CHRIS17-4.1B

Paper for Information of CHRIS

ECDIS type approval

Submitted by:	SHOM
Executive Summary:	The analysis of the dysfunctions observed on a type-approved ECDIS, shows that it is necessary to supplement the certification standards with requirements on the design and development of software, as well as to give the means to control their implementation. The HOs may consider that they are not involved in such technical issue. However mariners do not use ENCs directly: they use an ECDIS which is populated with ENC data. Experience shows that poor experience of the former will be interpreted as poor quality of the latter. Advice from CHRIS is asked for before submission of the case to IEC and IMO.
Related Documents:	IMO A.817 (19) IEC 61174, IEC 60945,IEC 61924 IHO S64
Related Projects:	-

1 Introduction

During WEND 8, France reported that tests provided in S-64 are not sufficient to qualify software and was tasked to communicate to IHB proposed additional features for incorporation into IEC 61174 / S-64. (done).

In the discussion the WEND Secretary stated that the test are consistent with IEC standards but are not exhaustive, and Germany stated that it is as important to convey changes to IEC in order to affect type certification.

WEND 9 has been informed that SHOM sent a letter on the subject to the French Maritime Authority, to the national mirror group of TC 80 of IEC, and to Mared (Maritime Equipment Directive: Mared is the co-ordination group for the Notified Bodies assigned by the Member States to carry out the conformity assessment procedures referred to in the Marine Equipment Directive (COUNCIL DIRECTIVE 96/98/EC of 20 December 1996 on Marine Equipment). This letter is enclosed to this CHRIS paper.

The report of WEND9 meeting states:

> *"France provided some additional comments regarding IHO Publication S-64 (ECDIS Test Data Sets) and ECDIS type-approval (Doc. WEND8-INF5). This matter has been referred to CHRIS, and will also be brought to the attention of IMO and IEC. Germany made specific mention that this matter needs to be addressed by IEC TC80 for the next edition of IEC 61174 (ECDIS: Methods of Testing and Required Test Results).*
>
> …

> *WEND 9 Action 2:* ***France*** *to contact IEC TC80 regarding recommended changes to ECDIS type -approval testing.”*

Before sending the required letter to IEC TC80, France is seeking advice from Chris about the proposed solution to remedy the weakness in the control of the functional safety of software

2 Analysis

1. Is the subject addressed by the proposal considered to be within the scope of IHO objectives?

The analysis of the dysfunctions observed on a duly type-approved ECDIS, shows that it is necessary to supplement the certification standards with requirements on the design and development of software, as well as to give the means to control their implementation.

The HOs may consider that they are not involved in such technical issue. However mariners do not use ENCs directly: they use an ECDIS which is populated with ENC data. Experience shows that poor experience of the former will be interpreted as poor quality of the latter.

Furthermore the revised WEND principles take into account the future mandatory carriage of ECDIS as prepared by IMO in order to foster the ENC production and availability by the coastal States. It is to date quite impossible to imagine a paperless bridge if the systems continue not to be safe enough.

.2 Is the subject of the proposal within the scope of an item of the current IHO work programme?

Yes, at least through the WEND work

.3 Do adequate industry standards exist?

Probably yes (IEC 61508 for instance) but they have to be referred to in the relevant standards for INS (61924, 60945) and ECDIS (61174).

.4 Do the benefits justify the proposed action?

It is to date quite impossible to imagine a paperless bridge if the systems continue not to be safe enough. One of the goal of WEND is to make such a paperless bridge possible for nautical charting.

.5 Benefits

The clear benefit is to make it possible in the near future to really take advantage of the ECDIS concept to enhance the safety of navigation.

.6 Working groups

It is a matter of consistency in the work of IHO, IMO and IEC. The CHRIS itself is within the IHO the competent body for the required technical advice.

.7 Any other relevant information not covered elsewhere

No

. 8 Target completion date

The French Marine Safety Agency will submit an action proposal to the next IMO MSC 81. It is expected to have an IHO authorized technical advice on the proposed solution. Note that IHO WEND has already asked SHOM to bring the matter to IMO and IEC: this would be more effective if the solution is supported or commented.

The target date will then be the date when ECDIS will begin to be mandatory onboard some categories of ships (2008 to be confirmed by IMO).

.9 Action required

CHRIS to endorse the technical solution as proposed in the attached document: namely:

“A simple solution would be to make reference to the IEC 61508 standard for all the electronic bridge equipments related to the safety of navigation. The drafting correction could be to re-use in the IEC 61924 standard, the § 4.2.3 of the IEC 60945 modified in order to quote the IEC 61508 not only as an example but as an applicable standard, instead of making reference to the ISO 9000 series.

This solution may be quickly implemented: it would however need to make explicit the provisions to be applied, and this would greatly benefit from the important work already done in the aeronautic domain with the DO-178 B standard, even if this standard has to be fitted to the maritime world.”

SHOM 16 February 2005

to : French National Maritime Authority
copy: National TC80 Group, Mared

Please find enclosed herewith a report which takes into account the defaults of functioning of an ECDIS yet duly certified as meeting the IMO A 817(19) requirements, in order to shed light on insufficiencies in the corpus of standards presently available.

It is necessary to note the observed insufficiencies in the ECDIS certification standards and to supplement these standards with requirements on the design and development of software, as well as to give the means to control their implementation.

A simple solution would be to make reference to the IEC 61508 standard for all the electronic bridge equipments related to the safety of navigation. The drafting correction could be to re-use in the IEC 61924 standard, the § 4.2.3 of the IEC 60945 modified in order to quote the IEC 61508 not only as an example but as an applicable standard, instead of making reference to the ISO 9000 series.

This solution may be quickly implemented: it would however need to make explicit the provisions to be applied, and this would greatly benefit from the important work already done in the aeronautic domain with the DO-178 B standard, even if this standard has to be fitted to the maritime world.

It is urgent to create an expert group (HGE could be an example of such a group) for elaborating an effective quality standard for the design and development of the ECDIS software, and for up-dating the IMO A 817(19) resolution in order to take into account requirements concerning the safety of functioning (upstream enough from the development) in relationship with the manufacturers of the ECDIS equipment or of the cartographic kernels used in these ECDIS. This work should be extended to all the interlinked software of a bridge linked to the safety of navigation.

REPORT

1/ Dysfunction of a type-approved ECDIS

The French Navy Survey Ship Beautemps Beaupré entered in service in January 2004. For electronic navigation, she is fitted with an ECDIS which has been certified by Det Norske Veritas as meeting the IMO A 817(19) requirements: for this certification IEC has developed the standard IEC 61174 for type approval and testing procedures: this standard uses IHO publications S57 and S52.

The experience gained with this type-approved ECDIS shows dysfunctions which are described schematically in annex and can be summed up as follows:

- lack of robustness of the system (route monitoring, errors due to a deficient sensor, ..)
- lack of reliability (system blockage and necessity to re-boot) due to the implementation of various components for which it seems that no “functioning safety” methodology has been applied.

Such an amount of deficiencies is not acceptable for the safety of an equipment which can lead to a catastrophe (grounding of a tanker or of a ferry for example)

2/ The type-approving tools

IEC has developed the 61174 standard for type-approval of the ECDIS. This standard has no requirement for the software design and design, and is limited for the software aspects to performance tests.

As asked for by IEC, IHO has produced S64 publication “Test data sets for ECDIS” which is used by ECDIS type-approving organisms. It is of course possible to add new tests in order to take into account the defaults observed by SHOM onboard Beautemps Beaupré.

But increasing the number of tests in order to take into account the defaults observed leads to a dead-end because the number of potentially abnormal situations increases dramatically with the number of states of the various parameters. S64 tests are necessary, at least to give evidences for the behaviour of the ECDIS system and for facilitating the understanding by the development teams, but the proofs which are provided are always incomplete because they concern only a limited sample of the entry states[1]. In order to validate a software tests are needed (which have to take into account its internal architecture as stated by the standards dealing with critical software) but it is also vital to give evidences on the conformity to a ECDIS software design and development standard.

3/ The other IEC standards

IEC 60945 is quoted in the list of standards applicable to IEC 61174. IEC 60945 deals mainly with physical environment (mechanics, electric, electro-mechanics, …) but it however refers to software in a § 4.2.3 requiring the design and testing method to be

[1] This is clearly stated in numerous publications, of which the « Software System Safety Handbook” of the US DOD.

described and the conformity with an internationally recognized quality standard: the ISO 9000 series are then quoted but only as an example (they are not referred in the applicable standards list) without explaining how they have to be applied!

As a part of an integrated bridge, ECDIS has to be in compliance with IEC 61924 which surprisingly does not deal with design and development of software even if there are a lot of interlinked systems within such a bridge.

In fact IEC standards exist which are dealing with functional safety of software (61508). These standards (in 5 books) have been developed by the IEC committee 65. They detail all aspects linked to design and development of software! In the introduction they provide that these standards are intended to be utilised by technical committees when preparing standards complying with IEC/ISO 104 and 51. It is obvious that the 80TC has not taken into account this 61508 standard when elaborating the 61174 standard, maybe because of its youth.

4/ Lessons from other domains

In the aeronautic field the need to standardize requirements concerning the safety of functioning of software is clearly simply obvious.

An important deal of work concerning the safety of the aeronautic navigation software has led to the DO-178 B standard “software considerations in airborne systems and equipment certification” which is supported by a standardization corpus already published (for example ISO/IEC 12207, 12119 and 15504; EUROCAE/RTCA ED 76, RTCA DO 200 and 201).

DO-178 B could be a canvass[2] to give the proof of the good functioning of ECDIS software.

Maritime and airborne navigations present many similar aspects: kinematics are different but the decisions are to be taken in very short timeframe, and if the aircraft cannot stop, the ship has a high inertia which makes anticipation vital. It is irrational and even contrary to the know-how in software system engineering that the prevention measures of one of these domains could be considered as useless in the other domain.

[2] It defines, for example, 5 categories for the criticity linked to a default, and for these categories more or less constraining requirements are attached to the safety of a given software component: when defining these categories specificities of maritime navigation are to be taken into account, but it would be very surprising that none of the ECDIS software components were not identified in one of the critical categories of DO-178B.

ANNEX TO THE REPORT

Dysfonctions of ECDIS onboard Beautemps-Beaupré – safety of functionning

1- Used documents

Information given in paragraphs 2 and 3 hereafter come from following documents:

- « Liste de problèmes survenus aux équipements passerelles » en provenance du Beautemps-Beaupré (de mai 2004 à juillet 2004),
- N-E n°184 EPSHOM/INF/NP of 14 June 2002 «Evaluation de l'ECDIS Seamap-Kongsberg »,
- Note n° AA/03/218039 SPN/ASM/COM « Dysfonctionnements des systèmes de visualisation de cartes électroniques » of 7 October 2003, giving a synthesis of the feedbacks concerning the Beautemps-Beaupré ECDIS,
- List of guarantee trial minutes from SPN and related to Beautemps-Beaupré ECDIS

2- Observed dysfonctions

2-1 List given by the crew of Beautemps-Beaupré

Date –Equipment	*Problems and solutions*
May 2004 ECDIS SM10	Doctor Watson at the end of a monitored track in AUTOTRACK mode→ on/off and back to the nominal situation
May 2004 ECDIS SM10	Doctor Watson at the end of a monitored track in AUTOTRACK mode → on/off and back to the nominal situation
June 2004 ARPA starboard	Alarm + window « system running out of virtual memory », automatic stop → manual restart and back to the nominal situation
June 2004 ECDIS SM10	Window «system running out of memory". Screen non legible. Bug → Off, manual restart and back to the nominal situation
June 2004 ARPA port	Window «system running out of virtual memory, please close some application »
June 2004 ARPA port	Automatic stop. Loss of the automatic pilot. Alarm on the 2 radars et on the ECDIS.
June 2004 ECDIS	Window « system process out of virtual memory. Tour system is running low on virtual memory. Please close some application » → closing of the window.
June 2004 ARPA port	Window «system running low on virtual memory, please close some application »
June 2004 ECDIS SM10	Total failure after the message "system running out of virtual memory" → Off, manual restart and back to the nominal

SM10	situation.
June 2004 ARPA port and starboard	Window «system running low on virtual memory, please close some application ». the radar image is frozen → restart.
June 2004 ARPA port	Window «system running low on virtual memory, please close some application ».
June 2004 ECDIS SM10 et PL10	A monitored route for casting off is erased → off and manual restart : the route is recovered
June 2004 PL10	Total failure when recording a validated route
July 2004 automatic pilot on ECDIS	The follow of a route is unsatisfactory in TRACK mode. The ship tacked 10 m left to 10 m right of the monitored track → change the mode in heading mode
July 2004 ECDIS SM10	After pressing the offset key, blue screen. When reinitializing, window Doctor Watson → on/off and back to the nominal situation

Nota The restarts for solving the problems described in the above table take less than 5-6 mn.

Other points reported by the crew of Beautemps-Beaupré :

- ECDIS autotrack mode ineffective, due to the base of the loch,
- Total failures, and slowing down of PL 10 disappeared after implementation of a 256Mb RAM,
- Impossibility to find an ARCS chart which had been used before.

2-2 Synthesis of SPN tests (SPN : Service of the French Procurement Agency in charge of the Naval Programmes)

(extracts)

- Lost of the position tacking when the ground longitudinal speed is close to 0 and the surface longitudinal speed is not null. It seems that the ECDIS calculates an infinite radial speed: the ship position is moved of several 10th of Miles from the previous position. There must be some division by zero,
- At sea, it has been impossible to use the tracking mode of the ECDIS to follow a route : shifts from the route, when the system does not fail, are greater than 20 m and reach 200 m,
- Several times, it has been impossible to have the control of the main display unit of ECDIS,
- Impossible to use ARCS charts, both on the navigation and preparation display units,
- The ECDIS being in route tracking mode, following events appeared regularly during 3 weeks:
    - Freezing of the system, with a fix image, no operative function except on/off. No problem or alarm after restart,

  - Freezing of the system, the screen goes out, no operative function. No problem or alarm after restart,
  - Freezing of the system, with a blue screen full of memory addresses, the system indicates an insufficiency of memory, no operative function. No problem or alarm after restart,

  We can note that no alarm is given during these freezing, which is particularly dangerous when the image is fixed, all the more in narrow passages,

- During several weeks, the use of ECDIS is very difficult due to the extreme slowness of the running of the programme. Changing a scale takes up to 30s, changing a menu 25s. When creating complex routes the software regularly fails and stops, with a lost of the work which has not been recorded.
- In the route preparation mode, the screen becomes frozen, full of figures and letters and the following message is displayed : "beginning dump of physical memory, physical memory dump complete". After on/off back to the nominal situation.

The trial minutes show that the trials at quay have been rather limited and often refer to the fact that the ECDIS has been type approved by «DET NORSKE VERITAS », in accordance with IHO/IMO resolutions and IEC standard (in particularly 61174).

2-3 Note by EPSHOM/INF (Computer Centre of SHOM)

Three main problems have been identified :

- Impossibility to take into account official updates a little bit more elaborated than those of the « IHO-DATASETS-TESTS »,
- Impossibility to read the planned routes used during a previous session and to restore recorded routes.
- The failures need a full restart, with a non negligible loss of time.

2-4 Observations by EPSHOM ENC production division *(during the acceptance phase of the ECDIS)*

It seems that the ECDIS of Beautemps Beaupré is mainly based on a cartographic CMAP kernel (CMAP-SDK 3.4.4). The added value is to be found in the interface design which is used for operating the functions of this kernel. Due to this architecture, it was difficult for the manufacturer to modify its software when the dysfunctions concern one of the functions of the kernel (for example the impossibility to import certain updates is due to the kernel).

September 2002 : the admission of the ECDIS realised by EPSHOM, shows dysfunctions and deviations from IMO standards. For instance there is no alarm when the system does not take into account such or such up-date, and this is a major problem since nearly 40% of the updates are rejected…

October 2003 : a part of the previously rejected updates is now accepted by the ECDIS. This has been solved thanks to a modification of the kernel. But 10% of the updates are still rejected…

None of the other mentioned problems have been solved.

3- <u>Comments on safety aspects</u>

Firstly, there is no formal requirement for system safety in the design of ECDIS (there is no reference in IMO OMI A.817(19), even if there are some requirements concerning the back-up). From the examples above, the consequence seems to be:

- lack of robustness of the system (route tracking, dysfunctions link to a failing sensor like the loch…),
- lack of reliability (freezing of the system and necessity to restart), due to the on the shelf components integration for which no integration method complying with safety requirements seem to be applied.
- maintainability : the ECDIS of Beautemps-Beaupré is still under guaranty an is regularly upgraded. The support teams of the manufacturer operate 24/24 and 7/7 in order to take into account the dysfunctions. Worth to be noted is the fact that such a support will cease at the end of the guaranty period, with foreseeable problems for the taking into account of the evolutions of the standards (eg S63). No clear answer on this point from the manufacturer.
- the availability of the system relies on a back-up system and on a set of paper charts.

A quick reading of IEC 61174 shows that the tests realized are relevant for the functionalities of an ECDIS as defined in the IMO resolution A.817 (19), and give a possibility to a rough functioning control of the ECDIS, but one more time in a safety perspective (a requirement level has to be defined) and this seems to be insufficient (a posteriori consideration).