Dot Ai Gen2 ZiM Bridge User Manual

A Comprehensive Guide to Seamless IoT Integration and Optimization

William Reny

Chief Customer Experience Officer

Charles Holman

Director of Quality, Enhancement and Development

Dec 21, 2024

Table of Contents

1. Introduction

Welcome to the Dot Ai Gen2 ZiM Bridge Training Manual, your go-to resource for understanding, installing, and optimizing this cutting-edge IoT solution. At Dot Ai, we are committed to enabling businesses to seamlessly connect physical assets with digital platforms through innovative, zero-infrastructure technology. Whether you are new to the Gen2 ZiM Bridge or seeking to enhance your expertise, this manual provides detailed guidance tailored to meet industry benchmarks.

The Gen2 ZiM Bridge is a pivotal component in modern IoT ecosystems, designed to address the challenges of integrating diverse devices and protocols into a unified system. It acts as a communication hub, supporting a wide array of protocols such as MQTT, CoAP, HTTP/HTTPS, Zigbee, Z-Wave, and BLE, ensuring compatibility and efficiency. By leveraging advanced edge processing capabilities—such as data filtering, transformation, compression, and analytics—the Gen2 ZiM Bridge delivers secure, real-time insights that empower informed decision-making and operational excellence.

This manual equips users with the necessary tools and knowledge for a seamless experience, from initial setup to advanced troubleshooting, ensuring that every user can maximize the potential of the Gen2 ZiM Bridge within their unique operational context.

1.1 Purpose of the Manual

This manual is designed to:

- Provide step-by-step instructions for the installation, configuration, and operation of the Gen2 ZiM Bridge.
- Serve as a reference guide for troubleshooting and maintenance.
- Enhance user confidence and efficiency through clear, concise, and actionable information.
- Support compliance with industry standards and best practices in IoT hardware deployment and management.

1.2 Scope

The Gen2 ZiM Bridge manual covers:

- **Device Features and Specifications:** Understanding the capabilities of the Gen2 ZiM Bridge.
- **Installation Procedures:** Detailed guidance for setting up the device in various environments.
- **Diagnostic and Maintenance Protocols:** Ensuring operational continuity through systematic diagnostics and proactive maintenance.

- **Safety Guidelines:** Protecting personnel, devices, and data during all phases of usage.
- **Advanced Functionality:** Leveraging the Gen2 ZiM Bridge for edge computing, data processing, and integration with cloud platforms.

This user manual applies to the following Hardware Version Identification Numbers (HVINs):

- **ZiM Marker Bridge - DAIC-MCB-XN**
- **ZiM Access Bridge - DAIC-ACB-XN**

All model variants share identical operating procedures, specifications, safety guidelines, and compliance information as described in this manual.

1.3 Target Audience

This manual is intended for:

- **Technicians and Installers:** Professionals responsible for the physical setup and initial configuration of the device.
- **Operational Staff:** End-users who monitor and utilize the device for day-to-day operations.
- **IT Specialists:** Teams managing system integration, diagnostics, and maintenance.
- **Decision Makers:** Stakeholders evaluating the device's impact on operational efficiency and scalability.

1.4 Key Features of the Gen2 ZiM Bridge

The Gen2 ZiM Bridge is designed with cutting-edge technology to meet the evolving needs of IoT environments. Key features include:

- **Multi-Protocol Support:**
    - Supports MQTT, CoAP, HTTP/HTTPS, Zigbee, Z-Wave, and BLE for maximum compatibility.
- **Edge Processing Capabilities:**
    - Data filtering, transformation, and compression for optimized cloud ingestion.
    - Localized analytics for real-time insights and decision-making.
- **Scalability:**
    - Adaptable for operations ranging from small facilities to enterprise-scale deployments.
- **Seamless Integration:**
    - Easy interoperability with existing IoT systems and cloud platforms.

- **Enhanced Security:**
    - Built-in encryption and secure access protocols to protect data integrity.

1.5 Industry Applications

The Gen2 ZiM Bridge is versatile and serves multiple industries:

- **Logistics and Supply Chain:**
    - Real-time asset tracking and route optimization.
- **Warehousing and Inventory Management:**
    - Enhanced visibility of inventory with actionable data analytics.
- **Industrial Automation:**
    - Facilitates predictive maintenance and M2M communication.
- **Healthcare:**
    - Tracks medical equipment and monitors environmental conditions for compliance.

1.6 Business Benefits for implementing Dot Ai Gen2 ZiM Bridge

Organizations adopting the Dot Ai Gen2 ZiM Bridge experience significant operational advantages:

1. **Cost Efficiency:**
    - Reduces infrastructure requirements with its zero-infrastructure design.
    - Eliminates the need for proprietary handhelds and antennas.
2. **Enhanced Operational Visibility:**
    - Provides real-time tracking and actionable insights to improve decision-making.
3. **Flexibility and Scalability:**
    - Grows with organizational needs, supporting a wide range of operational scales.
4. **Rapid Deployment:**
    - Plug-and-play setup minimizes downtime and accelerates integration.
5. **Data-Driven Insights:**
    - AI-powered analytics optimize processes and reduce inefficiencies.

1.7 How to Use This Manual

This manual is organized for easy navigation and practical usability:

- **Quick Start Guides:** Simplified instructions for immediate setup and operation.
- **Detailed Sections:** Comprehensive coverage of features, installation, and troubleshooting.

- **Appendices:** Additional resources, including a glossary of terms and technical specifications.

The Dot Ai Gen2 ZiM Bridge Training Manual serves as an indispensable resource for mastering the integration and operation of this advanced IoT gateway. By bridging the gap between IoT devices and cloud platforms, the Gen2 ZiM Bridge enables secure, efficient, and reliable data transmission while supporting a broad range of communication protocols and edge processing functionalities.

This manual provides step-by-step guidance for every phase of the device's lifecycle, ensuring users can seamlessly integrate it into their operations, troubleshoot effectively, and unlock its full potential. By adopting the Gen2 ZiM Bridge, organizations can streamline operations, enhance decision-making, and achieve significant cost efficiencies.

Whether you are just beginning to explore the capabilities of the Gen2 ZiM Bridge or refining your expertise, this manual is designed to support your journey toward operational excellence in IoT deployment.

2. Safety Guidelines

As a company specializing in the IoT devices, we operate in a dynamic and fast-evolving field where technology connects devices, systems, and people in unprecedented ways. With these advancements comes the responsibility to ensure a safe, secure, and compliant working environment for all employees, contractors, and stakeholders. This training manual serves as a comprehensive guide to the safety protocols and procedures essential for maintaining the integrity of our operations and the well-being of our team and partner companies.

Our approach to safety integrates both physical and digital considerations, recognizing the unique challenges of IoT ecosystems. From protecting sensitive data to ensuring safe handling of hardware and devices, every aspect of our operations has been designed with safety as a top priority. Adherence to these protocols is not only a regulatory requirement but also a fundamental part of fostering a culture of accountability and excellence within our organization.

This manual is designed to provide clear, actionable guidance on best practices, potential hazards, and response measures. Whether you are onboarding as a new employee, engaging in advanced technical work, or managing operations, this document will serve as a valuable resource. Together, we can uphold the high standards of safety that define our commitment to innovation and reliability in the IoT industry.

2.1 General Safety Precautions

Before beginning installation or operation, follow these general safety guidelines to minimize risks.

1. **Conduct a Site Risk Assessment:**
    - Inspect the workspace for hazards such as:
        - **Electrical Risks:** Exposed wiring, overloaded circuits, or high-voltage equipment.
        - **Physical Risks:** Moving machinery, unstable structures, or cluttered walkways.
        - **Environmental Risks:** Poor lighting, wet floors, extreme temperatures, or airborne particles.
    - Address any identified hazards before proceeding with installation.
2. **Restrict Access to Work Areas:**
    - Use safety barriers, cones, or warning signs to cordon off the installation area.
    - Notify nearby personnel about ongoing installation activities to prevent interference.
3. **Pre-Test Equipment Off-Site:**
    - Assemble and test IoT devices, including the Gen2 ZiM Bridge, in a controlled environment.
    - Verify compatibility with the network and system requirements to reduce onsite troubleshooting.
4. **Plan for Emergencies:**
    - Identify emergency exits and ensure that personnel know evacuation procedures.
    - Locate nearby fire extinguishers, first aid kits, and emergency contact numbers.

2.2 Required Safety Gear

All personnel must wear appropriate Personal Protective Equipment (PPE) during installation and maintenance to ensure their safety.

- **Hard Hats:** Protect against head injuries from falling objects.
- **Safety Glasses or Goggles:** Shield eyes from debris, sparks, or dust.
- **Gloves:**
    - Insulated gloves for electrical work.
    - General-purpose gloves for handling tools or components.
- **High-Visibility Vests:** Make personnel easily identifiable in busy environments.
- **Non-Slip Safety Shoes:** Prevent slips and protect feet from heavy objects.

- **Hearing Protection:** Required in areas with loud machinery or prolonged noise exposure.
- **Harnesses and Fall Protection:** Mandatory for working at heights above 6 feet. Ensure proper anchorage points are available.

2.3 Installation Steps with Safety in Mind

Follow these steps to ensure a safe and efficient installation of the Gen2 ZiM Bridge.

1. **Prepare the Workspace:**
    - Organize tools and equipment, ensuring they are in good working condition.
    - Eliminate clutter and secure the area to prevent accidents.
2. **Device Installation:**
    - Mount the Gen2 ZiM Bridge securely on a stable surface, following the manufacturer's instructions.
    - Use proper tools to avoid over-tightening screws or damaging components.
    - Avoid overreaching or improper posture when working at heights.
3. **Secure Connections:**
    - De-energize electrical circuits before connecting any power cables.
    - Use insulated tools for handling live connections.
    - Confirm that all connections are properly grounded and insulated.
4. **Perform System Checks:**
    - After installation, verify the device is operational by conducting a basic functionality test.
    - Check for proper power supply and network connectivity.
5. **Restore the Work Area:**
    - Remove all tools, debris, and barriers from the workspace.
    - Confirm the area is safe and ready for normal operations.

2.4 Operational Safety During Use

Once the Gen2 ZiM Bridge is operational, follow these guidelines to maintain safety:

- **Avoid Overloading:**
    - Do not exceed the recommended number of connected devices or data throughput limits.
- **Monitor for Faults:**
    - Regularly check for warning indicators such as abnormal LED signals, error messages, or overheating.
- **Protect Against Cyber Threats:**
    - Use secure passwords and encryption for device access.

- Regularly update firmware to address vulnerabilities.

2.5 Final Safety Checklist

Before leaving the site, ensure all safety measures have been followed:

- ☐ All devices are securely installed and tested.
- ☐ Electrical circuits are properly grounded and insulated.
- ☐ No tools, debris, or temporary barriers remain in the workspace.
- ☐ All safety incidents, if any, have been documented and reported to the supervisor.

2.6 Emergency Preparedness

Being prepared for emergencies can prevent injuries and minimize damage in critical situations.

1. **Emergency Shutdown:**
   - Familiarize personnel with procedures for deactivating the Gen2 ZiM Bridge in case of a malfunction or safety threat.
2. **Fire Safety:**
   - Ensure fire extinguishers are readily accessible near the installation site.
   - Avoid placing the Gen2 ZiM Bridge near flammable materials or heat sources.
3. **First Aid Response:**
   - Train onsite personnel in basic first aid techniques.
   - Provide immediate care for injuries and report incidents to safety officers.

2.7 Regulatory Compliance

The installation and operation of the Gen2 ZiM Bridge must comply with all relevant safety and environmental standards, including:

- **Electrical Safety Standards:** Adhere to local electrical codes and best practices.
- **Environmental Protection:** Dispose of packaging materials and obsolete equipment responsibly to minimize environmental impact.
- **Occupational Safety Standards:** Follow OSHA or equivalent guidelines for workplace safety.

2.8 Battery Safety & Replacement

Approved replacement battery

- Use only ONE 18650 lithium-ion (Li-ion) rechargeable cell (18 × 65 mm).

- Do NOT use AA/AAA/C/D, CR123A, 18350, 14500, 21700, coin cells, alkaline, NiMH/NiCd, or primary (non-rechargeable) lithium cells.

Replacement battery identification marking (for product label and battery compartment)

- REPLACEMENT BATTERY: 18650 Li-ion only (Ø18×65 mm).
- POLARITY: Match + and – symbols.
- HAZARD: Risk of fire/burn/explosion if wrong type/size, reversed, shorted, damaged, or >60 °C (140 °F).

Instructional safeguard — warnings to prevent misuse

- Use the correct size/type only; do not force a battery that does not fit.
- Observe polarity; do not install the battery in reverse.
- Do not use damaged, rewrapped, swollen, leaking, or modified cells.
- Do not short the terminals or carry loose cells with metal objects.
- Charge only with the charger/method specified for this product; never charge non-rechargeable cells.
- Keep away from heat, flames, liquids, and temperatures above 60 °C (140 °F).
- Keep batteries out of reach of children.

Emergency

- If the device or battery becomes hot, swells, smokes, or leaks: move away from combustibles, do not touch, ventilate, and after cooling dispose of the battery per local rules.

2.9 RF Exposure Warning (Mobile Use — Maintain 20 cm Separation)

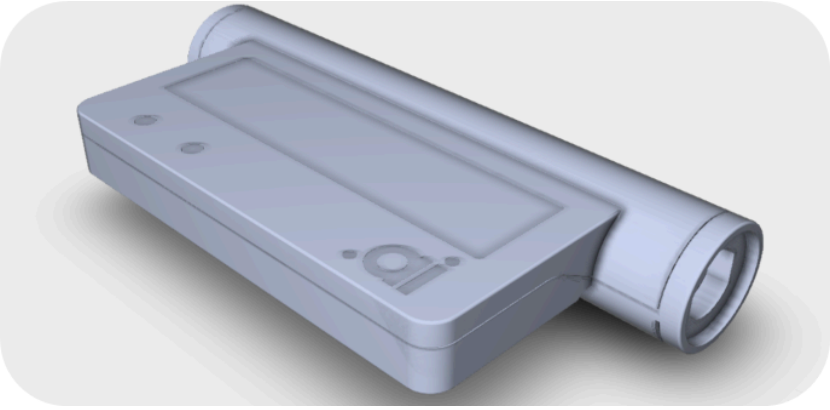
This equipment must be installed and operated with a minimum distance of **20 cm (8 in.)** between the radiator (antenna) and all persons. Do not operate the device closer than 20 cm to bystanders during normal use. This transmitter must **not** be co-located or operated in conjunction with any other antenna or transmitter unless a separate RF exposure evaluation demonstrates compliance.

2.10 Safety Summary

Safety is a shared responsibility that ensures the well-being of individuals and the reliability of operations. By adhering to these guidelines, users and technicians can confidently install, operate, and maintain the Gen2 ZiM Bridge while minimizing risks.

Always prioritize safety, remain vigilant, and address potential hazards proactively. Together, these practices ensure the successful deployment of cutting-edge IoT technology in a safe and compliant manner.

3. System Overview



The Dot Ai Gen2 ZiM Bridge is a pivotal component of the Dot Ai zero-infrastructure IoT ecosystem, designed to seamlessly connect IoT devices with cloud platforms. This section provides a comprehensive overview of its purpose, features, and operational benefits, emphasizing how the bridge enhances real-time data management and operational efficiency.

3.1 Overview of the Gen2 ZiM Bridge

The Dot Ai Gen2 ZiM Bridge is an advanced IoT gateway that acts as a communication hub between IoT devices and the cloud. It facilitates secure, efficient, and reliable data transmission, supporting multiple communication protocols to ensure compatibility with a wide range of devices.

Key features include:

- **Protocol Support:**
  - MQTT, CoAP, HTTP/HTTPS, Zigbee, Z-Wave, and Bluetooth Low Energy (BLE).
- **Edge Processing:**
  - Data filtering, transformation, and compression to optimize cloud ingestion.
- **Scalability:**
  - Supports a large number of connected devices, making it ideal for warehouses, logistics, and industrial settings.

3.2 Key Applications

The Dot Ai Gen2 ZiM Bridge is designed to solve real-world challenges in diverse industries, including:

- **Warehousing and Inventory Management:**
    - Enables precise asset tracking and inventory control with real-time updates.
    - Reduces manual errors and improves operational efficiency.
- **Logistics and Supply Chain:**
    - Facilitates seamless tracking of goods in transit, providing visibility at every stage.
    - Optimizes routes and reduces delays through real-time data integration.
- **Industrial Automation:**
    - Enhances machine-to-machine (M2M) communication.
    - Supports predictive maintenance by collecting and analyzing performance data.

3.3 Integration Capabilities

The Dot Ai Gen2 ZiM Bridge is engineered for easy integration with existing infrastructure and systems:

- **Plug-and-Play Design:**
    - Simple setup process with minimal configuration required.
- **Cloud Connectivity:**
    - Connects directly to Dot Ai's cloud-based dashboard, which aggregates, analyzes, and visualizes data in real time.
- **Seamless Compatibility:**
    - Works with industry-standard IoT protocols and is adaptable to custom workflows.

3.4 Key Product Variants

The Dot Ai Gen2 ZiM Bridge is available in three differentiated models to address specific operational needs:

1. **Marker:**
    - Ideal for static locations, such as designated storage zones or inventory shelves.
    - Focuses on high accuracy and reliability in fixed environments.
2. **Access:**
    - Positioned at entry points, such as doors or gates, to monitor asset movements.
    - Provides data-driven insights into traffic flow and access control.

3.5 Operational Benefits

The Dot Ai Gen2 ZiM Bridge delivers significant advantages that help organizations streamline operations and achieve their goals:

- **Cost Efficiency:**
    - Eliminates the need for proprietary hardware, antennas, or fixed installations.
    - Reduces infrastructure costs while enabling rapid deployment.
- **Enhanced Decision-Making:**

    - Provides actionable insights through AI-driven analytics.
    - Facilitates process optimization and demand forecasting.
- **Scalability and Flexibility:**
    - Supports scaling from small operations to enterprise-wide deployments without additional infrastructure investments.

3.6 Notifications and Alerts

The Gen2 ZiM Bridge integrates with Dot Ai's cloud software to enable proactive notifications and alerts:

- **Visual and Audio Alerts:**
    - Notify users directly through the bridge for immediate action.
- **Mobile Notifications:**
    - Push real-time alerts to mobile devices, ensuring stakeholders stay informed.

3.7 Onboarding Process for the Gen2 ZiM Bridge

The onboarding process ensures a seamless integration of the Gen2 ZiM Bridge into your IoT ecosystem. This step-by-step guide is designed to simplify setup, minimize errors, and enable users to get started quickly.

3.7.1 Gateway Onboarding

The first step is to onboard the gateway device, which connects the Gen2 ZiM Bridge to your cloud platform.

1. **Power Up the Gateway:**
    - Connect the gateway to a reliable power source.
    - Ensure the LED indicators are active, signaling readiness for setup.
2. **Open the Wiliot Mobile App (Installer Mode):**
    - Log in using your installer credentials.
    - Navigate to the "Gateway Setup" section.
3. **Reset the Gateway:**
    - Use a small pin or paperclip to press the reset button on the gateway until the LED flashes, indicating it is in setup mode.
4. **Connect to Wi-Fi:**
    - Follow the in-app instructions to connect the gateway to the desired Wi-Fi network.
    - Ensure a strong and stable connection to facilitate reliable data transmission.
5. **Link the Gateway to the Dot Ai Instance:**
    - Log into your Dot Ai dashboard and navigate to **Devices > Asset Gateway**.
    - Select **More Actions > Add Gateway**.
    - Enter the **Gateway ID** and **Gateway Name** (found on the "Gold Sheet" accompanying the device).

- Click **Confirm** to complete the onboarding process.

3.7.2 Item Creation

Items are assets that need to be tracked using the Dot Ai Gen2 ZiM Bridge. Follow these steps to add items to the platform.

1. **Access the Dot Ai Instance:**
   - Log into your Dot Ai dashboard Https://track-xxx.stg.daic.ai/
2. **Navigate to the Trackables Section:**
   - From the dashboard menu, select **Trackables > Items**.
   - Click **+ Add** to create a new item entry.
3. **Input Item Information:**
   - Scan the item barcode or manually enter details such as:
     - **Item ID**
     - **Item Name**
     - Other relevant metadata (e.g., category, location).
4. **Save and Create:**
   - Click **Create** to finalize the addition of the item to the platform.

3.7.3 Asset Tag Creation

Asset tags are physical identifiers placed on items for tracking. They must be linked to the corresponding item in the system.

1. **Navigate to the Asset Tags Section:**
   - From the dashboard menu, go to **Devices > Asset Tags**.
2. **Add a New Asset Tag:**
   - Select **More Actions > Add** to initiate a new asset tag entry.
3. **Link the Asset Tag to an Item:**
   - Input the **Item ID Link** to associate the asset tag with the item created earlier.
4. **Enter the Asset Tag Barcode:**
   - Scan or manually input the barcode associated with the asset tag.
5. **Save and Create:**
   - Click **Create** to assign the asset tag to the corresponding item.

3.7.4 Final Validation

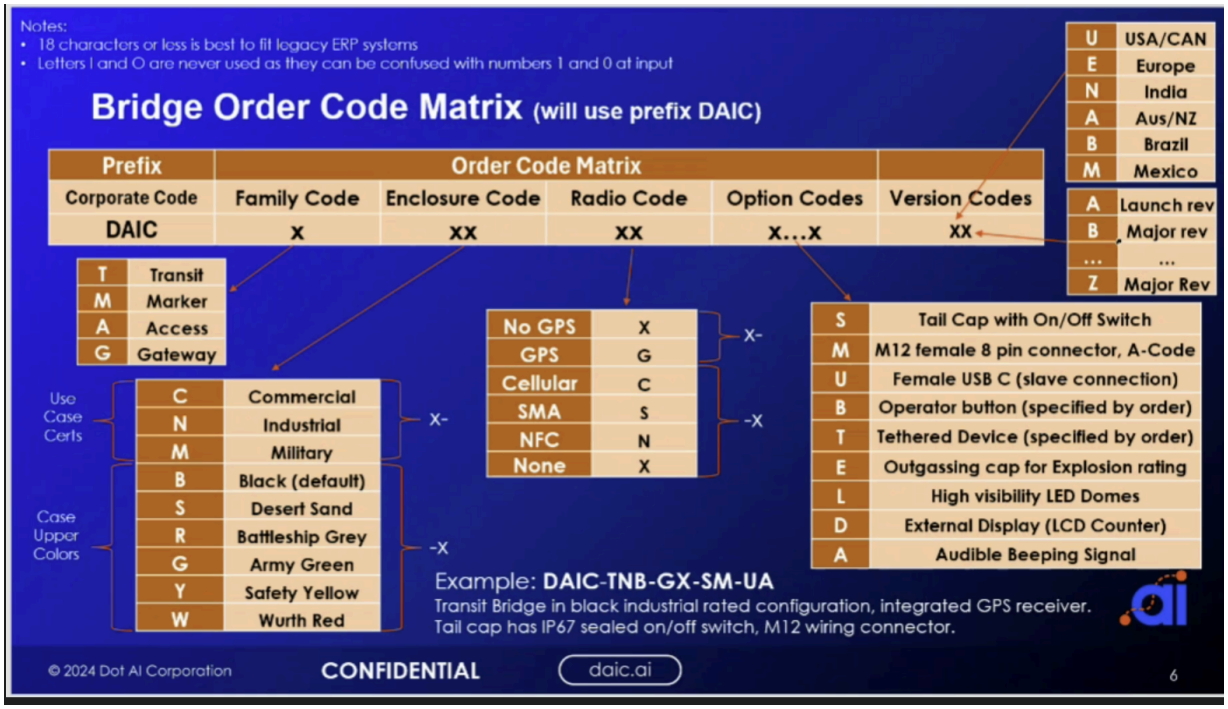
To ensure successful onboarding, perform the following checks:

- Verify that the gateway appears as active in the Dot Ai dashboard.
- Confirm that all items and asset tags are correctly listed and associated.
- Test connectivity by simulating a data transmission or movement event.

3.7.5 Important Notes for Onboarding:

- Ensure all items, asset tags, and gateways are registered in the correct Dot Ai instance.
- Use the **Gold Sheet** accompanying the device to verify IDs and names.
- If errors occur during onboarding, consult the troubleshooting section for resolution steps.

3.8 Bridge Order Code Matrix:

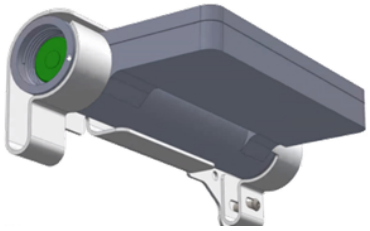


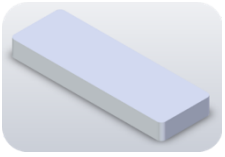
Part Number	Description
DAIC-ACB-XN	Access Bridge for ZIM system, integrated BLE/ZIM and LoRA/LRL radios, NFC Slave. Industrial M12 connector, 8 pin A-code female for wired I/O and power. High visibility signal and diagnostic LEDs. IP54 enclosure. Includes mounting pad
DAIC-MCB-XN	Marker Bridge for ZIM system, integrated BLE/ZIM and LoRA/LRL radios. NFC slave. Bright signal LEDs. IP54 enclosure. Includes mounting pad.

ZIM Bridge enclosure **Mounting Bracket and Pad**

optional external connection port at head of tube

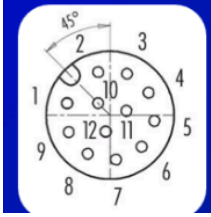
optional security latch feature integrated





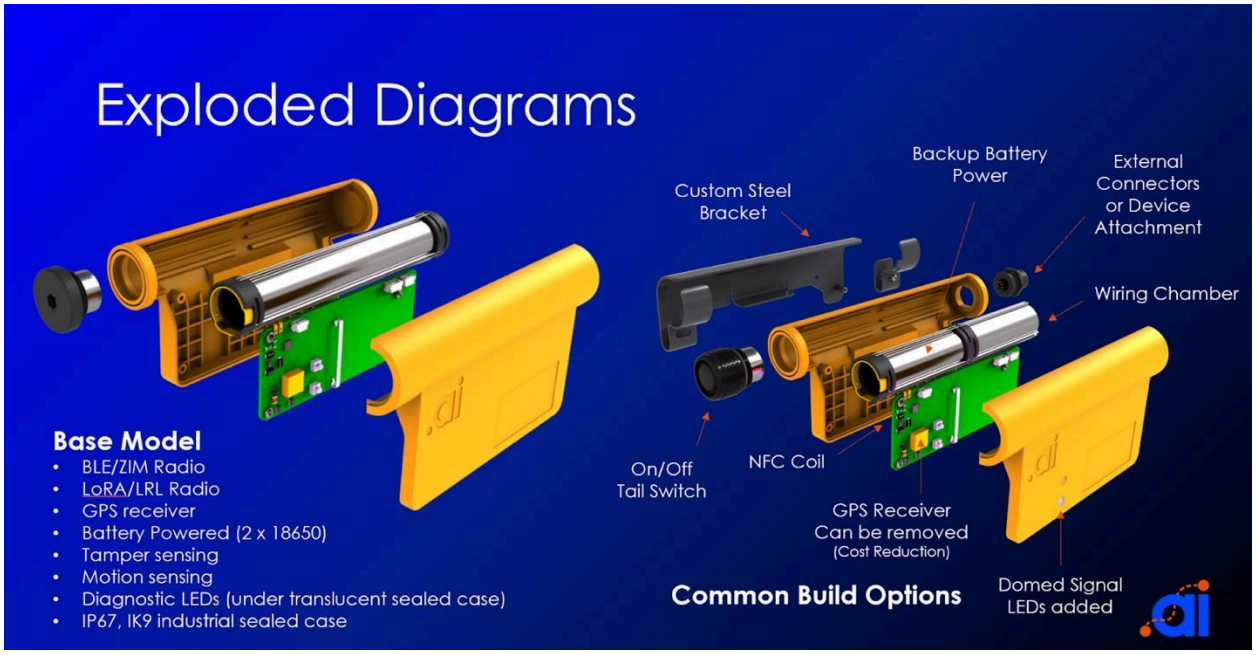
3.9 M12 Connector wiring detail:

A Code, 8 Pole Female Socket



12 Pole for test only

Pin	in mm X	in mm Y	Color	Description
1	2.69	0.57	Brown	GPIO – 1 (3.3 VDC)
2	0.57	2.69	Blue	GPIO – 2 (3.3 VDC)
3	-1.66	2.2	White	GPIO – 3 (3.3 VDC)
4	-2.75	0.19	Green	GPIO – 4 (3.3 VDC)
5	-1.94	-1.94	Pink	Ground
6	0.19	-2.74	Yellow	Ground
7	2.2	-1.65	Black	V- (6 – 28 VDC)
8	0	0	Grey	V+ (6 – 28 VDC)
9			Red	Tx
10			Violet	Rx
11			Orange	SWDIO
12			Light Green	SWCLK



4. Diagnostic Principles

4.1 Diagnostic Philosophy

The Dot Ai diagnostic philosophy for the Gen2 ZiM Bridge is crafted to meet and exceed industry benchmarks by emphasizing precision, efficiency, and sustainability. This approach ensures that IoT systems maintain optimal performance while minimizing downtime and resource expenditure. The guiding principles include:

Proactive Diagnostics: Predict and Prevent

- **Real-Time Monitoring:**
    - Utilize continuous data collection from IoT devices, the Gen2 ZiM Bridge, and connected systems to monitor performance indicators such as latency, packet loss, and connectivity stability.
    - Implement anomaly detection algorithms to flag irregular patterns before they evolve into system failures.
- **Predictive Analytics:**
    - Leverage historical data and machine learning models to predict potential failures or maintenance needs.
    - Incorporate environmental and operational factors (e.g., temperature, usage cycles) into predictive models.
- **Scheduled Health Checks:**

    - Define routine diagnostic intervals tailored to the usage intensity and environmental conditions of the device.
    - Ensure system calibration and firmware updates are part of the preventive maintenance schedule.

Systematic and Iterative Approach: Diagnose with Confidence

- **Logical Workflow:**
    - Follow a structured diagnostic process to ensure no variables are overlooked.
    - Use industry-standard frameworks like the **ISO 9001 Plan-Do-Check-Act (PDCA)** cycle for continuous improvement in troubleshooting processes.
- **Standardized Documentation:**
    - Maintain detailed records of all diagnostic activities, including identified symptoms, actions taken, and resolutions achieved. This enables knowledge sharing and consistency across diagnostic teams.
- **Iterative Problem Solving:**
    - Break down complex problems into manageable components to isolate root causes effectively.
    - Reevaluate and refine diagnostic processes based on outcomes and new insights.

Root Cause Resolution: Fix the Core, Not Just the Symptom

- **Focus on Fundamentals:**
    - Emphasize resolving the underlying cause rather than treating surface-level symptoms. This reduces the likelihood of recurrence and ensures long-term stability.
- **Comprehensive Root Cause Analysis (RCA):**
    - Employ advanced RCA techniques like fault tree analysis (FTA) and failure mode and effects analysis (FMEA) to systematically identify and mitigate risks.
    - Integrate feedback from RCA into system updates, improving design and functionality.
- **Preventive Actions:**
    - Implement design or process modifications based on diagnostic insights to address systemic weaknesses.
    - Create proactive workflows to manage recurring issues identified during diagnostics.

Collaborative Diagnostics: Leverage Expertise

- **Cross-Functional Collaboration:**
    - Facilitate communication between technicians, engineers, and end-users to pool knowledge and insights during diagnostics.

    - Develop a centralized diagnostic hub where all stakeholders can access shared resources, including diagnostic logs, standard operating procedures (SOPs), and troubleshooting guides.
- **Feedback Integration:**
    - Use real-world diagnostic outcomes to refine the Gen2 ZiM Bridge and its supporting documentation.
    - Establish a formal feedback mechanism to capture insights from technicians and end-users, driving continuous improvement.

Efficiency through Innovation: Automate and Accelerate

- **Diagnostic Automation:**
    - Incorporate diagnostic scripts and AI-driven tools to identify and resolve common issues autonomously.
    - Enable remote diagnostics to reduce the need for onsite interventions, saving time and resources.
- **Smart Alerts:**
    - Configure the Gen2 ZiM Bridge to send real-time alerts with detailed diagnostic data to technicians.
    - Include actionable recommendations with alerts to streamline issue resolution.

Benchmark Alignment: Meeting Industry Standards

- Adhere to global IoT and diagnostic standards, including:
    - **ISO/IEC 30141**: Internet of Things (IoT) Reference Architecture for system robustness.
    - **ITIL Framework**: Best practices for incident management in IoT environments.
    - **ISO 27001**: Ensure diagnostic processes align with information security management protocols to protect sensitive data.
- Stay updated on industry trends and emerging technologies to ensure diagnostic strategies remain state-of-the-art.

4.2 Chrysler-Inspired Approach to Troubleshooting

The Chrysler-Inspired Approach to Troubleshooting adapts an established, methodical diagnostic methodology, emphasizing precision, repeatability, and efficiency. This structured approach, widely respected in the automotive and manufacturing industries, is tailored here to meet the needs ofDot Ai's IoT environments like the Gen2 ZiM Bridge, where seamless connectivity and real-time data flow are critical.

Key Elements of the Chrysler-Inspired Approach

This troubleshooting approach is divided into five fundamental stages, ensuring every possible cause is systematically explored and resolved. Each stage is designed to minimize downtime and optimize device performance.

Step 1. Observe and Document Symptoms

Objective: Collect detailed, precise, and comprehensive information about the problem.

- **Record Observations:**
  - Note when and where the issue occurs.
  - Document any related system behaviors (e.g., error messages, device logs, connectivity interruptions).
  - Record environmental conditions (e.g., temperature, humidity, nearby interference sources).
- **Ask the Right Questions:**
  - What were the last actions performed before the issue occurred?
  - Is the problem consistent or intermittent?
  - Are other systems or devices affected?
- **Visual Inspection:**
  - Inspect the hardware for physical damage (e.g., frayed wires, loose connections, or damaged tags).
  - Ensure power and data connections are secure and stable.

Step 2. Analyze and Hypothesize

Objective: Use available data to develop possible causes for the problem.

- **Review Logs and Data:**
  - Examine IoT device logs and the cloud dashboard for abnormalities.
  - Look for patterns in errors (e.g., recurring error codes, increased latency, or failed communications).
- **Narrow Down Variables:**
  - Focus on elements directly involved in the issue, such as:
    - Protocol compatibility.
    - Environmental interferences (e.g., RF signal disruption).
    - Software or firmware versions.
- **Leverage Historical Data:**
  - Refer to prior troubleshooting cases with similar symptoms to identify potential root causes.
  - Utilize a knowledge base or diagnostic database to enhance hypothesis accuracy.

Step 3. Test Hypotheses Systematically

Objective: Validate or eliminate each potential cause through controlled testing.

- **Isolate Components:**
    - Disconnect non-essential devices or systems to reduce complexity.
    - Test each component individually (e.g., test a single sensor with the Gen2 ZiM Bridge to check compatibility).
- **Simulate Scenarios:**
    - Replicate the problem in a test environment to confirm conditions that trigger the issue.
    - Use diagnostic tools, such as network analyzers, to monitor communication between the IoT device, bridge, and cloud.
- **Iterative Testing:**
    - Modify one variable at a time (e.g., change the communication protocol or firmware version).
    - Record results after each adjustment to pinpoint the variable causing the issue.

Step 4. Resolve and Implement Solutions

Objective: Apply the solution identified through testing to resolve the issue effectively.

- **Execute Repairs:**
    - Update or reconfigure software and firmware.
    - Repair or replace faulty hardware components.
- **Document the Fix:**
    - Record the steps taken to resolve the issue for future reference.
    - Include details about replaced components, updated configurations, and the timeline for implementation.
- **Ensure Compliance:**
    - Verify that all changes adhere to relevant standards (e.g., ISO 27001 for data security, or industry-specific protocols).

Step 5. Validate the Resolution

Objective: Confirm that the problem has been resolved and the system is operating normally.

- **Conduct Functional Tests:**
    - Recheck all system components to ensure they function as expected.
    - Run end-to-end system tests to confirm seamless data flow between the IoT device, Gen2 ZiM Bridge, and cloud platform.
- **Stress Test the System:**
    - Test the system under typical and extreme operating conditions to confirm stability and reliability.

- **Monitor Post-Resolution:**
    - Keep the system under observation for a designated period to ensure no residual or secondary issues arise.

Best Practices for Applying the Chrysler-Inspired Approach

1. **Standardized Tools and Templates:**
    - Use predefined checklists and templates to ensure consistency in data collection and analysis.
    - Provide technicians with diagnostic tools such as signal analyzers, multimeters, and software log viewers.
2. **Collaboration:**
    - Encourage open communication between team members, ensuring insights and observations are shared promptly.
    - Use collaborative diagnostic platforms to document findings in real time.
3. **Training and Knowledge Sharing:**
    - Conduct regular training sessions for technicians to familiarize them with the troubleshooting methodology.
    - Develop a knowledge base with detailed case studies to assist in future diagnostics.

Benefits of the Chrysler-Inspired Approach

- **Efficiency:** Reduces time spent diagnosing and resolving issues by systematically narrowing down root causes.
- **Repeatability:** Ensures consistent results, regardless of the technician or location.
- **Knowledge Building:** Captures valuable insights for continuous improvement in troubleshooting and system design.

4.3 Five-step Diagnostic Process

The five-step diagnostic process is a structured and iterative framework designed to identify and resolve issues in the Dot Ai Gen2 ZiM Bridge. This methodology ensures that diagnostics are thorough, efficient, and aligned with best practices in the IoT and technology industries. By following this approach, technicians can systematically address system problems while minimizing downtime and resource use.

Step 1: Gather Information

Objective: Collect comprehensive data to understand the problem's context and scope.

- **System Data Collection:**

    - Extract logs from the Dot Ai Gen2 ZiM Bridge, IoT devices, and the cloud platform.
    - Look for anomalies such as connectivity drops, unexpected latency, or error codes.
    - Use diagnostic software to consolidate data from multiple sources.
- **User Feedback:**
    - Interview end-users or operators to capture firsthand accounts of the issue.
    - Ask specific questions, such as:
        - When did the issue first occur?
        - What actions were being performed at the time?
        - How often does the issue happen?
- **Environmental Assessment:**
    - Inspect the physical installation for potential external factors, such as:
        - Electromagnetic interference (EMI) from nearby equipment.
        - Temperature or humidity levels outside the recommended operating range.
        - Power supply fluctuations or interruptions.
- **Document Observations:**
    - Record all findings in a structured diagnostic report to maintain a clear audit trail.

Step 2: Verify the Problem

Objective: Confirm the problem exists and identify the specific conditions that trigger it.

- **Reproduce the Issue:**
    - Attempt to replicate the problem in the actual operating environment.
    - If unsafe or impractical, simulate the issue in a controlled testing environment.
- **Analyze System Behavior:**
    - Monitor the Gen2 ZiM Bridge during testing using diagnostic tools such as:
        - Protocol analyzers to evaluate data exchange.
        - Spectrum analyzers to identify signal interference.
- **Check System Dependencies:**
    - Verify that all dependencies (e.g., network connectivity, power supply) are functioning correctly.
    - Ensure that software and firmware versions are compatible and up-to-date.
- **Confirm Consistency:**
    - Determine if the issue is repeatable or intermittent, which helps narrow potential causes.

Step 3: Perform Root Cause Analysis

Objective: Identify the fundamental cause of the problem using systematic analysis.

- **Data Analysis:**
  - Review error codes, system logs, and test results to pinpoint anomalies.
  - Correlate symptoms with potential causes using diagnostic charts or graphs.
- **Structured Problem Solving:**
  - Use established root cause analysis tools, such as:
    - **Fishbone Diagram (Ishikawa):** Categorize causes into hardware, software, environmental, and user-related factors.
    - **5-Why Analysis:** Continuously ask "why" to trace the issue back to its source.
- **Eliminate Probable Causes:**
  - Test potential causes individually and eliminate those that do not produce the observed symptoms.
  - Focus on the most likely root cause based on data and testing.

Step 4: Repair and Replace

Objective: Implement corrective actions to resolve the identified issue.

- **Execute Repairs:**
  - For software-related issues:
    - Update or reinstall firmware.
    - Reconfigure device settings or network parameters.
  - For hardware-related issues:
    - Replace faulty components, such as power supplies, connectors, or antenna modules.
    - Ensure new components are tested for compatibility before full integration.
- **Validate Changes:**
  - Conduct functional tests immediately after implementing fixes to confirm resolution.
  - Use system benchmarks to compare performance before and after the repair.
- **Document Actions:**
  - Record all corrective measures in the diagnostic report, including:
    - Components replaced.
    - Software or firmware changes.
    - Time and resources required.

Step 5: Test and Validate

Objective: Ensure the issue is resolved and the system functions within expected parameters.

- **Systematic Testing:**
    - Perform comprehensive tests across all system components, including:
        - Connectivity and data transmission tests.
        - Device integration with IoT ecosystems.
        - Stress tests to evaluate performance under peak load conditions.
- **Monitor for Stability:**
    - Place the system under observation for an extended period to ensure no recurring issues.
    - Enable automated alerts for real-time monitoring of system health.
- **Engage End-Users:**
    - Allow users to interact with the system and confirm that it meets operational expectations.
    - Provide a feedback mechanism for reporting any residual issues.
- **Close the Diagnostic Loop:**
    - If the issue reappears, revisit earlier steps and refine the diagnostic approach.
    - Use lessons learned to improve future diagnostics and system resilience.

Key Considerations for Success

1. **Documentation:**
    - Maintain a detailed diagnostic log to track progress, ensure transparency, and facilitate future reference.
2. **Standardization:**
    - Use standardized tools, templates, and processes to ensure consistent and repeatable results across different teams and locations.
3. **Collaboration:**
    - Foster teamwork between technicians, engineers, and end-users to enhance problem-solving effectiveness.
4. **Continuous Improvement:**
    - Review diagnostic outcomes to identify areas for improvement.
    - Update training, documentation, and diagnostic tools based on real-world experiences.

5. Tools and Equipment

5.1 Required Diagnostic Tools

5.2 Software Requirements

5.3 Calibration and Maintenance of Tools

6. Diagnostic Procedures

Diagnostic procedures are critical for maintaining the operational efficiency of the Dot Ai Gen2 ZiM Bridge. This section provides a detailed step-by-step approach for systematically diagnosing and resolving issues, ensuring minimal disruption to operations and long-term system reliability.

Step 1: Gather Information

Objective: Obtain accurate, comprehensive data to understand the issue's context and potential causes.

- **System Logs and Data Analysis:**
  - Extract error logs, performance metrics, and event data from the Gen2 ZiM Bridge and connected systems.
  - Use diagnostic tools like log analyzers or cloud dashboards to identify patterns and anomalies.
  - Check for error codes, warnings, or alerts generated by the system.
- **Physical Inspection:**
  - Inspect hardware for physical damage such as loose connections, wear and tear, or overheating components.
  - Verify that the device is powered and all connections are secure.
- **Environmental Assessment:**
  - Note any external factors such as temperature, humidity, or electromagnetic interference that could impact performance.
- **End-User Feedback:**
  - Collect detailed accounts from operators or users experiencing the issue.
  - Document the sequence of events leading up to the problem.

Step 2: Verify the Problem

Objective: Confirm the problem exists and is replicable under defined conditions.

- **Replication in Real-World Conditions:**
  - Test the system under similar conditions to those reported by the user.
  - Attempt to replicate the issue using the same hardware and software configurations.
- **Controlled Environment Testing:**
  - Isolate the device in a test setup to minimize external influences.
  - Use a sandbox environment to verify software behavior without impacting live systems.
- **System-Wide Checks:**
  - Confirm that all connected devices and dependencies (e.g., network, cloud services) are functioning properly.
  - Validate software and firmware versions for compatibility.

Step 3: Perform Root Cause Analysis

Objective: Identify the underlying cause of the issue using structured diagnostic methods.

- **Root Cause Analysis Techniques:**
  - **Fishbone Diagrams:** Categorize potential causes under hardware, software, environmental, and procedural factors.
  - **5-Why Analysis:** Drill down to the core issue by repeatedly asking "Why?" until the root cause is identified.
- **Cross-Component Testing:**
  - Test individual components (e.g., power supply, communication modules, sensors) to pinpoint the faulty element.
  - Monitor device behavior under different configurations to identify potential conflicts.
- **Refer to Knowledge Base:**
  - Use historical data, troubleshooting guides, or error code libraries to identify similar issues and their resolutions.

Step 4: Repair and Replace

Objective: Implement corrective actions to resolve the identified issue.

- **Corrective Actions:**
  - For software issues:
    - Reinstall or update firmware and software.
    - Reconfigure device settings or reset to default configurations.

    - For hardware issues:
        - Replace defective components such as antennas, connectors, or power supplies.
        - Ensure new hardware meets the device's specifications.
- **Temporary Solutions:**
    - If a permanent fix is not immediately feasible, implement a workaround to maintain functionality until the issue can be fully resolved.
- **Compliance and Safety:**
    - Verify that repairs adhere to safety guidelines and relevant industry standards.
    - Ensure all modifications are documented for traceability.

Step 5: Test and Validate

Objective: Confirm that the problem is resolved and the system functions as expected.

- **Functional Testing:**
    - Run diagnostics to ensure all components are operating correctly.
    - Test the system under normal and stress conditions to verify stability.
- **Monitor for Recurrence:**
    - Place the system under observation for an appropriate period to ensure the issue does not reoccur.
    - Enable real-time alerts to detect any deviations from expected performance.
- **End-User Validation:**
    - Have operators test the system and confirm that their requirements are met.
    - Gather feedback to identify any residual issues or concerns.

7. Case Studies

Example 1: Network Connectivity Issue

Example 2: Sensor Calibration

Example 3: Firmware Failure

8. Dot Ai: Best Practices for IoT Hardware

Implementing best practices ensures the reliability, efficiency, and longevity of IoT hardware like the Dot Ai's Gen2 ZiM Bridge. These practices guide diagnostics, customer communication, and

knowledge sharing, providing a comprehensive framework for maintaining high standards and customer satisfaction.

8.1 Standardized Diagnostic Workflow

A standardized diagnostic workflow is critical for efficient problem resolution and maintaining operational continuity.

Defining Diagnostic Steps:

- Establish a clear diagnostic sequence to streamline troubleshooting:
    1. Collect and analyze system logs.
    2. Identify anomalies and correlate with error codes.
    3. Perform root cause analysis using established tools.
    4. Apply corrective actions and validate solutions.

Checklists and Templates:

- Use pre-designed templates for documenting:
    - Diagnostic findings.
    - Steps taken during the troubleshooting process.
    - Solutions implemented and their outcomes.

Automation and Tools:

- Leverage diagnostic tools such as:
    - **Network Analyzers:** For real-time monitoring of data flow and connectivity issues.
    - **Cloud Dashboards:** To track system health and performance metrics.
- Implement AI-driven diagnostic scripts to identify recurring issues and predict failures.

Continuous Improvement:

- Review the effectiveness of diagnostic workflows regularly.
- Integrate lessons learned from past diagnostics to refine processes.

8.2 Importance of Customer Communication

Effective communication builds trust and ensures customers feel supported during troubleshooting and resolution processes.

Setting Expectations:

- Provide clear timelines for issue resolution based on the severity of the problem.
- Share a detailed roadmap of the diagnostic process with customers.

Regular Updates:

- Keep customers informed of progress at every stage:
    - Diagnostic findings.
    - Steps being taken to resolve the issue.
    - Estimated completion times.

Clear and Accessible Language:

- Avoid technical jargon; use simplified language for non-technical users.
- Provide visual aids, such as diagrams or screenshots, to explain complex issues.

Proactive Engagement:

- Notify customers about potential issues before they escalate.
- Share firmware and software update schedules to preemptively address compatibility issues.

Feedback Mechanisms:

- Encourage customers to provide feedback on their experience.
- Use this feedback to improve communication strategies and support services.

8.3 Documentation and Knowledge Sharing

Robust documentation practices and knowledge-sharing systems enhance diagnostic efficiency and reduce resolution times.

Comprehensive Documentation:

- Maintain a centralized repository containing:
    - System logs and diagnostic reports.
    - Manuals, error code libraries, and troubleshooting guides.
    - Case studies of resolved issues and their solutions.

Version Control:

- Use version control systems to track updates to documentation, ensuring the latest information is always accessible.

Knowledge Base:

- Develop an internal and external knowledge base for stakeholders:
    - **Internal:** Detailed technical documentation for technicians and engineers.
    - **External:** User-friendly guides and FAQs for customers.

Training Programs:

- Conduct regular training for field technicians and support staff on the latest diagnostic tools and methodologies.
- Share best practices and lessons learned from field operations to ensure continuous improvement.

Collaboration Tools:

- Utilize collaboration platforms to facilitate real-time knowledge sharing among teams.
- Encourage cross-functional communication to leverage diverse expertise during complex diagnostics.

9. Troubleshooting Tips

9.1 Common Issues and Quick Fixes

9.2 Do's and Don't for Effective Diagnosis

10. Appendices

10.1 Glossary of Terms

5G - The fifth-generation wireless network that provides faster speeds and lower latency, enhancing IoT device connectivity.

Actuator - A component that receives a signal and performs an action, such as turning on a light or moving a motor.

Artificial Intelligence (AI) - The use of algorithms and machine learning to process IoT data, enabling devices to learn and act intelligently.

Big Data - Large volumes of structured and unstructured data generated by IoT devices, requiring advanced processing and analysis techniques.

Blockchain in IoT - A decentralized ledger technology used to enhance IoT security, trust, and data integrity.

Cloud Computing - Delivery of computing services, including storage, processing, and software, over the internet to support IoT applications.

Connected Car - A vehicle equipped with IoT technology for navigation, diagnostics, entertainment, and communication.

Cybersecurity in IoT - Practices and technologies used to secure IoT devices, networks, and data from unauthorized access and threats.

Digital Twin - A virtual representation of a physical asset or system, used for monitoring, simulation, and analysis.

Edge Computing - The processing of data at or near the source of data generation (e.g., IoT devices) to reduce latency and bandwidth usage.

Embedded System - A computer system with a dedicated function within a larger device, often used in IoT devices.

Firmware Over-the-Air (FOTA) - The process of updating IoT device firmware remotely, without requiring physical access.

Haptics in IoT - Technology that provides tactile feedback (e.g., vibrations) to enhance user interaction with IoT devices.

Industrial IoT (IIoT) - Application of IoT technology in industrial settings, such as manufacturing, energy, and logistics.

Interoperability - The ability of IoT devices and systems to communicate and work together, regardless of manufacturer or protocol.

Internet of Things (IoT) - A network of physical devices connected to the internet, capable of collecting, sharing, and acting on data.

IoT Analytics - The practice of examining data generated by IoT devices to extract insights and drive decision-making.

IoT Analytics Engine - Tools or software that process and analyze data from IoT devices to generate actionable insights.

IoT Ecosystem - The combination of IoT devices, networks, platforms, and applications that work together to deliver IoT solutions.

IoT Gateway - A device that connects IoT devices to the cloud or other networks, facilitating communication, data aggregation, and protocol translation.

IoT Platform - A software framework that manages and connects IoT devices, collects data, and enables application development.

IoT Protocols - Communication standards specifically designed for IoT, such as MQTT (Message Queuing Telemetry Transport), CoAP (Constrained Application Protocol), and Zigbee.

IoT Security - Measures and protocols to protect IoT devices and systems from vulnerabilities, cyberattacks, and data breaches.

LPWAN (Low Power Wide Area Network) - A type of wireless communication technology designed for long-range, low-power IoT applications, such as LoRaWAN or Sigfox.

M2M (Machine-to-Machine) - Direct communication between devices using wired or wireless networks, without human intervention.

NB-IoT (Narrowband IoT) - A cellular network technology designed for IoT applications requiring low bandwidth and power consumption.

Protocol - A set of rules and standards that define how data is transmitted between devices (e.g., MQTT, CoAP, HTTP).

RFID (Radio Frequency Identification) - A technology used to wirelessly identify and track objects using tags and readers.

Sensor - A device that detects and measures physical or environmental properties (e.g., temperature, motion, humidity) and converts them into data.

Smart City - An urban area that uses IoT devices and systems to improve efficiency, sustainability, and quality of life for residents.

Smart Device - An electronic device that connects to the internet and can be controlled remotely or autonomously.

Smart Home - A residential setup where IoT devices automate and control lighting, climate, security, and appliances.

Telemetry - The automatic transmission and collection of data from remote sensors or devices.

Telemetry Data - Information automatically collected and transmitted from IoT devices to a central system for analysis.

Wearables - IoT-enabled devices worn on the body (e.g., fitness trackers, smartwatches) that collect and share data.

10.2 Reference Tables (Error Codes, Connectivity Standards, etc.)

10.3 Contact Information for Technical Support

- Email: support@dotai.com
- Phone: 888-733-4301
- Support Hours: Monday-Friday, 9 AM to 5 PM (PST)

11. Feedback and Continuous Improvement

A robust feedback and continuous improvement system is essential for enhancing the usability and effectiveness of the Dot Ai Gen2 ZiM Bridge manual. It ensures that user experiences, evolving industry practices, and technological advancements are integrated into future updates.

11.1 How to Report Issues with this Manual

Reporting Mechanism:

- Email: support@dotai.com
- Phone: 888-733-4301
- Support Hours: Monday-Friday, 9 AM to 5 PM (PST)

11.2 Incorporating User Feedback for Future Revisions

Feedback Evaluation Process:

1. **Collect Feedback:**
    - Consolidate feedback from all reporting channels.
    - Categorize feedback into themes (e.g., clarity, accuracy, additional content needs).
2. **Prioritize Issues:**
    - Address critical inaccuracies immediately in the form of online addenda or errata.
    - Plan less urgent updates for the next scheduled revision.
3. **Analyze Trends:**

    - Identify recurring themes in feedback to uncover systemic issues.
    - Use analytics to track common pain points or areas of confusion.
4. **Collaborate Across Teams:**
    - Involve cross-functional teams (e.g., technical writers, engineers, and support staff) to validate feedback and develop solutions.
5. **Test Improvements:**
    - Pilot changes with a focus group before integrating them into the manual.
    - Use real-world testing to ensure that updates improve usability and address user concerns.

Revision Scheduling:

- **Minor Updates:**
    - Address small corrections or clarifications quarterly.
- **Major Revisions:**
    - Incorporate significant feedback, new features, or industry changes annually.

Version Control:

- Assign clear version numbers and publication dates to each revision.
- Maintain an archive of previous manual versions for reference.

11.3 Continuous Improvement Initiatives

User-Centered Design:

- Regularly engage with end-users through surveys, interviews, or focus groups to understand their evolving needs.
- Tailor content to address common challenges and preferences identified during user engagement.

Benchmarking Against Industry Standards:

- Periodically compare the manual against industry-leading documentation to ensure best practices are followed.
- Integrate innovative approaches such as interactive digital manuals or augmented reality (AR)-based guides.

Internal Review Processes:

- Conduct biannual internal reviews of the manual, led by a multidisciplinary team.
- Use checklists to assess clarity, completeness, and compliance with company standards.

Technology Integration:

- Develop a dynamic online version of the manual that:
    - Allows real-time updates based on user feedback.
    - Provides interactive elements like videos, animations, or troubleshooting flows.

11.4 Metrics for Measuring Improvement

To gauge the effectiveness of updates and feedback processes, track the following metrics:

1. **User Feedback Metrics:**
    - Volume of feedback received.
    - Percentage of resolved issues or implemented suggestions.
2. **Usage Metrics:**
    - Number of downloads or accesses of updated manuals.
    - Average time users spend on the digital manual.
3. **Customer Satisfaction:**
    - Ratings or reviews from customers on the usability of the manual.
    - Net Promoter Score (NPS) specifically for documentation.
4. **Operational Efficiency:**
    - Reduction in support tickets related to documentation gaps.
    - Improvement in first-call resolution rates for issues tied to manual clarity.

12. Regulatory Compliance Information

12.1 FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

12.2 ISED Canada Statement

This device contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's licence-exempt RSS(s). Operation is subject to the

following two conditions:
(1) This device may not cause interference; and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil contient des émetteurs/récepteurs exemptés de licence conformes aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :
(1) l'appareil ne doit pas produire de brouillage, et
(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

12.3 RF Exposure Information

This device meets the applicable limits for radio frequency (RF) exposure set forth by the FCC and ISED Canada.

Cet appareil respecte les limites applicables d'exposition aux radiofréquences (RF) établies par la FCC et ISED Canada.