National Transportation Safety Board
Office of Research and Engineering
Washington, DC 20594

DCA23FM036

UNDERWATER CAMERA

Specialist's Factual Report
October 18, 2024

TABLE OF CONTENTS

A. ACCIDENT

Location:	900 Nautical Miles east of Cape Cod, Massachusetts
Date:	June 18, 2023
Time:	0945 Eastern Daylight Time (EDT)
Submersible:	OceanGate Titan

B. UNDERWATER CAMERA SPECIALIST

Specialist	David Case Computer Engineer / Vehicle Recorder Specialist National Transportation Safety Board (NTSB)

C. DETAILS OF THE INVESTIGATION

In agreement with the Investigator-In-Charge, an underwater camera group was not convened and a summary was prepared.

The NTSB Vehicle Recorder Division received the following underwater video recorder:

Device Manufacturer/Model:	SubC Rayfin Mk2 Benthic Camera
Part Number:	Rayfin-MK2-HDE-6000-DBH13-LO
Device Serial Number:	SUBC21014

1.0 Device Description

The Subc Rayfin Mk2 Benthic is a camera designed to record video and still images underwater, up to a rated depth of 6,000 meters. Data can be stored to onboard memory, or to an attached computer, dependent on configuration.

The camera's body is made of titanium, and the camera's front optical window is made of synthetic sapphire crystal to protect the lens and electronics inside.

1.1 Data Recovery

The camera was recovered from the wreckage location and delivered to the Vehicle Recorder Laboratory. The camera's outer casing was intact (figure 1), but it was noted that the camera's lens, as viewed through the sapphire optical window, was shattered (figure 2).

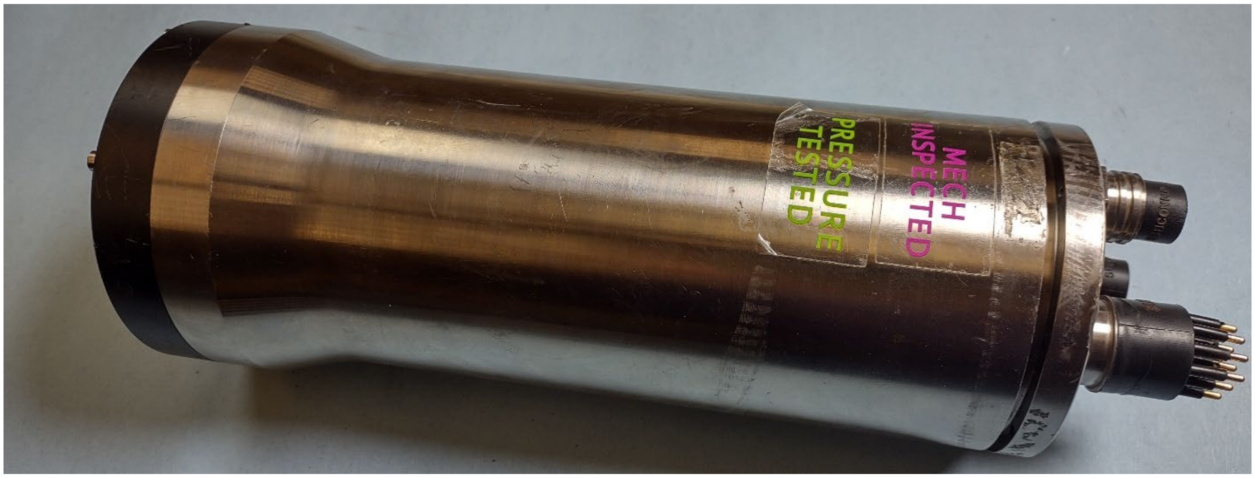

Figure 1. SubC Rayfin Mk2 Benthic camera, side view.

Figure 2. SubC Rayfin Mk2 Benthic camera, front view.

The outside casing was gouged but remained intact. The casing was carefully disassembled and an interior examination revealed the printed circuit boards were partially damaged (figures 3-4). The connectors, used to mechanically join the boards and pass electrical signals had sheared off. Several electrical components had also separated from the circuit boards.

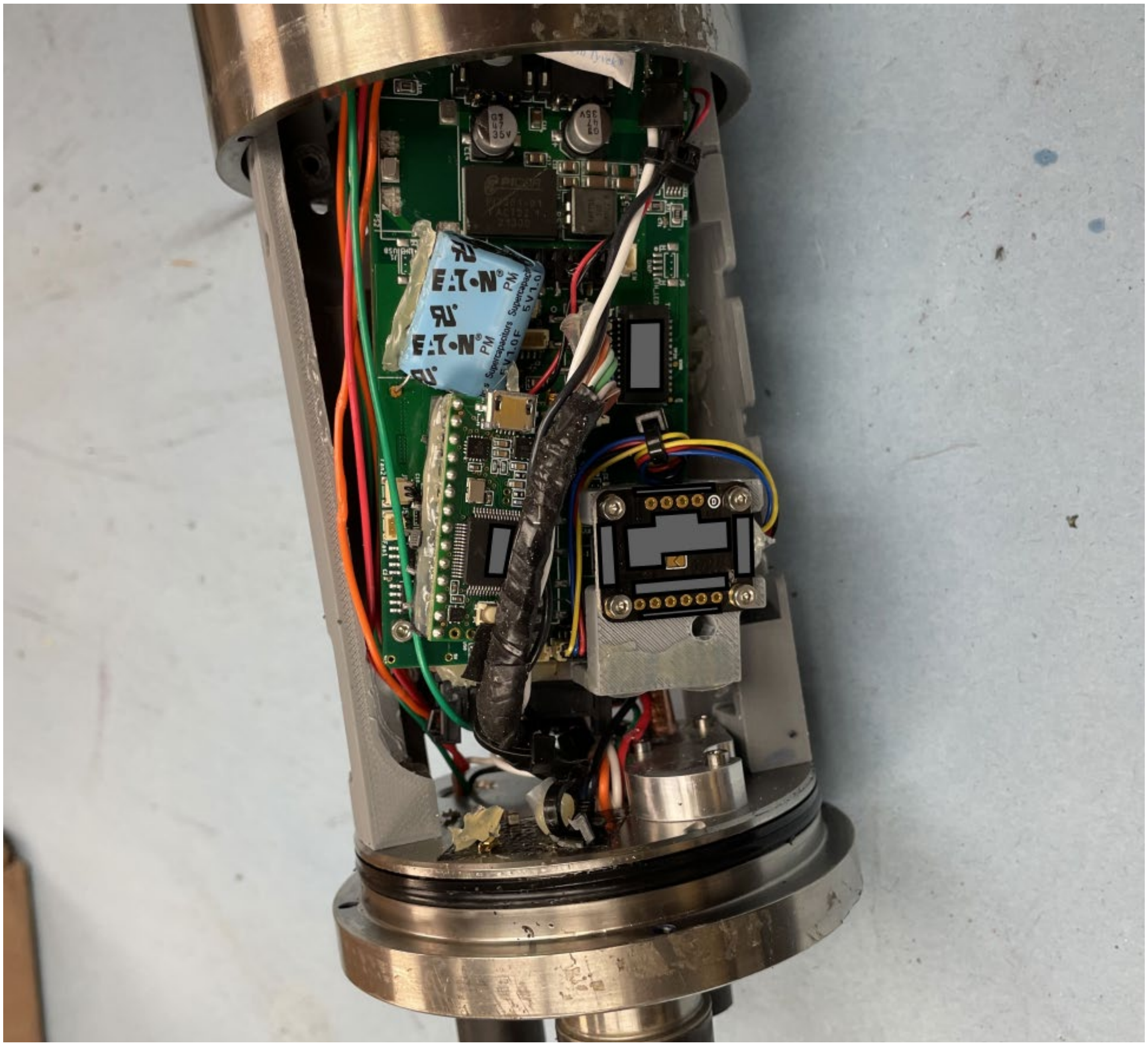

Figure 3. The camera's circuit board and electrical components, after removing the outer casing. The manufacturer of the camera had requested certain components of the device be redacted. Portions of this image have been redacted.

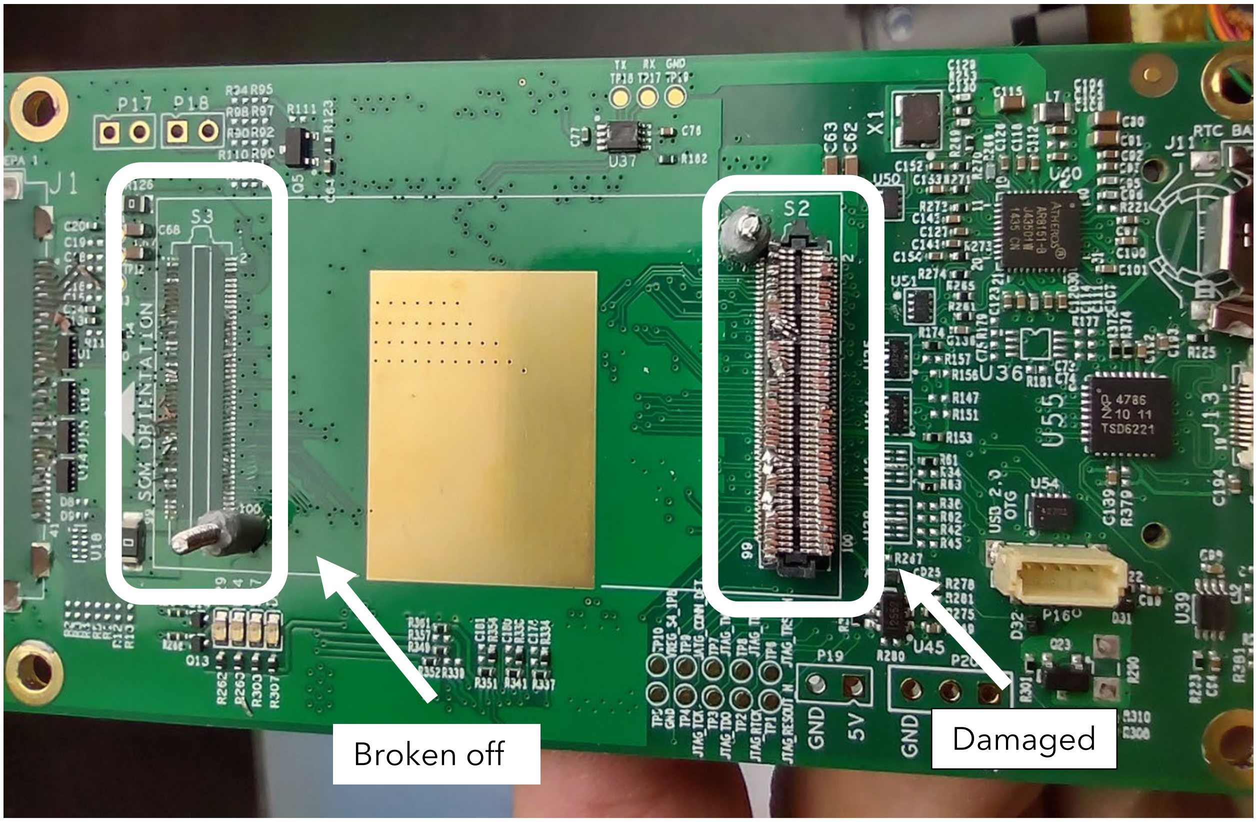

Figure 4. Broken off and damaged inter-board connectors.

Contained on one of the circuit boards, a Secure Digital (SD) memory card was found undamaged (figure 5).

Figure 5. Removed SD card. The manufacturer of the camera had requested certain components of the device be redacted. Portions of this image have been redacted.

An exact binary image of the SD card was made and examined with lab equipment. It was determined that the card was partitioned into a small area for holding operating system[1] updates before they were applied, and a much larger partition that was consistent with being fully encrypted.

Further examination revealed that the operating system version in the update partition was from 2016, and would typically have used File Based Encryption (FBE[2]) to encrypt it's user data partition. The larger partition on the card was encrypted similarly to Full Disk Encryption (FDE[3]), which is an older encryption method used by versions of the operating system from this same time frame. FDE is implemented using the Linux Unified Key Setup (LUKS[4]) system, however, there was no LUKS

[1] The camera manufacturer, Subc, has requested that the actual name of the operating system not be mentioned for trade secrecy. It will be referred to here as 'the operating system'.

[2] File based encryption is where the files are encrypted, but the file system is not. You can still mount the filesystem and get a list of filenames, sizes, etc. but the files themselves are unreadable unless decrypted.

[3] Full disk encryption means the entire partition is encrypted, including the directory information. You cannot mount the filesystem without the key.

[4] LUKS is a standard for marking an encrypted partition with an unencrypted header that provides

header found. Since the partition was fully encrypted, it was likely the file system was encrypted through a custom configuration using dm-crypt[5]. The dm-crypt configuration requires the use of a decryption key that is either stored separately from the encrypted partition or entered by the user of the device.

SubC Imaging initially confirmed that camera data were stored on the SD card, and they could download the data from the accident card at their office in Canada. However, SubC determined that they were unable to perform this download procedure using their own test card removed from a camera and placed in a surrogate camera of the same model.

The encryption key for the camera could not be found on the SD card, and the SD card did not contain the boot partition for the camera. The circuit boards were examined, and a System-On-Module (SOM) board was found. SOM's are a popular product for small companies that wish to make a device that needs significant computing resources without having to spend thousands of hours designing a complex small computer on their own. The SOM contained a Central Processing Unit (CPU or microcontroller), Random Access Memory (RAM), and a Non-Volatile[6] Random Access Memory (NVRAM) chip for permanent storage on a premade circuit board (figure 6). Software and documentation to make the board function is generally provided by the SOM manufacturer as part of a Board Support Package (BSP[7]).

---

information about the encrypted partition. It contains details on what cipher and hashing function are being used.

[5] dm-crypt is the Linux subsystem for encrypting file systems that is also available in the operating system used on the device. dm-crypt provides many options for encrypting a file system, including whether or not you use a LUKS header.

[6] Non-volatile memory is a type of computer memory that is retained if the device is turned off. It typically contains the software needed to run the device and is also typically used to permanently store data. On this particular device, the NVRAM stored the operating system, the camera software, and all the configuration information needed to run the camera. The data generated by the camera was stored on the SD Card.

[7] A BSP is typically provided by the SOM manufacturer as a set of documentation, software, and hardware. They get the operating system working on the device and provide that preloaded onto the SOM board. The hardware part of the package is typically an SOM with the operating system preloaded and a second circuit board with extra circuitry needed to make the SOM function (typically a power supply and connectors for peripherals).

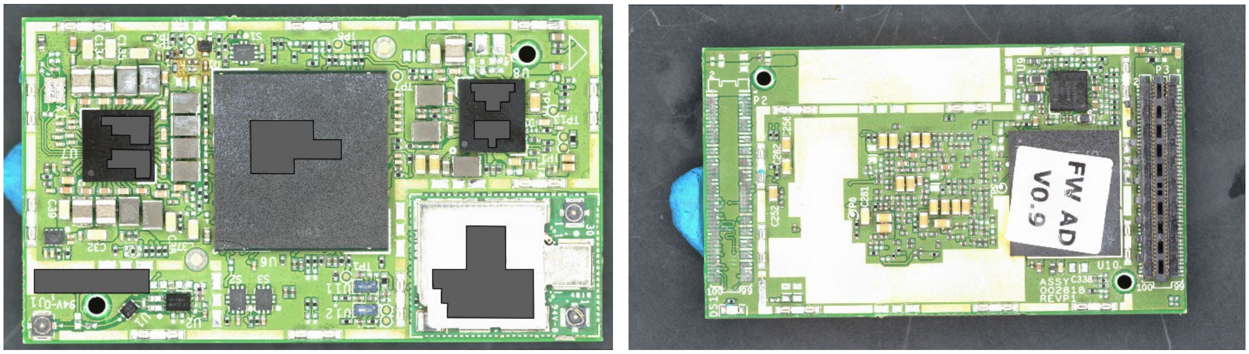

Figure 6. SOM top view (left) and bottom view (right). The manufacturer of the camera had requested certain components of the device be redacted. Portions of this image have been redacted.

The SOM showed signs of being damaged in the accident. There was a crack in the CPU chip, the inter-board connectors and several passive electronic components were broken or had snapped off (figures 6-7).

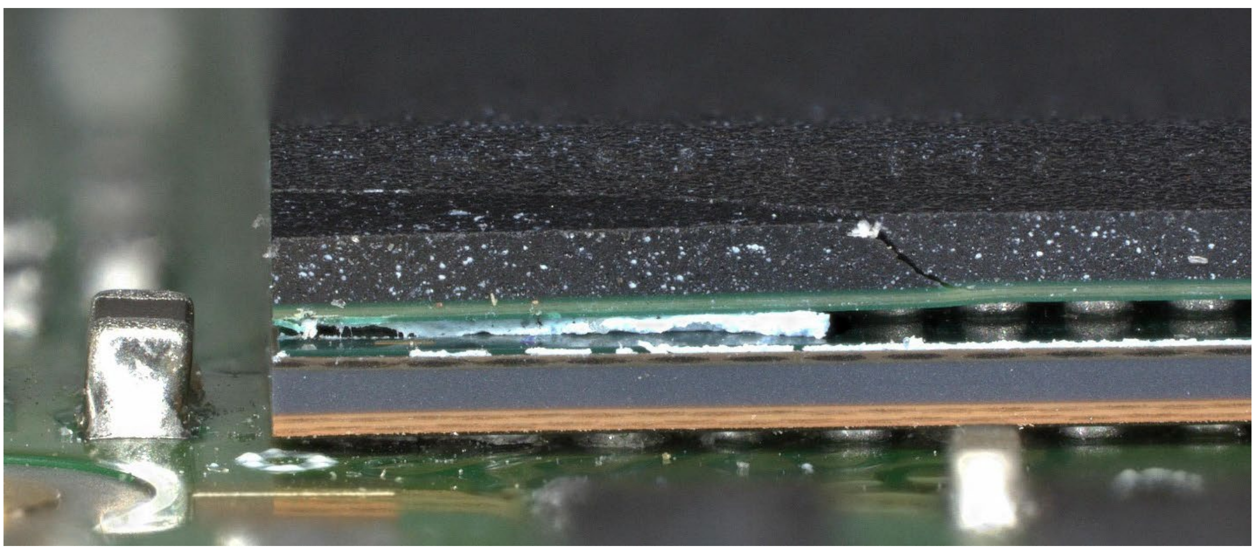

Figure 7. The broken corner of the top die of the microcontroller on the SOM board.

It was likely the camera manufacturer may have never attempted to read the SD card directly, since that would require disassembling the camera, which would add wear on the water protection seal. Therefore, the SD card would always have been accessed by a device connected to the back of the camera using an interface cable. In this process, the operating system may encrypt and decrypt data without the camera manufacturer's knowledge.

Depending on configuration, the keys would be stored either on the NVRAM, or as part of a system called TrustZone[8] that stores encryption keys directly on the

[8] TrustZone is a complex web of technologies that in the context of this report could be used to hide the cryptographic key for the SD Card. This would effectively mean that the key would be stored on

CPU. Keys in the TrustZone would generally be irretrievably lost, given the broken status of the CPU.

The SOM board manufacturer was contacted, and they said that they provided a sample operating system install with the boards when they shipped them, and that they did not knowingly set up encryption for the user data partition. They also confirmed that any keys stored would be either on the NVRAM chip, or in the CPU's TrustZone.

Two likely paths to get at the data on the SD Card were postulated. One method would be to read the contents of the NVRAM chip on the SOM, look for a key, and then use that key to decrypt the data (the Software Route). The other method would be to move the NVRAM's contents to another SOM module and attempt to boot off of the accident's NVRAM on that device (the Hardware Route). The software route was problematic because it could be time intensive, and the hardware route was difficult because it would require the chips to be programmed and soldered on to a new board, which increases the risk of the activity, and the new NVRAM was not guaranteed to be compatible with the surrogate SOM.

Lab equipment was used to remove the NVRAM chip from the SOM (Figure 8). It was determined that the chip was not a standard eMMC flash device, but used another technology called Universal Flash Storage[9] (UFS). The SOM manufacturer was consulted, and a chip reader that would work with a UFS device was purchased. The chip was successfully read with the UFS reader, and it was determined that the contents of the NVRAM were not encrypted, but the key for the SD Card was likely hidden in files that were generated by the CPU chip manufacturer, who was reticent to supply the tools to decode the information.

---

the CPU and could only be used to decrypt the data if the physical CPU from the accident was used.

[9] Most of the similar devices we see use eMMC flash memories that are electrically identical to an SD card and can easily be read with standard lab equipment. UFS is a newer standard designed to replace eMMC and this is the first one we have seen.

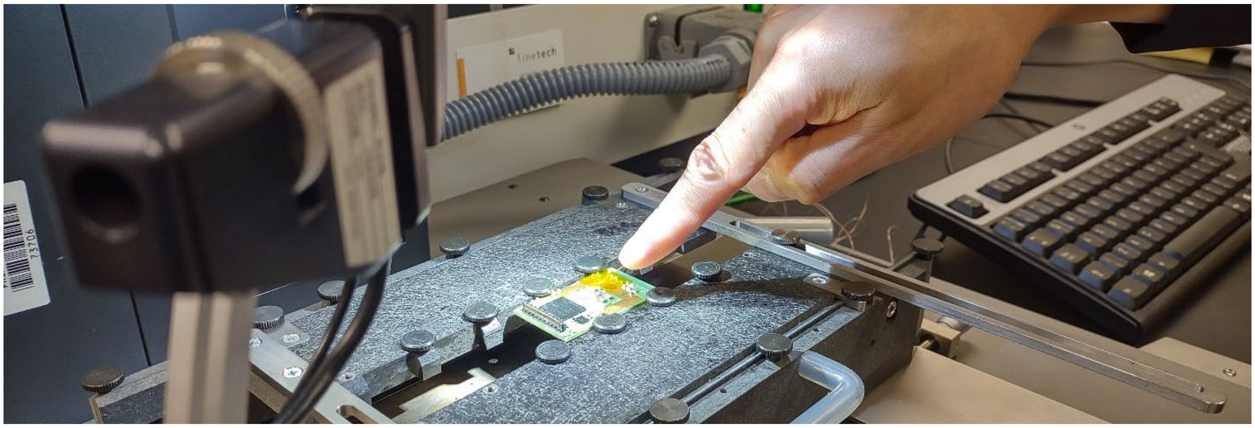

Figure 8. Preparing the NVRAM chip to be removed from the SOM board.

After obtaining a good copy of the data on the NVRAM chip, it was determined to focus on the hardware route as a means of practical data recovery. The camera manufacturer was contacted and said they would provide a surrogate SOM board to put a copy of the NVRAM on, but did not provide ancillary equipment needed to make the board work.

A phone meeting with SubC and the Canadian Transportation Safety Board (TSB)[10] was convened, and during the resulting conversation, it was determined that SubC thought the data was not encrypted, but simply in a file system that they couldn't figure out how to access.

The camera manufacturer was supplied with the methodology used by the NTSB to determine if the data on the SD Card were encrypted. After deliberation, SubC agreed that the data on the SD Card were encrypted. SubC also agreed that if the key was stored in the NVRAM, we should be able to decrypt the SD Card using the NVRAM chip on a surrogate SOM board.

With the cooperation of the TSB and SubC, an agreement was made for the surrogate SOM board to be taken to SubC's Clarenville, Newfoundland office to attempt a read out of data using SubC's equipment to be performed in conjunction with both the NTSB and the TSB.[11]

Two SOM boards were populated with a new NVRAM chip; one with a copy of the original NVRAM chip, and one with the original accident NVRAM chip. Two SD

[10] "The TSB is an independent Canadian agency and is conducting its own independent investigation into this occurrence. NTSB consulted the TSB as the TSB has jurisdiction in Clarenville NL where SubC is located.

[11] Thank you to both SubC and the TSB's Newfoundland office for all the support provided.

Cards were also flown to Clarenville, the original, and a byte-for-byte copy using the same manufacturer and model of SD Card.

The copied NVRAM and SD card were connected to the manufacturer's hardware, and the data on the SD card were successfully downloaded using the manufacturer's procedure (figure 9).

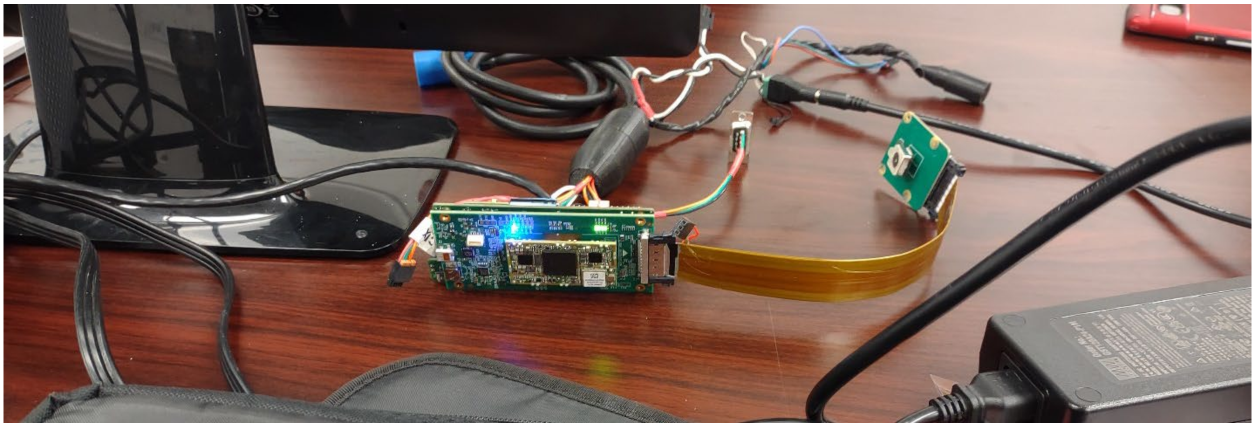

Figure 9. Device being downloaded in Clarenville

1.2 Device Recording Description

12 still images and 9 videos were recovered from the device.

2.0 Image/Video Files Information

The Rayfin camera stored still images at a resolution of 4056x3040 pixels, and video with a resolution of 3840x2160 pixels at 25 frames per second (figure 10).

Recorded imagery data were stored on the SD card built into the camera, and in regular use would be retrieved through the download cable interface over an ethernet connection. Figure 10 is an image recovered from the camera.

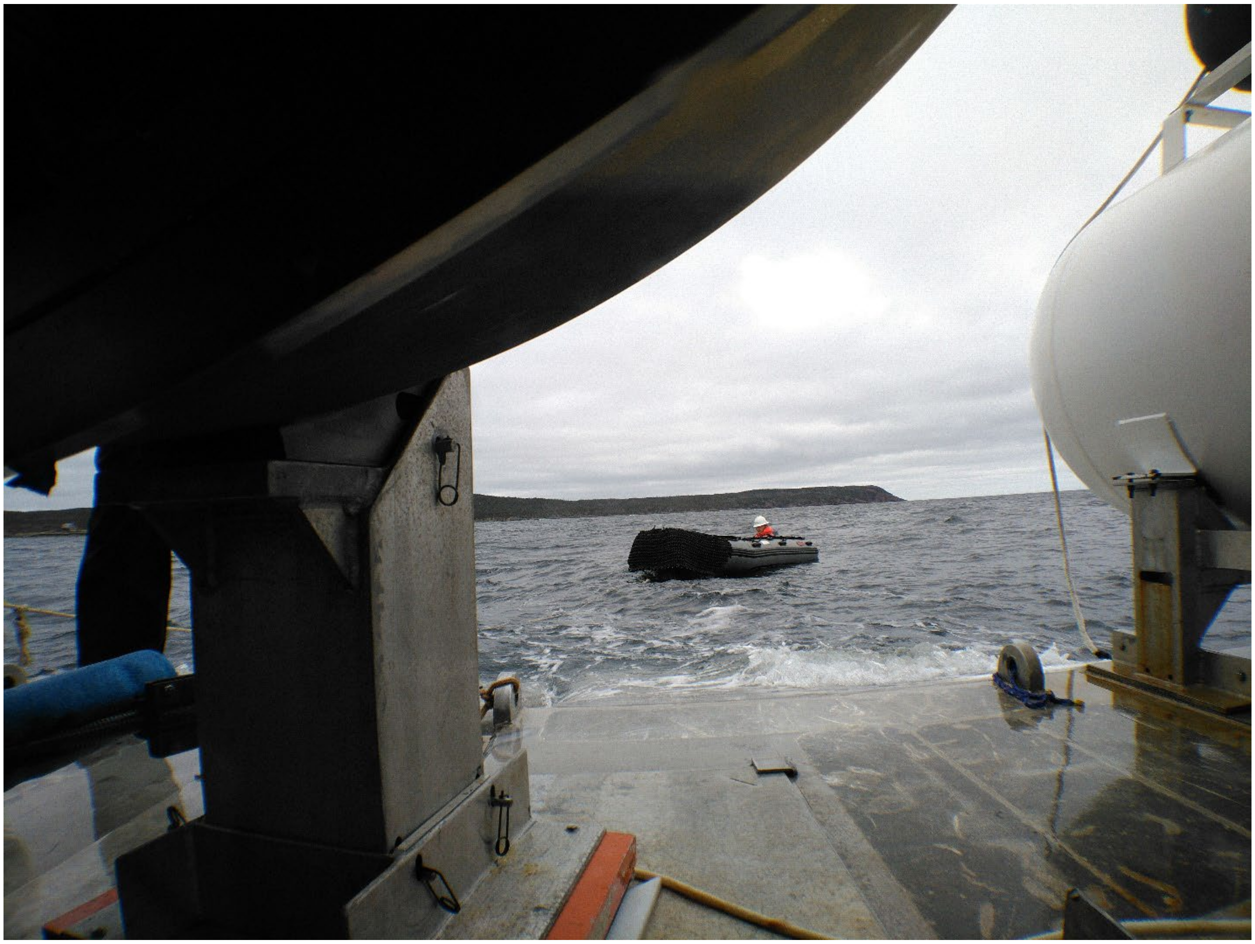

Figure 10. Image from the SubC camera showing the camera field of view.

3.0 Timing and Correlation

The camera was designed to acquire the current time from an attached computer through the Network Time Protocol (NTP). If a computer was not attached to the camera, the camera would set the time to midnight, January 1, 1970, Coordinated Universal Time (UTC).

The files were written with the time zone set to Newfoundland Daylight Time (NDT), which is UTC minus 2 hours 30 minutes. The files were mostly written within a few minutes of the camera being turned on, so the invalid timestamps are mostly in the last hours of 1969.

Two files on the SD card were given valid time stamps. The first file is a video, consistent with being taken on the quay at Holyrood, Newfoundland, showing the rear wheel and stabilizer arm of a crane taken on May 10, 2023. The second file is an image taken at sea on May 16, 2023. A 5-gallon bucket and the toe of a work boot was in the field of view (figure 13).

Three images without timestamps taken on the quay at Holyrood show a boat, the Research Vessel (RV) *Ludy Pudlak* sitting on blocks on the quay (figure 11). Automatic Identification System (AIS) data were found for the *Ludy Pudlak* during the timeframe when the Oceangate Titan was in Holyrood and only one GPS position was reported as being on the quay, which likely confirms these images were taken the morning of May 5, 2023.

Figure 11. Image taken on the quay at Holyrood, the *Ludy Pudlak* can be seen behind the LARS placed out of the water on blocks.

Three videos were taken underwater, all with similar lighting conditions and the immediate environment around the camera being the same. The Launch and Recovery System (LARS) can be seen, and light is filtering down from the surface.

OceanGate was able to identify the diver in the video from his diving suit and gear. This diver was only involved in Missions 1 and 2 of 2023, and was only present for shallow water training, likely near Bay Bulls Newfoundland. The accident dive was 2023 Mission #5.

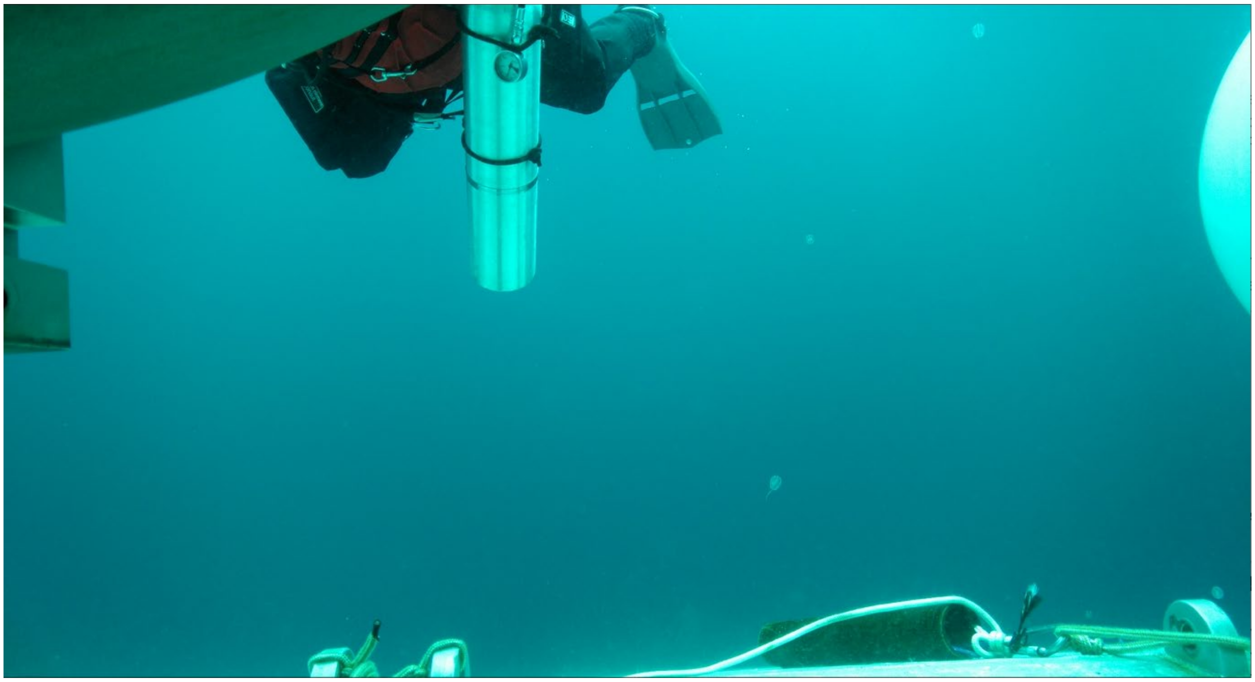

Figure 12. Still image taken from underwater video, showing the diver.

Three videos were also taken in the Marine Institute main campus ROV shop. The time of recording could not be determined (figure 13).

Figure 13. The Titan sitting in the ROV shop at the Marine Institute.

3.1 Timing and Correlation Note

The camera stored still images in a directory named 'Stills', and video in a directory named 'Videos'. One still image was stored in a different directory:

```
mnt/nas/Stills
```

SubC was consulted, and they had seen this behavior before. The camera can be configured to store data on a connected device, and not to internal storage. If the external device was not connected, or the path to the connected device was incorrectly entered, the camera would create all the directories needed to store the images wherever the user configured to put them. The file system on the camera stores all files in the same tree, so mounted network file shares are indistinguishable from the local filesystem from the camera software's perspective.

It is likely that the camera was being configured to store its data to the onboard computer on May 16th, with one image being stored accidentally to the camera's SD Card and then configured properly to store data to the computer on board the submersible (Figure 13). No data with a timestamp after May 16th was found on the camera, so it is likely that none of the data recorded on the SD Card were of the accident voyage or dive.

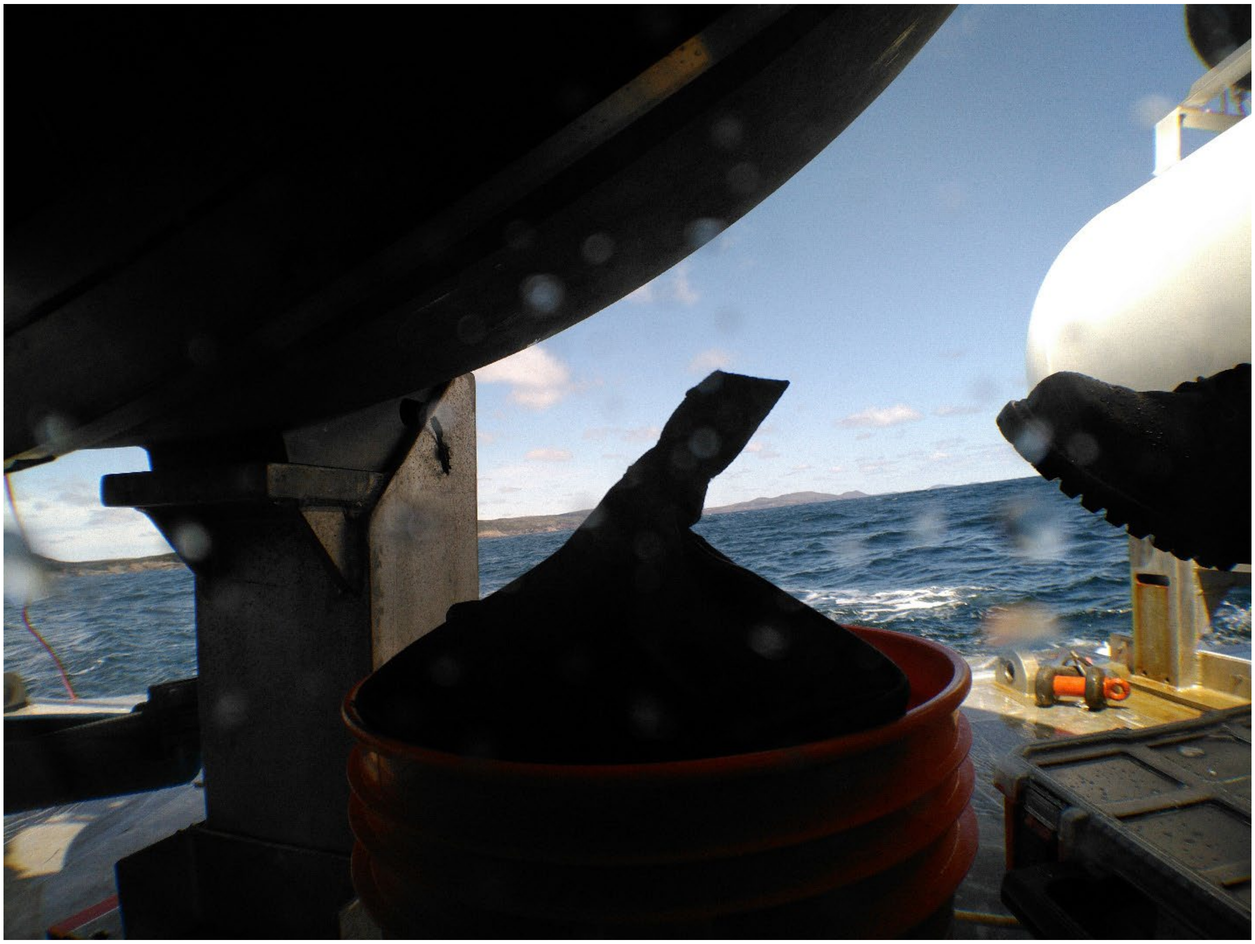

Figure 13. The last image stored to the SD card with a timestamp on May 16, 2023.

Submitted by:

David L. Case
Computer Engineer / Vehicle Recorder Specialist