NMEA OneNet Test Bench Final Report

A Development SDK, Education, and Security Assessment Suite

Spencer Beer, Maria DiValentin, Steven Strevell

Systems Cyber Research Group - Dec 2, 2024

Contents

Final report submitted in partial fulfillment of the requirements for SYSE 530 at Colorado State University

Executive Summary

The maritime industry is going through a big shift, with modern vessels relying more on advanced electronic systems for navigation, communication, and daily operations. Moreover, a new standard has been introduced in the industry: OneNet. It is not meant to be a replacement for NMEA 2000/0183 standards, but to deliver the benefits of a high bandwidth (up to 10Gbps) standard, that interoperates with legacy standards. It's been designed with the systems engineering life cycle in mind. This means the industry has put together a standard that focuses on a streamlined setup for the "visionary developer" and "boat-builder", offering: seamless and secure data pairing, flexibility, and device certification [1]. But, that last point becomes an issue regarding the understanding of the security model surrounding the protocol. That's why the SystemsCyber team at Colorado State University (CSU) has developed the OneNet Test Bench. The following section elaborates on the reasoning behind the development of this product and its need for the newly released OneNet protocol. The System of Interest (SoI) has been modeled using SysML Magic Grid methods centered around the design and optimization for a typical router architecture, customized for OneNet.

It's important to note this project has been completed in part for SYSE 530, Overview of Systems Engineering Processes, and will incorporate methods used in the class to develop the system throughout its life-cycle [2,3]. The methods described in this report are part of the Magic Grid method [4]. and prove why using these methods help create more successful systems. This project further shows how the functional requirements have been satisfied through testing of throughput to support OneNet bandwidth demands, and other non-technical satisfactions. The non-functional requirements have been satisfied through parametric diagrams.

Project Motivation and Objectives

To meet the growing need for faster and more reliable data sharing between marine devices, the NMEA OneNet standard was introduced. This Ethernet-based protocol offers higher speeds, greater flexibility, and better compatibility with existing systems like NMEA 2000 [1]. However, its adoption has been slow due to the lack of helpful tools, such as a Software Development Kit (SDK), clear open-source documentation, and tools to properly check its security. On top of this, the process of implementing new protocols is often complicated and unpredictable. To solve these problems, the NMEA OneNet Test Bench (ONTB) was created. This toolkit is designed to help in three key areas:

1. Security Testing:
    - 1.1. Ensuring OneNet is safe from cyber threats
    - 1.2. Verifying the OneNet protocol standard implementation lies free from interpretation, potentially fostering insecure cyber-physical systems
2. Development Support:
    - 2.1. Providing tools and resources on top of the OneNet Certification Tool to make building OneNet applications easier
3. Education:
    - 3.1. Helping the industry learn and transition to this modern standard

The goal of this project is to fully test NMEA OneNet based on version 1.001 of its standard. By ensuring it works as intended, ONTB will help build confidence in OneNet as a reliable and secure solution for the future of marine technology. The list below highlights the most important aspects of the ONTB:

- A customized embedded operating system designed specifically for OneNet
- Software libraries and tools to help developers
- Security binaries and tools to strengthen OneNet's defenses
- Documentation hosted on Github for education, training, and maintenance
- A landing page and tool for interacting with the OneNet gateway for less experienced users
- Custom routing software for conversion between legacy NMEA protocols and NMEA OneNet

Design and Modeling Process

Stakeholder Needs: Value Proposition Canvas and SysML Model

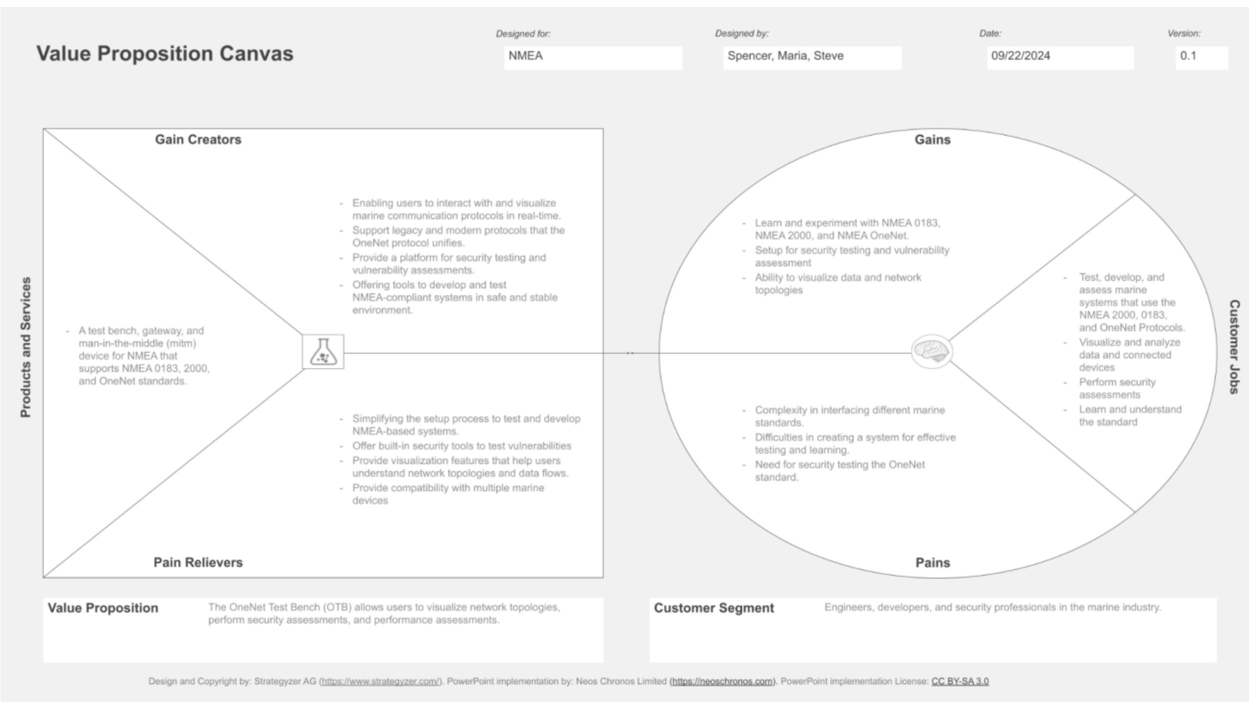

Figure 1 and 2, Value Proposition Canvas

#	Name	Text	Sterotype
1	SN2 Need for Safe and Secure Communication	"The primary purpose of the standard is boating safety." - Stakeholders need a reliable and secure way to communicate between marine device to ensure safety	Requirement [Class]
2	SN3 Need for Technological Evolution	"The natural technological evolution from NMEA 0183 to NMEA 2000 to OneNet." - Stakeholders need modern networking standards whilst being compatible with legacy systems	Requirement [Class]
3	SN4 Need for Interoperability	"OneNet provides a common network infastructure for marine devices and/or services on IPv6" - Stakeholders need a unified networking standard that can work across different devices	Requirement [Class]
4	SN5 Need for Scalability	"To discover devices and services automatically to create an extendible and scalable network architecture" - Stakeholders need the ability to adapt and scale new devices and services without major reconfigurations	Requirement [Class]
5	SN6 Need for Coexistence	"OneNet to coexist with other protocols and services that operate in parallel on the same network." - Stakeholders need coexisting protocols, whether that is marine or non-marine	Requirement [Class]
6	SN7 Need for High-Bandwidth Support	"To support high-bandwidth applications such as audio/video data transport." - Stakeholders need high data throughput	Requirement [Class]
7	SN8 Need for Open Standard and Cooperation	"To define an open interface to interoperate with current and upcoming open services." - Stakeholders need open standards that facilitate future growth, and compatiblity.	Requirement [Class]

Figure 3, Stakeholder Needs [5]

The OneNet Test Bench (ONTB) was designed by analyzing the NMEA OneNet Standard and identifying the critical needs of engineers, developers, and security professionals in the marine industry, as identified through analysis of the OneNet Standard. By incorporating the requirements of these stakeholders, we ensured the system meets the demands of a secure, scalable, and interoperable maritime communication environment.

The stakeholder needs were derived using insights from the Value Proposition Canvas (Figure 3) and reflect the technical and operational gaps addressed by the ONTB.

System Context:

The ONTB is a platform designed to test, analyze, and validate NMEA 0183, NMEA 2000, and OneNet communication protocols. Shown below in figure 4, the platform has been designed with components that can interact with serial communication (for NMEA 0183), CAN (for NMEA 2000), and connectors that are already built into the Commercial Off-The Shelf (COTS) device. In our case the BeagleBone Black, which has been proven to work in intensive environmental conditions [6], and has been modeled in respect to its external interfaces shown in figure 4.

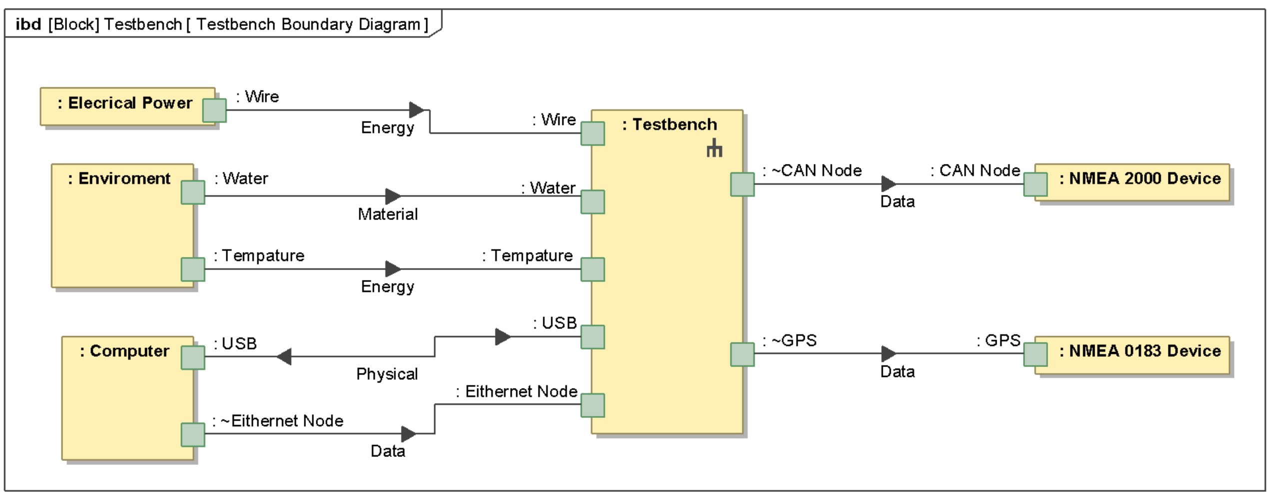

Figure 4, Internal Block Diagram showcasing interactions between interfaces of the ONTB [5]

Under this diagram there are a few key components and interactions:

1. **Electrical Power:** Provides energy through wired ethernet connections to ensure uninterrupted operation in various maritime conditions, and provides a seamless way to connect the ONTB to the network using either PoE, or a PoE to 5v adapter compatible with the system.
2. **Environment:** Inputs include water and temperature variations, representing typical environmental factors for maritime applications. Outputs include the test bench being designed to resist water ingress and operate efficiently across a wide temperature range.
3. **Computer Interface:** USB and Ethernet Connections enable physical connections for data transfer and system monitoring, providing access for configuration and debugging.

4. **External Devices:** NMEA 2000 devices, typically used to interact through CAN nodes, supporting modern maritime communication protocols. NMEA 0183 devices, typically used to communicate via GPS nodes to support legacy systems.

In summary, the ONTB interfaces with its environment, power sources, external devices, and user systems. It draws power via wired inputs, communicates with NMEA-compliant devices using CAN and GPS nodes, and supports remote management through USB and Ethernet connections, ensuring reliable performance in maritime conditions. The diagram was created in respect to the ONTBs parent system (the OneNet Protocol) and the subsystems (the user interface, etc.). This diagram allows us to effectively communicate where our system lies within another complex system, allowing customers to visualize the need for such a comprehensive product.

Use Cases:

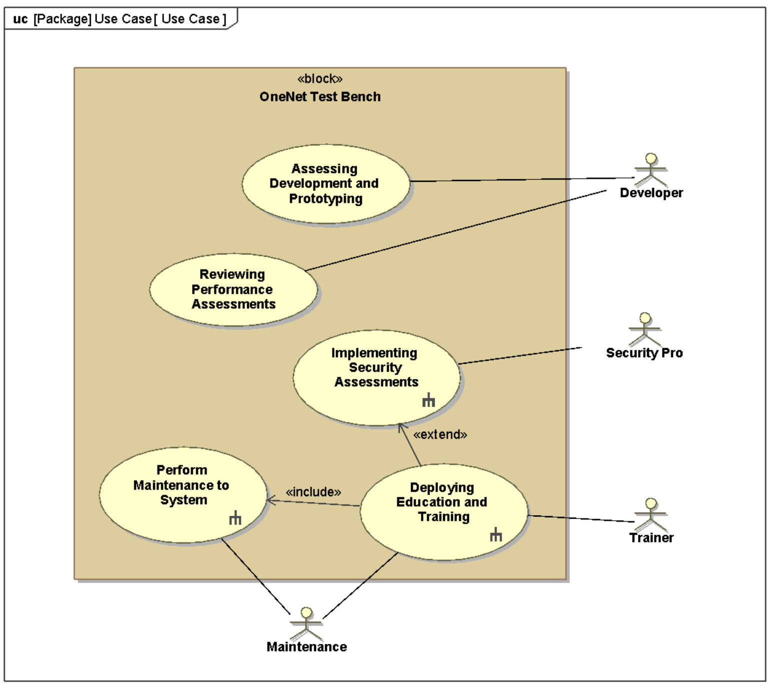

Figure 5, Use Case SysML diagram showcasing functions the ONTB can serve [5]

Figure 6, 7, and 8, Embedded activity diagrams [5]

The OneNet Test Bench supports five primary functions that address stakeholder needs, focusing on development, testing, security, training, and maintenance. They are listed below.

1. Assessing Development and Prototyping:
   - **Actor**: Developer
   - **Description**: Developers create, prototype, and test NMEA-compliant applications in a controlled environment.
   - **Goals**: Ensure compatibility with NMEA standards, debug, and optimize performance.
   - **Outcome**: Validated and ready-to-deploy applications.
   - **Magic Grid Context**:

        - Links stakeholder needs for technological evolution (SN3) and interoperability (SN4) by enabling seamless prototyping for modern and legacy protocols.

2. Reviewing Performance Assessments
    - **Actor**: Developer
    - **Description**: Developers use monitoring tools to evaluate application performance.
    - **Goals**: Monitor behavior, throughput, and latency under various conditions.
    - **Outcome**: Applications meet performance benchmarks.
    - **Magic Grid Context**:
        - Supports high-bandwidth needs (SN7) and scalability (SN5) by ensuring the system performs efficiently in demanding environments.
3. Implementing Security Assessments
    - **Actor**: Security Professional
    - **Description**: Identify vulnerabilities and test system security.
    - **Goals**: Conduct penetration testing and ensure compliance with security standards.
    - **Outcome**: Secured and resilient systems.
    - **Magic Grid Context**:
        - Aligns with safe and secure communication (SN2) and supports coexistence (SN6) by ensuring robust cybersecurity across networks.
4. Deploying Education and Training
    - **Actor**: Trainer
    - **Description**: Provide hands-on training for NMEA protocols and system operations.
    - **Goals**: Enhance stakeholder proficiency in using and maintaining the system.
    - **Outcome**: Stakeholders are knowledgeable and confident in system usage.
    - **Magic Grid Context**:
        - Addresses stakeholder needs for open standards and cooperation (SN8) by fostering understanding and collaboration among users.
5. Performing Maintenance to System
    - **Actor**: Maintenance Personnel
    - **Description**: Ensure the Test Bench remains operational through diagnostics and updates.
    - **Goals**: Perform repairs, update software, and minimize downtime.
    - **Outcome**: A fully operational system with consistent performance.
    - **Magic Grid Context**:
        - Directly addresses maintenance (SN5) and indirectly supports interoperability (SN4) by maintaining compatibility and functionality over time.

Measures of Effectiveness:

The OneNet Test Bench is evaluated using specific Measures of Effectiveness (MoEs) to determine its performance and operational success. These MoEs align with system objectives and stakeholder needs, focusing on real-time communication, deployment efficiency, and system robustness.

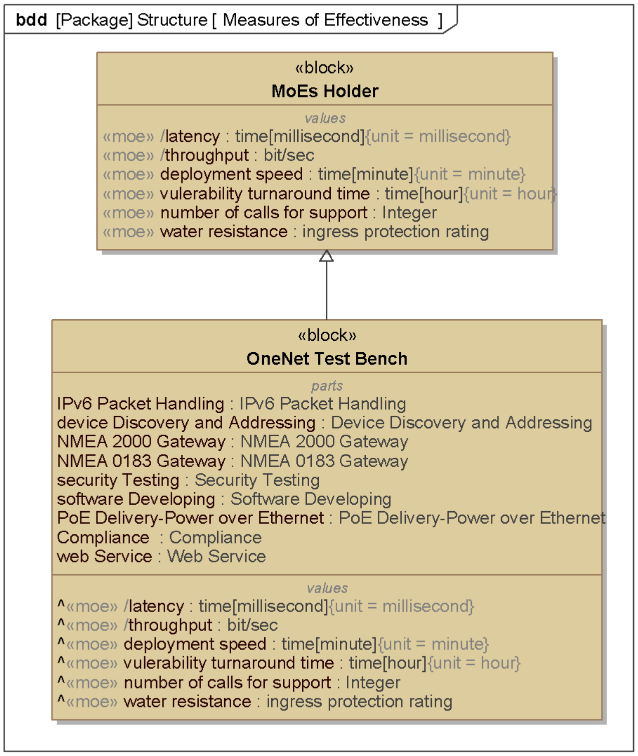

Figure 9, Measures of Effectiveness (MoE) showcasing SysML ability to evaluate product [5]

Below describes some of the most important measures of effectiveness used to satisfy ONTB requirements shown in figure 9:

- **Latency:** is the time required for packers to traverse the system, measured in milliseconds. The target is to minimize latency to support high-speed data exchange. To evaluate the performance of the latency, systems testing would include using tools like ping, iperf, netperf, and traceroute, all which are built into the command line interface of the ONTB. If the latency is measured on an average of less than 100 ms, then the system is considered acceptable.
- **Throughput:** is the amount of data transferred per second, with the goal to maximize throughput to handle large-scale network traffic. To evaluate the performance of throughput on the ONTB, systems testing would include using tools such as iperf. If the throughput is measured on an average of greater than > 10Mbps according to the OneNet standard requirements.
- **Deployment Speed:** is the time required to deploy the system, measured in minutes, with the goal to ensure quick deployment in various maritime environments. To evaluate the effectiveness of the ONTB deployment speed, we would consider setting up the SoI within 30 minutes to be acceptable.
- **Vulnerability Turnaround Time:** The time to identify and resolve security vulnerabilities, measured in hours, with the goal to minimize this turnaround time. To evaluate the effectiveness of the vulnerability turnaround time, we would consider an average time of less than a week to be considered acceptable, given different experience levels.
- **Number of Support Calls:** The frequency of support requests from users, with the goal to reduce the number of calls. To evaluate the effectiveness of the number of support calls, we

would measure the average time between support requests for maintenance to return the system to an operable state. As shown in the Subsystem Analysis section of this report, we consider MTBM of 1 year to and a failure rate of 1% to be acceptable. This should also satisfy the environmental requirements, because given the system can withstand temperatures typically encountered in marine environments, then the number of support requests should be low and at an average of 1 year.

- **Water resistance:** The systems protection rating for water resistance, the system must meet or exceed the required IP rating for marine applications (IPX6).

These MoEs are directly tied to critical system components:

1. **Latency and Throughput**: Managed through IPv6 packet handling, device discovery, and addressing.
2. **Deployment Speed**: Enabled by modular software and hardware design, including the NMEA gateways.
3. **Vulnerability Turnaround**: Supported by security testing tools integrated into the test bench.
4. **Water Resistance**: Ensured by robust hardware like the BeagleBone Black and PoE infrastructure.

The Measures of Effectiveness (MoEs) are critical in system design, enabling evaluation of how well the OneNet Test Bench (ONTB) meets stakeholder needs. MoEs such as latency, throughput, deployment speed, and vulnerability turnaround time provide measurable performance metrics within the system boundary, ensuring alignment with priorities like scalability, interoperability, and security.

In the Magic Grid Method, MoEs connect stakeholder needs to system requirements and architecture by:

1. Translating Needs to Design: For example, latency and throughput address high-bandwidth support (SN7) and scalability (SN5), while vulnerability turnaround time supports secure communication (SN2).
2. Validating Performance: MoEs test and refine key ONTB subsystems, such as the networking stack and software suite, to meet performance benchmarks.
3. Driving Improvement: Feedback from MoEs guides iterative enhancements, ensuring the ONTB adapts to evolving maritime communication needs.

By embedding MoEs into the ONTB's design, the Magic Grid Method ensures traceability, validates system performance, and addresses critical industry requirements.

Conceptual Subsystems:

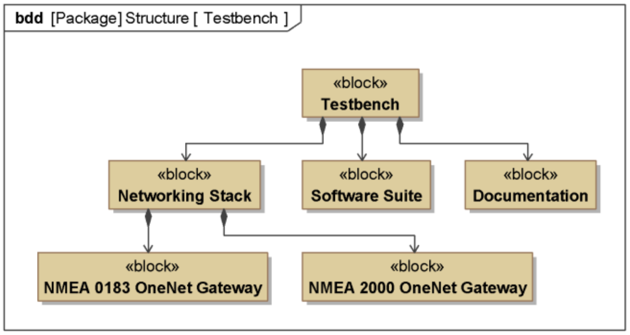

Figure 10, BDD describing the subsystems used [5]

The OneNet Test Bench is composed of modular subsystems, each designed to fulfill specific functions essential for testing, validating, and supporting NMEA communication protocols. These subsystems are integrated to ensure comprehensive functionality while maintaining modularity for scalability and maintainability.

The various subsystems are listed below.

1. **Networking Stack**
   - **Purpose**: Provides the underlying framework for handling communication between devices and protocols.
   - **Key Features**:
     i. Supports IPv6 communication via Ethernet nodes.
     ii. Handles data exchange for NMEA 0183 and NMEA 2000 devices using CAN nodes.
   - **Role in the System**: Ensures seamless data transfer across devices and supports legacy (NMEA 0183) and modern (NMEA 2000, OneNet) protocols.
2. **NMEA 0183 OneNet Gateway**
   - **Purpose**: Acts as the bridge for integrating legacy NMEA 0183 devices into the OneNet ecosystem.
   - **Key Features**:
     i. Converts NMEA 0183 protocol data for compatibility with the testbench.
     ii. Facilitates GPS-based communication
   - **Role in the System**: Enables legacy devices to communicate within the testbench framework, ensuring backward compatibility.
3. **NMEA 2000 OneNet Gateway**
   - **Purpose**: Facilitates testing and communication for devices using the NMEA 2000 standard.
   - **Key Features**:
     i. Supports high-speed CAN-based communication.
     ii. Provides a testing environment for devices with advanced protocol features.
   - **Role in the System**: Serves as the backbone for testing modern maritime devices, ensuring compliance with NMEA 2000 standards.

4. **Software Suite**
    - **Purpose**: Provides the tools and interface for developers, testers, and security professionals.
    - **Key Features**:
        i. Includes a GUI for user interaction.
        ii. Features a network analysis tool (e.g., Wireshark) for debugging and performance evaluation.
        iii. Powered by Debian and PRU software to enable real-time processing.
    - **Role in the System**: Supports the development, testing, and analysis of NMEA-compliant applications.
5. **Documentation**
    - **Purpose**: Offers comprehensive guidance for users to operate and maintain the Test Bench.
    - **Key Features**:
        i. Includes detailed explanations of the Test Bench's functionality.
        ii. Provides training materials for stakeholders such as developers and security professionals.
    - **Role in the System**: Ensures proper use of the system and reduces the learning curve for stakeholders.

The Test Bench integrates these subsystems through a central Single Board Computer (using a BeagleBone Black), which coordinates the interaction between hardware and software components. The modular design ensures:

1. Flexibility to add or replace components as needed.
2. Scalability for supporting additional devices and protocols.
3. Ease of maintenance and troubleshooting.

By conveying how subsystems interact with each other, the conceptualization of subsystems helps us manage complexity of systems such as the ONTB.

Functional Analysis:

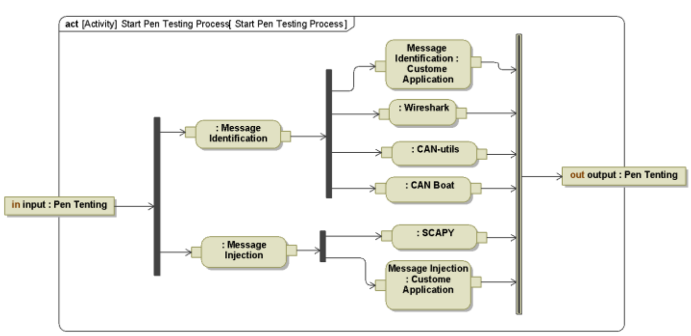

Figure 13, Internal FFBD / activity diagram for the penetration testing process [5]

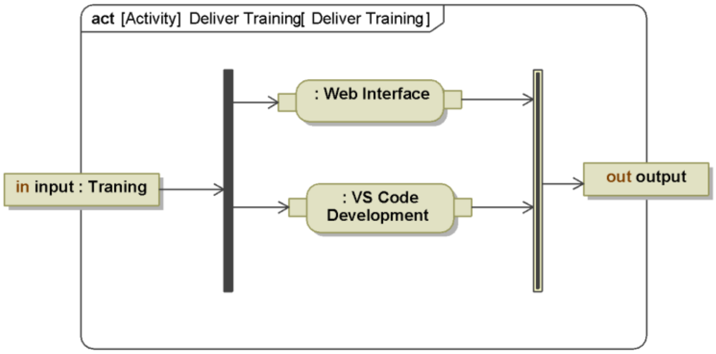

Figure 14, Internal FFBD / activity diagram for the education, and development process [5]

Through performing functional analysis on the OneNet Test Bench (ONTB) two key functions were identified—Delivering Training and Starting Penetration Testing (Pen Testing) Process—derived from the use cases. These functions ensure the ONTB meets stakeholder requirements for usability, security, and system optimization.

1. **Deliver Training**
    - **Purpose**: This function supports trainers in providing hands-on education on NMEA protocols and ONTB system operations.
    - **Process:**
        i. **Input:** Training materials or scenarios.
        ii. **Activities:**
            1. **Web Interface**: The ONTB provides an intuitive web interface for accessing training modules.
            2. **VS Code Development**: Hands-on coding and development sessions are facilitated through VS Code, enabling users to work with NMEA-compliant applications.
        iii. **Output**: Knowledgeable users capable of utilizing and maintaining the ONTB effectively.
    - **Value to Users**:
        i. Improves user proficiency in system operations.
        ii. Reduces onboarding time for developers and stakeholders.
        iii. Builds confidence in handling complex communication protocols.

2. **Start Pen Testing Process**
    - **Purpose**: This function assists security professionals in identifying vulnerabilities and ensuring robust system defenses.
    - **Process**:
        i. **Input**: Pen testing objectives or scenarios.
        ii. **Activities**:

1. **Message Identification**: Tools like Wireshark, CAN-utils, CAN Boat, and SCAPY are employed to analyze and log data traffic for vulnerabilities.
2. **Message Injection**: Custom applications inject simulated or malicious data into the system to test security boundaries.

iii. **Output**: Comprehensive assessment of the ONTB's security integrity.

- **Value to Users**:
  i. Enables proactive identification and mitigation of system vulnerabilities.
  ii. Ensures the ONTB meets high-security standards required in maritime environments.
  iii. Improves trust in the system's reliability for critical operations.

Requirements:

#	Name	Text	Refined By	Satisfied By	Verified By
1	DR1 Network Speeds	The ONTB network speeds shall be capable of handling NMEA OneNet traffic (Ethernet, IPv6), with up to 100Mbps level speeds.	Reviewing Performance Assessmer Network Packets	Cat 5e Cat6 Cat6A Ethernet Backbone Switch Wire	Test with internet connection to m
2	DR2 Computing	The ONTB shall use a BeagleBone Black devices.	Assessing Development and Protot Network Packets	BeagelBone Black	Design Check
3	DR3 MTBM - Hardware	The ONTB shall have a meant time between maintenance of one year for hardware	Perform Maintenance to System	Maintenance BeagelBone Black Cat 5e Cat6 Cat6A USB RJ45 Wire	MTBM
4	DR4 MTBF	The ONTB shall have a mean time between failure of 1500 hours.	Perform Maintenance to System	BeagelBone Black Cat 5e Cat6 Cat6A Maintenance RJ45 Software USB Wire	MTBF
5	DR5 Water Resistance	The ONTB shall have a IPX6 water resistance rating.	Stakeholder Needs/Requirements	Cat 5e Cat6 Cat6A BeagelBone Black USB RJ45 Wire	Water Inclusion Test
6	DR6 MTBM - Software	The ONTB shall have a mean time between maintenance 1 month for software updates.	Perform Maintenance to System	Software	MTBM
7	DR7 Potability	The ONTB system shall be sized no larger 12in length x 12in width and 6in height.	Stakeholder Needs/Requirements Assessing Development and Protot	BeagelBone Black Cat 5e Cat6 Cat6A RJ45 USB Wire	
8	DR8 Retirement	The ONTB shall have a minimum life cycle of 10 years.	Stakeholder Needs/Requirements Perform Maintenance to System Deploying Education and Training	OneNet Standard	Durability Testing
9	DR9 Logging	The ONTB shall log every packet that passes through the gateway.	Network Packets Implementing Security Assessment Reviewing Performance Assessmer	Software GitHub Wireshark	All Depndacies are Met with SDK
10	DR10 Downtime	The ONTB downtime shall not exceed 24 hours for software/hardware maintenance.	Stakeholder Needs/Requirements Perform Maintenance to System	Software OneNet Test Bench	Marine Tech Trial - Group Sudy Durability Testing
11	DR11 Developer Deployment T	The developer using ONTB shall be able to deploy and start testing NMEA OneNet applications with in an hour with proper training.	Assessing Development and Protot Deploying Education and Training	OneNet Test Bench Software GUI BeagelBone Black Wire	Marine Tech Trial - Group Sudy
12	DR12 In-Use Temperatures	The ONTB shall operate at temperatures of 0C to 50C	Reviewing Performance Assessmer Stakeholder Needs/Requirements	BeagelBone Black Cat 5e Cat6 Cat6A USB Wire	Marine Tech Trial - Group Sudy Thermotron Testing
13	DR13 Storage Temperatures	The ONTB shall be durable to storage temperatures of -20C to 70C.	Stakeholder Needs/Requirements	BeagelBone Black Cat 5e Cat6 Cat6A USB Wire RJ45	Thermotron Testing Marine Tech Trial - Group Sudy

Figure 15, Design Requirements table [5]

The following requirements were gathered for the OneNet Test Bench (ONTB) to address stakeholder needs, ensure system functionality, and verify compliance with performance metrics. Each requirement is tied to specific use cases, refined through design elements, and verified through testing. A few are listed below:

1. **Network Speeds**
    a. **Description**: The ONTB shall support NMEA OneNet traffic, handling up to 100 Mbps speeds.
    b. **Refined By:** Network Packets
    c. **Verified By:** Testing with an internet connection.
2. **Computing**
    a. **Description**: The ONTB shall use BeagleBone Black devices for core operations.
    b. **Refined By**: BeagleBone Black
    c. **Verified By**: Design checks.
3. **MTBM (Hardware)** (Mean time between maintenance)
    a. **Description**: The ONTB shall have a mean time between maintenance of one year for hardware.
    b. **Refined By**: Maintenance, BeagleBone Black
    c. **Verified By**: MTBM analysis.
4. **MTBF** (Mean time between failure)
    a. **Description**: The ONTB shall have a mean time between failures of 1500 hours.
    b. **Refined By**: Maintenance, BeagleBone Black
    c. **Verified By**: MTBF analysis.
5. **Water Resistance**
    a. **Description**: The ONTB shall have an IPX6 water resistance rating for maritime environments.
    b. **Refined By**: Hardware Components
    c. **Verified By**: Water Inclusion Testing.

These requirements were developed based on the Magic Grid Method, ensuring alignment with stakeholder needs:

- **Use Case Refinement**: The requirements for maintenance, performance, and robustness are directly refined through use cases, such as performing maintenance, reviewing performance assessments, and implementing security protocols.
- **Block Satisfaction**: Key system blocks, such as the networking stack, software suite, and hardware components, fulfill the technical requirements.
- **Test Cases Verification**: Each requirement is validated through targeted testing activities, ensuring performance benchmarks and operational goals are met.

By ensuring these requirements are traceable and verifiable, the ONTB design aligns with stakeholder needs and operational priorities, supporting its scalability, security, and reliability in maritime environments.

Detailed Design and Subsystem Analysis

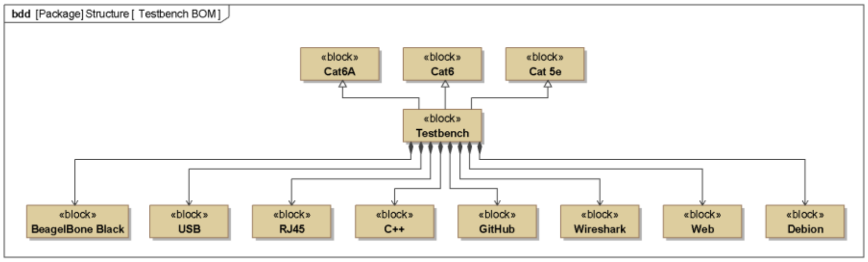

Figure 11, BDD describing further examples of subsystems used [5]

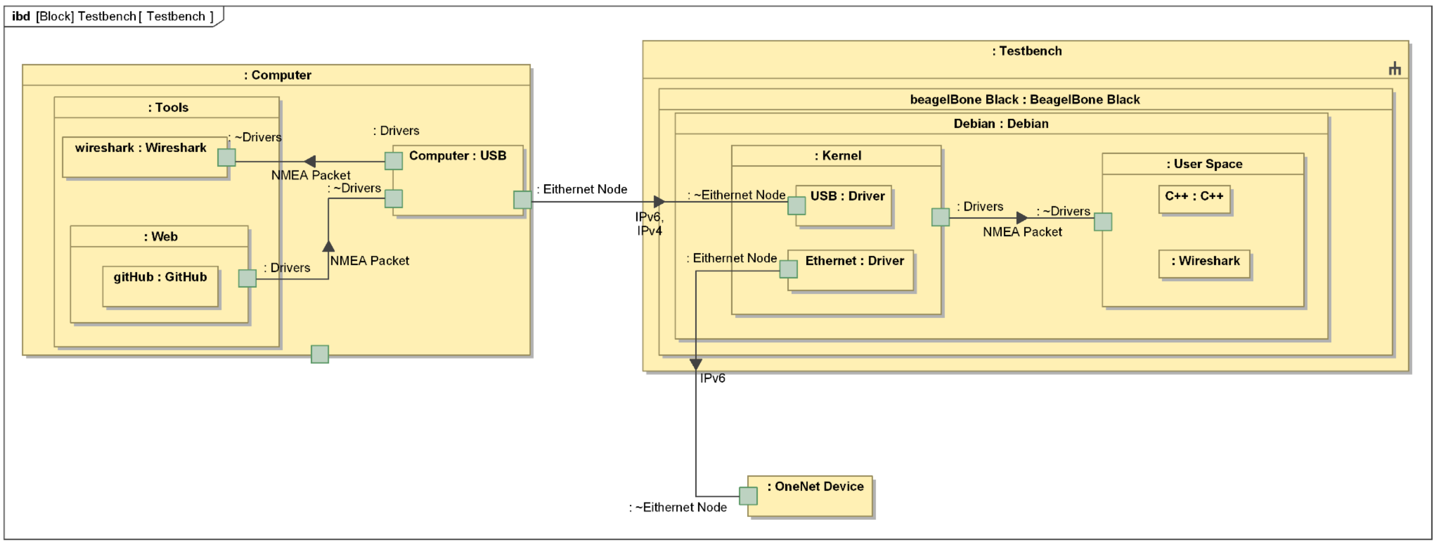

Figure 12, IBD describing subsystem connections

The key components for this system are hardware, and software. In hardware, there is the BeagleBone Black computational unit, the RJ45 Interface that connects external devices and networks, and lastly the cabling (Cat 5e, Cat 6, and Cat 6A). For software we have C++ programming language, Debian, Wireshark (network traffic analyzer), Web interface for remote config and monitoring, and GitHub for version control. In this system the interactions include network connectivity (ethernet cables and RJ45 interface data exchange), user interaction (access via web interface), and data analysis using Wireshark.

The system integrates internal components like the BeagleBone Black and external interfaces, including network connectivity through Cat 5e, Cat 6, and Cat 6A cables

The Queuing of NMEA Packets subsystem models the behavior of packet flows within the OneNet Test Bench. This subsystem is critical for ensuring the efficient processing of packets under varying network loads, enabling the evaluation of system performance, latency, and throughput in real-world maritime applications.

The queuing system is represented using a probabilistic approach based on queuing theory. The model calculates the probability P_n of having n packets in the queue at any given time:

$P_n = (1 - \frac{\lambda}{\mu}) \times (\frac{\lambda}{\mu})^n$ where

- λ: **Packet arrival rate** (packets per second)
  - Derived from network traffic patterns and device communication rates
- μ: **Packet service rate** (packets per second)
  - Dependent on system processing speed and hardware capabilities
- P_n: **Probability of n packets in the queue**
- n: **Queue length**
  - Number of packets waiting to be processed in the buffer
- **Performance metrics**
  - $p = \frac{\lambda}{\mu}$: Utilization
    - Indicates the fraction of time the system is busy
  - Queue delay: average time a packet spends in the queue
  - Throughput: Rate of successfully processed packets

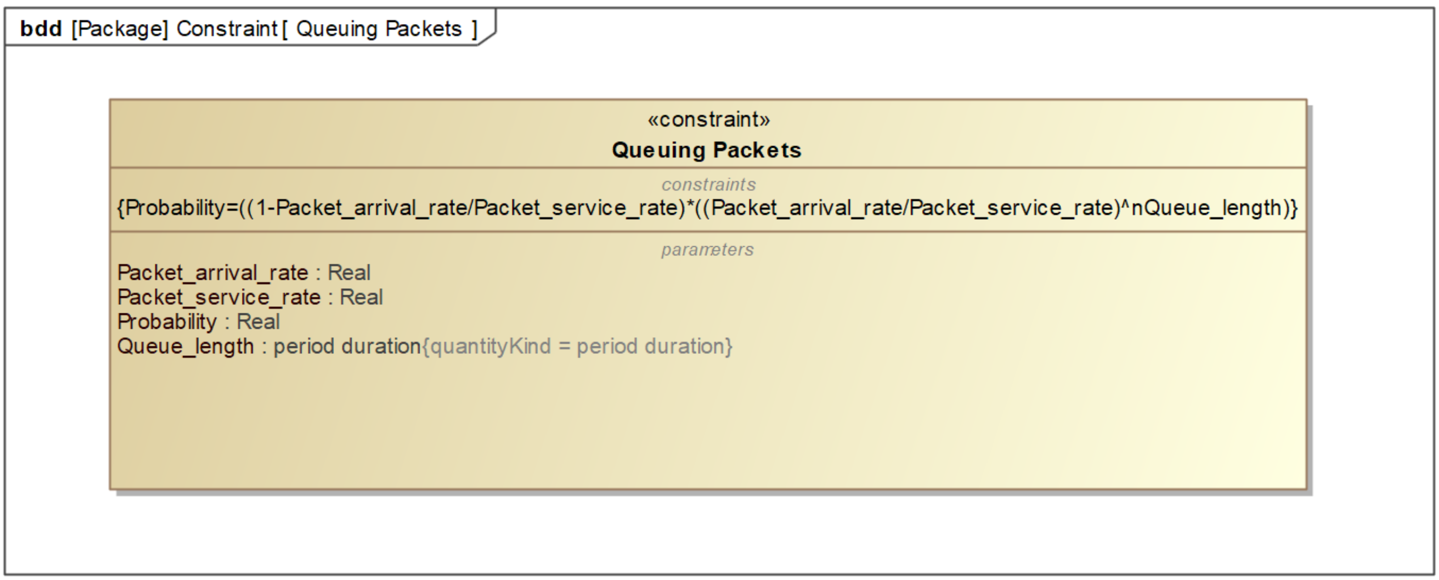

Figure 16, Constraint block [5]

This formula assumes an M/M/1 queue (single server, exponential interarrival and service times) with infinite buffer capacity.

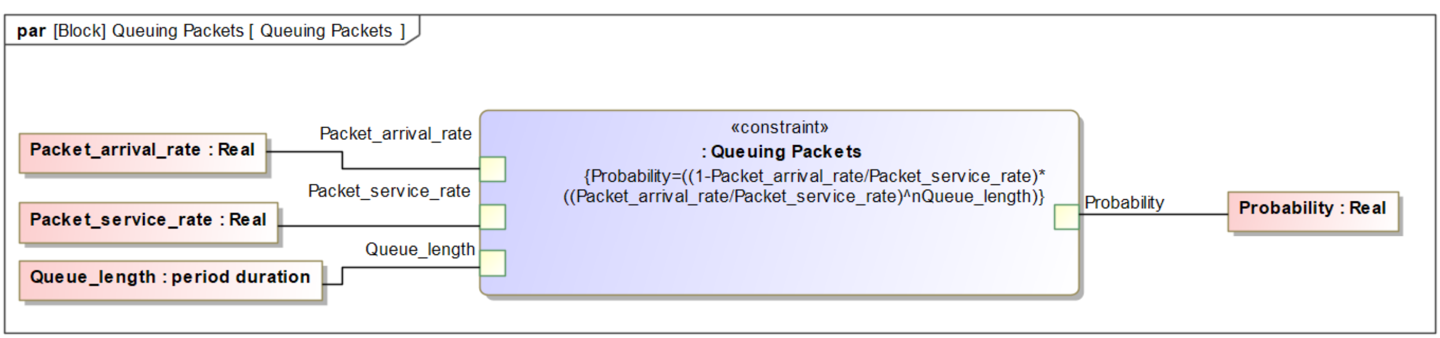

Figure 17, Parametric diagram showcasing requirement of throughput satisfaction

From the simulation of queuing analysis, we are able to perform the evaluations listed below.

1. **Packet Loss Probability**
    - For finite buffers, packets exceeding buffer capacity are dropped.
    - Loss probability is directly tied to buffer size and traffic intensity (ρ).
2. **Queue Length Distribution**:
    - Probability distribution P_n provides insights into system congestion under different traffic conditions.
3. **Latency Analysis**:
    - End-to-end delay includes both queuing and service times, critical for real-time applications.

In terms of subsystem traceability, the queuing analysis satisfies the original stakeholder needs through the following ways.

1. Supporting high-bandwidth packet processing for NMEA protocols.
2. Reducing latency for real-time communication in maritime systems.
3. Providing a scalable framework to test different traffic loads and network conditions.

The queuing subsystem models packet flow behavior, enabling performance evaluation under varying conditions. By analyzing key metrics such as queue delay, packet loss, and throughput, the system ensures reliable and efficient communication in NMEA-compliant networks.

Non-Functional Requirements Analysis

The reliability and maintainability of the OneNet Test Bench are critical for ensuring the system's ability to perform without interruption and to recover quickly from failures. These analyses demonstrate how the system design satisfies stakeholder needs for robust and efficient operation in maritime environments.

1. **Maintainability Analysis**
    - Maintainability measures the ease and speed with which a system can be restored to operational status following a failure.
    - The Mean Time Between Maintenance (MTBM) is calculated using this model

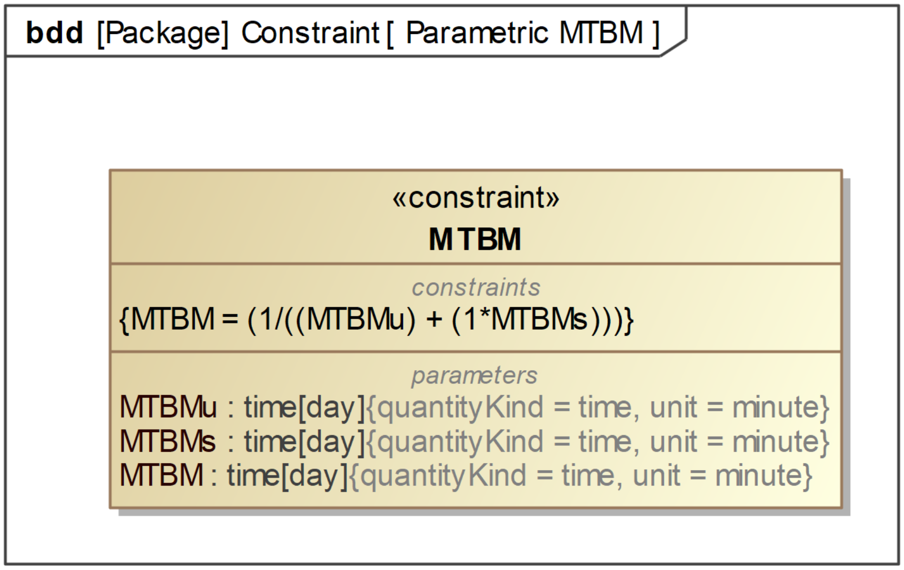

Figure 18, MTBM Constraint Block [5]

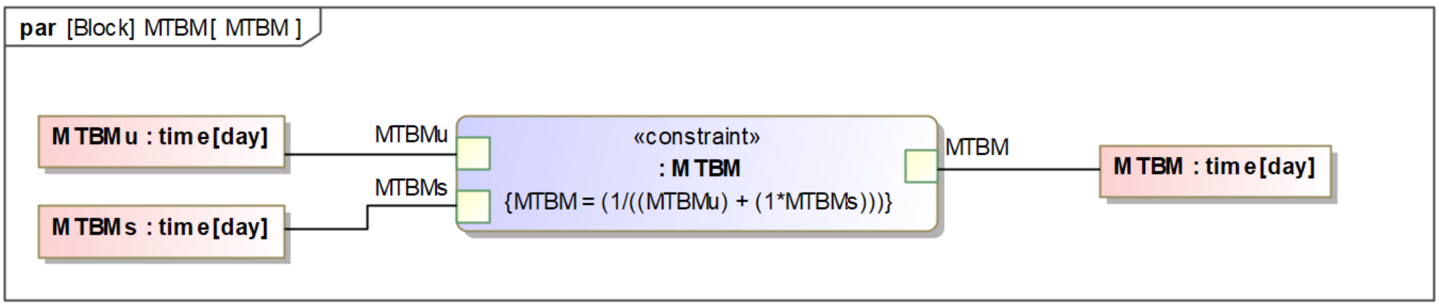

Figure 19, MTBM Parametrics [5]

$$MTBM = \frac{1}{\left(\frac{1}{MTBM_U} + \frac{1}{MTBM_S}\right)}$$

where

- $MTBM_U$: **Mean time between unscheduled maintenance**
    - Derived from system logs or simulated data for scheduled and unscheduled maintenance events
- $MTBM_S$: **Mean time between scheduled maintenance**
- **Results**:
    - The modular design of the Test Bench, with distinct gateways and software components, reduces repair complexity and downtime.
    - Maintainability is enhanced by accessible documentation and a real-time operating system (RTOS) to support diagnostics.
- **Traceability to Stakeholder needs:**
    - SN4: Need for interoperability. Maintainability ensures the system can adapt to new devices and services across different vendors by simplifying updates and maintenance.

- SN5: Need for scalability. Maintainable systems can accommodate growing networks and additional devices without requiring excessive effort.

2. **Reliability Analysis**
    - Reliability measures the probability that a system operates without failure over a specified time period.
    - The Mean Time Between Failures (MTBF) is calculated using this model

$$MTBF = MTBM + MTTR$$

where

- $MTBM$: **Mean time between maintenance**
    - Derived from system logs or simulated data for scheduled and unscheduled maintenance events
- $MTTR$: **Mean time to repair**
    - Where reliability R(t) is computed using the exponential reliability function:

      $R(t) = e^{-\frac{t}{MTBF}}$ where

    - t: operating time without failure
- Reliability block diagrams (RBD) are used to evaluate system configurations
    - Series Configuration
    - Parallel Configuration
- **Traceability to Stakeholder needs:**
    - SN1: Need for safe and secure communication. Reliability minimizes failures that could compromise secure and continuous communication.
    - SN3: Need for technological evolution. Reliable systems ensure that transitions to newer protocols (from NMEA 0183 to OneNet) occur smoothly and without disruptions.

Conclusion

The ONTB proof of concept allows users to connect via USB, to a terminal based system, with access to a development environment, and a web based GUI. The system also comes fully equipped with a security assessment software suite, and tools, such as virtualized NMEA 2000 and 0183 networks. The full OneNet functionality has not yet been certified, but has been implemented in a way adjacent to the needs of the OneNet protocol. This has all been completed within a semester, showcasing the reliability and efficiency of systems engineering methods such as magic grid SysML modeling.

References:

[1] Boating Magazine, "OneNet for Networking Marine Electronics," *Boating Mag*, [Online]. Available: https://www.boatingmag.com/gear/onenet-for-networking-marine-electronics/.

[2] IEEE Standard for Application and Management of the Systems Engineering Process, IEEE Std P1220-1994, Institute of Electrical and Electronics Engineers, New York, NY, USA, 1994.

[3] B. S. Blanchard and W. J. Fabrycky, *Systems Engineering and Analysis*, 5th ed. Upper Saddle River, NJ, USA: Pearson, 2011.

[4] J. L. Martin, *The Magic Grid Methodology: Bridging Stakeholder Needs and System Design*, 3rd ed., Wiley, 2020.

[5] SysML Diagram Repository, "OneNet Test Bench Use Case and System Diagrams," Academic Project Documentation, Colorado State University, 2024.

[6] "NASA-TAMU Hermes Project Using BeagleBone," BeagleBoard.org, Jun. 10, 2019. [Online]. Available: https://www.beagleboard.org/blog/2019-06-10-nasa-tamu-hermes.