Impact Analysis of S-63 (Encryption) and S-58 (Validation) on ECDIS

The purpose of this paper is to try and quantify the impact that the encryption and validation have on the ECDIS when importing ENCs to SENC. The following sections are provided to give a brief background and understanding of the requirements for each process.

The S-58 Validation Checks

The IHO S-58 Standard specifies the checks that, at minimum, producers of ENC validation tools should include in their validation software. This software will be used by **hydrographic offices** to help ensure that their ENC data are compliant with the S-57, Appendix B1 ENC Product Specification. The checklist has been compiled for the IHO from lists of checks provided by a number of hydrographic offices and software companies.

It is the responsibility of the hydrographic offices to verify and validate the content and structure of all ENCs. In most instances ENCs are further validated by Regional ENC Co-ordinating Centres (RENCs) to ensure each country's ENCs are produced to a common standard in respect of quality and consistency.

Unfortunately most manufacturers have implemented these validation checks into their ECDIS software to varying degrees. A system carrying out the full suite of S-58 checks will have to cycle through all the checks for each ENC data set (base cells and updates). There are nearly 500 checks in S-58 some of which are quite complex and an ENC exchange set may have many thousands of ENC data files.

In July 2006 the IHB sent a letter to all manufacturers strongly recommending that they turn off/remove the S-58 validation checks (see ANNEX B). That is with the exception of those specifically identified for ECDIS and listed in the table below:

Checks Relating to ECDIS		
1	Check that the file extension is sequential until a new edition of the base set is issued.	Error
2	Check if DSID-UPDN is out of sequence.	Error
3	Check for proper usage of file extension, EDTN, UPDN, UADT and ISDT for re-issues of an ENC.	Error
4	Check that EDTN starts one higher than the previous edition number.	Error
5	Check that the file names of a base set and the re-issue are identical.	Error

S-63 Encryption

ENCs are encrypted according to the IHO S-63 Data Protection Scheme. There are three elements to the scheme As follows:

1. Authentication (Encrypted ENCs are signed). This provides assurance to the customer that the ENCs have come from a trusted source.
2. Encryption (ENCs are encrypted with a unique key). This prevents unlawful copying of and unauthorised use of the ENCs.
3. Licencing (Customer specific ENC Cell Permits). This allows selective access to only those ENCs that a customer is licenced for.

It is considered that these processes do not impact to any great effect on the performance of the ECDIS. When authenticating and decrypting ENCs prior to conversion to SENC there are only three validations to run as follows:

- Check each ENC signature file is compatible with the public key stored independently on the ECDIS and embedded in the IHO signed certificate.

- Check that an ENC permit is available for a given ENC and the unique encryption key can be extracted and verified against the hardware ID (dongle) of the ECDIS.
- Check that the extracted cell key will uncompress and decrypt the ENC.

Each of these processes is very linear in nature and subject to simple validation checks. It was always considered that S-63 did not unduly compromise the performance of the import process a view borne out by the OEMs. The following tests were carried out to confirm this opinion.

ECDIS Metrics Tests

The following tests were carried out to determine whether there was any impact on systems in respect of the following:

- S-63 Data Protection
- S-58 Validation
- Hardware resources and specifications

It is unknown to what extent each manufacturer has implemented the S-58 validation checks. What is known, judging by the log files generated, is that the C-Map kernel uses most if not all of them. The only real benchmark by which we can measure each system is the MARIS ECDIS900. This ECDIS only carries out those tests prescribed in S-58 for ECDIS and listed in the table above.

Test Data

VAR DMT supplied two exchanges sets, one encrypted the other unencrypted. These exchanges sets were based on AVCS Base 3 (issued WK17/10) and each contained 1230 GB ENCs. The folder and file structures for both encrypted and unencrypted exchange sets were identical, i.e. hierarchal.

Results

ECDIS Metrics Test				
ECDIS	**Unencrypted ENCs**	**Encrypted ENCs**		**Operating System**
MARIS	32 min	35 min	+3 min	SDRA Business PC (Windows XP SP2)
Furuno (FEA 2807-2007 version)	1hr 03 min	55 min	- 8 min	SDRA Business PC (Windows XP SP2)
MARIS	1hr 34 min#	1hr 24 min	-10 min	HP Compaq 6715b, Laptop (Windows XP SP2)
Transas	2hrs 11 min	2hrs 20 min	+9 min	HP Compaq 6715b, Laptop (Windows XP SP2)
SAM ChartPilot	2hrs 22 min	2hrs 28 min	+6 min	SAM Electronics ChartPilot (2009, running on Linux)
Furuno (FEA2807-2009 version)	2 hrs 31 min	2hrs 27 min	+ 4 min	Furuno FEA 2807 ECDIS (Windows XP SP2)
Kelvin Hughes (7Cs Kernel)	2hrs 50 min	2hrs 57 min	+ 7 min	Business PC running Windows 2000
JRC JAN-901B	3hrs 19 min	3hrs 24 min	+ 5 min	HP Compaq 6715b, Laptop (Windows XP SP2)
PC Maritime (C-Map Kernel) (Second Check)	10hrs 51 min	3hrs 17 min*	?	SDRA Business PC (Windows XP SP2)
PC Maritime (C-Map Kernel)	10hrs 58 min	3hrs 26 min*	?	SDRA Business PC (Windows XP SP2)

JRC NDI-2000	5hrs 29 min	5hr 33 min**	+ 4 min	JRC Hardware (Windows XP SP2)

* Includes 25 minutes copying encrypted data to the hard drive and 9 minutes decrypting it.
** This is an older JRC system (2007) the newer ones have removed the S-58 validation checks and are much quicker.
# the system dwelt prior to import while it prepared the charts for installation. This may account for the system taking longer to load unencrypted data.

Conclusion

It was not possible to test all the ECDIS on the same platform (OS) as some could only be run on the specific OEM hardware. Where it was possible to run the same system on different platforms it soon became obvious that the SDRA Business PC was the faster by far. This can be seen by comparing the MARIS and Furuno FEA 2807 results. The load times were significantly faster on the business PC than the laptop where the only real difference was the processors being used. ANNEX B identifies the properties of each computer.

Whilst it can be seen that the S-63 element does, in some instances, add some time to the import process it is not significant. Taking the worst case scenario of 10 minutes for 1230 ENCs that is only about half a second per ENC. With some systems this is considerably less and some imported encrypted ENCs faster than unencrypted. The reason for this is probably down to the method of import and how the ECDIS manages the import processes.

It is acknowledged that each ECDIS re-compiles the ENC data into its own proprietary SENC format. These different formats are unique to that system and are produced to optimise the performance of the ECDIS when the ENCs are being panned/zoomed and their associated screen re-draw times. This may have a limited affect on the conversion and import times.

It is known that the MARIS system does not carry out any of the S-58 checks and can import and convert the encrypted exchange set in 35 minutes. Compare this with the 3 hours and 17 minutes it took the C-Map kernel to complete the same processes on the same machine. It is worth noting that most of the other ECDIS used in these tests were faster than C-Map even though they were running on less resourced machines. The Furuno ECDIS was about an hour and a half slower than when the same software was run on the business PC.

To conclude, if the ECDIS manufacturers were to switch of their S-58 validation routines as directed by the IHB, this would significantly improve the load times and ultimately the customer experience.

Richard Coombes
ANPS
30th April 2010

ANNEX B

18th CHRIS MEETING
Cairns, Australia, 25-29 September 2006

IHB LETTER ON S-58 ENC VALIDATION CHECKS

IHB File No. S3/8151/ECDIS 20 July 2006

To: ECDIS System Manufacturers

Dear Sir,

It has been brought to the attention of the IHO that some ECDIS system manufacturers have mistakenly incorporated some or the entire suite of ENC validation checks listed in IHO publication S-58 - *Recommended ENC Validation Checks*. This has resulted in mariners being presented with misleading error messages indicating that officially produced and released ENC data contains errors, when it does not. In some cases, official ENC data is even being reported as not suitable for navigational use.

The purpose of this letter is to make it clear that the majority of the checks in S-58 are intended for use in the ENC validation software that is used by Hydrographic Offices or Regional ENC Coordinating Centres. **These S-58 checks were not intended to be used in ECDIS software.** The introduction to S-58 reads, in part "*…specifies the checks that, at a minimum, producers of ENC validation tools should include in their validation software. This software will be used by hydrographic offices to help ensure that their ENC data are compliant with the S-57, Appendix B1 ENC Product Specification...*"

Of particular concern are the S-58 checks classified as '*warnings*.' These checks are intended to highlight apparent discrepancies in the data so that HO's or RENCs can investigate them further. Upon investigation, the data will usually be found to be correct and no change to the ENC data is required. Such investigations are carried out by the ENC producer, as well as by the Regional ENC Coordinating Centre before the data is released. Once an ENC has been officially released, it is therefore not necessary or recommended that these checks be performed again by ECDIS software, since any warnings of this type that are generated will be incorrect and will be misleading for the user.

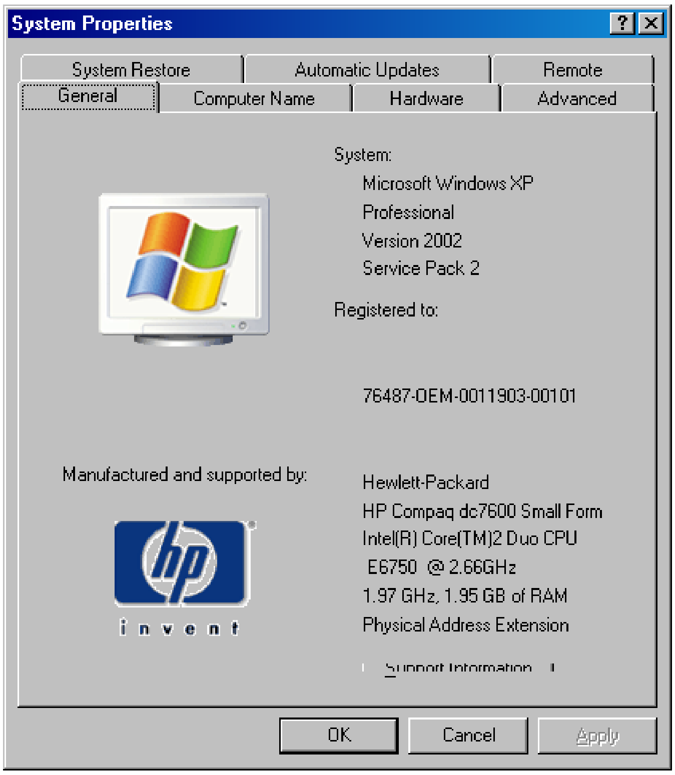
In section 2.3 of S-58 there is a short list of '*Checks relating to ECDIS*'. These are the only checks that are intended for incorporation in ECDIS software. If there are additional checks that ECDIS manufacturers feel are necessary for safe operation they should forward proposals to the IHO Transfer Standard and Application Development Working Group (TSMAD) for inclusion in section 2.3 of S-58. In this way, a single, agreed list of tests will be maintained.

In the meantime, it is strongly recommended that those ECDIS manufacturers who have mistakenly incorporated the S-58 checks intended for ENC producers should remove them from their software as soon as possible. The IHB or the established RENCs can provide further guidance to manufacturers on which ECDIS may be affected.

On behalf of the Directing Committee
Yours sincerely,
Rear Admiral Kenneth BARBOR
Director

ANNEX B

SDRA Business PC (XP SP2) using an Intel Core 2 Duo CPU



System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2

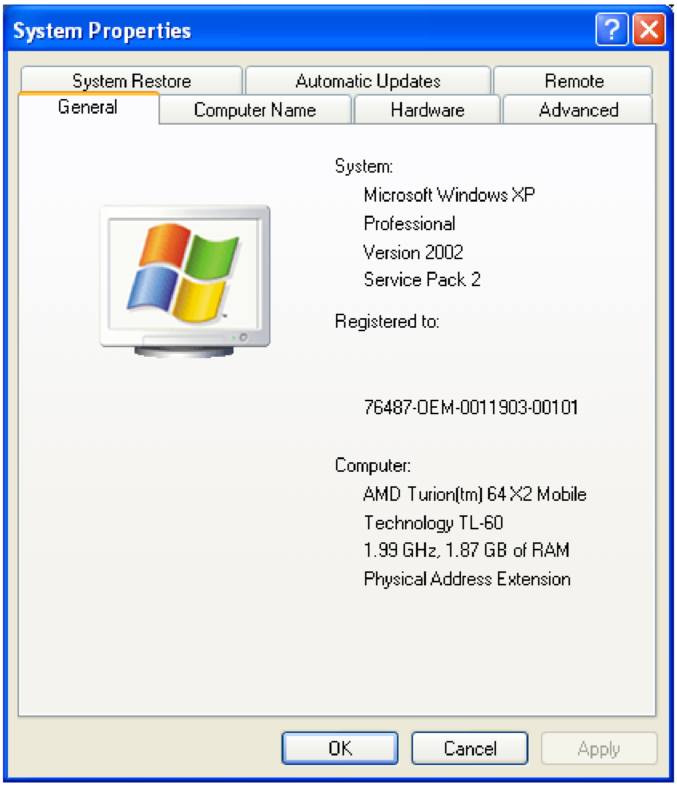
Registered to:

76487-OEM-0011903-00101

Manufactured and supported by:

Hewlett-Packard
HP Compaq dc7600 Small Form
Intel(R) Core(TM)2 Duo CPU
E6750 @ 2.66GHz
1.97 GHz, 1.95 GB of RAM
Physical Address Extension

HP Compaq 6715b, Laptop (XP SP2) using an AMD Turion 64X2 Mobile processor.



System:
Microsoft Windows XP
Professional
Version 2002
Service Pack 2

Registered to:

76487-OEM-0011903-00101

Computer:
AMD Turion(tm) 64 X2 Mobile
Technology TL-60
1.99 GHz, 1.87 GB of RAM
Physical Address Extension