# Clear Skies

A Reference Architecture for Resilient Alaskan Microgrid Cyberinfrastructure


John Haverlack

**Author**: John Haverlack



**Version**: 0.0.1

**Date**: 2025-11-07

**State**: DRAFTING

# Contents

# Chapter 1

# Executive Summary

TBD

# Chapter 2

# Introduction

### 2.0.1 Vision Statement

**Clear Skies** is a locally grown initiative to build **community-owned, cloud-free digital infrastructure** across rural Alaskan microgrid communities. It empowers villages, tribes, and regional utilities to host and secure their own data, communications, and operational systems — right where they live and work without reliance on distant cloud services.

By bringing computing power, cybersecurity, and communications back under local control, **Clear Skies** advances *digital sovereignty* as as a modern expression of community and tribal self-determination.
It strengthens self-reliance, ensures continuity during network outages, and creates a foundation for innovation that reflects Alaska's values of **independence, stewardship**, and **cooperation**.

The following reference architecture outlines how Clear Skies can be implemented in scalable layers, from physical infrastructure to regional collaboration.

## 2.1 Problem Statement

Alaska has the worlds highest concentration of island-ed micro-grids in the world. The remote communities are not connected by roads or transmission lines. Most generate power primarily with diesel, and the fuel is expensive, especially if the community is not on a the coast or river systems where fuel can be barged in. For those remote communities fuel must be flown in.

Internet access in these communities is also a constrained resource. Some coastal communities have access to high speed fiber optic connections, while others have been limited to expensive geosynchronous satellite communications. Though in 2 of the last 3 years, sea ice has cut burred cables resulting several month service outages. Low earth orbit (LEO)("Low Earth Orbit" 2025) satellite systems have be come available in recent years, however also carries the unaddressed risk of Kessler syndrome("Kessler Syndrome" 2025), where a cascading

collision of satellites starts a chain reaction leaving the entire LEO orbital space unusable for potentially centuries.

Rural Alaskan micro-grid communities range between less than a hundred to over 3000 people. The energy utilities in these communities are commonly operated by a handful of individuals. Staffing rural utilities is a challenging balance between keeping energy costs low and attracting skilled workers.

For much of the United States, the Federal Energy Regulatory Commission (FERC)("Home Page | Federal Energy Regulatory Commission" n.d.) is the regulator agency that governs energy utilities in the U.S. FERC mandates that energy utilities in the United States to follow the North American Electric Reliability Corporation (NERC)("NERC" n.d.) Critical Infrastructure Protection (CIP)("Reliability Standards" n.d.) standards in regards to cybersecurity compliance for energy utilities Operational Technology networks. However compliance criteria are based largely on transmission capabilities. Because no utility in Alaska is connected to the lower 48 power grid, Alaska utilities have been effectively exempt from cybersecurity regulation. Recently the Railbelt Reliability Council (RRC)("Alaska Railbelt Reliability Council" 2025) has drafted a set of modified CIP standards("(CIP) Critical Infrastructure Protection" 2025) for the State of Alaska which are based on the NERC CIP standards but tuned to accommodate Alaskan specific criteria. Once adopted by the Regulatory Commission of Alaska (RCA)("Regulatory Commission of Alaska" n.d.) the RRC CIP standards are expected to become a regulator compliance requirement for those Alaskan power producer connected to the Railbelt energy grid.

While the RRC CIP standards address the comprehensive scope of risks for critical energy infrastructure, rural islanded Alaskan microgrids will remain largely exempt from compliance because they do not meet the transmission criteria. Additionally meeting cybersecurity standards would represent a significant cost to rural communities already struggling with the cost of energy. Not only would these communities need to pay for expensive cybersecurity expertise, but would likely mean expensive upgrades to existing network equipment.

# Chapter 3

# Strategic Architecture

Clear Skies is built on a simple principle: **local-first by design.**
Every system — from the smallest sensor to the community data center — operates independently of the cloud services, ensuring that essential services remain available, secure, and under local control even when Internet connectivity is lost.

Clear Skies adopts a layered approach to build increasingly complex modular capabilities on top of a resilient cyberinfrastructure foundation.

## 3.1 Layer 0 - Hardware (HW)

The hardware selection can be based on 3 tiers to accommodate different cost, scalability, and resiliency needs.

### 3.1.1 Tier 1 - Camp Site

**Purpose:** Portable or training-scale deployments for small teams and pilot projects.

- Commodity Grade Hardware
- Low Cost of Entry and Maintenance
- Portability
- Limited Capacity
- Basic Services
- Limited Resiliency
- Scales to 10's of People

### 3.1.2 Tier 2 - Village Site

**Purpose:** Fully featured, community-level cyberinfrastructure supporting daily operations.

- Commodity Grade Hardware
- Low Cost of Entry and Maintenance

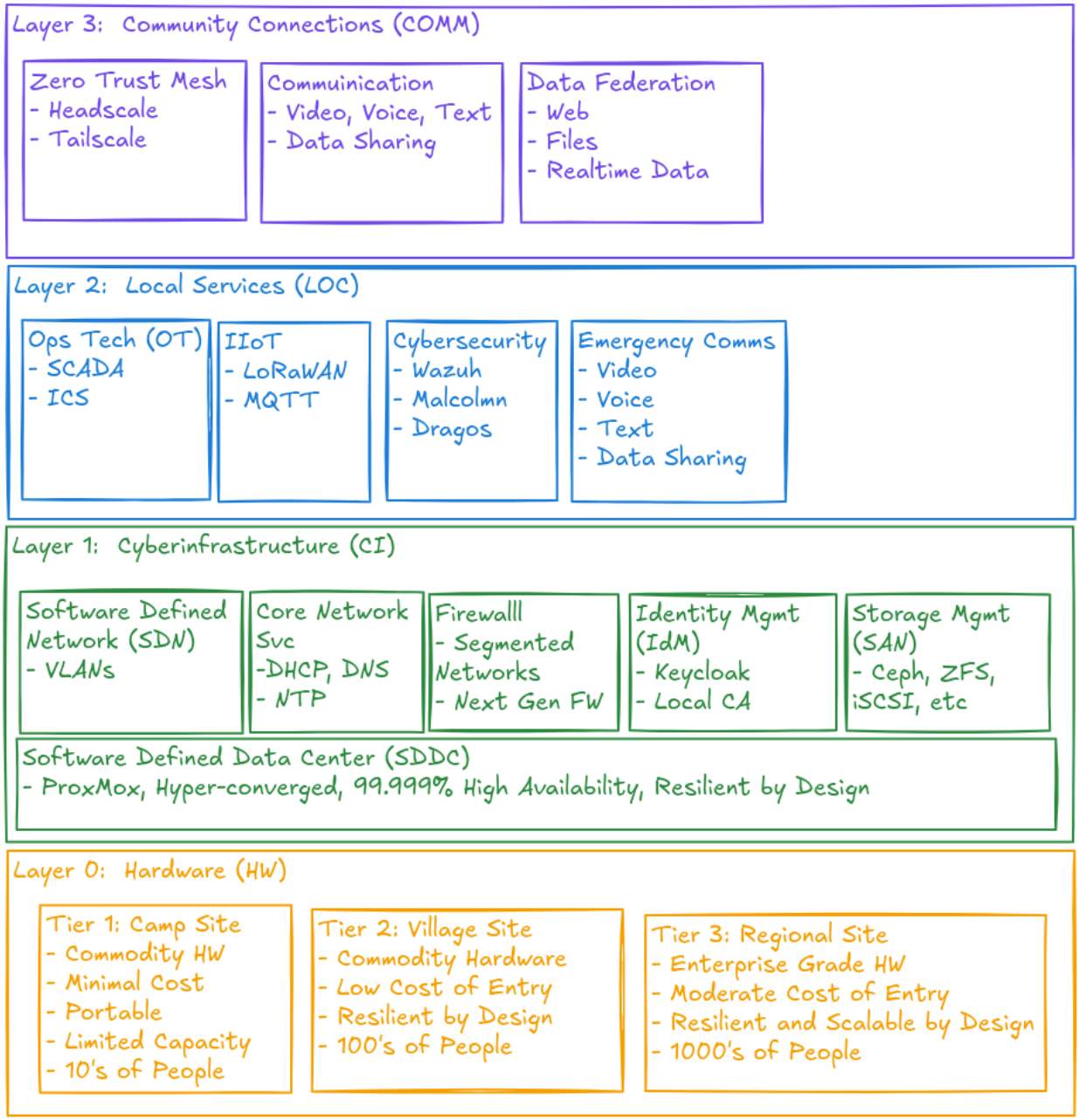


Figure 3.1: Clear Skies Reference Architecture

- Full Stack Service Capabilities
- Full Resiliency - Zero Single Points of Failure
- Scales to 100's of People

### 3.1.3 Tier 3 - Regional Site

**Purpose:** High-capacity, multi-community or research hub supporting advanced services and federation.

- Enterprise Grade Hardware
- Moderate Cost of Entry and Maintenance
- Full Resiliency - Zero Single Points of Failure
- Scales to 1000's of People

## 3.2 Layer 1 - Cyberinfrastructure (CI)

The Cyberinfrastructure (CI) Layer forms the digital powerhouse of a Clear Skies deployment.
It establishes the **core network and compute services** that allow every community site — from Camp Site to Regional Site — to operate independently of outside cloud resources.

The CI Layer is implemented as a **Software-Defined Data Center (SDDC)**("Software-Defined Data Center" 2025): a cluster of virtualized servers that pool compute, storage, and networking into one resilient platform.
This approach provides enterprise-grade reliability using open-source tools and commodity hardware, enabling small teams to manage complex infrastructure with minimal overhead.

### 3.2.1 Networking & Segmentation

- VLAN-aware switching and software-defined routing using **OPNsense** or similar open firewalls.
- Segregated networks for Management, Operational Technology (OT), Data, and DMZ zones.
- Local DNS, DHCP, and NTP ensuring that critical systems function offline.

### 3.2.2 Identity & Trust

- **Keycloak** provides single sign-on and multi-factor authentication.
- **Smallstep CA** or similar certificate authority issues short-lived internal certificates, enabling encrypted, trusted communication between devices and services.

### 3.2.3 Storage & Resiliency

- **Ceph** or **ZFS-based** distributed storage replicates data across all nodes.

- Snapshots and versioned backups protect against corruption or accidental deletion.
- Air-gap or offline backup options for disaster recovery.

### 3.2.4 Monitoring & Automation

- **Prometheus + Grafana** for metrics, alerting, and visibility.
- **Ansible** or **Chef** for configuration management and repeatable deployments.
- Logs aggregated locally via **Elastic / Wazuh / Loki** stacks.

### 3.2.5 Security & Perimeter

- Dual-node firewall pairs provide high-availability failover.
- Intrusion detection (Zeek/Suricata) can run as virtual appliances inside the same SDDC.
- Role-based access control and network segmentation enforce the "least privilege" model.

### 3.2.6 Data Backup & Synchronization

- Automated local backups using **Restic**, **Borg**, or similar tools
- Optional cross-site replication between Village and Regional Sites when connectivity permits.
- All data remains encrypted and community-owned.

## 3.3 Layer 2 - Local Services (LOC)

Layer 2 builds upon the Cyberinfrastructure (CI) foundation to deliver the mission-specific functions that keep a community operating, informed, and connected. These following modular service areas are locally hosted—able to run entirely within the community network—and can be added, removed, or upgraded without disrupting the lower layers.

Each category reflects a practical application of the local-first philosophy: keeping critical data, control, and communication inside the community while remaining interoperable with regional and research partners.

### 3.3.1 Operational Technology (OT) / SCADA / ICS

**Purpose:** maintain safe, efficient, and observable microgrid operations under all conditions.

- Supervisory control and monitoring for generation, distribution, and storage systems.
- Secure, segmented access for operators, engineers, and vendors.
- Local data historians for real-time visibility even during WAN outages.

- Integration with open-source or vendor SCADA platforms (e.g., Rapid SCADA, Ignition Edge, OpenPLC).

#### 3.3.1.1 Industrial Internet of Things (IIoT) Networks

**Purpose:** gather and use data from across the community—power, heat, water, environment—to inform decisions locally.

- LoRaWAN, Modbus TCP, and MQTT telemetry from sensors across the community.
- Local brokers and dashboards (Node-RED, Grafana) for low-bandwidth visualization.
- Edge analytics and rule-based automation without cloud dependence.

### 3.3.2 Emergency Communications

**Purpose:** ensure situational awareness and coordination during disasters or outages.

- Local voice, text, and alerting systems that function when commercial networks fail.
- Interoperable with radios, satellite links, or FirstNet gateways when available.
- Capable of community-wide paging, siren control, or automated messaging through existing IoT endpoints.

### 3.3.3 Local Community Communications

**Purpose:** strengthen community cohesion and digital inclusion through local, private communication spaces.

- Locally hosted chat, video, and bulletin-board tools (Matrix, Jitsi, etc).
- Intranet portals for schools, clinics, and tribal councils.
- Content caching and offline web access for education and information sharing.

### 3.3.4 Additional Service Categories (Expandable)

- **Cybersecurity Operations:** IDS/IPS, log correlation, vulnerability scanning, and SOC visualization.
- **Education & Research Sandboxes:** student training, network simulation, or data-science environments.
- **Local Data Services:** GIS, asset management, or archival storage tied to community projects.

### 3.3.5 Outcome

Layer 2 turns Clear Skies from infrastructure into impact — providing the tools that make a self-reliant community not only operationally resilient but also informed, connected, and empowered.

## 3.4 Layer 3 - Community Connections (COMM)

Layer 3 extends Clear Skies beyond individual communities.
It enables **secure collaboration, knowledge sharing, and regional coordination** between sites — while preserving each community's digital sovereignty.
These connections are intentional, encrypted, and always under local control. ### Secure Networking and Federation - **Tailscale / Headscale Zero-Trust Network Access (ZTNA) Bridges:** lightweight, encrypted overlays that connect Camp, Village, and Regional sites into a trusted mesh without public exposure. - **Cross-Site Data Sharing:** optional, policy-driven replication of telemetry, research, and analytics data between communities or partner institutions. - **Federated Identity and Trust:** local identity systems (Keycloak / Smallstep CA) exchange only the credentials necessary for inter-site collaboration. - **Bandwidth-Aware Synchronization:** asynchronous, store-and-forward file and database replication designed for limited or intermittent connectivity.

### 3.4.1 Collaborative Applications

- Shared monitoring dashboards and situational-awareness maps.
- Federated educational resources and research datasets.
- Inter-community communication tools for regional operations centers or cooperative utilities.

**Purpose:** build a network of sovereign digital islands — each self-reliant, yet capable of cooperating across Alaska's vast geography through secure, transparent, and low-bandwidth bridges.

### 3.4.2 Outcome

Layer 3 transforms Clear Skies from isolated local systems into a **distributed ecosystem of collaboration**.
Communities retain full control of their data and infrastructure while participating in a resilient, Alaska-wide digital commons built on trust, openness, and shared stewardship.

# Chapter 4

# Technology Selection

*Design and Implementation Blueprint for the Clear Skies Architecture*

This section details the specific technologies, configurations, and open-source components recommended for each layer and tier of the Clear Skies architecture.
Selections emphasize **resilience**, **local autonomy**, and **open interoperability** across all deployment scales.

---

## 4.1 Layer 0 — Hardware Foundations

### 4.1.1 Tier 1 — Camp Site

*Portable / Training-Scale Deployment* - Example hardware platforms (NUC, MiniPC, low-power servers) - Typical storage configuration (ZFS mirror, 1 GbE) - Lightweight Proxmox or single-node SDDC - Local UPS / Power considerations

### 4.1.2 Tier 2 — Village Site

*Community-Scale Deployment* - Cluster of 3 × MiniPC/Protectli-class nodes - Ceph or ZFS-replicated storage - Dual OPNsense firewall HA pair - Local PoE switch with VLAN segmentation - External backup (USB or second site)

### 4.1.3 Tier 3 — Regional Site

*Federated Multi-Community Hub* - Enterprise-grade rackmount servers (ECC RAM, redundant PSU) - 10 GbE backplane networking - Dedicated Ceph cluster - Multi-site replication and Tailscale/Headscale federation

---

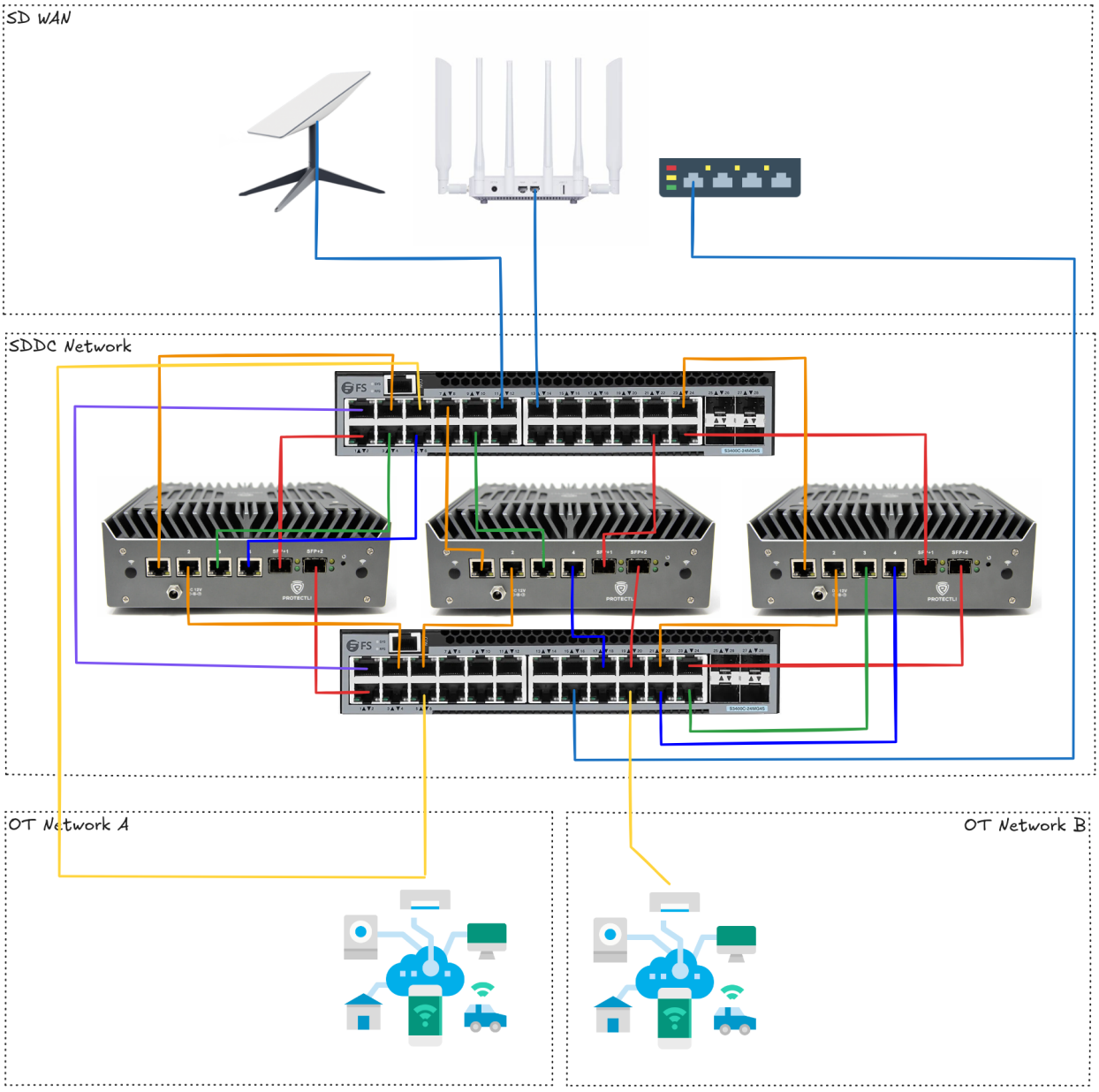


Figure 4.1: Zero Single Point of Failure SDDC

## 4.2 Layer 1 — Cyberinfrastructure (CI)

- Virtualization Platform: **Proxmox VE / KVM**
- Networking Stack: **OPNsense**, **FRR**, VLAN trunking
- Storage: **Ceph**, **ZFS**, **Restic/Borg**
- Identity: **Keycloak**, **Smallstep CA**
- Monitoring: **Prometheus**, **Grafana**, **Loki**, **Wazuh**
- Configuration: **Ansible** or **Chef**

---

## 4.3 Layer 2 — Local Services

- OT/SCADA: **Rapid SCADA**, **OpenPLC**, **Ignition Edge**
- IIoT: **Mosquitto (MQTT)**, **Node-RED**, **Grafana**, **LoRaWAN**
- Comms: **Matrix (Synapse)**, **Jitsi**, **Rocket.Chat**
- Cybersecurity: **Zeek**, **Suricata**, **Wazuh**, **Elastic**
- Education / Research: **JupyterHub**, **Docker / LXC Sandboxes**
- Data: **PostgreSQL**, **GeoServer**, **Nextcloud**

### 4.3.1 Industrial Internet of Thing (IIoT)

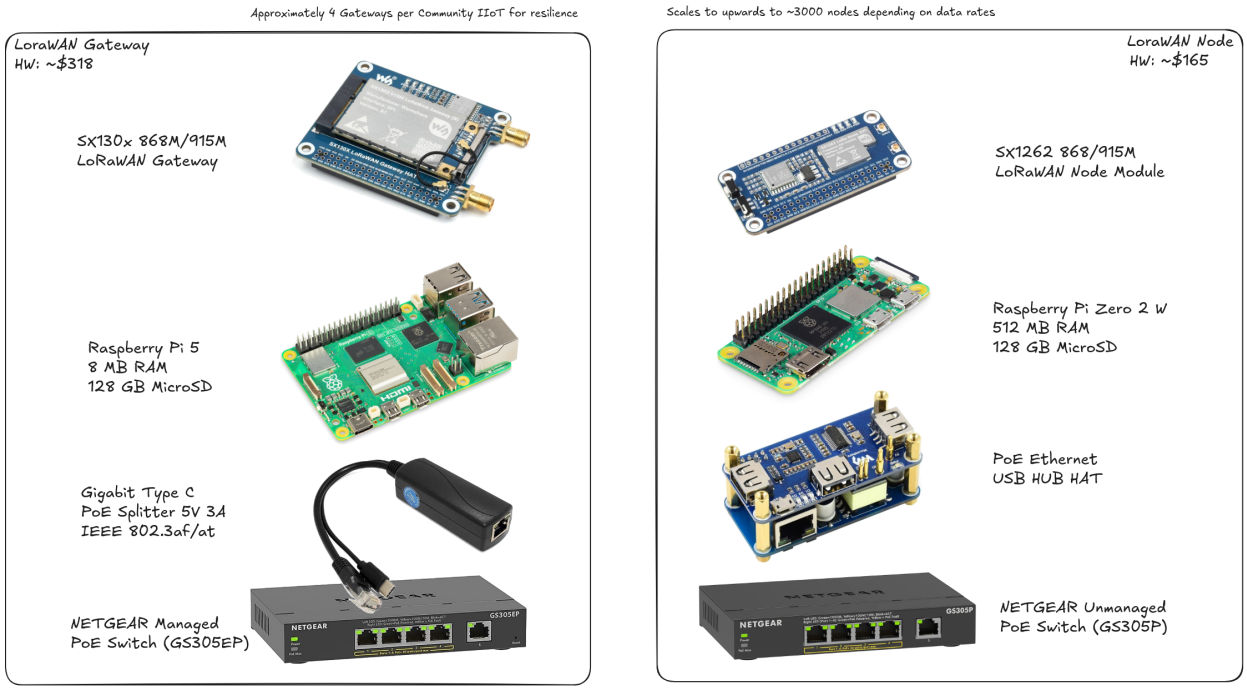


Figure 4.2: IIoT

---

## 4.4 Layer 3 — Community Connections

- Secure Networking: **Tailscale / Headscale (ZTNA Mesh)**
- Federation: **Keycloak Federation**, **Smallstep cross-trust**
- Data Sync: **Syncthing**, **rsync**, **MinIO Gateway**
- Shared Visualization: **Grafana Federation**, **Kibana Dashboards**
- Optional: Integration with **FirstNet**, **Starlink**, or terrestrial backhaul for redundancy

# Chapter 5

# Terminology

| Acronym | Term | Description |
|---|---|---|
| **AC** | Alternating Current | ~60 Hz 120 Volt power with an oscillating voltage. |
| **ACEP** | Alaska Center for Energy and Power | University of Alaska Fairbanks research center focused on applied energy systems and innovation in rural and microgrid environments. |
| **CA** | Certificate Authority | Service that issues and manages digital certificates used to authenticate and encrypt communications. |
| **Ceph** | — | Open-source distributed storage system providing block, object, and file storage across clustered nodes. |
| **CI** | Cyberinfrastructure | The foundational compute, storage, and network systems enabling digital services to operate locally and independently. |
| **DC** | Direct Current | Contant Voltage Power Systems such as provided by batteries. |
| **DMZ** | Demilitarized Zone | Network segment that isolates external-facing systems from internal critical infrastructure. |
| **DNS** | Domain Name System | Converts human-readable hostnames into IP addresses. |
| **DHCP** | Dynamic Host Configuration Protocol | Automatically assigns IP addresses to devices on a network. |
| **HW** | Hardware | Physical computing, storage, and network devices forming the foundation of the infrastructure. |
| **ICS** | Industrial Control System | Hardware and software used to monitor and control industrial processes such as generation and distribution. |
| **IIoT** | Industrial Internet of Things | Networked sensors and devices that collect and exchange data for monitoring and automation in industrial settings. |

| Acronym | Term | Description |
|---|---|---|
| **LAN** | Local Area Network | Internal network connecting devices within a limited geographic area such as a facility or village. |
| **LLM** | Large Language Model | AI model trained on vast text corpora to generate and analyze natural language. Used locally for automation and data analysis. |
| **LOC** | Local Services Layer | Layer 2 in the Clear Skies architecture providing operational, communication, and data services within the community. |
| **MQTT** | Message Queuing Telemetry Transport | Lightweight publish/subscribe messaging protocol optimized for low-bandwidth IIoT networks. |
| **NTP** | Network Time Protocol | Synchronizes system clocks across devices on a network. |
| **OPNsense** | — | Open-source firewall and routing platform providing VLAN segmentation, VPNs, and intrusion detection. |
| **OT** | Operational Technology | Systems that monitor and control physical devices, processes, and infrastructure. |
| **PLC** | Programmable Logic Controller | Industrial computer used to automate electromechanical processes. |
| **Proxmox VE** | Virtual Environment | Open-source virtualization environment used to create Software-Defined Data Centers (SDDC). |
| **PSU** | Power Supply Unit | A hot swapable power supply in a rack mount server or other equipment. |
| **SCADA** | Supervisory Control and Data Acquisition | System for remote monitoring and control of industrial and utility operations. |
| **SDDC** | Software-Defined Data Center | Virtualized data center architecture where compute, storage, and networking are abstracted from hardware. |
| **SDN** | Software-Defined Networking | Network architecture enabling centralized, programmable control of traffic and segmentation. |
| **SOC** | Security Operations Center | Centralized facility or function for monitoring, detecting, and responding to cybersecurity threats. |
| **Tailscale / Headscale** | — | Zero-trust networking tools that establish secure, peer-to-peer mesh connectivity across sites. |
| **UPS** | Uninterruptable Power Supply | A batter backup DC to AC inverter system to provide AC power during intermittent short duration power outages. |
| **ZTNA** | Zero Trust Network Access | Security framework that assumes no implicit trust and enforces strict identity-based access controls for every connection. |

# Citations


"Alaska Railbelt Reliability Council." 2025. *RRC Local*. https://www.akrrc.org/.

"(CIP) Critical Infrastructure Protection." 2025. *RRC Local*. https://www.akrrc.org/matters/category/cip critical-infrastructure-protection.

"Home Page | Federal Energy Regulatory Commission." n.d. https://www.ferc.gov/. Accessed November 7, 2025.

"Kessler Syndrome." 2025. *Wikipedia*, October.

"Low Earth Orbit." 2025. *Wikipedia*, October.

"NERC." n.d. https://www.nerc.com/Pages/default.aspx. Accessed November 7, 2025.

"Regulatory Commission of Alaska." n.d. https://rca.alaska.gov/RCAWeb/home.aspx. Accessed November 7, 2025.

"Reliability Standards." n.d. https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx. Accessed November 7, 2025.

"Software-Defined Data Center." 2025. *Wikipedia*, September.