Ship Observations Team

~ integrating & coordinating international ship-based observing programmes for JCOMM ~

Ship Safety & Security

PMO-IV and Support to Global Ocean Observations using Ship Logistics
8-10 December 2010, Orlando, FL, USA

Graeme Ball
Chair SOT

Outline

- Situation at PMO-III
- Developments Since PMO-III
- ENCODE Proposal

Situation at PMO-III

Discussion at SOT-IV

Definitions

REAL	Official ITU callsign of the ship.
SHIP	Non-unique identifier. REAL is unilaterally replaced by the letters SHIP.
MASK	Unique, repeating identifier. MASK is assigned by the NMS that recruited by the ship.
ENCODE	Unique, non-repeating identifier. Derived by encrypting specific elements of the message, e.g. callsign + latitude + longitude

Option 1 - REAL

Advantages	Disadvantages
Default option of all NMS.	Ships can easily be identified on publicly available NMS or similar products displaying callsign.
Real-time and delayed-mode quality monitoring are not compromised.	
REAL included in national updates to WMO No. 47, hence the integrity of WMO No. 47 is retained.	

Option 2 - SHIP

Advantages	Disadvantages
Identity of the ship is hidden.	Non-unique (advantage ?).
Implemented at source before sending of the observation **OR** at the NMS before GTS dissemination.	Real-time quality monitoring of **SHIP** is impossible unless non-masked data are supplied separately to the monitoring centres and NMSs.
Immediate implementation if quality monitoring concerns are ignored.	Delayed-mode quality monitoring not possible with **SHIP**.
Ships cannot be tracked individually on publicly available NMS or similar products that routinely show callsign.	Renders WMO No. 47 largely unusable

Summary - SHIP

- Largely eliminates vessel tracking.
- Impacts on the usability of WMO No. 47.
- **SHIP** without additional measures to assist with QM:
  - » No real-time QM by monitoring centres;
  - » No delayed-mode QM; and
  - » Data excluded from long-term climate studies.
- **SHIP** with additional measures to assist with QM:
  - » Enables real-time and delayed-mode quality monitoring.

Option 3 - MASK

Advantages
Identity of the ship is hidden.
Short to medium term implementation.
Real-time and delayed-mode quality monitoring.
REAL included in national updates to WMO No. 47.
Independent of the official ITU callsign of the ship which often changes.

Option 3 - MASK

Disadvantages
Overheads to maintain a database of **REAL** v **MASK**.
Possible that **MASK** may impinge on **REAL** of another country.
Monitoring centres and NMSs need real-time access to a centralised database of **MASK** v **REAL**.
NMSs must keep up-to-date the **MASK** v **REAL** database for access by the monitoring centres.
Ships can be tracked on publicly available NMS or similar products routinely showing callsign.
E-SURFMAR implementation impacts on long-term climate monitoring.

Summary - MASK

- Unique identifier. Independent national schemes.
- Repeating identifier:
  - » Enables real-time and delayed-mode quality monitoring; but
  - » Does not eliminate vessel tracking.
- No impact on WMO No. 47.
- Effective implementation for QM requires:
  - » Centralised **MASK** v **REAL** database; and
  - » Access routines by monitoring centres and NMS.

Option 4 - ENCODE

Advantages	
Identity of the ship is hidden.	Real-time and delayed-mode quality monitoring are not compromised.
3rd party users of ship data would receive **ENCODE**.	One proposed solution is to uses a public key for encoding and a private key (restricted distribution) for decoding.
REAL included in national updates to WMO No. 47.	
Ships cannot be tracked with **ENCODE** because the encrypted value changes with each observation.	Permits the random selection of elements in the message to be encrypted as **ENCODE**.

Option 4 – ENCODE (cont)

Disadvantages
Requires all monitoring centres and NMSs to upgrade their message recognition and switching systems to include encoding and decoding routines.
The length of **ENCODE** exceeds the currently permitted callsign length in the message recognition software in some NMSs.
BUFR is regarded by some as the preferred message format in which to transmit **ENCODE**, however BUFR is not mandatory until 2012.

Summary - ENCODE

- Only requires encode and decode routines.
- 3rd party data users get the **ENCODE** version of data.
- No impact on WMO No. 47.
- Permits the random selection of elements to be encrypted.
- Requires BUFR due to the length of **ENCODE**.

Conclusions

- **SHIP** satisfies the requirement for ship anonymity and largely eliminates vessel tracking.
- **SHIP** without additional measures to assist with QM is not recommended for the VOS.
- **MASK** satisfies the requirements for ship anonymity and quality monitoring, plus it eliminates data loss when **REAL** changes during a voyage.
- **MASK** is recommended for the VOS.

Conclusions (cont)

- **ENCODE** satisfies the need for ship anonymity and quality monitoring, plus it largely eliminates vessel tracking.

- **ENCODE** is recommended as the long-term solution for the VOS.

Recommendations

- **ENCODE** to be promoted as the preferred long-term SOT solution with a recommendation to EC-LIX requesting that all NMSs and monitoring centres eventually incorporate SOT approved encoding and decoding routines in their message recognition and switching centres.

- In the shorter-term **MASK** is preferable to **SHIP** in the case where **SHIP** is implemented without additional measures to assist with QM. The use of **SHIP** in this manner should be discouraged.

Recommendations (cont)

- For **SHIP** to meet all requirements, it is proposed that countries implementing this scheme at the NMS level:
  - » Collect the raw (non-masked) BBXX in a secured database and provide these data to the monitoring centres or NMSs as required;
  - » If these data are not provided in real-time then perform the real-time QM on ships that it masks and provide feedback to the appropriate VOS FP;
  - » Delayed-mode data must use **REAL**; and
  - » Technical solutions to supply the raw data to be developed in collaboration with the receiving centres to ensure there is one agreed delivery method.

Recommendations (cont)

- Establish a *Task Team on Callsign Masking and Encoding* (Chairs of SOT, VOSP, ETMC, SOT TC):
  - » Oversee the implementation of **MASK** and **ENCODE** and develop guidelines as necessary;
  - » Review and approve national **MASK** schemes to ensure they remain unique and do not impinge on:
    - » The ITU callsign series allocated to a country, or
    - » any other marine or oceanographic identification scheme used by WMO, e.g. buoy identification numbers;
  - » Ensure the **MASK** v **REAL** database is kept up-to-date by NMSs implementing **MASK**;
  - » Develop the **ENCODE** encryption strategy; and
  - » Develop the encoding and decoding keys.

Recommendations (cont)

- For **MASK** to meet all requirements, it is proposed:
  - » That JCOMMOPS hosts the centralised **MASK** v **REAL** database;
  - » The database is password protected from unauthorised access; and
  - » Countries implementing **MASK** to supply:
    - » Quarterly VOF list of **MASK** v **REAL**, and
    - » Monthly update of significant changes to its list of **MASK** v **REAL**.

- VOS Programme Manager to be the national focal point for callsign masking of all national ship-based observing programmes, e.g. SOOP and ASAP.

ENCODE Proposal

ENCODE Proposal

- ENCODE proposal developed by Scott Woodruff and team at NOAA/ESRL for TT on Callsign Masking & Encoding.
- Proposal approved by TT


SHIP OBSERVATIONS TEAM
JCOMM