STX-2G - Signal Transmitter Experimental Platform - Galileo SIS ICD Evolution
NCS-V3 Navigation Constellation Simulator
Time-to-First Fix | RedCED
Precise Point Positioning | HAS
Navigation Message Authentication | OS-NMA

STX2G - Final Presentation

Programmatic Topics

Program

- ESA NAVISP Element 2

Project

- ESA contract no. 4000131934/20/NL/MP/mk
- ID NAVISP-EL2-061 ‚STX2G'
- Contract start: 01.09.2020, with planned duration of 12 months
- The final duration was 16 months

Milestones

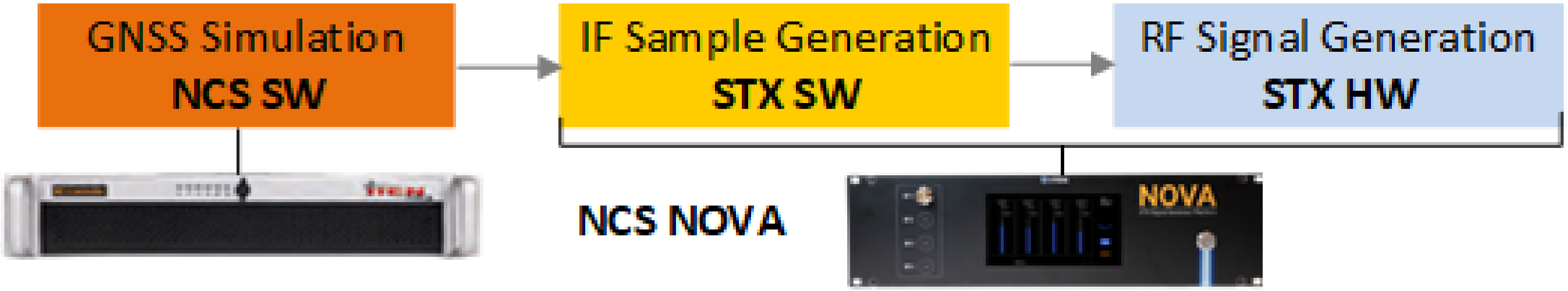
ID	Title	Schedule Date	Achieved Date	Place
KO	Kick-Off Meeting	T0 + 1 m	01.10.2020	Teleconference
PDKP	Preliminary Design Key Point	T0 + 2 m	08.02.2021	Teleconference
MS1	Design Review (DR)	T0 + 4 m	29.03.2021	Teleconference
MS2	Test Readiness Review (TRR)	T0 + 8 m	26.07.2021	Teleconference
MS3	Final Review (FR)	T0 + 12 m	08.12.2021	Teleconference

→ PDKP was inserted on ESA request

Objectives and Context

Context – IFEN ‘NCS NOVA’ GNSS RF Simulator Extension

- 8 topics proposed for upgrade (4 for NCS simulator, 4 for RF signal generator ‘NOVA+’,)
  - Initial request to extend RF Signal Generator HW platform ‘NOVA(STX)’ was skipped
    → ‘STX2G’ project was re-focused on enhancing the ‘NCS simulator’ only



GNSS Simulation
NCS SW

IF Sample Generation
STX SW

RF Signal Generation
STX HW

NCS NOVA

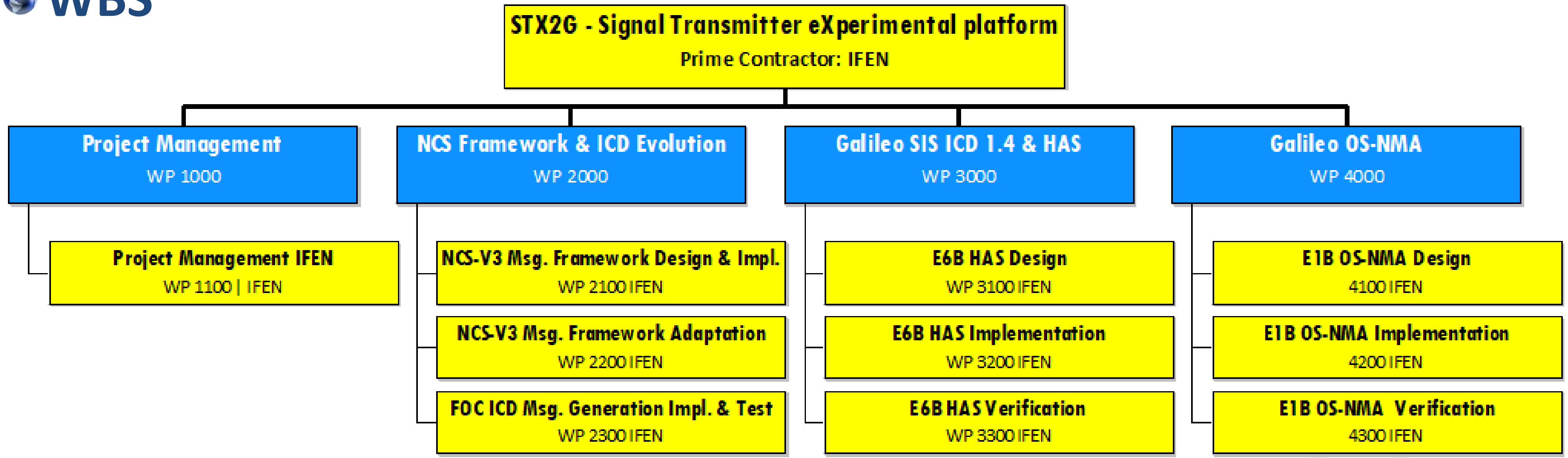
Objectives for NCS Simulator Extension

- NCS simulator v2.6 was supporting Galileo OS ICD v1.3
- But new Galileo ICDs were already available or expected to be released soon

NCS v2.6:	**→ STX2G: NCS V2.8 draft (prototype)**	
→ OS ICD v1.3	→ OS ICD v2.0 (full)	
x	→ OS-NMA Test Spec. v1.1	(no GPS cross authentication,..)
x	→ HAS ICD v1.2 → 1.4	(limited to Service Level 1)
- FlexNav Msg Generator	→ New Msg Generator	

Workplan Activities

- 4 major design and development tasks linked to objectives
  - New message generation framework
    - Replacing previous FlexNav framework: Was highly flexible, but resulting in high complexity
  - Support of new OS ICD 2.0 (→ SSP, → RedCED, → RS-FEC) features
  - Support of new Open Service Navigation Message Authentication (OSNMA) on Galileo E1B signal
  - Support of new High Accuracy Service (HAS) on GalileoE6B signal
- WBS



STX2G - Signal Transmitter eXperimental platform
Prime Contractor: IFEN

Project Management
WP 1000

- Project Management IFEN
  WP 1100 | IFEN

NCS Framework & ICD Evolution
WP 2000

- NCS-V3 Msg. Framework Design & Impl.
  WP 2100 IFEN
- NCS-V3 Msg. Framework Adaptation
  WP 2200 IFEN
- FOC ICD Msg. Generation Impl. & Test
  WP 2300 IFEN

Galileo SIS ICD 1.4 & HAS
WP 3000

- E6B HAS Design
  WP 3100 IFEN
- E6B HAS Implementation
  WP 3200 IFEN
- E6B HAS Verification
  WP 3300 IFEN

Galileo OS-NMA
WP 4000

- E1B OS-NMA Design
  4100 IFEN
- E1B OS-NMA Implementation
  4200 IFEN
- E1B OS-NMA Verification
  4300 IFEN

Test Tools and Outputs

Test Tools, a major challenge for the project

- For OS ICD testing:
  - Tested against **FOC TUR-N** receiver
- For OS-NMA testing:
  - Initially tested against the FHG-IIS **GOOSE** receiver (provided 'on loan')
  - Finally tested against **FOC TUR-N** receiver
- For HAS testing:
  - IFEN **'PHOENIX' PPP** prototype using HAS (EUSPA 'Fundamental Elements' project)

Outputs

- NCS-V2.8 Prototype SW (NCS simulation SW as part of GNSS RF simulator)
  - Full ‚NCS NOVA' provided to ESTEC on loan for testing (with NCS prototype SW)
- 8 Technical Notes
  - TN0 - Requirements Document (1.0, 1.1)
  - TN1-TN4 - Design Documents (Gen3Nav Design, SIS ICD Design, HAS Design, OSNMA Design)
  - TN5 - Test Plan and Procedures (1.0, 1.1, 1.2, 1.3)
  - TN6 - Test Report (1.0, 1.1, 1.2, 1.3)
  - TN7 – User Manual

OS-ICD Design and Development and Test

SSP (Secondary Synchronisation Pattern)

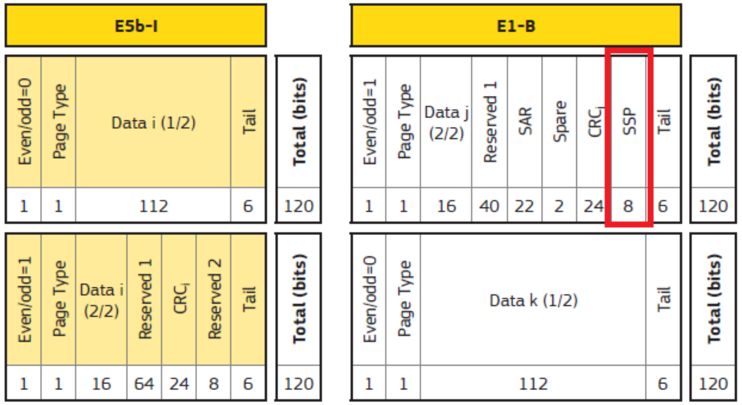
- New in OS-ICD 2.0 for E1B I/NAV, occupying previously reserved bits

RedCED (Reduced Clock and Ephemeris Data)

- New in OS-ICD 2.0 for E1B I/NAV, new word type 16

RS-FEC (forward Error Encoding using Reed-Solomon coding)

- New in OS-ICD 2.0 for E1B I/NAV, new word types 17 - 20



E5b-I				
Even/odd=0	Page Type	Data i (1/2)	Tail	Total (bits)
1	1	112	6	120

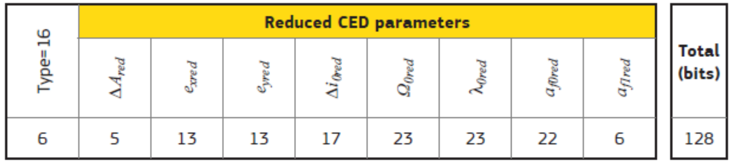
E1-B									
Even/odd=1	Page Type	Data j (2/2)	Reserved 1	SAR	Spare	CRC_j	SSP	Tail	Total (bits)
1	1	16	40	22	2	24	8	6	120

Even/odd=1	Page Type	Data i (2/2)	Reserved 1	CRC_i	Reserved 2	Tail	Total (bits)
1	1	16	64	24	8	6	120

Even/odd=0	Page Type	Data k (1/2)	Tail	Total (bits)
1	1	112	6	120

Table 36. I/NAV Nominal Page with Bits Allocation

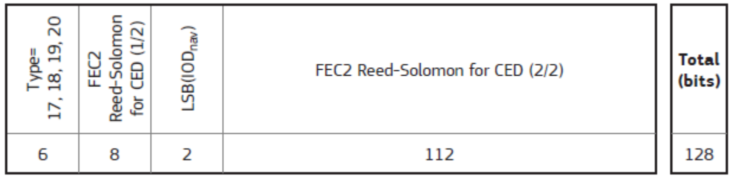
Word Type 16: Reduced Clock and Ephemeris Data (CED) parameters



Type=16	Reduced CED parameters								Total (bits)
	ΔA_{red}	e_{xred}	e_{yred}	Δi_{0red}	Ω_{0red}	λ_{0red}	a_{f0red}	a_{f1red}	
6	5	13	13	17	23	23	22	6	128

Table 50. Bits Allocation for I/NAV Word Type 16

Word types 17, 18, 19, 20: FEC2 Reed-Solomon for Clock and Ephemeris Data (CED)



Type= 17, 18, 19, 20	FEC2 Reed-Solomon for CED (1/2)	$LSB(IOD_{nav})$	FEC2 Reed-Solomon for CED (2/2)	Total (bits)
6	8	2	112	128

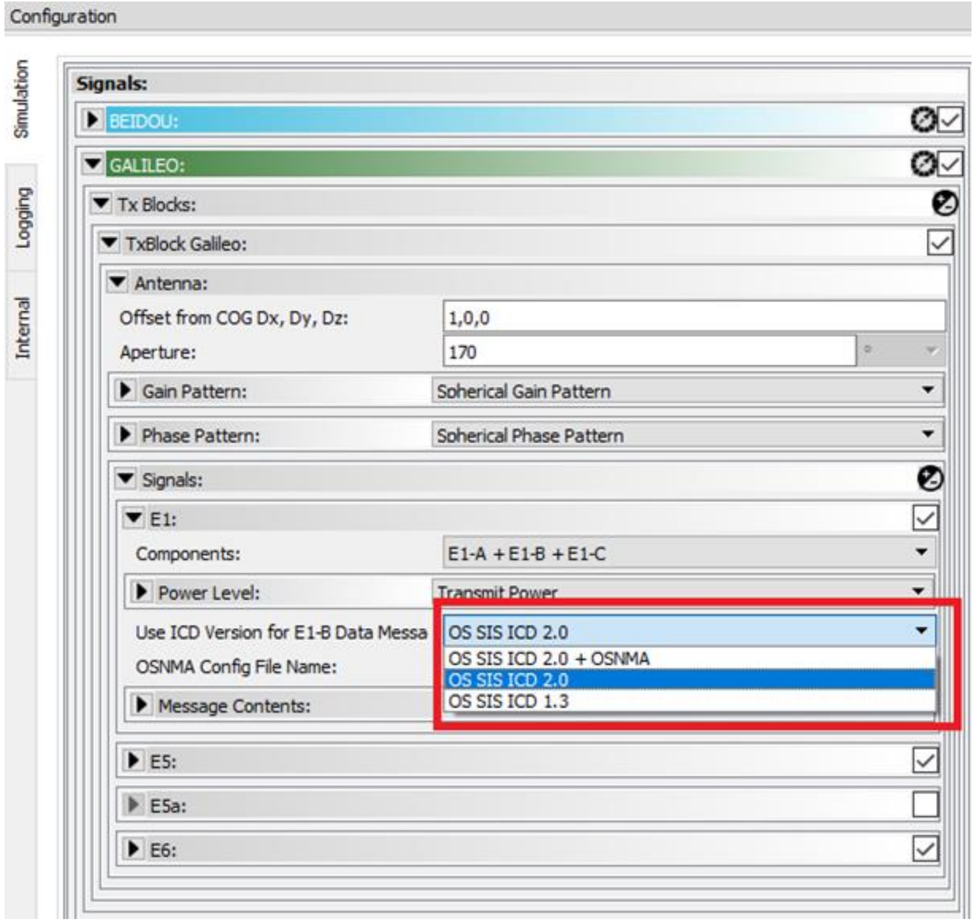
Table 51. Bits Allocation for I/NAV Word Types 17, 18, 19, and 20

- New Message Generation Framework developed for the simulator
- ICD version to be used selectable by the user
- In case ICD 2.0 is selected, the new features are incorporated in the I/NAV message on E1B

OS-ICD Configuration and Test

Configuration

- ICD version (ICD 1.3 or 2.0) to be used configurable in the simulator GUI
- Selectable both for E1, but also for E5a and E5b; no effect on E5 signals



Signals:

- BEIDOU: ☑
- GALILEO: ☑
  - Tx Blocks:
    - TxBlock Galileo: ☑
      - Antenna:
        - Offset from COG Dx, Dy, Dz: 1,0,0
        - Aperture: 170
        - Gain Pattern: Soherical Gain Pattern
        - Phase Pattern: Soherical Phase Pattern
      - Signals:
        - E1: ☑
          - Components: E1-A + E1-B + E1-C
          - Power Level: Transmit Power
          - Use ICD Version for E1-B Data Messa: OS SIS ICD 2.0
            - OS SIS ICD 2.0 + OSNMA
            - OS SIS ICD 2.0
            - OS SIS ICD 1.3
          - OSNMA Config File Name:
          - Message Contents:
        - E5: ☑
        - E5a: □
        - E6: ☑

Test Results

- Tests run to compare generated navigation message from both ICD versions
- Incorporation of SSP was verified
- Incorporation of word types 16 – 20 was verified
- TTFF with ICD 2.0 was shorter, as expected
- PVT with RedCED was less accurate, as expected
- All tests successful

OS-NMA Specification I

Navigation Message Authentication (NMA)

- Navigation Data are authenticated by a Message Authentication Code (MAC) with a Key.
- The Key is authenticated by a TESLA Chain and a final KROOT.
- The KROOT is authenticated by an ECDSA Signature.

Events

- Public (ECDSA) Key Renewal
- Public (ECDSA) Key Revocation
- Key Chain Renewal
- Key Chain Revocation

Further Cryptographic Operations

- New public ECDSA Keys (Key Renewal /Revocation) are authenticated by the root of a Merkle Tree.

OS-NMA Specification II

OS-NMA consists of

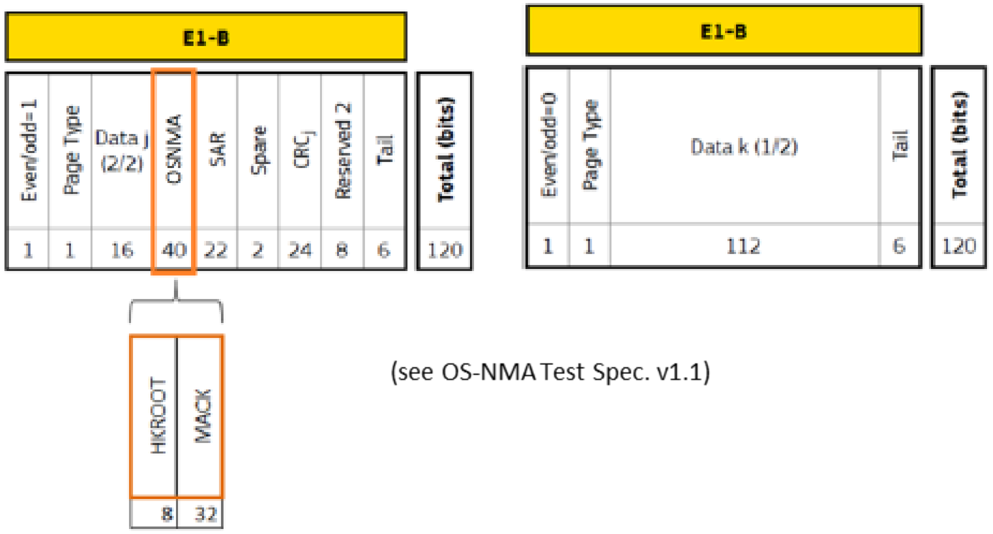
- HKROOT Section
- MACK Section

HKROOT Section contains

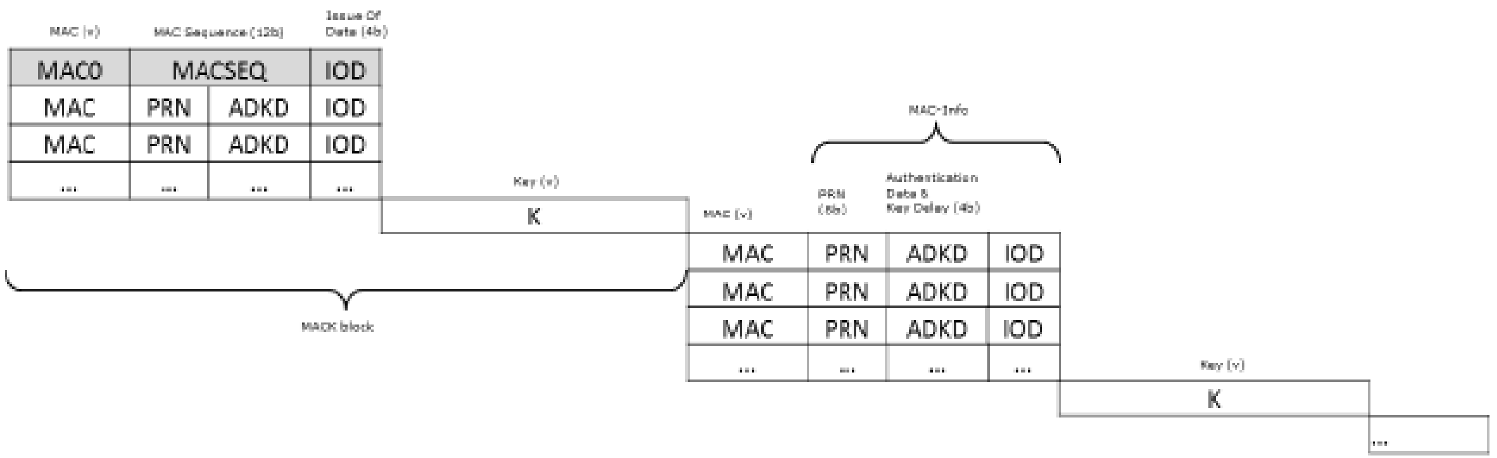
- DSM KROOT (Digital ECDSA Signature)
- DSM PKR (new Public ECDSA Key during Event)

MACK Section contains MACK Blocks comprising

- MACs
- MAC Infos
- TESLA Key



(see OS-NMA Test Spec. v1.1)



(see OS-NMA Test Spec. v1.1)

OS-NMA Configuration

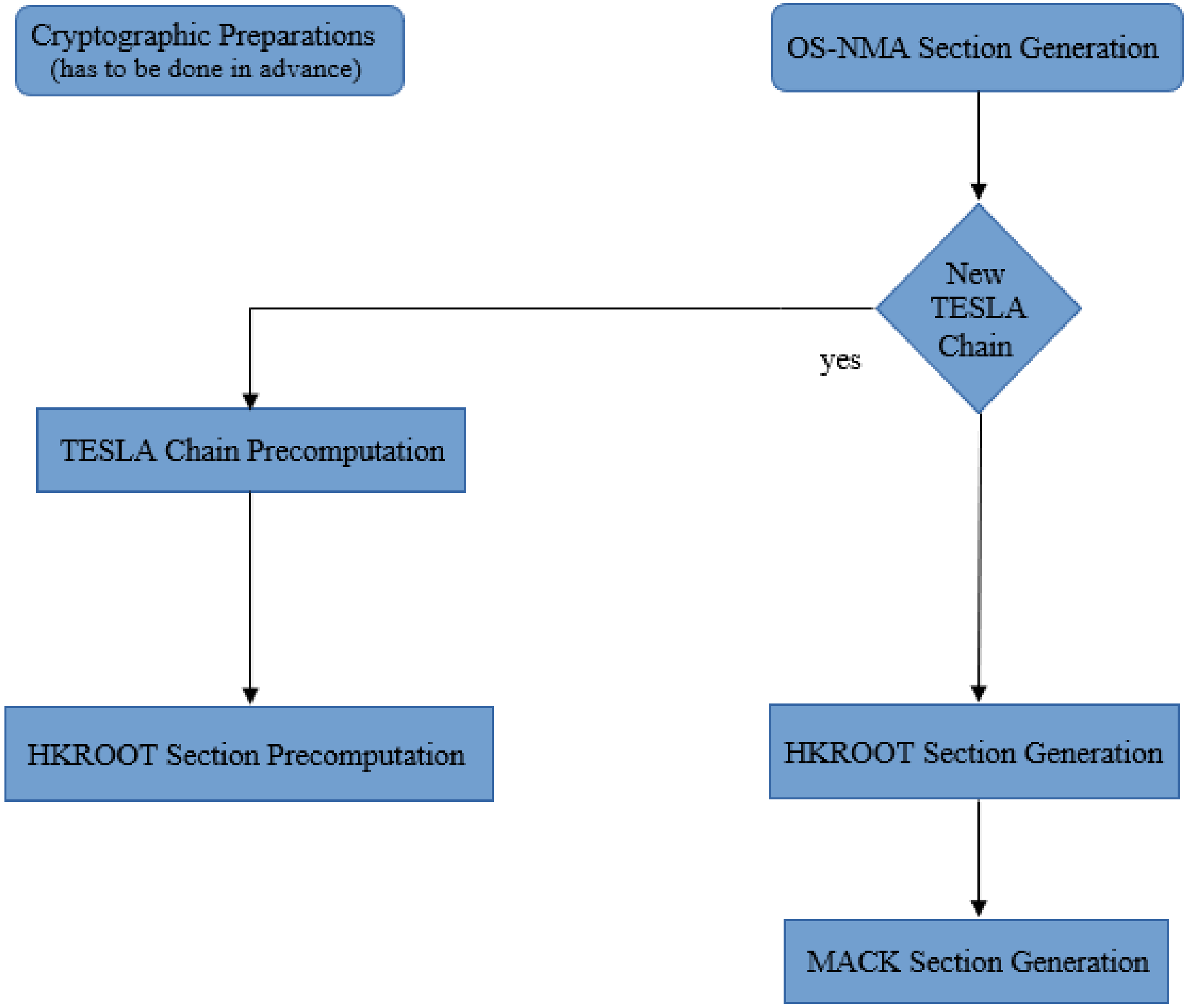
Flexible Parameters

- ADKD sequence (sequence of the respectively authenticated navigation data)
- Authenticating and cross-authenticated satellites
- Events during the simulation
- I/NAV subframes per TESLA chain
- ECDSA type (P-224, P-256, P-384, P-521)
- Private ECDSA keys
- NS (maximal number of different TESLA keys per MACK block)
- Hash function for TESLA chain (SHA-256, SHA3-224, SHA3-256)
- TESLA key size (96, 104, 112, 120, 128, 160, 192, 224, 256)
- MAC hash function (HMAC-SHA-256, CMAC-AES)
- MAC field size (10, 12, 14, 16, 18, 20, 24, 28, 32, 40)
- MACK offset (true, false)

OS-NMA High Level Design

Three Major Components:

- Cryptographic Preparations (Private and Public ECDSA Keys / Merkle Tree)
- Precomputation of the TESLA Chain and the HKROOT Section
- Generation of OS-NMA Sections


Cryptographic Preparations
(has to be done in advance)
OS-NMA Section Generation
New TESLA Chain
yes
TESLA Chain Precomputation
HKROOT Section Precomputation
HKROOT Section Generation
MACK Section Generation

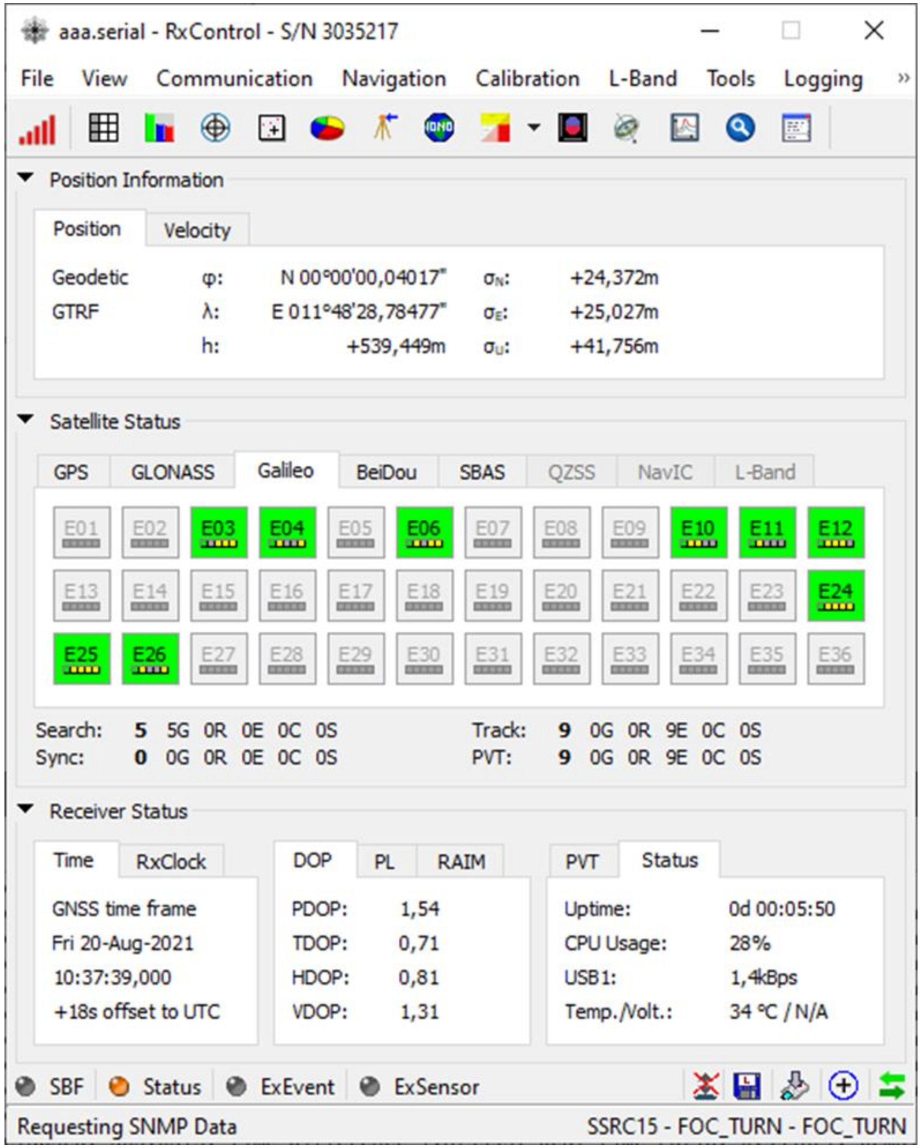
OS-NMA Configuration and Test

Configuration

- First tested with the FHG-IIS GOOSE receiver
  - ADKD Types 0, 4, 12 / Key Renewal Event / further configuration settings…
- Second tested with the FOC TUR-N
  - Remaining Event Types: Chain Renewal, Chain Revocation, Key Revocation
- Also used an own post processing tool (ORC)

Test Results

- The tests have been successfully passed



Geodetic	φ:	N 00°00'00,04017"	σN:	+24,372m
GTRF	λ:	E 011°48'28,78477"	σE:	+25,027m
	h:	+539,449m	σU:	+41,756m

E01	E02	🟩 E03	🟩 E04	E05	🟩 E06	E07	E08	E09	🟩 E10	🟩 E11	🟩 E12
E13	E14	E15	E16	E17	E18	E19	E20	E21	E22	E23	🟩 E24
🟩 E25	🟩 E26	E27	E28	E29	E30	E31	E32	E33	E34	E35	E36

```
Search:  5  5G 0R 0E 0C 0S        Track:  9  0G 0R 9E 0C 0S
Sync:    0  0G 0R 0E 0C 0S        PVT:    9  0G 0R 9E 0C 0S
```

GNSS time frame
Fri 20-Aug-2021
10:37:39,000
+18s offset to UTC

PDOP:	1,54
TDOP:	0,71
HDOP:	0,81
VDOP:	1,31

Uptime:	0d 00:05:50
CPU Usage:	28%
USB1:	1,4kBps
Temp./Volt.:	34 °C / N/A

Requesting SNMP Data

SSRC15 - FOC_TURN - FOC_TURN

HAS Design and Development

High Accuracy Service for Global PPP Solutions

- Orbit, clock, code and phase bias corrections
- Correction data broadcast as part of the C/NAV pages of E6B Navigation Message

Calculation of Correction Values

- „Truth“ and „Error“ values are known in the simulation
- Corrections are basically calculated as differences thereof
- Pure differences would yield perfect corrections (resulting accuracy = 0)
- Some noise added to the differences to obtain certain Target Accuracy Level (e.g. 20 – 50 cm)

Generation of Broadcast Message

- Integrated in new Message Generation framework

HAS Context and Configuration

Context of HAS service

- HAS for global PPP solutions:
  - 20 cm horizontal, 40 cm vertical accuracy
  - Galileo and GPS supported augmentation
  - Phased HAS Deployment covering Phase 1 Initial Service

Configuration

- Activation of HAS Message Generation by the user in the simulator GUI
- Values for the algorithmic parameters specified in a configuration file
  - Validity interval
  - Service phase
  - Number of broadcasting satellites
  - GNSS to be corrected
  - Signals to be corrected
  - Target accuracy level
  - Weights for orbit, clock, code and phase bias corrections

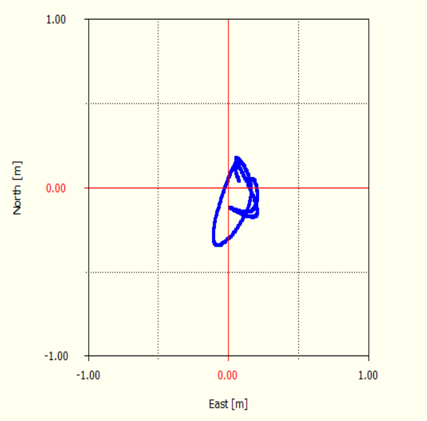
HAS Tests

4 Test Configurations

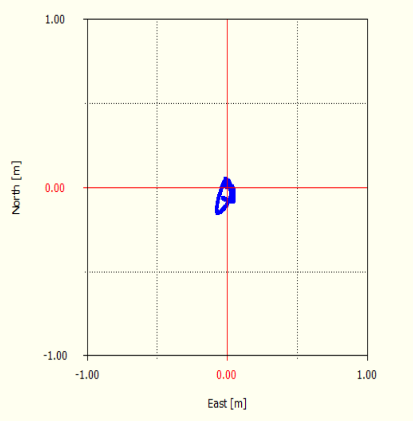
- HAS Correction Parameters Functionality
- HAS Configuration Parameters Functionality
- HAS Messages Time Frame Functionality
- HAS Messages Accuracy Functionality

Test Results

- General Functionality ⇨ passed
- Configuration Parameters Functionality ⇨ passed
- Message Time Frame Functionality ⇨ passed
- Messages Accuracy ⇨ passed



50 cm vs. 20 cm target accuracy



Conclusions and Acknowledgement

Conclusions

- STX2G was a highly successful project, nearly within the planned timeframe
- Also the challenging ‘test’ tasks were finally completed successfully
- NAVISP Element 2 is a very important GNSS program line, enabling to
  - Stay competitive on the global market
  - Generate unique capabilities, enabling further market penetration

Acknowledgement

- IFEN appreciates the excellent interaction with our ESA TOs
- IFEN appreciates the extensive technical support from ESTEC team during testing
- IFEN appreciates the support from FHG-IIS in providing their GOOSE receiver and the supporting interactions for basic testing of OSNMA
- IFEN especially acknowledges the support from DLR and ESA, enabling us to perform the ‘STX2G’ project, being an important step in our GNSS RF simulator strategic development roadmap

Portfolio and Roadmap

Portfolio

Standard
- Single-RF Quad-Band or Dual-RF Dual-Band
- Up to 100 channels
- All GNSS ICDs

NCS NOVA

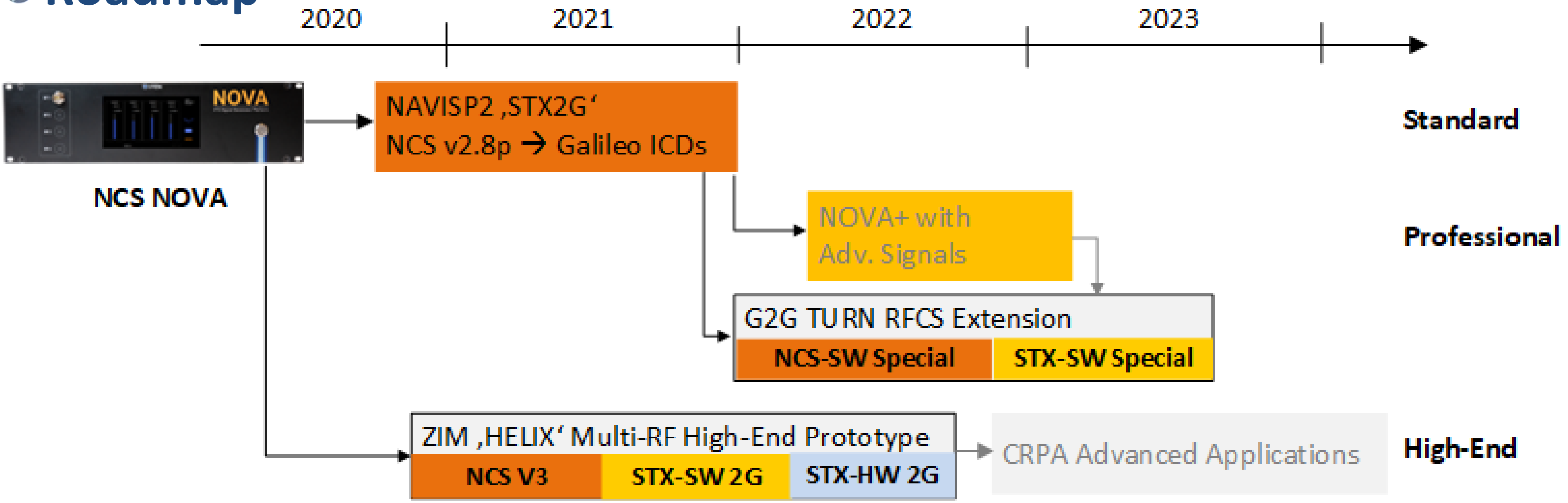
Professional
- Dual-RF Quad-Band or Quad-RF Dual-Band
- Up to 200 channel
- Advanced SW-Signal Gen.

NCS NOVA+

High-End
- Multi-RF Quad-Band or Multi-RF Dual-Band
- > 200 channel
- New RF-HW Generation

NCS HELIX

Roadmap



2020 | 2021 | 2022 | 2023

NCS NOVA

NAVISP2 ‚STX2G‘
NCS v2.8p → Galileo ICDs

NOVA+ with Adv. Signals

G2G TURN RFCS Extension
NCS-SW Special | STX-SW Special

ZIM ‚HELIX‘ Multi-RF High-End Prototype
NCS V3 | STX-SW 2G | STX-HW 2G

CRPA Advanced Applications

Standard

Professional

High-End