Vertical Entry Robot for Navigating Europa
--VERNE--

Mission Operational Concept

Phillip Szot, GT SSDL	Lead Systems Engineer
Dr. Britney Schmidt, GT EAS	Principal Investigator
Dr. Glenn Lightsey, GT SSDL	Co-Investigator

Abbreviations and Acronyms:

COM – Communications

CDH – Command and Data Handling

EPS – Electrical Power System

GNC – Guidance, Navigation and Control

PAY - Payload

SCI – Science System

SHS – Sample Handling System

STR – Structures

SYS – Systems Engineering

VERNE – Vertical Entry Robot for Navigating Europa

Table of Contents

Table of Figures

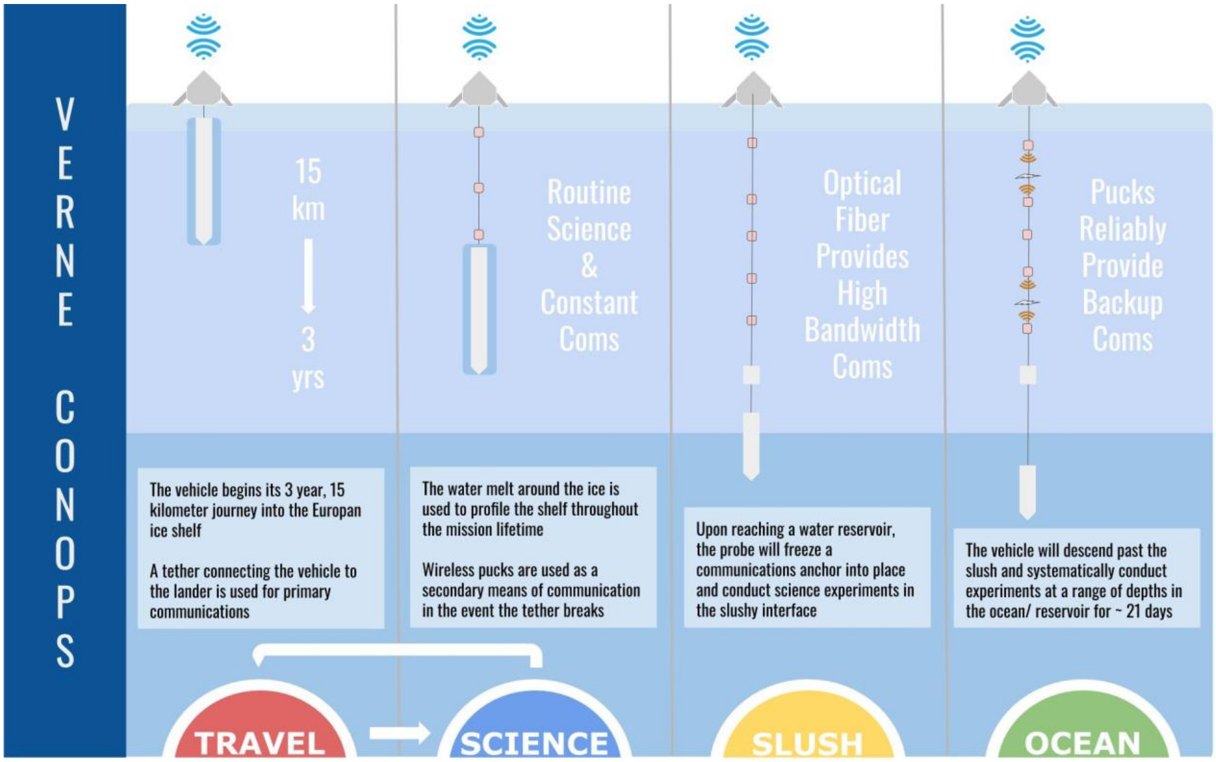
Table of Tables

Document Scope:

VERNE is currently in the mission concept study phase and is not a mission contracted for launch and operations, but this document focuses on the operational challenges and definitions that would be necessary for the design team to address if VERNE were to continue past this initial concept study.

Mission Overview

The goal of the Vertical Entry Robotic Navigation of Europa (VERNE) mission is to explore the ice shelves and water reservoirs of Europa in support of the search for signs of life. Europa is widely regarded as one of the best candidates in the solar system for finding past or present signs of life. As new technologies are matured over the coming decades, this type of mission becomes possible. It is the goal of this mission concept study to establish a vehicle and mission architecture that maximizes the likelihood of overall mission success from landing to end-of-life. This study will highlight modern day technologies that will enable the mission to be completed as well as highlight technology gaps that need to be filled before this type of mission will be fully possible. This mission concept study is being performed for the Subsurface Access Mechanism for Europa (SESAME) program [5]. Under the terms of this concept study, VERNE will already have been provided with the necessary support to proceed from launch to landing on Europa. Once landed, the probe will travel toward the under-ice water reservoirs, conducting life finding science and geochemistry measurements both along the way and at the ice-ocean interface. This is highlighted in the Mission CONOPS Diagram shown in Figure 1. This mission will be the first of its kind, so novel architecture and new subsystem designs are a necessity.



The vehicle begins its 3 year, 15 kilometer journey into the Europan ice shelf

A tether connecting the vehicle to the lander is used for primary communications

The water melt around the ice is used to profile the shelf throughout the mission lifetime

Wireless pucks are used as a secondary means of communication in the event the tether breaks

Upon reaching a water reservoir, the probe will freeze a communications anchor into place and conduct science experiments in the slushy interface

The vehicle will descend past the slush and systematically conduct experiments at a range of depths in the ocean/ reservoir for ~ 21 days

Figure 1. Mission CONOPS Diagram of VERNE [1]

Mission Timeline

The following is a possible timeline for all phases of the VERNE mission, including the work that is currently being done in Spring 2020. It is meant to capture realistic technology development times and vehicle/mission preparation time, with reasonable contingencies built into the timeline.

Pre-Phase A

This document is being written at the end of the first year of the mission concept study. The goals are to complete an initial system design while identifying technology gaps that need to be closed. This task was completed in preparation for the Mission Concept Preliminary-Design Review in April 2020. The next year will be spent conducting technology development on a small number of critical hardware items that the study team will address. This may include the communication pucks, the profiler, or other areas that are currently being developed. Pre-Phase A will complete at the end of the mission concept study, which is planned for Spring 2021.

Phase A

Once Pre-Phase A is complete, if the project is continued into the next Phase, a project plan will be defined where the exact developments of the continuing work will be highlighted and what staffing and facilities will be necessary to complete the mission will be defined. Necessary external technology developments will also be established. The mission and design requirements will also be reviewed and finalized at this time. An updated Work Breakdown Structure will be used to establish the workload responsibilities for all subsystems and sub-subsystems.

Phase B

Necessary technology developments will take place to build and test a full system prototype where each subsystem will be prototyped (1:1) with modern day technologies to better identify architectural issues and technology gaps. This prototype could be tested in an Earth analog environment such as Antarctica. It will also be necessary to fully down select which instruments VERNE will be carrying in order to complete the interface design between the payload and the rest of the vehicle.

Phase C

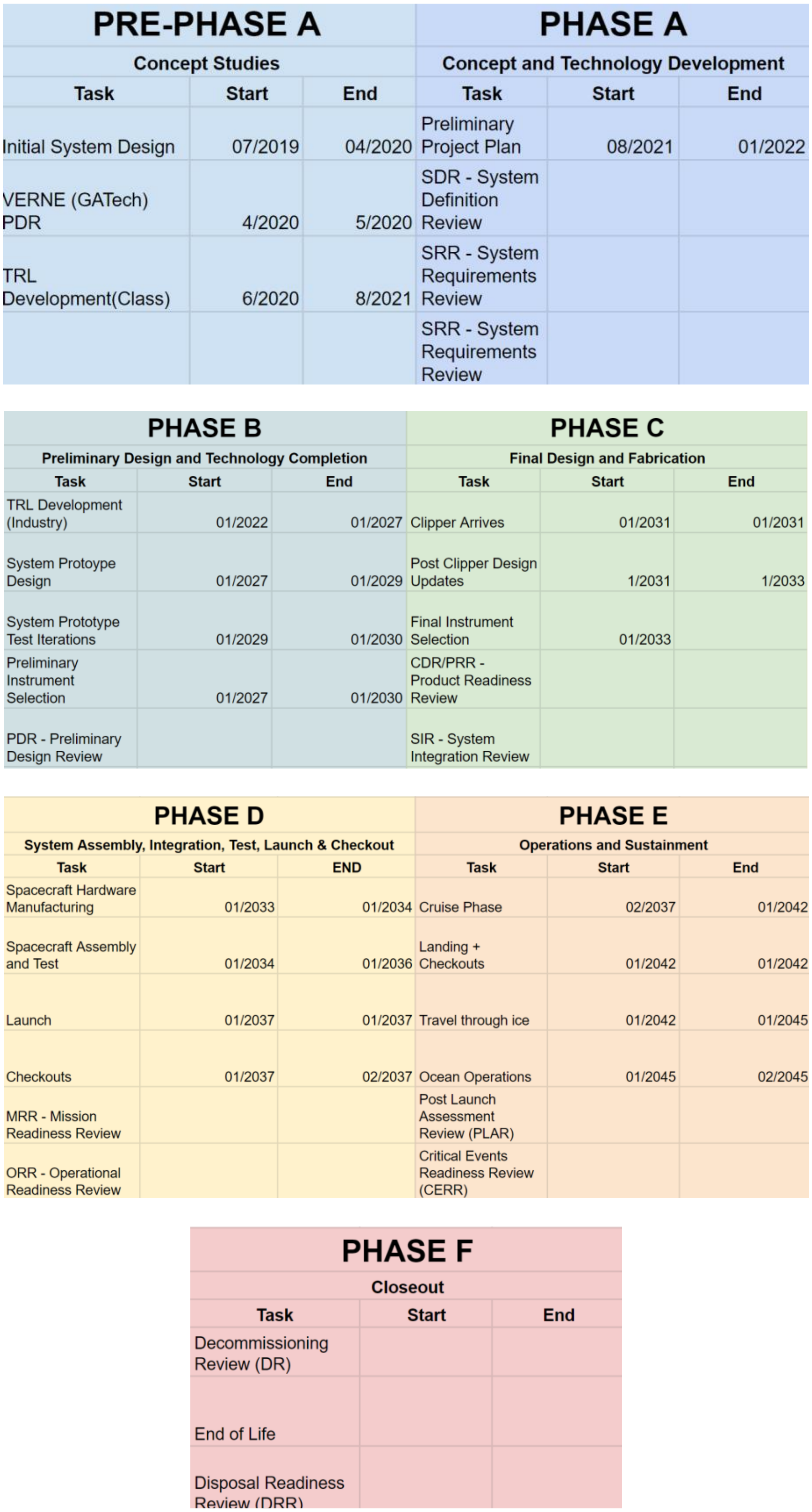
Europa Clipper is expected to arrive and reveal data relevant to VERNE in 2031. These data could instigate design changes and perhaps even architecture changes to VERNE, so the timeline includes additional time to accommodate these changes. For example, Clipper may reveal that there is no ice shelf landing zone with a thickness less than 20 km. Since the design is built to 15 km max, the design would have to be reworked to accommodate 5 km more tether and pucks to close the COM design.

Phase D

Once the design is finalized after reviewing Clipper data, the spacecraft and its hardware will then be manufactured, assembled, and tested, which should take about 3 years to complete. This is the mission Phase that unexpected slips can occur in the timeline, which is typical for a flagship mission such as VERNE. Disregarding any time slips, this schedule poses a realistic launch date of 2037.

Phase E and F

Post launch and Earth escape maneuvers, a five-year cruise to Jupiter can be expected, with VERNE landing on Europa in 2042. With a successful landing, VERNE will begin its 3-year journey into the ice shelf conducting science until VERNE reaches the underwater ocean reservoir where it will conduct ice/water interface science along the way until end of life in 2045. The water profiling science is expected to last around 3 Jovian tidal cycles, or about 21 Earth days. It is possible that profiling science mode is continued if the vehicle health allows it, but it is not considered necessary for full mission success.



PRE-PHASE A			PHASE A		
Concept Studies			Concept and Technology Development		
Task	**Start**	**End**	**Task**	**Start**	**End**
Initial System Design	07/2019	04/2020	Preliminary Project Plan	08/2021	01/2022
VERNE (GATech) PDR	4/2020	5/2020	SDR - System Definition Review		
TRL Development(Class)	6/2020	8/2021	SRR - System Requirements Review		
			SRR - System Requirements Review		

PHASE B			PHASE C		
Preliminary Design and Technology Completion			Final Design and Fabrication		
Task	**Start**	**End**	**Task**	**Start**	**End**
TRL Development (Industry)	01/2022	01/2027	Clipper Arrives	01/2031	01/2031
System Protoype Design	01/2027	01/2029	Post Clipper Design Updates	1/2031	1/2033
System Prototype Test Iterations	01/2029	01/2030	Final Instrument Selection	01/2033	
Preliminary Instrument Selection	01/2027	01/2030	CDR/PRR - Product Readiness Review		
PDR - Preliminary Design Review			SIR - System Integration Review		

PHASE D			PHASE E		
System Assembly, Integration, Test, Launch & Checkout			Operations and Sustainment		
Task	**Start**	**END**	**Task**	**Start**	**End**
Spacecraft Hardware Manufacturing	01/2033	01/2034	Cruise Phase	02/2037	01/2042
Spacecraft Assembly and Test	01/2034	01/2036	Landing + Checkouts	01/2042	01/2042
Launch	01/2037	01/2037	Travel through ice	01/2042	01/2045
Checkouts	01/2037	02/2037	Ocean Operations	01/2045	02/2045
MRR - Mission Readiness Review			Post Launch Assessment Review (PLAR)		
ORR - Operational Readiness Review			Critical Events Readiness Review (CERR)		

PHASE F		
Closeout		
Task	**Start**	**End**
Decommissioning Review (DR)		
End of Life		
Disposal Readiness Review (DRR)		

Figure 2. Full Mission Timeline of VERNE

Mission Operational Modes

There are many mission modes that will be necessary to achieve full mission success. All mission modes are described in detail below. In Table I, each subsystem function for each operating mode is provided. In Table I, the darker gold boxes signify which subsystems are performing the majority of the functions in that mode while the lighter gold boxes signify limited function from that subsystem.

Start of Mission Mode

The mission begins once VERNE is securely on the surface of Europa in the desired vertical orientation with the drill in contact with the icy surface. GNC will require more power than nominal because it will have to mechanically penetrate the ice. This is because of the extreme cold expected at the surface, which will cause the surface to be harder than steel by current estimates. Penetrating the ice, releasing the optical COM tether, and securing the vehicle into the ice will be the main focus of this mode. At this time, all other priorities are secondary.

Travel Mode 0 -> 15 km

This mode will run in a repetitive sequence with Science - Ice Profiling, Communications, and Obstacle avoidance. When in travel mode, VERNE will be thermally drilling into the ice while running the obstacle detection sensors. COM will continue to spool out the tether and provide telemetry to the lander. If the Payload system has samples or data to analyze, it can do so without a high-power demand. It is also possible that the Sample Handling System will take continuous samples throughout the entire travel mode.

Science - Ice Profiling Mode

At regular intervals (every 250 m), VERNE will take and analyze discrete samples through the instruments. EPS will divert the necessary power to each instrument to enable nominal operations, even if this means off nominal power for other subsystems. This will create many large data packets of raw and processed payload data that will be managed by the Command and Data Handling system.

Comms Mode

Data that should be transmitted to the lander will be communicated internally up to the COM computer, which will then transmit data up the optical communications tether if it is fully intact. If there is a break, the vehicle will still transmit up the tether until the last puck before the break. The puck will use internal power to cross the gap of the break, and the receiving puck will send the data via tether up to the lander. This architecture supports multiple breaks. The necessary power will be diverted to ensure communication with the lander during this mode.

Obstacle Avoidance Mode

In the event that the GNC system detects an obstacle, the vehicle will decide if the obstacle is avoidable. If the vehicle is far enough to turn and avoid the obstacle, then it will initiate obstacle avoidance mode. A maneuvering system (i.e. hot water jets, skates, etc.) will torque the vehicle, slightly adjusting its attitude. This will allow VERNE to maneuver around any small obstacles that were not previously detected by Europa Clipper. Avoiding the obstacle will be a priority in this mode, so all other subsystems will run on low power.

Obstacle Impact Mode

Since there will be detailed Clipper data of the landing site and travel path prior to the mission, VERNE is mitigating the risk of coming upon an obstacle too big to maneuver around. In the unlikely event VERNE comes upon an impassable obstacle it needs to break through, it will divert power to mechanical and thermal drilling with the intention of breaking up the obstacle in front of it. Ideally, this will only slow it down. If unsuccessful, this could lead to early end-of-life.

Early Water Reservoir Operations

The hope is to reach the under-ice ocean reservoir located 15 km beneath the surface of Europa. However, there is the possibility that VERNE happens upon a large and impassable water reservoir before it reaches 15 km and 3 years of travel. In this case, it will focus on releasing the anchor ahead of the reservoir and lowering the vehicle into the water reservoir to begin the Water Profiling mode.

Anchoring Mode

Ahead of the target for water science (reservoir or ocean), the anchor must be left behind to control vehicle descent for the remainder of the mission. This mode can only be triggered once. The Comms module will be stage separated and left behind the vehicle in the freezing water. It will freeze into place as the vehicle continues to descend on a reinforced tether that is providing constant communication and power between the COM anchor and the vehicle.

Water Profiling Mode

After the anchor is deployed, the rest of the vehicle will descend using the reinforced tether for descent control. It will descend into the slush expected at the ice/water interface. It will be taking both continuous and discrete samples as it enters the liquid water and descends to its ultimate depth. This ultimate depth will either be the end of the tether (100 m) or earlier if the vehicle is in a shallower water reservoir. It will then return to the top of the tether completing the profile and beginning the next. This will continue until End-of-Life.

End-Of-Life Mode

If VERNE is in the ocean, operators may choose to cut the tether and communicate to the COM anchor via RF until out of range. During the rapid descent, VERNE can conduct final experiments and take final measurements at depths far below what was possible while attached to the tether. After going out of COM range, all subsystems except the COMs anchor will be lost.

Table I. Expected Operational Modes of VERNE [2]

Operational Mode	GNC	COM	PAY	EPSTHE	SHS	STR
Start of Mission	**Mechanically penetrate the ice**	**Telemetry and begin spooling tether**	None	**Power the Drill and maintain thermal contr.**	None	None
Travel 0 -> 15 km	**Thermal Drill, Telemetry, Enviro. Sensing, Attitude and Traj. Control**	**Telemetry and Tether**	**Analyzing Continuous Samples (Low Power)**	**Power to Drill and Thermal Control**	**Taking Continuous Samples**	None
Science - Ice Profiling	**Limit Drill Power, Limited T+C**	**Limited COM, Raw Data Handling and Tether**	**Full Science Operation**	**Redivert Power to Pay. + Thermal Control**	**Take Discrete Samples and distribute samples to inst.**	None
Comms	**Limit Drill Power, Limited T+C**	**Maximize Data Rate to lander, Tether**	None	**Thermal Control**	None	None
Obstacle Avoidance	**Maximize Turning and Sensing**	**Telemetry and Tether**	None	**Thermal Control**	None	None
Science 2.0 - Water Profiling	**No Drilling, Sense Depths**	**Communicate with Lander (likely via pucks)**	**Full Science Operation**	**Power to the Profiler and COM, Maintain Anchor**	**Full Sampling Capability**	**Stage Separation, Anchor, Profiler Operation**
End of Life	**Fall and Sense**	**Try to Communicate for as long as possible**	**Limited Analysis**	**Power COM until the end**	**Sample quickly**	None

Mission State Flow Logic Diagram

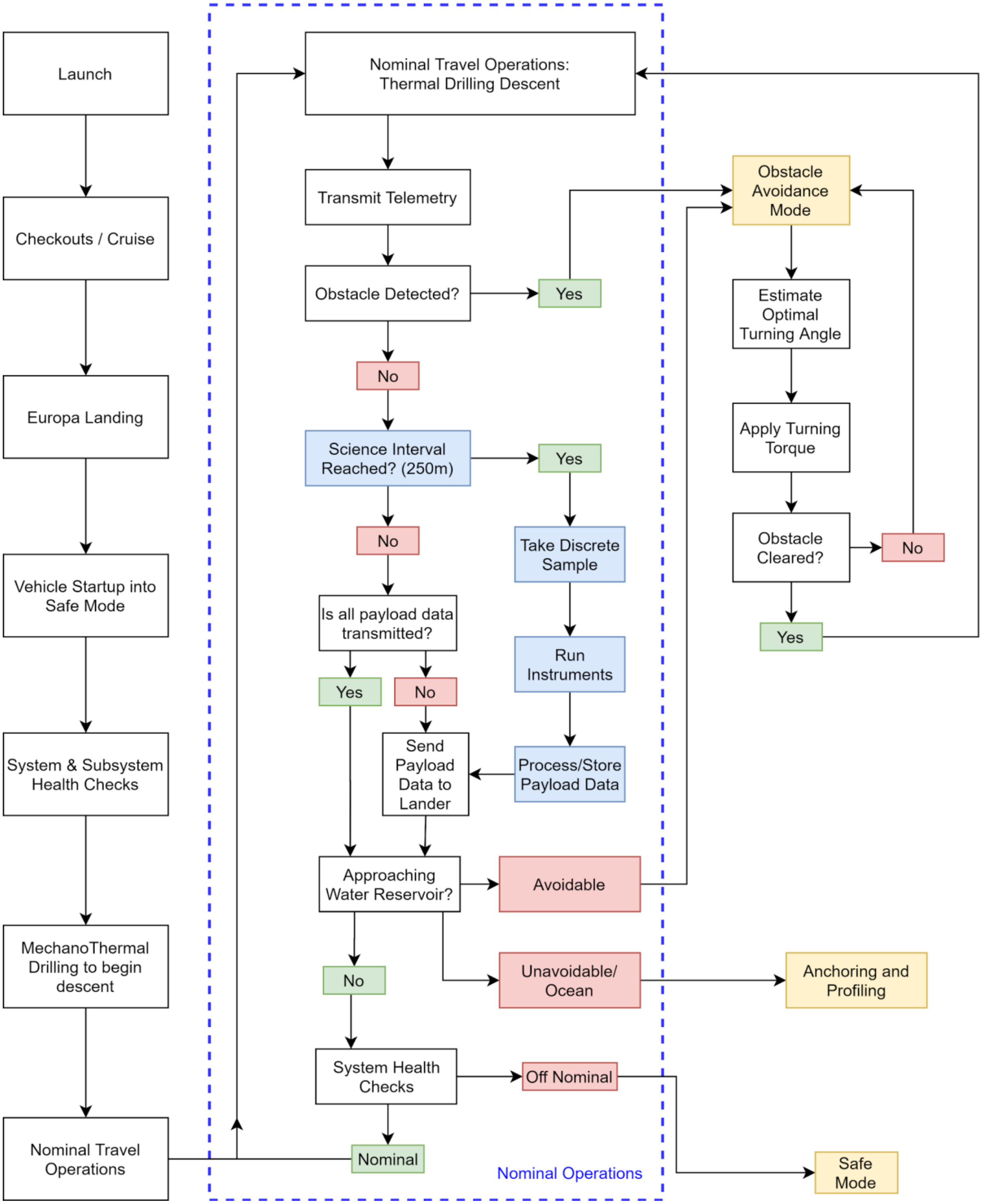


Figure 3. Mission State Flow Logic Diagram for Nominal Mission Lifetime

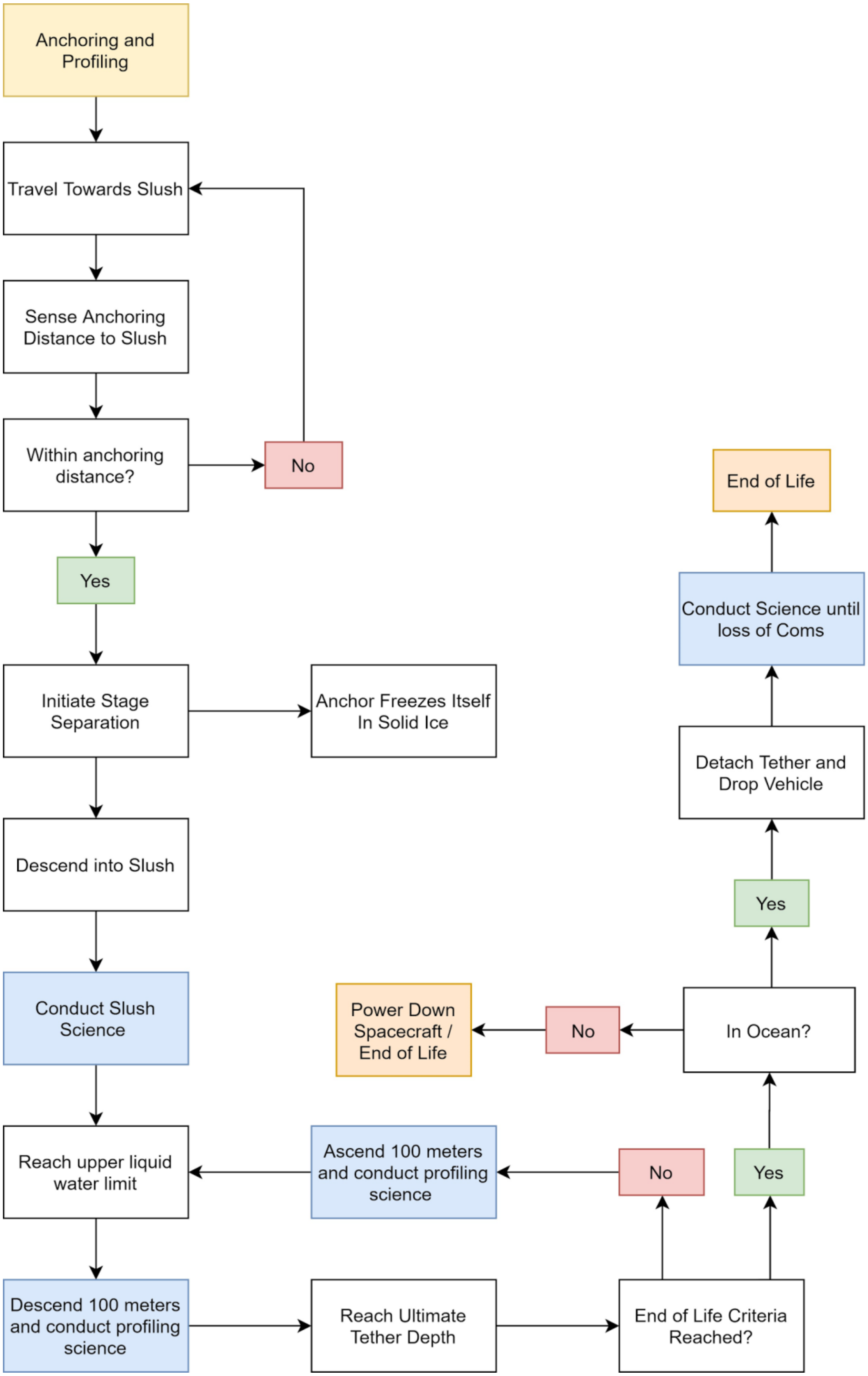


Figure 4. Mission Flow Logic Diagram further detailing the Anchoring and Profiling Mode

Communication Plan

According to the SESAME call, VERNE is not required to establish the architecture that will communicate the payload data back to Earth. The design must only show how the payload data will be communicated from the vehicle back to the lander. However, it is worth establishing that there are two obvious solutions for the Lander/Earth communications link. The more desirable option is to have an orbiter that can routinely uplink and downlink data to and from the lander while having regular and frequent intervals of line of sight with Earth and the Deep Space Network. The alternative is to forego extra orbital infrastructure and simply communicate directly to the Earth via an antenna directly on the lander. This will be less frequent as operators will need to wait for Earth to be visible in the sky above the lander. The size and weight of the infrastructure necessary for this option may be prohibitive with respect to the mass of the lander.

Simple estimates for access times can be estimated as follows:
If the criteria for line-of-sight between Earth and the Lander is simplified to the Earth simply being in the Europan sky, then one can say that ideally there will be access half of the time, giving operators 1.5 years of access time. However, considering a 10 degree above the horizon visibility margin and also excluding times where Jupiter is obstructing the view of Europa, one should assume less than 1.5 years of access time. If the orbiter relay option is considered, with a more complex (perhaps Molniya-esque) orbit, regular high bandwidth data dumps from the lander to the orbiter can be ensured. This means each pass could see a successful downlink of all pending data. The burden of communication then falls onto the relay orbiter, but the orbiter should have both a longer lifespan and less failure modes than the lander (apart from radiation challenges), allowing for a more robust and long-term data communication system. A more detailed access time analysis will have to be conducted in order to validate these ideas.

Regardless of what option is chosen for Lander/Earth communications, VERNE's responsibility is to communicate its data to the lander throughout its lifetime. This will be done one of two ways. The primary communication system is an optical tether that will facilitate high speed and high-volume communications between the vehicle and lander until the tether breaks. Since the tether breaking is expected because of the high tectonic activity expected at Europa, a secondary communications system that utilizes wireless pucks has been implemented.

From the start of the mission, repeater pucks will be deployed as the vehicle descends into the ice and the tether is unraveled. The pucks will be linked to the tether, and their spacing will be determined based on the optimal communications capability of the pucks. While the tether is intact, the wireless pucks will serve little to no communications purpose. They will ping their health throughout the mission so operators can be aware of any repeater malfunctions before switching to secondary communications.

Once the tether breaks, the lander will experience a complete Loss of Signal. In this event, once the tether failure has been confirmed, the lander will send a signal down the length of the cabling through each connected repeater. Once a repeater is unable to acknowledge receiving a signal, the location of the break will be isolated. The repeaters at each end of the break will serve as the link between both ends of the tether. The overall communications system will be limited to the data rate and bandwidth of the repeaters at that point (a bottleneck), but repeater to repeater communication will still be supported by the tether (minus the break point). The exact number of pucks required is flexible.

This architecture allows for an arbitrary number of break combinations that still closes the link, while not completely sacrificing communication performance after the first break occurs. If the tether were to completely fail, lander to vehicle communications would still be supported by the secondary COM system, providing VERNE with the necessary level of redundancy to ensure mission success.

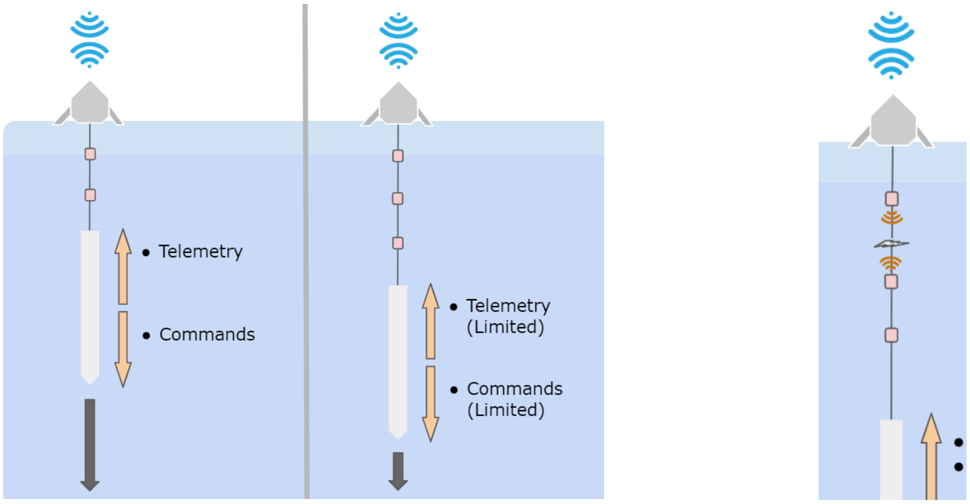


Figure 5. Communications Architecture [3]

Description of User Elements

While a User Interface for controlling the VERNE vehicle from the ground has not been developed, and likely will not be for some time, it is still possible to synthesize commands that a controller will likely have to send to the vehicle throughout the mission lifetime. The table below, Table II, shows the expected commands, their descriptions, and when they might be necessary. Keep in mind that the vehicle is expected to behave autonomously for the majority of the mission lifetime.

Table II. Detailed description of each expected command

Command	Description	Scenario
Leave Safe Mode	Puts vehicle into Systems Checkout Mode	After launch before cruise phase, and after any troubleshooting event.
Leave Systems Checkout Mode	Returns vehicle to normal operations	After leaving Safe Mode and once confident in vehicle health
Telemetry Request	Automatically pulls processed telemetry data from the vehicle and sends it to the lander	At any point during the mission timeline, especially during hazardous situations.
Enter Systems Checkout Mode	Enters vehicle into passive state until a problem can be identified or to assure that a problem has been remedied	If out-of-family health readings are observed. If vehicle should slow down for any reason.
Separate from Lander	Disengages vehicle from the lander at the beginning of the descent part of the mission.	When nominal contact is made between vehicle and ice-surface and the vehicle is ready for nominal operations
Manual Anchoring	Manually disengages anchor from vehicle	When the vehicle is approaching its final anchoring location and it has not already automatically anchored
Edit Profiling Range	Changes the range of depths that the vehicle will autonomously profile during water profiling mode	After anchoring and once the operator is confident in the ranges they would like to analyze, or if they would like to edit the ranges during the profiling mode
Begin Profiling	Manually begins profiling	Once the profiling ranges have been confirmed and the vehicle has not already automatically started profiling
Edit Rate of Communications	Changes how often telemetry and payload data are transmitted	If puck battery needs to be conserved to last until end of mission
Enter End of Life (Safe)	Permanently powers down the vehicle in anchored place.	At the end of the mission if Deathdrop is not an option
Enter End of Life (Deathdrop)	Disengages tether, allowing vehicle to drop into ocean and conduct science until out of range	At the end of the mission if Deathdrop is possible

Plan for Ground Operations

From Earth, the likely interface for communications is the Deep Space Network (DSN). This architecture will be able mission controllers to communicate with either the lander or the relay orbiter, with either option having similar ground operation schemes. During the cruise phase, it is expected that the launch and lander providers will monitor vehicle health while VERNE is in a low power, low operation state. VERNE dedicated operators will establish regular operations once the probe begins its nominal operations.

Once nominal travel and operations begin, a small team will be dedicated to monitoring the mostly autonomous operations. They will manually send commands when necessary, safe the vehicle if out-of-family telemetry is detected and receive and distribute payload data as it arrives via DSN. This small team will conduct these nominal operations for the entirety of the three-year travel time. In the event that the vehicle is placed into a contingency safe mode for the purpose of troubleshooting, a larger team of subsystem experts will convene until the vehicle can resume nominal operations. Because the vehicle is purposely built to operate autonomously, it is not necessary for this larger team to be dedicated to nominal operations.

Once the vehicle reaches the ice/water interface, the small team will ensure COM Module anchoring, entering the water profiling stage. In this stage, a larger team of payload experts should be present to analyze raw data as it transmits via DSN. A preprogramed science plan will be on board. This plan dictates the ranges of the profiling and frequency of science experiments with a focus on specific depths of interest. However, a command will be available to edit and reupload this profiling plan at the discretion of the payload and science team.

Launch and Early Operations

At launch, VERNE will not need operate until the vehicle has reached Europa. It will, however, need to conduct systemwide health checks post launch to ensure no faults have occurred during launch and periodically throughout spacecraft cruise mode. The same health checks should be conducted before landing operations. A larger team of subsystem experts should be made available to address any issues that may arise during these health checks. This team should also be present at full vehicle startup once thermomechanical drilling begins. This will be an operating mode that requires an unpredictable amount of power due to the low temperatures, and the team may react and alter the mission profile once the vehicle is interacting with the environment.

Mission Unique Operational Elements

This spacecraft design is unlike most historical spacecraft. Not even the most advanced rover designs take on the operational challenges that VERNE faces. The spacecraft will be in a vacuum environment as well as a pressurized liquid environment and environments inside that range, so it must be designed to withstand these environments as well as the following operational challenges.

The spacecraft, while operational, will never be in direct sunlight and so it must provide its own power for the entirety of the mission as it cannot use external means such as solar panels. The spacecraft will implement RTGs to work around this element. This power architecture has flight heritage based on past rovers and spacecraft, although it is not typical. For a mission of this complexity, however, a nuclear powered generator architecture would be ideal and even recommended for this time of mission concept exploration, but VERNE is unique in the SESAME team in that the design chooses to use the readily available RTG architecture in pursuit of the most feasible design. This is not without its drawbacks, as an RTG design is currently proving difficult to close to ensure the 15 km in 3-year requirement. It is possible that the mission operations change to a shorter depth, or a longer mission timeline.

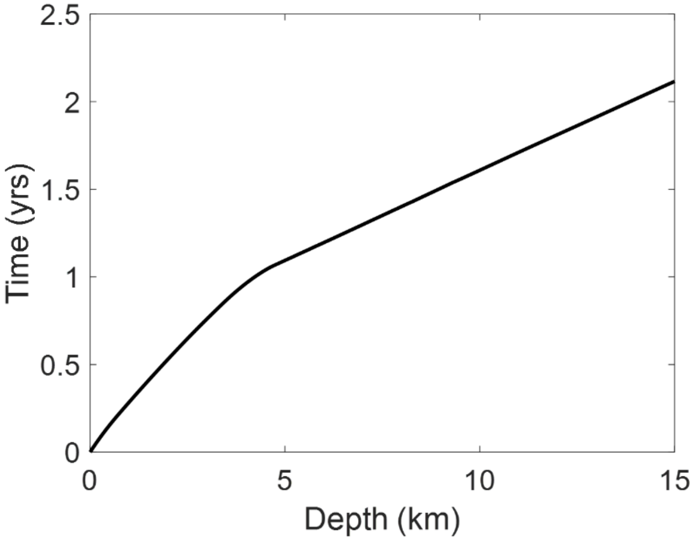


Figure 6. The vehicle descent rate with 60 RPM, 45 degree rake and 3 teeth [1]

VERNE’s travel is also unlike that of any other spacecraft. Traditionally, a spacecraft operator would input some delta-V command, whether it be a thruster to change an orbit, or a wheel rotation to move a rover across a body’s surface. In this scenario, the descent rate will vary based on the structure and temperature of the ice beneath the vehicle. It is possible to model what the descent may look like, but nothing will be exact. The descent with a mechanical drilling design of 60 RPM, 45 degree rake angle and 3 teeth is shown in Figure 6. Since the science profiling schedule is based on location and not time, it will be impossible to predict when science may occur, since one is unable to know at which point VERNE is going to reach a depth until it is approaching that depth. The consequence of this is that if the science team must be present during science operations, scheduling must be reactive rather than planned out years in advanced like typical space missions. It is also unclear when VERNE will exactly reach the ocean or an early water reservoir, so the complex water profiling stage is unable to be scheduled ahead of time. This leads to some untraditional operational practices, but with a dedicated team of operators and scientists at the ready, vehicle operation and payload processing is still manageable.

The primary and secondary communications architecture of VERNE is also unique to the mission. While the tether is intact, there will be a surplus of available telemetry and payload data that can easily transmitted to the lander as long as the power system allows for it. During this time, there will be no practical rationing of the data VERNE transmits unless it is restricted due to the capability of the Deep Space Network. Operationally, operators will have the freedom to liberally interact with the vehicle on an hourly basis if they see fit. If the tether breaks, however, this operational scheme changes for the rest of the mission. With the current link budget, when reduced to an acoustic puck communication scheme, the vehicle will only communicate a reduced amount of telemetry once every hour and will only communicate processed and compressed payload data rather than the preferred raw data. The acoustic pucks will be designed to survive, with respect to power, based on their worst case scenario on time estimates, but these estimates to do not take into account manual operator interaction with the vehicle, only the autonomous operation and communication. If an operator were to continually interact with the vehicle on the acoustic puck network, this may drain the batteries in the operational pucks. If this were to happen, and a puck were to cease being operational, the communication link would be broken, and VERNE would lose contact with the vehicle. Therefore, in the event of the secondary communications going into effect, operators must optimize the on time of the pucks which means they must optimize their interactions with the vehicle to ensure that the vehicle can at least transmit one payload sample analysis from the ocean or water reservoir at the end of the mission. If the acoustic puck network were to fail before then, the mission would not achieve minimum mission success.

Probe-Lander Link Budget

Parameter	**CBE**	**Comments**
Frequency	5 kHz	
Separation	0.9 km	
Data Rate	10 kbps	Bandwidth-limited
Bandwidth	7.47 kHz	± 3dB rule
Transceiver		
Directivity Index	14.3 dBi	25 deg beamwidth
Acoustic Power	1 W	~3 W input
Line Loss	4 dB	Assumption 2 dB each side
Ambient Noise	37.4 dB	Frequency-dependent model
Link		
Pointing Loss	2 dB	Assumption
Path Loss	59.1 dB	
Attenuation Loss	39.4 dB	Model for Antarctic ice @ 261K
SNR	18.8 dB	
Eb/No	17.6 dB	
Required Eb/No	10.5 dB	QPSK with BER=10^{-6}
Link Margin	7.1 dB	3 dB minimum

Table III. VERNE Link Budget [1]

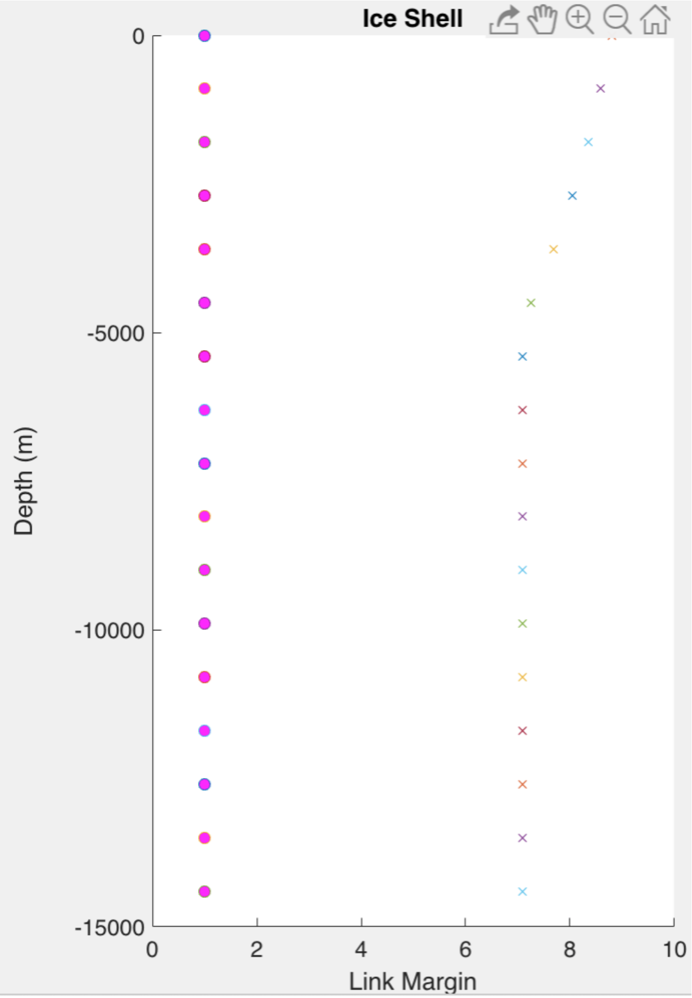


Figure 7. Puck distribution and associated link margin

The secondary communications architecture is designed to close the link budget shown in Table III across an optical tether break point. Therefore, a link budget must be closed to prove that each puck will communicate with the aft and fore puck relative to it. The link budget was closed using worst case scenario attenuation and noise, and with a consistent puck spacing of 0.9 km. The Transceiver and Antenna designs are realistic with modern technologies and commercial availability. Figure 7 shows the spacing and associated link margin between each puck. The link margin is increased for shallower pucks because the colder temperature ice contributes to the greatest loss in signal. After 5 km, the design is consistent as the signal loss is consistent in the model. With less stringent mass requirements, VERNE would ideally carry twice as many pucks as necessary to have redundancies in the event of single puck failure.

Operational Failures and Risk Analysis

The SESAME call and the VERNE mission concept have inherent complications and risks that should be considered in the design and operational concepts of the mission. Each subsystem has isolated a handful of errors that they have focused on mitigating in their designs [4]. These risk mitigation practices do not completely negate the effect of the risks occurring during operation, but the mitigation practices attempt to either reduce the severity of the risk or the probability of the failure occurring. In the following analysis, each subsystem's Risks and Consequences are rated based on their Likelihood and Severity. The Likelihood scales from Unlikely (1) to Definite (5) and the Severity scales from Insignificant (A) to Catastrophic (E). The mitigation method is defined and the Likelihood and Severity is assessed and defined again. The changes are trackable in the matrices by following the black reference letters to their corresponding teal reference letter. The risk analysis places each risk into a category of the following, shown in Figure 8 with Low Risk requiring no further action, Medium Risk has the option to take action, High Risk requiring action, and Extreme Risk requiring immediate action.

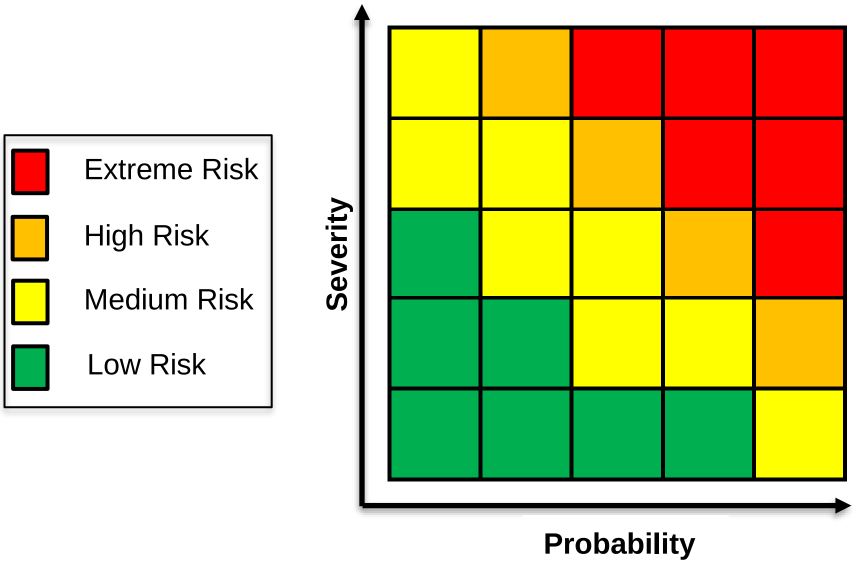
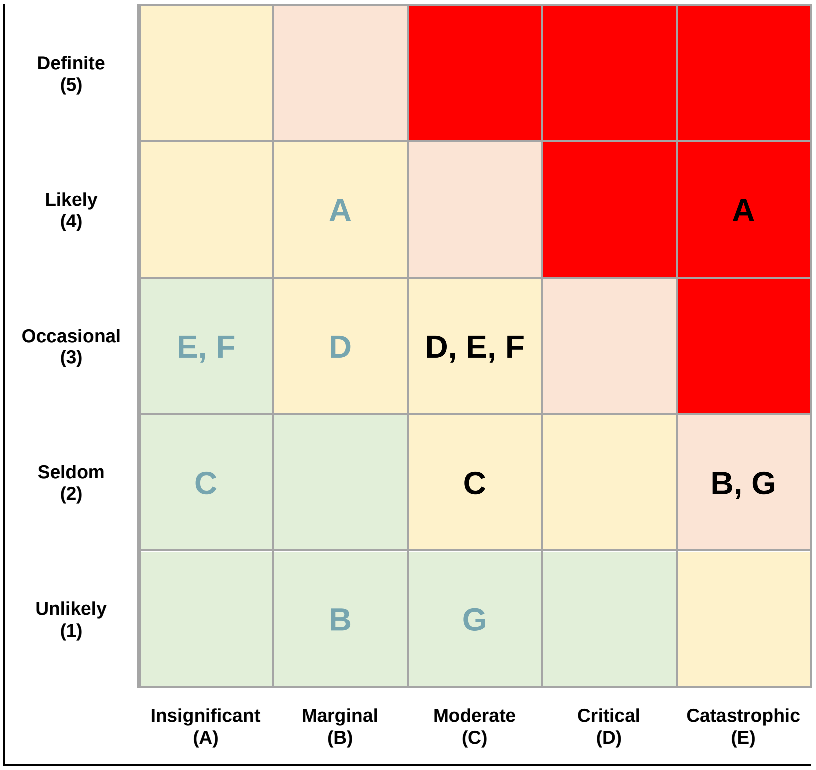


Figure 8. Risk Analysis Legend

Communication Command and Data Handling (CDH)

Table IV. CDH Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Tether breaks in solid ice	4	Loss of wired communication	E	4E	2ndary method: wireless repeaters	4B
B	Tether breaks in melt pocket while puck deployed	2	Pucks is not supported from above	E	2E	Repeaters are buoyant + anti-torque system	1B
C	Water does not refreeze in places	2	RF communication may fail	C	2C	Acoustic repeaters used throughout ice shell w/ 6dB margin	2A
D	Environment is colder than predicted	3	Batteries and other electronics may fail	C	3C	Insulation and RHUs sized for 15K lower than modeled environmental temperatures	3B
E	Higher concentrations of salt that predicted	3	RF communication may fail, acoustic will have higher attenuation	C	3C	Acoustic repeaters used throughout ice shell w/ 6dB margin	3A
F	Higher water/ice ratio than predicted	3	RF communication may fail, acoustic will have higher attenuation	C	3C	Acoustic repeaters used throughout ice shell w/ 6dB margin	3A
G	Tether breaks in melt pocket w/out puck deployed	2	No force to pull pucks and tethers out of communication module	E	2E	Repeaters are buoyant + anti-torque system	1C



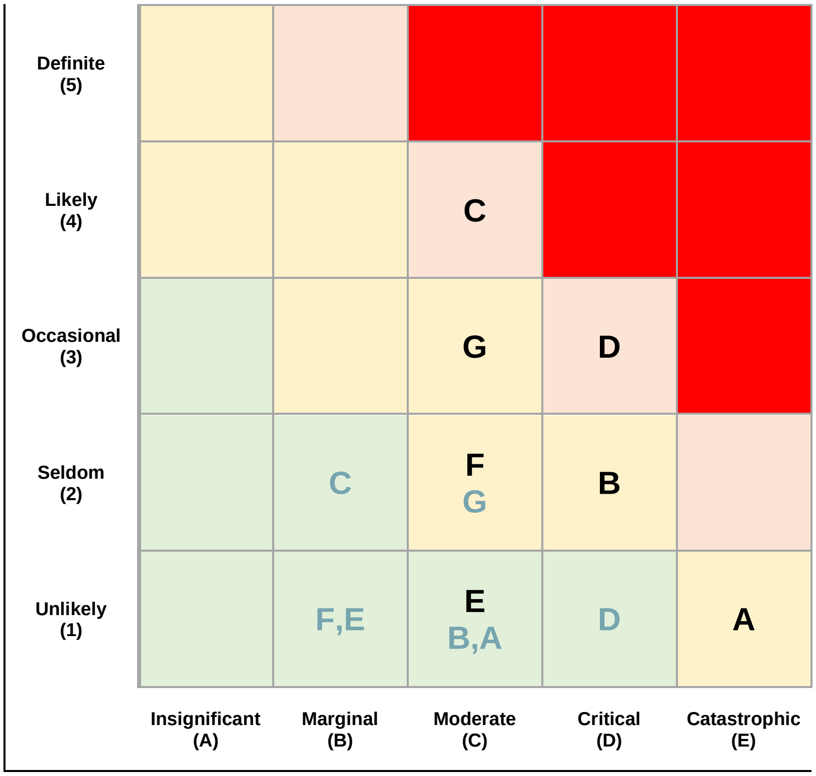
	Insignificant (A)	Marginal (B)	Moderate (C)	Critical (D)	Catastrophic (E)
Definite (5)					
Likely (4)		A			A
Occasional (3)	E, F	D	D, E, F		
Seldom (2)	C		C		B, G
Unlikely (1)		B	G		

Figure 9. CDH Risk Matrix

Electrical Power Systems (EPS)

Table V. EPS Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Disconnection of Power System	1	Vehicle loses all function	E	1E	Robust connections, margin in bend, temp, thickness of wiring	1C
B	Surge in Voltage/Current	2	Damage to equipment	D	2D	Robust PCDU, Battery to smoothen transients	1C
C	Power Demand Exceeds Supply	4	Equipment failure, or not all functions performed	C	4C	Battery, Circuitry prioritizes critical functions	2B
D	Wiring/Electronics/Battery outside Temp Limits	3	Damage to equipment	D	3D	Temp Analysis informs wire placement, fine thermal control	1D
E	Drill Motor Overheating From Large Power Input	1	Performance loss	C	1C	Thermal analysis and thermal control	1B
F	Radiation Exposure of Electronics	2	Loss of data, damage to electronics	C	2C	Fault tolerant design, radiation hardened electronics	1B
G	Power Cable from Lander Breaking (Assuming Umbilical Design)	3	Slower descent rate	C	3C	Robust Cable	2C



	Insignificant (A)	Marginal (B)	Moderate (C)	Critical (D)	Catastrophic (E)
Definite (5)					
Likely (4)			C		
Occasional (3)			G	D	
Seldom (2)		C	F G	B	
Unlikely (1)		F,E	E B,A	D	A

Figure 10. EPS Risk Matrix

Guidance Navigation and Control (GNC)

Table VI. GNC Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Environment is colder than predicted	4	Slower descent rate	C	4C	Dump more heat out	4B
B	Drill head corrosion	4	Lower mechanical drill efficiency	C	4C	Reinforce exterior with hardened material	4B
C	Thermal fluid loops breaking	2	Slower descent rate	D	2D	Increase usage of intact loops	1D
D	Anti-torque system breaks	3	Have to accommodate small counter torque	C	3C	Add spikes to leaf springs	3B
E	Side wall further than predicted	4	Vehicle has tendency to tip over	D	4D	Incorporate safety factor into actuator design	3C
F	Mechanical Drill stalls	4	Slower descent rate, drill may get stuck	D	4D	Design for stall torque>torque required; alter operations to go slower; provide more heat	3C
G	Position and Attitude Determination failure	2	Unable to know position or attitude	D	2D	Add backup sensors	2B

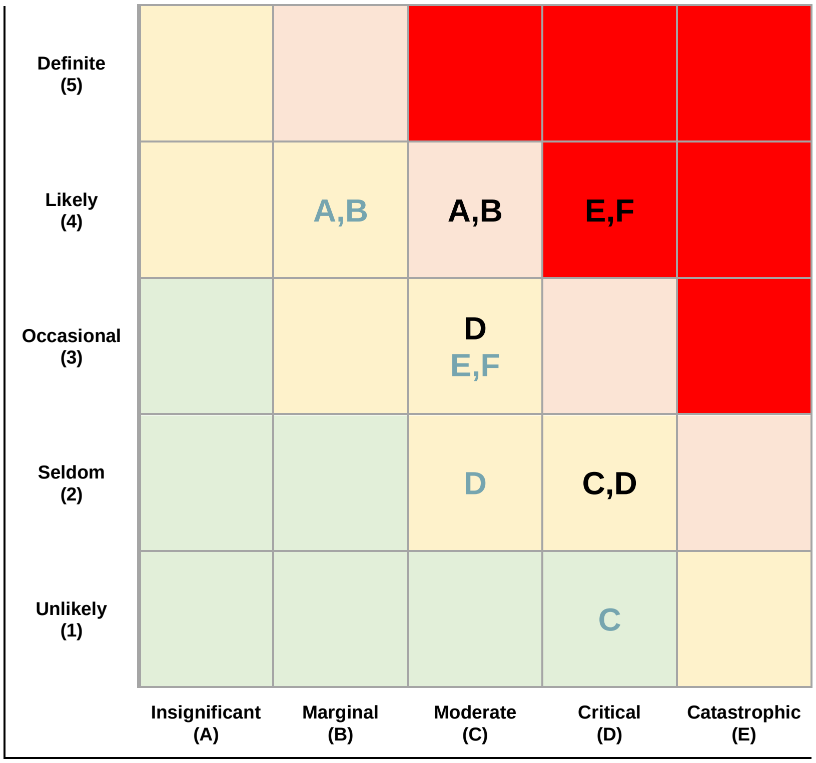


Figure 11. GNC RIsk Matrix

Sample Handling System (SHS)

Table VII. SHS Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Sample inlet port clogs	3	Samples cannot be collected	D	3D	Include multiple inlet ports per kilometer to switch to an unclogged port	2B
B	Pump stops functioning due to wear	4	Samples cannot be collected	D	4D	Include a strainer to filter out large particles before pump	2D
C	Inlet filter clogs due to solid particles or salts	3	Samples cannot reliably be collected	C	3C	Keep a hold of water used to flush pump backwards to dislodge particles	1C
D	Science payload chemically changes water samples	4	Samples cannot be excreted from vehicle - planetary protection	B	4B	Introduce a contaminated water hold on board to store chemically altered samples	4A

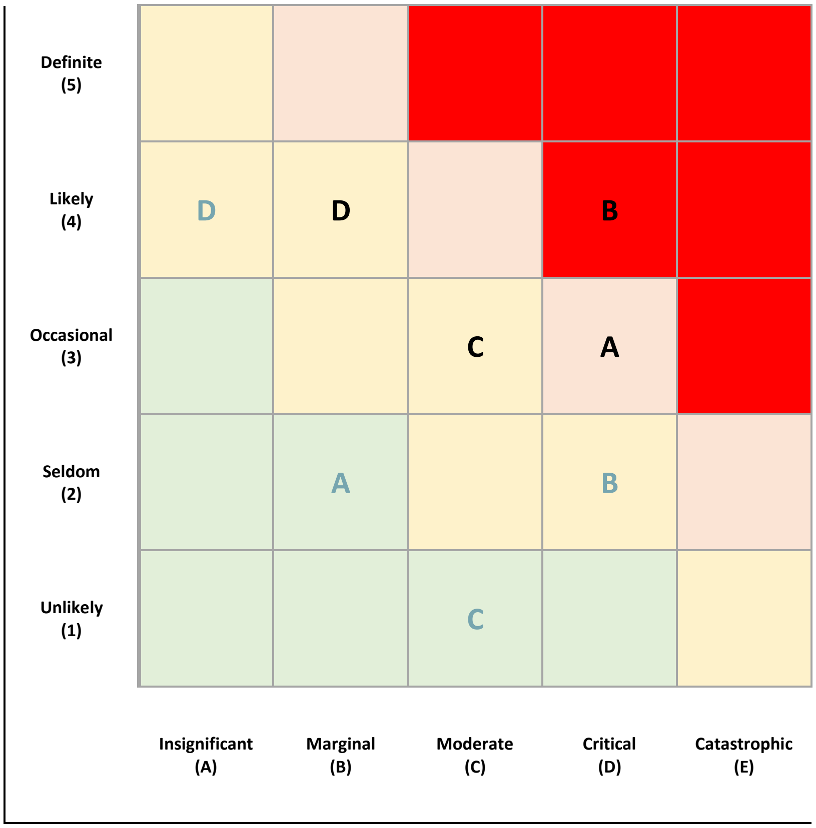


Figure 12. SHS Risk Matrix

Science Payload and Instruments (SCIPAY)

Table VIII. SCIPAY Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Sample inflow interrupted	3	Unable to process samples	D	4D	Sample Handling Mitigation Methods	2D
B	Mass and dimension requirements violated by LCMS	2	Instrument incompatible with vehicle	C	2C	Use miniaturised LCMS or GCMS	1B
C	False positive given for life detection analysis	3	Results of science investigation inconclusive	B	3B	Sensitive instrumentation; Relax life detection requirements; Triplicate sample analysis	2A
D	False negative given for life detection analysis	3	Results of science investigation inconclusive	B	3B	Sensitive instrumentation; Make life detection requirements more stringent; Triplicate sample analysis	2A
E	Run-out on pH/ORP sensor buffer	2	Measurement response will drift	C	2C	Carry reserve buffer	2B
F	Degradation of sensor electrodes	3	Measurement response will drift	C	3C	Use passive electrodes with inert lining protection inside instruments	2C
G	Microscope resolution insufficient to capture potentially biotic morphology	3	Missing relevant results	B	3B	Develop and use a flight-ready microscope with higher resolution	2A

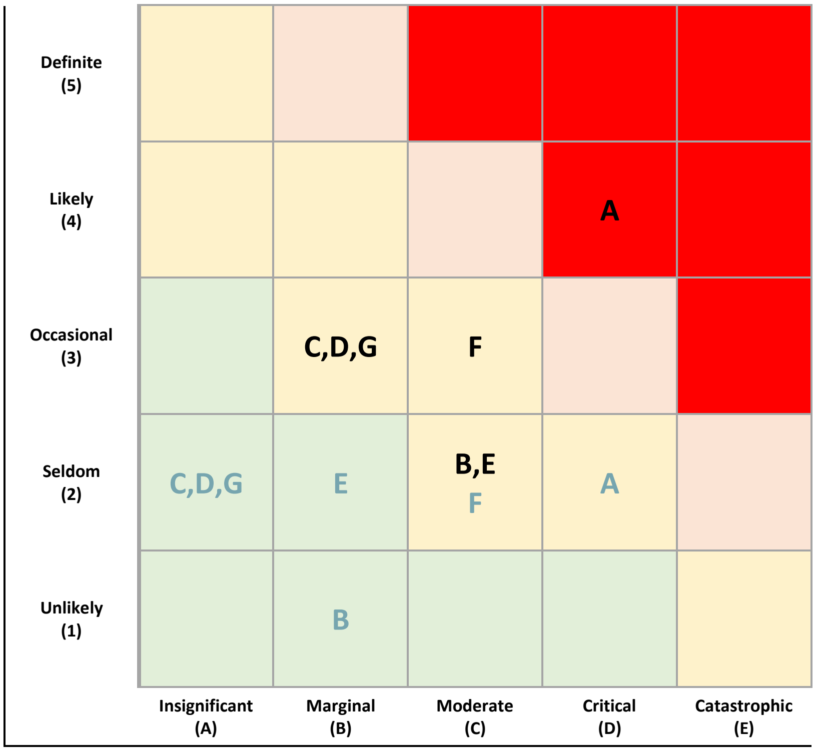
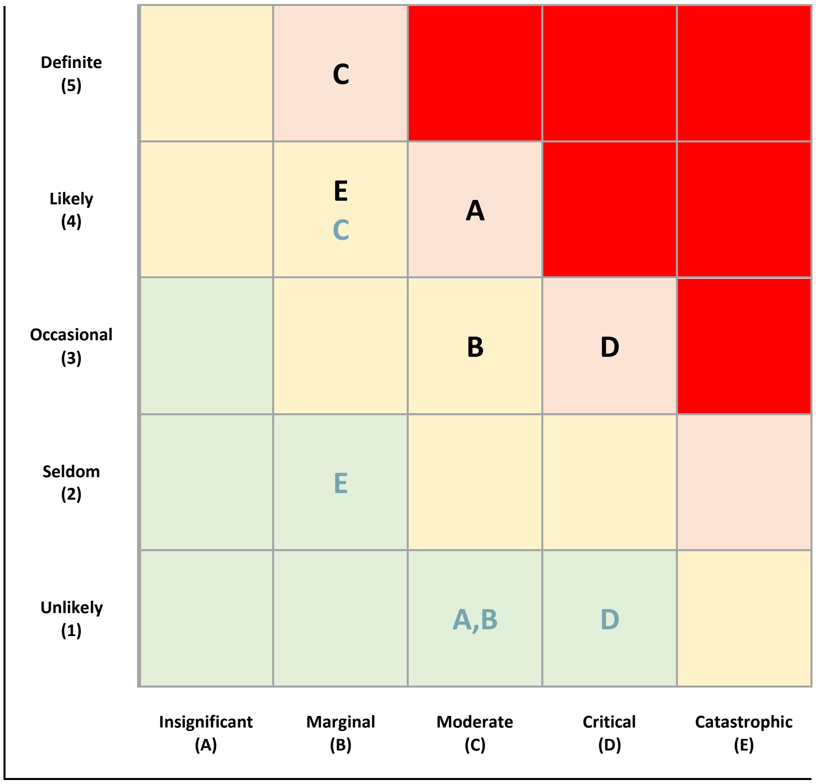


Figure 13. SCIPAY Risk Matrix

Structures (STR)

Table IX. STR Risk Analysis

Ref	RISK	Likelihood (1-5)	Consequence	Consequence (A-E)	Risk Rating	Mitigation Method	New Rating
A	Anchor module sinks in hole after separation	4	Anchor doesn't freeze in	C	4C	Separation assurance mechanism to hold anchor in place	1C
B	Separation module doesn't fully separate	3	Anchor doesn't freeze in, no profiling available	C	3C	Separation assurance mechanism to encourage full separation	1C
C	Structure of vehicle exceeds mass budget	5	Vehicle doesn't meet mass requirement	B	5B	Use composite material to reduce mass, alter length or number of heating plates	4B
D	Drilling, launch, or landing vibrations break vehicle	3	Vehicle cannot reliably continue mission	D	3D	Choose material strong enough to withstand vibrations, connections between vehicle are strong	1D
E	Excessive heat lost through vehicle hull	4	Thermal management has reduced effectiveness	B	4B	Infill honeycomb with aerogel, include extra insulation by external heating plates	2B



	Insignificant (A)	Marginal (B)	Moderate (C)	Critical (D)	Catastrophic (E)
Definite (5)		C			
Likely (4)		E C	A		
Occasional (3)			B	D	
Seldom (2)		E			
Unlikely (1)			A,B	D	

Figure 14. STR Risk Matrix

References

[1] Schmidt, Britney et al. “VERNE HQ 2020”, April 2020, https://docs.google.com/presentation/d/1UAtZp5ycIyo2eRYn1xJbI6uYyZbhTilSemD83-noAYk/edit?usp=sharing, PowerPoint Presentation

[2] Szot, Phillip “0M0201200 Operational Modes”, February 2020, https://docs.google.com/document/d/1ufM_2MzS5CM_55bBYpG0LBbmgzQ_yLWcQeSbkd7hFq8/edit?usp=sharing, Memo

[3] Szot, Phillip “4M1028191 Auxiliary Communications”, October 2019, https://docs.google.com/document/d/1dlzN6lcfykiaDZSu5p2achnGmNTLu-mkhony2Kd-9xA/edit?usp=sharing, Memo

[4] Szot, Phillip “0M0415200 Risk Analysis”, April 2020, https://docs.google.com/document/d/11z-wC-6EVlCLyt1W6qHx9u7hUfTAh-wis694cscyOPo/edit?usp=sharing, Memo

[5] NASA, “Scientific Exploration Subsurface Access Mechanism for Europa (SESAME).”, https://www1.grc.nasa.gov/space/pesto/space-vehicle-technologies-current/scientific-exploration-subsurface-access-mechanism-for-europa-sesame/