From: [redacted]
To: [redacted] [redacted]
Subject: FW: Kongsberg Post Interview Pending Questions
Date: Monday, December 6, 2021 3:42:15 PM
Attachments: NTSB Questions Kongsberg OCT 2021 answered 2021-11-09.PDF

[CAUTION] This email originated from outside of the organization. Do not click any links or open attachments unless you recognize the sender and know the content is safe.

Gentlemen,

Ben and I just spoke, and he let me know there are outstanding written questions from NTSB that we (Kongsberg) have not answered. I apologize, but the only written questions from NTSB I can find in my file or my inbox are referenced below and answered in the attached. If there are others we have not answered, could you please re-send those questions?

Best,
Marc

Marc G. Matthews
Phelps Dunbar LLP
910 Louisiana Street, Suite 4300
Houston, TX 77002
Direct: [redacted]
Mobile: [redacted]
Fax: [redacted]
Email: [redacted]

CONFIDENTIALITY NOTICE - This e-mail message, including any attachments, is private communication sent by a law firm, Phelps Dunbar LLP, and may contain confidential, legally privileged information meant solely for the intended recipient. If you are not the intended recipient, any use, distribution, or copying of this communication is strictly prohibited. Please notify the sender immediately by replying to this message, then delete the e-mail and any attachments from your system. Thank you.

From: Marc Matthews (5275) <[redacted]>
Sent: Tuesday, November 9, 2021 3:09 PM
To: [redacted])' <[redacted]l>; MATHESON, ERIC <[redacted]>; FITZGERALD, DANIEL <[redacted]>; [redacted]; 'Christopher Ryan Paiz' [redacted]>; [redacted]

Cc: [redacted]; Case David <[redacted]>; [redacted]
(USA) <[redacted]>
Subject: RE: Kongsberg Post Interview Pending Questions

In advance of tomorrow's call, attached please find Kongsberg's written responses to the written questions/comments from the NTSB.

Marc G. Matthews
Phelps Dunbar LLP
910 Louisiana Street, Suite 4300
Houston, TX 77002
Direct: [redacted]
Mobile: [redacted]
Fax: [redacted]
Email: [redacted]

CONFIDENTIALITY NOTICE - This e-mail message, including any attachments, is private communication sent by a law firm, Phelps Dunbar LLP, and may contain confidential, legally privileged information meant solely for the intended recipient. If you are not the intended recipient, any use, distribution, or copying of this communication is strictly prohibited. Please notify the sender immediately by replying to this message, then delete the e-mail and any attachments from your system. Thank you.

National Transportation Safety Board

Washington, D.C. 20594

Questionnaire

Subj: Questionnaire / Information Request: NTSB investigation into the grounding of M/V *Commodore* at Bushwick Inlet, New York, on June 5, 2021.

Accident No.: DCA21FM029

To: Mr. Josef Bjurbäck
TPM Manager Controls
Kongsberg Maritime Sweden AB

Dear Mr. Bjurbäck,

Please find enclosed follow-up information request / questions based on your interview on Wednesday, October 20, 2021. The questionnaire is not for public release.

The questionnaire is investigative information of the National Transportation Safety Board (NTSB) created as part of the NTSB's investigation into the grounding of M/V *Commodore* at Bushwick Inlet, New York, on June 5, 2021 (NTSB Accident No. DCA21FM029).

NTSB regulations prohibit the public release of investigative information prior to release by the NTSB without the permission of the NTSB Investigator in Charge (IIC). See 49 C.F.R. § 831.13(c). The IIC has not approved public release of this information at this time. Therefore, we request that you refrain from any further dissemination of this questionnaire.

Kindly review this questionnaire and provide response by **November 10, 2021.** Requests for an extension of this deadline must be in writing and received prior to the due date.

Thank you in advance for your attention to this matter. If you have any question regarding the process, please feel free to contact me.

I look forward to your response.

Best Regards,

Luke Wisniewski

Sr. Marine Investigator
Office of Marine Safety
National Transportation Safety Board
490 L'Enfant Plaza East, S.W.
Washington, DC 20594
Office: [redacted]
[redacted]

Background

I obtained a copy of the disk images from all 4 screens involved in the accident and converted them to Linux compatible dd disk images. Commands similar to the following were used to mount the disks:

```
sudo losetup --partscan --find --show monitora.001
```

```
sudo mount -o ro,noload /dev/loop2p1 /mnt/image
```

I then also performed the following command while located in the root directory of the mounted filesystem to find the last 10 files written to:

```
sudo find . -type f -exec stat -c '%X %n' {} \; | sort -nr | awk 'NR==1,NR==10 {print $2}'
```

I also performed a general survey of the files contained on the SD Cards. I determined that the software system contained on the disk is a mix of Java, PHP and a C program or two.

Questions

After examining the system, I came up with the following questions and observations:

1. It looks like Linux paging is turned off? It can be difficult to contain Java and PHP's memory usage, and it's difficult to handle all out of memory conditions in either language. If virtual memory is turned off, these problems can be exacerbated. On the other hand, if virtual memory is turned on, swapping to an SD Card is not good for wear levelling.
2. Are logs cached in memory before being written to disk? This is related to the issue above. If memory is getting filled with logs, an exception will eventually get thrown.
3. Why did logs stop at noon, but system was working when they cast off at 4?
4. In the Java part of the system, how is an out of memory condition taken care of?
    a. Is Java's OutOfMemoryError exception handled properly?
    b. Is it exhaustively handled on a case-by-case basis?
5. The system logs don't seem to be turned on, this is probably a good thing for avoiding writing to the SD Card, but can't provide help when there are issues.
6. Ext filesystem on an SD Card – may defeat wear levelling for cards designed to use FAT or NTFS.
7. There are other logs that repeat:
   Warnlog:
    - [com.rr.gui.blackmetal.core.handlers.CANMANHandler] Polltime too short! …
    - [com.rr.gui.blackmetal.core.Config] Theme NONE not found!
    - [com.rr.gui.blackmetal.core.handlers.UDPAlarmProxy] Translation key 'alarm_46' not found in bundle

8. Master_eeprom.conf – This is a one byte file that seems to be written fairly often – it's one of the last files written to on all 4 images.
9. Sensord.rrd – might be a problem for wear levelling given its nature of overwriting old data, and it also writes once a minute. From looking at the configuration, sensord is just writing CPU temperature data, can this system be safely turned off?
10. Could there be concurrency issues? The logs look like there may be 2 screens fighting over what the current state is.
11. Can you keep this system running in a degraded mode if the SD Card goes away?
    a. A lot of embedded ARM controller boards have an onboard SSD, could you boot from that read only?
    b. and then write logs to the SD Card?
12. Canman System GUI log Service Report / Rev A /2021-06-23 /Page 7 of 7. The failure log tab was flashing red when investigators rebooted the system as part of the follow-up testing, however there was no audible alarm or acknowledgement of the failure code *"Port water jet system twin inner redundant steering encoder ON/OFF"* was required by the operator.
    a. Does an audible alarm activate when the timeout failure is reached?
    b. When a main station display is rebooted?
    c. or the when the CanMan application has stopped?
13. Please provide a list of the 7 vessels and technical service reports that have encountered display monitor reboots / memory leakage shutdown (without warning) for the Kongsberg Maritime (Rolls-Royce) Quad (4) Kamewa Waterjet, CanMan Touch Control Systems.
14. Please explain the program logic / coding and periodicity requirement for the GUI log recording the 200,000 entries for the failure code *"Port water jet system twin inner redundant steering encoder ON/OFF"* from June 1, 2021 to June 5, 2021.

<u>Kongsberg Maritime Response</u>

1. Virtual memory is an integral part of the Linux kernel and cannot be turned off. Assuming that virtual memory page swapping to disk was the intended meaning, then yes, the platform does not have page swapping enabled. A crash due to a major memory leak would likely only be delayed by adding swap space.

2. Which log is identified as the cause of the flash corruption? The CanMan LOG_RRx.dat would get a lot of writes as answer to question 8.

   GUI logs doesn´t cache. Logs from the Java GUI are handled using log4j, which allocates log buffers in RAM before writing to disk. These buffers are handled by Java garbage collection. Likely, for log buffers to occupy significant memory before garbage collection runs, logging must happen with a very high frequency, such as when logging in a loop. For details regarding the main C application log, see the answer to question 8.

3. Probably SD card malfunction at noon, CanMan operates in RAM. Reboot occurred at approx. 1600 hours and didn´t boot up since SD card was not functioning.

4. (a+b) We reserve a limited amount of heap for the GUI at start-up. No specific out of memory exceptions are handled by the GUI application. In case the PC runs low on memory it will be handled by the OS where the PC will be rebooted.

5. Yes. This is correct. System logs are only written to tmpfs in RAM.

6. How wear levelling is handled by the SD card must be learned from the SD card manufacturer.

7. These log entries are usually written at start-up. "Polltime too short" might occur once or twice a month e.g. during a larger garbage collection.

8. The main C application implements an EEPROM emulation scheme wherein log and parameter data is first written into two memory-mapped files in RAM (under /tmp/). To store this data to disk, the system alternates between two sets of files: PAR_RR1.dat/LOG_RR1.dat and PAR_RR2.dat/LOG_RR2.dat. The master_eeprom.conf file is used to store which of these file sets that are currently in use. Switching between the file sets happens maximum once per second only if the RAM files were changed. The maximum size of the RAM files is allocated at start-up and so it cannot grow over time. After switching between file sets, the RAM files are" backed up" to the selected file set on disk. It appears the entire log/parameter file is written to disk each time something in the RAM copy changes.

9. The sensord.rrd file is unused and can be disabled. This logs temperature and voltage within the screen. This is maintained within RAM memory and never written to disc.

10. We don't understand this question/statement. We ask NTSB to evaluate further or rephrase the question.

11. (a,b) No, we cannot run in a degraded mode. The present implementation was provided by our supplier. It may be possible to move the root file system to the on-board memory and only log to the SD card. The file system may have to be slimmed down to fit the 1 GB disk.

12. This needs closer investigation into the Java source.

A. No audible alarm for this type of failure. Audible alarms are triggered only for critical failures.

B. Yes, if a Main station is rebooting Control failure will occur and audible/visible alarm will be presented/sounding. Same information will be presented on all other screens.

C. Yes, If CanMan in a Main station stops there will be a Control failure and an audible/visible alarm also on all screens. If the CanMan application is stopped the Watchdog will order a reboot of the screen.

13. Files will be sent in a separate email distributed through Marc Matthews.
14.

Background

The CanMan controller (in this case CCN14 Touch screen) has a CAN bus aimed for the local I/O cards connected to the controller.
A I/O card is called SLIO (Serial Linked I/O) and has a number of analog and digital inputs/outputs.
There are three types of SLIO:s, SLIO01, SLIO02 and Horn Encoder.
The difference between the types of SLIO is the number/configuration of I/O:s.
A Horn Encoder is working as a SLIO with one analog input used for reading the feedback (reversing bucket or steering) of the water jet unit.
The SLIO CAN bus can consist of max 16 SLIO:s addressed 0-15.
A SLIO sends CAN messages on the SLIO CAN bus to the CanMan controller with information of values/status of the inputs on the SLIO.
The address of a SLIO is converted to a 11 bit CAN message ID specific for that SLIO (SLIO 15 will have CAN ID 957).
Each SLIO sends its CAN message cyclic with a maximum cycle period of 150ms.
The CanMan controller has a supervision function for each SLIO to see that the SLIO is alive. It has to receive a new CAN message from a SLIO at least every 400ms, otherwise it will indicate failure for that SLIO.

To split the CAN bus into different isolated parts, Gateways (Firewalls) are used.
A Gateway is a CanMan CCN11 controller which has three isolated CAN bus ports (A, B and S) and running with a Gateway application software.
The Gateway application software is working as follows: a CAN message received on one CAN port is transmitted on the other two CAN ports.
Once every second the Gateway is sending a CAN message with its own status on all the three CAN ports.
A Gateway is set up to transmit the status message with a specific CAN ID (11 bit) in the range 1850 to 1855. If more than one Gateway are connected on the same CAN bus they will have different CAN ID:s in this range.

”Port water jet system twin inner redundant steering encoder" failure going ON/OFF in GUI

The ”Port water jet system twin inner redundant steering encoder" is set up with SLIO address 15 (= CAN ID 957).
On the same SLIO CAN bus there are two Gateways, each with a specific CAN ID in the range 1850-1853.

After investigation of the software code in the CanMan controller and performing various tests on a test system with the same configuration as the Vessel Sea Streak Commodore 491 at our test lab, following have been found:

The decoding of the SLIO address from the CAN ID for the receiving CAN messages in the CanMan controller software gives a mismatch only for the SLIO with address 15.
This mismatch only gives a problem when the CAN connection between the SLIO with address 15 and the CanMan controller is lost.

The SLIO address is decoded by masking out four bits of the 11 bits CAN ID for the receiving CAN message.
A CAN message received from SLIO 15 and a CAN message received from any of the Gateways will have the same bit pattern in the CAN ID for these four masked out bits.
This means that the CanMan controller will interpret a CAN message received from the Gateway as has been received from a SLIO with address 15.
In the normal case when the CAN connection between the SLIO with address 15 and the CanMan controller is working ok without any problems nothing will happen, the system will work as normal.
When the CAN connection between the SLIO with address 15 and the CanMan controller is lost following will happen:

- The CanMan controller will not receive any CAN messages from the SLIO with address 15 (in this case, inner redundant steering encoder).
- After 400ms, SLIO supervision function in the CAN controller will set the failure indication for SLIO 15 to ON.
- The CanMan controller will receive a CAN message from a Gateway which will be interpreted to come from SLIO 15. The SLIO supervision function will then reset the failure indication for SLIO 15 to OFF.
- Since it will take more than 400ms until the CanMan controller receive the next CAN message from a Gateway, the failure indication for SLIO 15 will go ON again and will be ON until the next Gateway message received.
- The SLIO 15 failure indication ”Port water jet system twin inner redundant steering encoder" will then periodically go ON/OFF. The cycle time of the periodicity may varies due to timings in the system, for example on CAN bus, between CanMan application and GUI etc.

Conclusion

Our hypothesis is that the initial problem for the failure ”Port water jet system twin inner redundant steering encoder" going ON/OFF with a short periodicity and executing many writings to the log files, is that the CanMan controller has lost the connection to the “inner redundant encoder” i.e. SLIO 15.
Due to a mismatch of the SLIO address decoding CAN ID from Gateways in the CanMan controller the failure indication for SLIO 15 will go ON and OFF.
NOTE! The problem will only be for SLIO with address 15 and when the CanMan controller loses connection to the SLIO 15.

This encoder is only used for indication when the primary indication for control has any failure detected.

Josef Bjurbäck

Printed Name of Person providing the above information

[redacted]

Signature of Person providing the above information

2021-11-09
Date