate for Authentication

Message rate for authentication:

$$d_{rate} = \left[(N_0 + N_{SL} + N_{MAC}) + N_s \left(1 + \frac{N_{MAC}}{n}\right) \right] / t_{TBA}$$

Header, SL length, MAC length, #Satellites

For CMA

For NMA

$$n = t_{TBA-NM} / t_{TBA}$$

Example for MAC=30b,SL=112b

Without NMA:

47bps (2.8%) with PKI info

37bps (2.2%) without PKI info

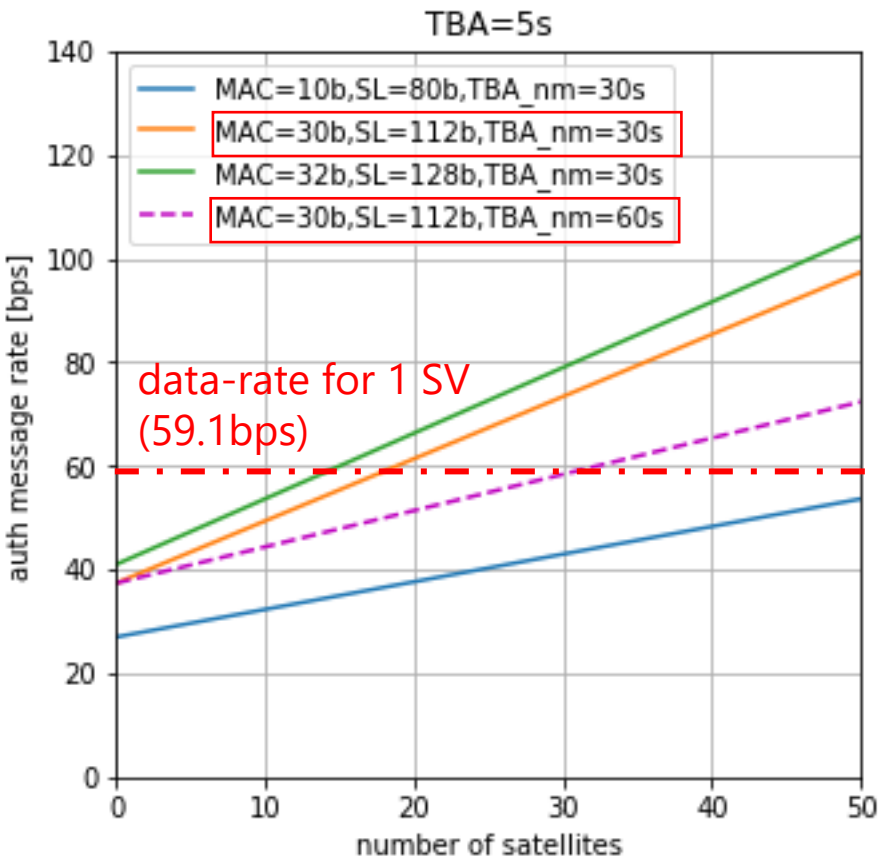
With NMA (20SVs, without PKI info):

$t_{TBA-NM} = 30sec$ ➡ 1.2bps/sat ➡ 61bps (3.6%)

$t_{TBA-NM} = 60sec$ ➡ 0.7bps/sat ➡ 51bps (3.0%)

Message rate for PPP-RTK correction (Compact SSR):

SIS : 7.6bps/sat
Local: 0.24bps/sat/grid ➡ 59.1bps/sat for CLAS (212grids)



one more satellite or authentication message?

Authentication Message Structure

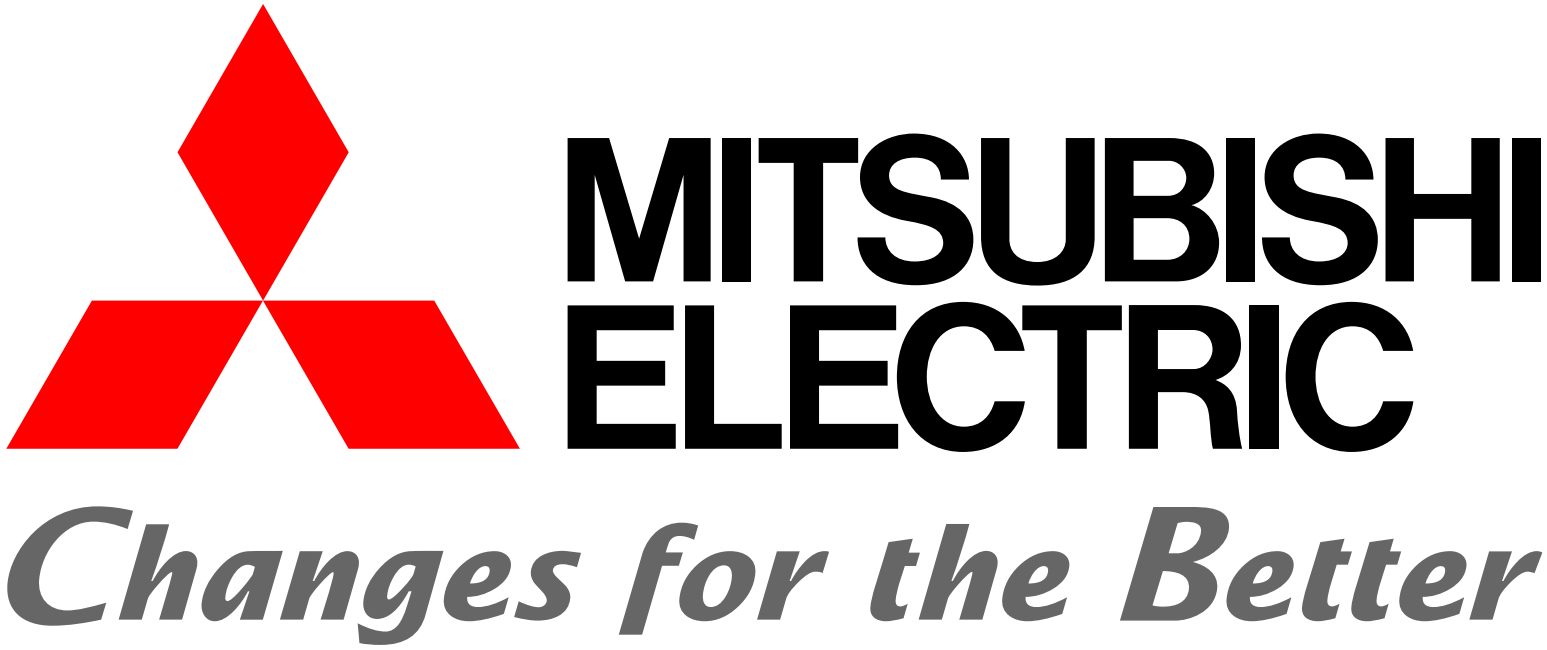
- Assigned for Compact SSR SubType 13 (RTCM 3 compatible)
- Parameters for TESLA is compatible with Galileo OS-NMA

- Parameters include:
  Encryption Type, Key-Size, MAC size,…
- PKI-info to send root-key/OTAR information
- NMA can be included as option, throughput can be minimized using mask.

MT: 4073
SubType: 13
MMI, IOD SSR
Encryption Type
NMA/Chain status
Chain ID
Hash/MAC function
Key/MAC/PKI size
MAC availability
Num of messages
PKI-info
Auth SV mask
MAC-CMA
MAC-NMA
Key

まとめ

- オープンな高精度補強サービスはQZSが世界をリードする分野であり、Galileo HASをはじめグローバルサービスの立ち上がりにより、普及期に向かう。
- 我が国の重要インフラであるQZSSのプレゼンスを維持・発展させるべく、機能・ユーザ利便性の向上に努めていく。
- また、海外サービスとの相互運用性の確保も普及のために重要であり、国際標準化活動等に関して引き続き活動していく。


MITSUBISHI
ELECTRIC
Changes for the Better