LOCFIT FINAL PRESENTATION

NAVISP-058 DEMONSTRATION OF GNSS POSITION BOUNDING

AGENDA

Time	Section
T0	Introduction
T0 + 5mn	Service-Level requirements
T0 + 10mn	System architecture tradeoffs
T0 + 15mn	Secure position-bounding concepts
T0 + 25mn	Security analysis
T0 + 30mn	Demonstration results
T0 + 40mn	Conclusion

INTRODUCTION

OUTLINE OF THE PROJECT

/// Design secure positioning system / algorithms for IoT use cases

- Main use case = Container Tracking
- Constraints of low-cost low-consumption user devices

/// Consortium

- TO = ESA – Gianluca CAPARRA – gianluca.caparra@esa.int
- Prime contractor = **Thales Alenia Space France**
  - Project Manager = Marc ESPINASSE– marc.espinasse@thalesaleniaspace.com
  - Product Design Architect = Etienne ROUANET-LABE – etienne.rouanet-labe@thalesaleniaspace.com
- Security analysis / Testbed responsible = **Qascom**
  - Security analysis responsible = Luca CANZIAN – luca.canzian@qascom.it
  - Testbed responsible = Federica ROZZI federica.rozzi@qascom.it
- Use Case analysis and Service-Level definition = **Traxens**
  - Use Case analysis responsible = Nazim BEN ABDESSELAM nazim.benabdesselam@traxens.com
- State-Of-The-Art of IoT responsible = Kinéis
  - SOTA responsible = Anthony COMBE acombe@kineis.com

ACTIVITIES PERFORMED

/// Use case analysis

- Derive KPIs for secure position bounding system
- Assign KPI values to identified use cases

/// System design

- Identify relevant system architectures
- Design secure position verification algorithms
- Preliminary performance assessment of the concepts

/// Demonstration phase

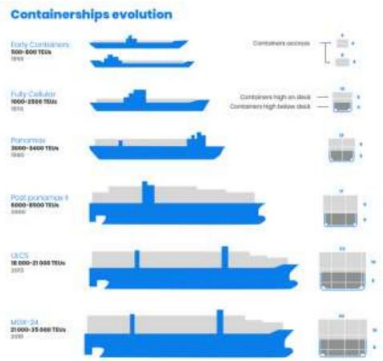
- Design Sw testbed
- Consolidated performance assessment of the concepts

USE CASE STUDY

VISIBILITY = CHALLENGE OF SATELLITE DIRECT ACCESS

/// Segmentation of container-tracking use case

- Phases of container flow
  - Maritime vessel
  - Rail transportation
  - Road transportation
  - Static phases (stacking in depots)
- Mission
  - Container visibility → Low accuracy, low positiong rate, no security reqs.
  - Container security → Higher accuracy, high positioning rate, security reqs.



/// Constraints on Satellite visibility

- Degraded visibility between stacks
- Azimuth mask (180°)

➔Introduction of Azimuth mask in Service-Level requirements

➔Introduction of local protocol in System design

KPI.S FOR SERVICE-LEVEL REQUIREMENTS

/// Demand requirements → ***Needs for telecom resources***

- Coverage area
- User density
- Geolocation period

/// Latency requirements → ***Time to transmit alarms to end-User***

- Asset-to-User maximum latency

/// Navigation Performance requirements → ***Definition of verifiable Distance + False / Missed Alarm Rates***

- Position Bound max. diameter (verifiable distance true-reported positions)
- PFA / PMD

/// Environment requirements → ***Applicable conditions of Reqs. above***

- Azimuth / Elevation masking angle
- Attack conditions
- Max. daily energy consumption

SUMMARY OF SERVICE-LEVEL REQUIREMENTS

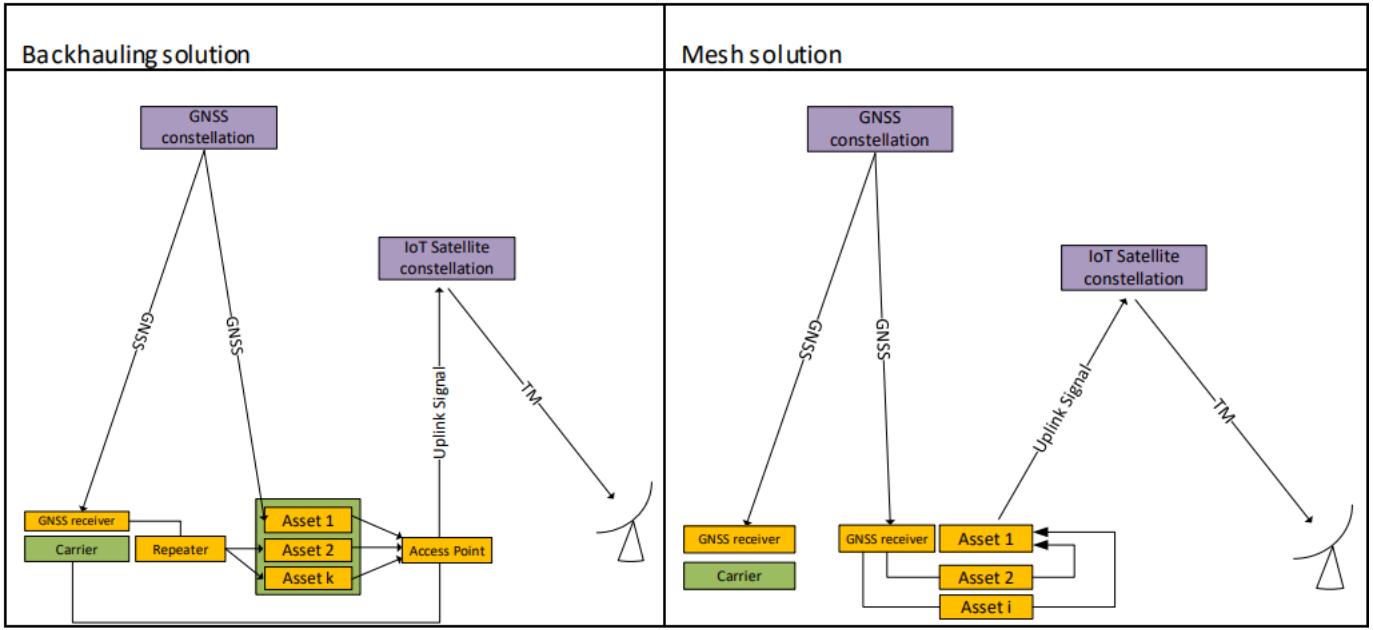
Global demand	8M		1.5M	500k
Peak asset density	4500 / km²		500 / km²	500 / km²
Primary positioning accuracy	200m	200m	200m	200m
Geolocation period	1h (moving) 48h (still)	2 to 6h (moving) 48h (still) + on alert	15mn (moving) 24h (still)	15mn (moving) 24h (still)
Acceptable positioning delay	30mn	2mn	30mn	2mn
Bound diameter	1km	300m	500m	300m
Probability of Missed Detection	1e-1 per attempt	1e-2 per attempt	1e-1 per attempt	1e-2 per attempt
Probability of False Alarm	1e-3 per hour	1e-3 per hour	1e-3 per hour	1e-3 per hour
Elevation mask	10°	10°	10°	10°
Azimuth mask	180°	180°	180°	360°
Vulnerability to attacks	Low	Very high	Average to high	High
Required daily power consumption	0.02Wh (1y Kinéis device life duration)	0.02Wh	0.02Wh	0.02Wh

SYSTEM TRADEOFFS

LOCAL PROTOCOL BEFORE SATELLITE ACCESS

/// Degraded local RF conditions (visibility / multipath) in Static phases / Maritime shipping

/// Two possible architectures : **Mesh** / **Backhauling**



DESIGN OF ALARMS IN LOCFIT SYSTEM

/// **A1** - Protection against tampering (asset tracker destruction) → Alarm on absence of transmission

- TTA depends on rate of asset Uplink transmission → Challenging for IoT
- + Requires high reliability / Robustness to masking to limit False Alarms

/// **A2** – Protection against signals degradation / masking attacks → Alarm on Navigation estimated Performance

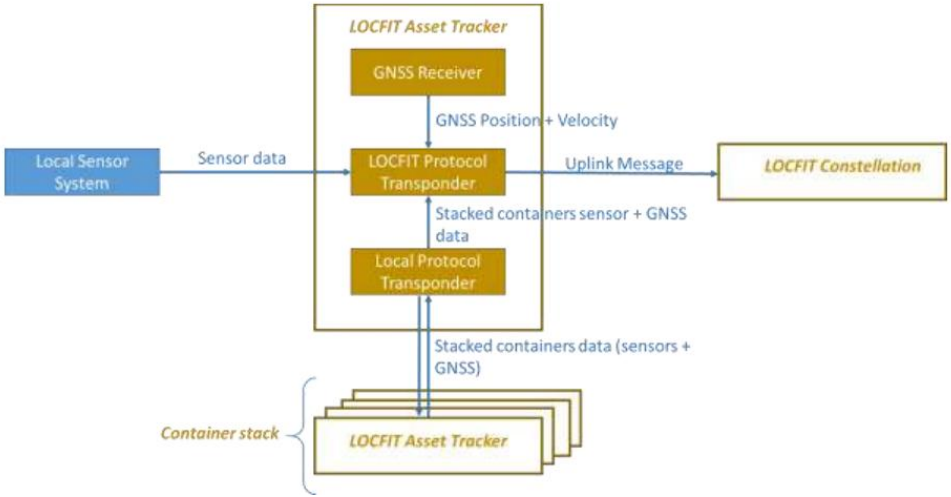
- System should ensure bound size with a certain probability

/// **A3** – Protection against spoofing attacks → Alarm on Ranging measurements consistency

CONTAINER TRACKER MISSIONS

/// Missions conducted by the asset tracker

- Local communication → Transponder for local protocol
- Container Integrity monitoring → Local sensors (door-opening / temperature)
- Satellite communication → Transponder for LocFIT constellation
- GNSS position reception → COTS GNSS receiver



CONTAINER INTEGRITY MESSAGE

/// Uplink message Design / Size

- Unitary message (single asset tracker)

Part of the message	Size	Justification
TOW	20	Maximum 604 800 seconds in a week.
GNSS encoded position	96	3 * FLOAT 32 values
Sensor data	32	18 *2 for margin
Total Payload data	148	
Total Payload data using ½ FEC encoding	296	

- Number of Uplinks for Unitary / Mesh / Backhauling

Footprint diameter	1.12km (1km² area) (container ship)	3.6km (10km² area) (container port)	800km	3000km
Number of containers	4.5k	45k	1M	3M
Total Uplink datarate (useful bits)	1480 bps	14.8 kbps	0.33 Mbps	1 Mbps
Number of Uplink transmitters	Unitary – 4.5k Mesh – 250 Backhauling – 0.225	Unitary – 45k Mesh – 2500 Backhauling – 2.25	Unitary – 1M Mesh – 56k Backhauling – 50	Unitary – 3M Mesh – 170k Backhauling – 150
Total Uplink datarate per Uplink transmitter (useful bits)	Unitary – 296 b per 15mn (1 message) Mesh – 5.3 kb per 15mn (between 1 and 18 messages) Backhauling – 6 Mb per 15mn (TBD)			

POSITION-BOUNDING ALGORITHMS

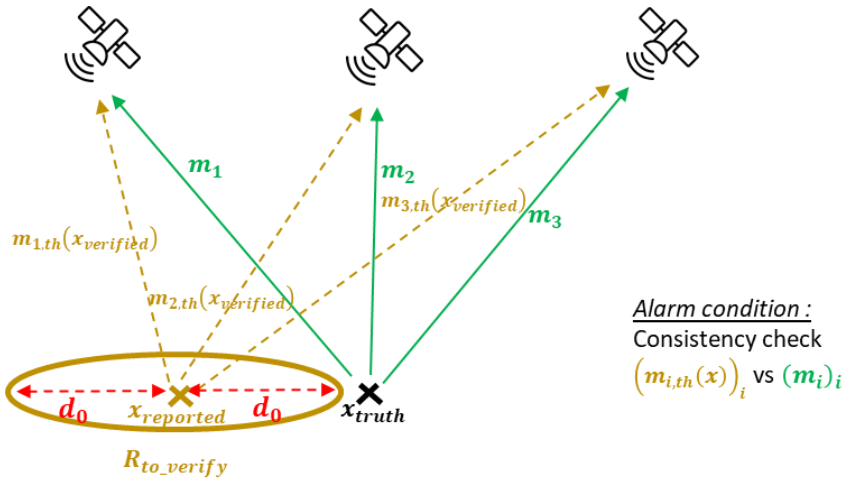
RETAINED CONCEPT – MEASUREMENTS CONSISTENCY CHECK

/// Principle :

- Compute residuals of measurements wrt. asset-reported GNSS position
- Compute thresholds based on ***[Nominal measurements / GNSS pos. dispersion]*** & ***[PFA value]***

/// Concept adapted to Multi-Epoch position verification

- No need of a user dynamics model
- Hypotheses = unspoofed GNSS



Alarm condition :
Consistency check
$\left(m_{i,th}(x)\right)_i$ vs $(m_i)_i$

TRADEOFF ON UPLINK MEASUREMENTS

/// 2 options

- UTDOA measurements
  - Estimation of Uplink transmission time
  - Comparison of estimated Rx time vs. tracker-embedded secure clock
- RTT measurements
  - Based on Distance-Bounding protocol

/// Tradeoff closed

- UTDOA shows Performance degrading quickly in time

- 1km Bound Diameter → 300ns std.
  - Low quality quartz : $\tau_{max} \cong 2.2.10^3 s$
  - High quality quartz : $\tau_{max} \cong 13h$
- 5km Bound Diameter → 1µs std.
  - Low quality quartz : $\tau_{max} \cong 4.6.10^3 s$
  - High quality quartz : $\tau_{max} \cong 28h$
- 10km Bound Diameter → 3µs std.
  - Low quality quartz : $\tau_{max} \cong 1.10^4 s$
  - High quality quartz : $\tau_{max} \cong 2.5j$

SECURITY ANALYSIS

TARGET ATTACKS

/// GNSS attack

- Only the asset reported position is spoofed
- The system is secured against this attack because the reported position is not compatible with the uplink measurements

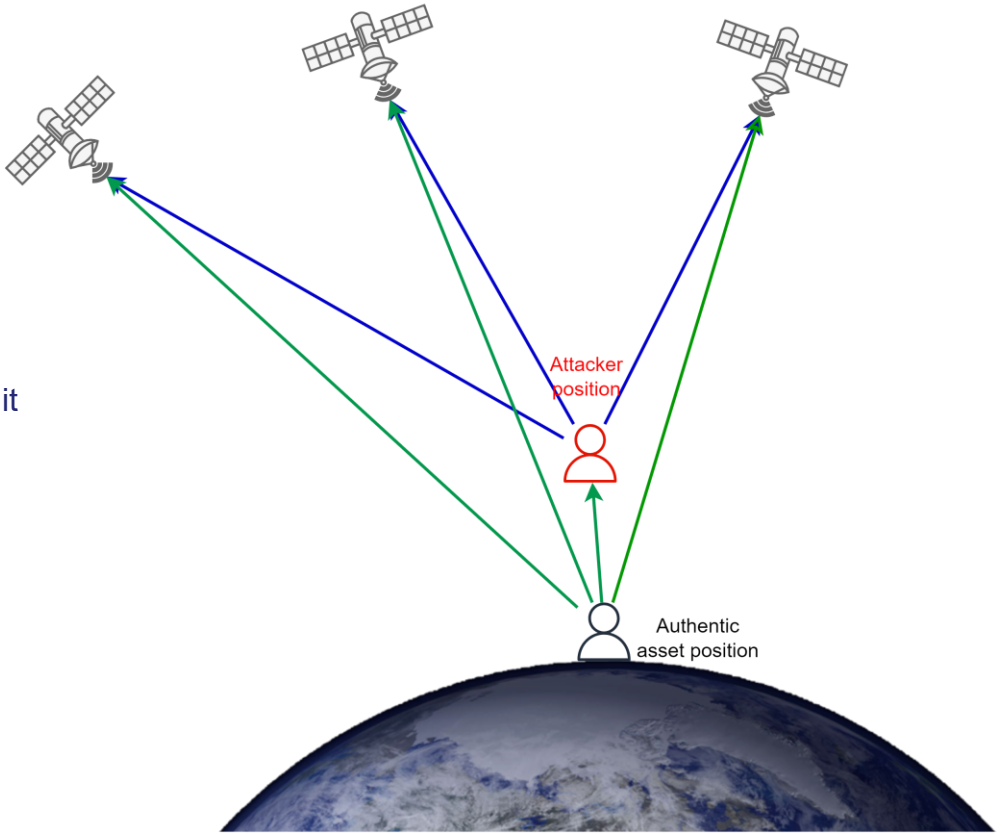
TARGET ATTACKS

/// GNSS attack

- Only the asset reported position is spoofed
- The system is secured against this attack because the reported position is not compatible with the uplink measurements

/// Man In the Middle (MIM) Record and Replay Attack

- The attacker is placed between asset and satellites
- The attacker receives the authentic signal, processes it and transmits it to all satellites in view, with a certain delay
  - No beamforming capabilities
- The system can detect this attack by identifying inconsistencies between actual and predicted measurements



DEMONSTRATION RESULTS

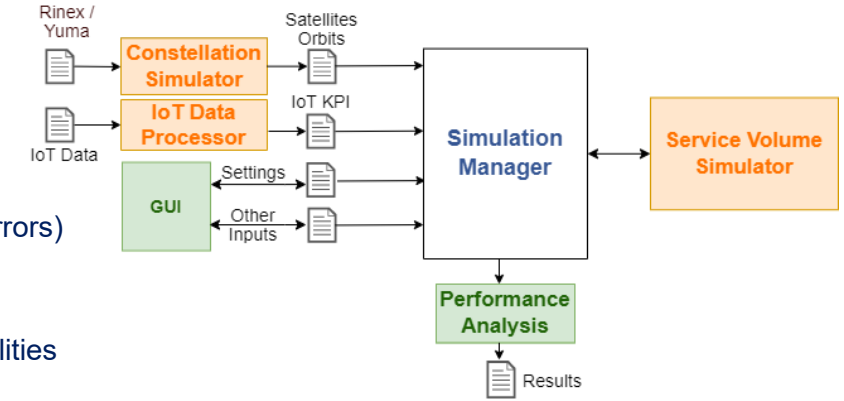
DEMONSTRATOR OVERVIEW

/// Goal

- Assess the performances of the protocol both in nominal and attack scenarios

/// Demonstrator Characteristics

- **Constellation Simulator**
  - Generate the satellite positions starting from a Rinex/ephemeris data
- **IoT Data Processor**
  - Process real IoT data to generate the measurement statistics (ToA errors)
  - COSPAS-SARSAT data are used for calibration
- **Service Volume Simulator**
  - Process satellite orbits and IoT data to simulate the system functionalities



/// KPIs

- **System availability,** A_{sys}: percentage of iterations the system does not trigger any alarm in nominal conditions
- **PFA for navigation**, $P_{fa,nav}$: probability that, in a nominal situation, the system raises an alarm
- **PFA for communication,** $P_{fa,comm}$: probability that, in a nominal situation, no uplinks are received inside a maximum time
- **Probability of misdetection,** P_{md}: probability that, in an attack scenario, the system misdetects the attack

TUNED PARAMETERS

/// Constellation

- Multiple potential constellations are considered
  - 8 State of the Art constellations: Astrocast, Kinéis, Globalstar, Myriota, Iridium, Lacuna, Orbcomm, Swarm
  - 2 Custom constellations containing >100 satellites
- Visibility analysis
  - 3 Visibility constraints

    The maximum time interval between two verifications shall be 15min (target geolocation period)

    The asset shall have at least 3 satellites in view

    The visibility periods, i.e. the time intervals in which the user has at least 3 satellites in view, shall have a duration of at least 2min, which are needed to carry out the bursts exchange
- 4 selected Constellations
  - Lacuna Space
  - Swarm
  - 2 custom constellations, named « Custom1 », « Custom2 »

/// Baseline settings

- 15h simulation, 3 bursts transmitted within a geolocation period of 15min
- Signal settings: UHF band, LR-FHSS waveform with channel bandwidth ~1.5MHz

DEMONSTRATOR RESULTS – NOMINAL SCENARIO

/// No false alarms are triggered

/// One-way and two-way techiques both reach 100% availability

/// Good performances also in case an azimuth mask is placed (mask $= [0, 180]°$)

ID	Constellation	Algorithm	Azimuth mask [deg]	A_{sys} [%]	$P_{fa,nav}$	$P_{fa,comm}$
1	Lacuna	UTDOA	[0, 360] / [0, 180]	100	0	0
2	Swarm	UTDOA	[0, 360] / [0, 180]	100	0	0
3	Custom1	UTDOA	[0, 360] / [0, 180]	100	0	0
4	Custom2	UTDOA	[0, 360] / [0, 180]	100	0	0
5	Lacuna	RTT	[0, 360] / [0, 180]	100	0	0
6	Swarm	RTT	[0, 360] / [0, 180]	100	0	0
7	Custom1	RTT	[0, 360] / [0, 180]	100	0	0
8	Custom2	RTT	[0, 360] / [0, 180]	100	0	0

DEMONSTRATOR RESULTS – ATTACK SCENARIO

/// GNSS attack only

- Attack Configuration
  - The distance between authentic and spoofed position is set to $\Delta x_{spoof} = 500\text{m}$
  - The asset clock is synchronised at the beginning of the simulation ($\Delta t_c = 0\text{days}$)
- Attack Detection
  - The spoofed position is not compatible with the uplink measurements
  - The estimated residuals are not compatible with their theoretical distribution
  - The misdetection probability drops to 0 for Δx_{spoof} >1km

ID	Constellation	Algorithm	Azimuth mask [deg]	Δt_c [days]	Δx_{spoof} [m]	P_{fa}^{comm}	P_{md}
9	Lacuna	UTDOA	[0, 360]	0	500	0	0
10	Swarm	UTDOA	[0, 360]	0	500	0	0
11	Custom1	UTDOA	[0, 360]	0	500	0	0
12	Custom2	UTDOA	[0, 360]	0	500	0	1.67
13	Lacuna	RTT	[0, 360]	0	500	0	0
14	Swarm	RTT	[0, 360]	0	500	0	8.33
15	Custom1	RTT	[0, 360]	0	500	0	1.67
16	Custom2	RTT	[0, 360]	0	500	0	3.33

DEMONSTRATOR RESULTS – ATTACK SCENARIO

/// GNSS +Record and Replay

- Attack Configuration
  - The spoofed GNSS position coincides with the attacker position, placed at $\Delta x_{spoof} = 500\text{m}$ from the authentic position
  - The asset clock is synchronised at the beginning of the simulation
- Attack Detection
  - The spoofed position is now compatible with the spoofed measurements
  - The attack is detected through an inconsistency between the estimated time (transmission or layover) and the authenticated time, whose difference does not follow the expected theoretical distribution
  - UTDOA performs worse than RTT because user clock divergence increases uncertainty and thresholds, potentially masking the presence of attacks, while RTT removes the user clock contribution by exploiting the layover time

ID	Constellation	Algorithm	Azimuth mask [deg]	Δt_c [days]	Δx_{spoof} [m]	P_{fa}^{comm}	P_{md}
17	Lacuna	UTDOA	[0, 360]	0	500	0	30
18	Swarm	UTDOA	[0, 360]	0	500	0	26.67
19	Custom1	UTDOA	[0, 360]	0	500	0	70
20	Custom2	UTDOA	[0, 360]	0	500	0	70
21	Lacuna	RTT	[0, 360]	0	500	0	1.67
22	Swarm	RTT	[0, 360]	0	500	0	11.67
23	Custom1	RTT	[0, 360]	0	500	0	11.67
24	Custom2	RTT	[0, 360]	0	500	0	6.67

DEMONSTRATOR RESULTS – ATTACK SCENARIO

/// GNSS +Record and Replay

- Asset Clock
  - The influence of asset clock synchronization is more clear in simulations exploiting an initial not synchronized user clock bias
  - Simulations are done using a clock with a 1day divergence (initial clock error is around few microseconds)
  - Lot of misdetections when UTDOA algorithm is used
  - Lower P_{md} when using RTT, as expected

ID	Constellation	Algorithm	Azimuth mask [deg]	Δt_c [days]	Δx_{spoof} [m]	P_{fa}^{comm}	P_{md}
25	Lacuna	UTDOA	[0, 360]	1	500	0	88.33
26	Swarm	UTDOA	[0, 360]	1	500	0	88.33
27	Custom1	UTDOA	[0, 360]	1	500	0	91.67
28	Custom2	UTDOA	[0, 360]	1	500	0	98.33
29	Lacuna	RTT	[0, 360]	1	500	0	1.67
30	Swarm	RTT	[0, 360]	1	500	0	1.67
31	Custom1	RTT	[0, 360]	1	500	0	16.67
32	Custom2	RTT	[0, 360]	1	500	0	23.33

CONCLUSION

SUMMARY

/// Achievements

- Development of robust position verification concept + algorithms
- 500m position verification achievable
- Robustness to attacks
- Development of testbed – sandbox for testing waveforms / algorithms / constellations

/// Remaining challenges for development of operational container-tracking system

- Standardization (frequencies, local access points)
- Local environment (RF conditions at ships / depots)