ENCWG3-5.8.1

Paper for Consideration by the ENCWG

S-63 needs extension of authentication

Submitted by:	Hannu Peiponen / IEC TC80 Chair
Executive Summary:	This paper proposes creation of a new revision ed 1.3.0 of S-63 to facilitate authentication of all data files in a delivery set.
Related Documents:	N/A.
Related Projects:	N/A

Introduction / Background

1. IHO has been recognized by IMO as being the governing body for providing nautical charts.

2. IHO have had for long time S-63 to provide cyber security for S-57 ENC charts and updates.

3. IMO has set generic guidelines to manage maritime cyber risk, see

- IMO MSC-FAL.1 Circ.3, Guidelines On Maritime Cyber Risk Management, 2017

4. IMO MSC-98, Jun 2017, published an IMO resolution MSC.428(98) which state that cyber risk is one of the issues to be addressed by ISM-code and the periodical audit of vessels for ISM-code shall include audit of management of cyber risk from 1st Jan 2021.

4. Response of industry has been creation of numerous private rules related to the IMO rules, for example

- BIMCO et.al., The Guidelines on Cyber Security Onboard Ships, 2017
- DNV-GL, Class Program DNVGL-CP-0231, Jan 2018
  This Class Program reference existing standard such as IEC 61162-460, which require authentication of data files and executables

5. IEC TC80 has also reacted by initiating drafting a new standard, IEC 63154 Cyber security, about what kind of mitigation against cyber risk the equipment onboard shall provide. Target of the new standard is to establish international consensus on the minimum technical level of mitigation against cyber risk. The timeline of this new standard is:

- Drafting by the workgroup until 1st quarter of 2020
- IEC approval process consisting of CDV and FDIS comments & votings from summer 2020 to the publishing planned for 2nd quarter of 2021

6. The current draft of the new standard IEC 63154 is based on the principle that all data files and executables should be authenticated for their source and integrity before use by the IEC 63154 compliant equipment (see IEC 80/883/CD). For IHO this means a need to provide authentication method of all data products from HOs to vessels regulated by SOLAS.

Analysis/Discussion

7. This time there is one new observation to note about the cyber security provided by the published ed 1.2.0 of S-63. Namely the fact that the provided signatures shall cover all data files of the service. This observation rises from the fact that in the existing S-63 ed 1.2.0 for S-57 ENC charts only the ENC charts and their update files (i.e. .000, .001, .002, etc.) are protected by the signature, while auxiliary files (.txt, .tif), up-to-date information file (products.txt) and service related files (catalog.031, readme.txt, serial.enc, media.txt, status.lst) are not protected by a signature.

8. The up-to-date information file, auxiliary files and service related files offer numerous ways how a hacker could cause serious issues for a vessel. For example, up-to-date information file could cause removal of ENC charts from onboard navigation equipment, use of content of auxiliary files could cause serious mistakes in route planning, etc.

9. About amending the existing S-63 to facilitate authentication of all files. This could be done either:

a) by adding a single additional file containing a signature calculated from all files not yet protected or

b) by adding multiple additional files containing signatures for files not yet protected.

ENCWG should debate which method is more suitable. The calculation of signature should be based on same the private key as the signatures already provided for the ENC chart file and update files.

10. The method proposed in paragraph 9 would be up and downward compatible.

- Older software versions based on S-63 ed 1.2.0 for onboard ECDIS would ignore the new signature files.
- Newer software versions based on the proposed new S-63 ed 1.3.0 for onboard ECDIS could be made to accept delivery packages based on both ed 1.2.0 and 1.3.0.
  Obviously, acceptance of delivery package based on ed 1.2.0 would then be based on the fact that there is an accepted exception to consume non-authenticated data-files.
  If not acceptable by the rules of that day, then the new ECDIS software versions could provide a warning standardized for exact wording by the ed 1.3.0 of S-63 (reference is made to IMO S-Mode and greater standardization of basic functionality).

Conclusions

11. Provision of the cyber security is a matter of urgency. Gap filling of S-63 for the noted deficiency is relatively small effort by ENCWG.

Recommendations

12. Recommendation is to agree that there is a need to create new revision ed 1.3.0 of S-63 to address the noted deficiency in the authentication of all data files.

13. Further recommendation is to act promptly in order that the new revision ed 1.3.0 of S-63 could be ready for approval by HSSC-11, year 2019. This would facilitate further approval by council and voting by member states. Result would be publishing around begin of year 2020.

Justification and Impacts

14. Justification for the proposed change is the fact the quite soon onboard ECDIS equipment are assumed to provide technical provisions to mitigate against cyber risk.

15. Impact for **new installation of ECDIS** would be very small. Just development of the added authentication checks for input of ENC charts and updates.

16. Impact for **existing ECDIS equipment** is partly similar as the sw update required for recent new edition of S-52 Presentation Library. Partly because this would need installation of new software, but this would not modify the overall work procedures by the crew to perform their weekly updates of the ENC charts nor amend the algorithms used in daily operation to consume more time for screen updates. This is because the fact that if the authentication of all files is passing then the end user experience is exactly same as before. In case of **existing ECDIS equipment not yet upgraded** the result is no impact as the proposed change is totally downward compatible.

17. Impact for **ENC publisher** (i.e. national HO). The change is such that they could implement this by their own schedule taking into account the risk associated with the obligation to provide the service and crowing pressure in the regulatory environment to provide cyber secure service.

18. Impact for **ENC delivery by physical means**, for example CD or DVD by postal delivery, is nearly nothing. Just a few additional bytes are consumed by the added signatures.

19. Impact for **ENC delivery by online methods** could be small adjustments for the method to specify which files are part of the online delivery in order to facilitate also online transfer of the added signature files.

Action Required of ENCWG

The ENCWG is invited to:

a) note the issue presented in this paper,

b) consider what actions are needed to facilitate prompt drafting of new revision ed 1.3.0 of S-63 to be ready for approval by HSSC-11, year 2019.