Távlink Remote Monitoring System

Final Year Project Semester 7

Zalán Tóth - 20102768
Computer Forensics and Security Year 4

SETU Waterford
School of Science and Computing
Department of Computing and Mathematics

Waterford City, Ireland
01/01/2026

Abstract

This paper includes the architecture design of Távlink, a secure and scalable remote monitoring system intended for critical infrastructure environments such as power plants. The system has the objectives of acquiring, transmitting, processing and storing data safely from devices that generate information that could be monitored and then make it available for retrieval for operators and maintainers remotely. The architecture has a layered approach on both operational technology (OT) and information technology (IT) domains and puts a large security focus on the convergence point of those two domains, as it is mandated in industry standards. This document serves as a blueprint and guide for building and implementing this system.

Executive Summary

Távlink is a proposed remote monitoring system designed to address the lack of remote monitoring for isolated critical infrastructure devices. Many such devices around the world still remain without remote monitoring features due to the strict regulatory requirements, making the implementations complex and difficult. Consequently, oversight is limited to only on-site and maintenance is more costly. This project defines a modular implementation to such a system while aligning with industry standards such as IEC 62443 and IEC 27001 for best practices. The architecture is designed to handle large amounts of data in a scalable, efficient and secure way.

Table of Contents

1. Introduction

1.1. Background

Modern power plants increasingly rely on remote monitoring and control systems to manage and oversee operations while also ensuring safety. [1] These remote systems, on the other hand, also introduce new security risks due to their internet exposure. While power plants are being built with these new technologies in mind, many around the world have so-called isolated black box scenarios which still remain completely offline, lacking remote operative insights. The absence of such features makes fault detection and maintenance more difficult.

1.2. Problem Definition

Small isolated industrial systems often do not get remote control and monitoring features due to the complexity and regulatory requirements surrounding their implementation. As a result, these systems operate without any remote data collection, logging or alerting features. In the event of abnormal behaviour or failure, data may become unavailable or even permanently lost, requiring more on-site human intervention. This makes maintenance and incident response more costly and difficult. With a remote monitoring system, the data can be safely retained, creating a trusted source of metrics that can support functions such as alerting or anomaly detection.

1.3. Objectives

The objective of this project is to design a secure, flexible and scalable remote monitoring system that aligns with industry standards for best practices. The system intends to support a wide range of devices, such as programmable logic controllers (PLCs) and IoT sensors, mainly in critical infrastructure environments. The proposed architecture focuses on monitoring functionality with only unidirectional data flow from the operational technology (OT) systems to the information technology (IT) domain. Future versions, however, may also introduce control features with bidirectional data flow.

1.4. Scope

The scope of this paper is limited to the architectural planning of the Távlink remote monitoring system, suitable for managing all kinds of reporting devices in an efficient and scalable way. The paper focuses on system structure, data flow, security controls and deployment, and it should be read as a blueprint that can guide future development and implementation.

2. Standards and Compliance Frameworks

Such a system must be designed with security in mind at every step. While the system is intended to support all kinds of devices for monitoring, its primary deployment context is critical infrastructure environments, which are highly regulated and often have country and region-specific regulatory requirements. As these regulations differ by country, it's quite difficult to comply with all jurisdictions. For this reason, this paper does not attempt to follow country-specific regulatory frameworks, but rather well-known global industrial standards such as IEC 62443 and IEC 27001. [1]

In addition, for the IT infrastructure which is planned to be hosted within the European Union, following the General Data Protection Regulation (GDPR) is also a must while implementing this system. It's also important to note that this work does not aim at any certification towards the mentioned industry standards and frameworks. It only attempts to align with their principles and guidelines for industry best practices.

2.1. ISA/IEC 62443

ISA (International Society of Automation) / IEC (International Electrotechnical Commission) 62443 is a globally recognised series of standards for securing industrial automation and control systems (IACS). It defines the requirements and processes for the implementation and maintenance of such systems while also taking an approach to bridge the gap safely between operational technology (OT) and information technology (IT) domains. [2]

2.2. ISO/IEC 27001

ISO (International Organization for Standardization) / IEC (International Electrotechnical Commission) 27001 is an international standard that provides requirements for establishing, implementing, maintaining and continually improving information security management systems (ISMS). The standard aims at preserving confidentiality, integrity and availability of information. The framework is built around risk management, and it can be used to identify, assess and address information security requirements. [3]

3. Methodology

3.1. Architectural Design Approach

The proposed architecture is based on a strict separation of two environments: operational technology (OT) and information technology (IT). Incidents in industrial environments are mostly reported to happen at the convergence points of these two domains, and therefore, this intersection must be highly secured. [4]

In the IEC 62443 terminology, the OT environment corresponds to the Control Zone, while the IT environment represents the Business Zone. Between these two zones lives the demilitarised zone (DMZ), acting as an intermediary. Generally, the DMZ is created by a firewall, and it is a logically separated forefront network. Jump servers generally live in this zone. [5]. Comparable IEC 62443-aligned architectures also adopt similar segmentation strategies. [6]

Industry standards further mandate network segmentation and the separation of security zones at least logically. This strategy is referred to as a defence-in-depth strategy, which is widely adopted in OT environments and is considered to be one of the most effective mechanisms for the mitigation of cyber threats in such systems. [7], [8], [9], [10]

The IT environment follows a layered architectural model based on a microservices approach, where each component has a clearly defined function. This design, while being modular, also helps maintainability and easily supports scaling and load balancing for communications, processing and data storage.

3.2. Security Design Approach

Industrial systems are subject to increasing cybersecurity pressure, making security by design mandatory for any critical infrastructure system. [4] The monitored OT devices generate sensitive operational data, and therefore, protecting data confidentiality, integrity, and availability is a fundamental design objective. All data must be stored and transmitted securely and made accessible upon request with appropriate authorisation.

The system must have robust identification and authentication mechanisms supported by role-based access control (RBAC) and enforcement of least privilege. [8] All major security-related and operational events must be logged using an independent logging system to ensure integrity and authenticity. Audit must be done on the systems regularly, and the system must complement and facilitate these processes. [3], [7] In case of an emergency, these logging and audit mechanisms are also able to support incident response effectively. [8]

Potential misuse cases must be identified and considered during the design phase to ensure appropriate mitigations are in place. [3], [7] Functional, security and reliability testing should be automated in the pre-production environment, while deployment to production systems must require human evaluation and approval, reducing accidents. [8] In addition, vulnerability scanning and penetration testing must be done continuously, and where appropriate, third-party testing and evaluation are recommended. [7], [10]

As most security breaches originate from human factors, designing the human risk out is a major architectural aim. More automation and appropriate access controls minimise such threats. [11], [7] Firewalls are baseline requirements for both OT and IT environments, but using additional defensive controls, such as intrusion detection systems, is highly recommended as well. [7] While it is out of scope for this project, physical security is still an essential component that has to be considered when planning, building, implementing and deploying such systems. [7]

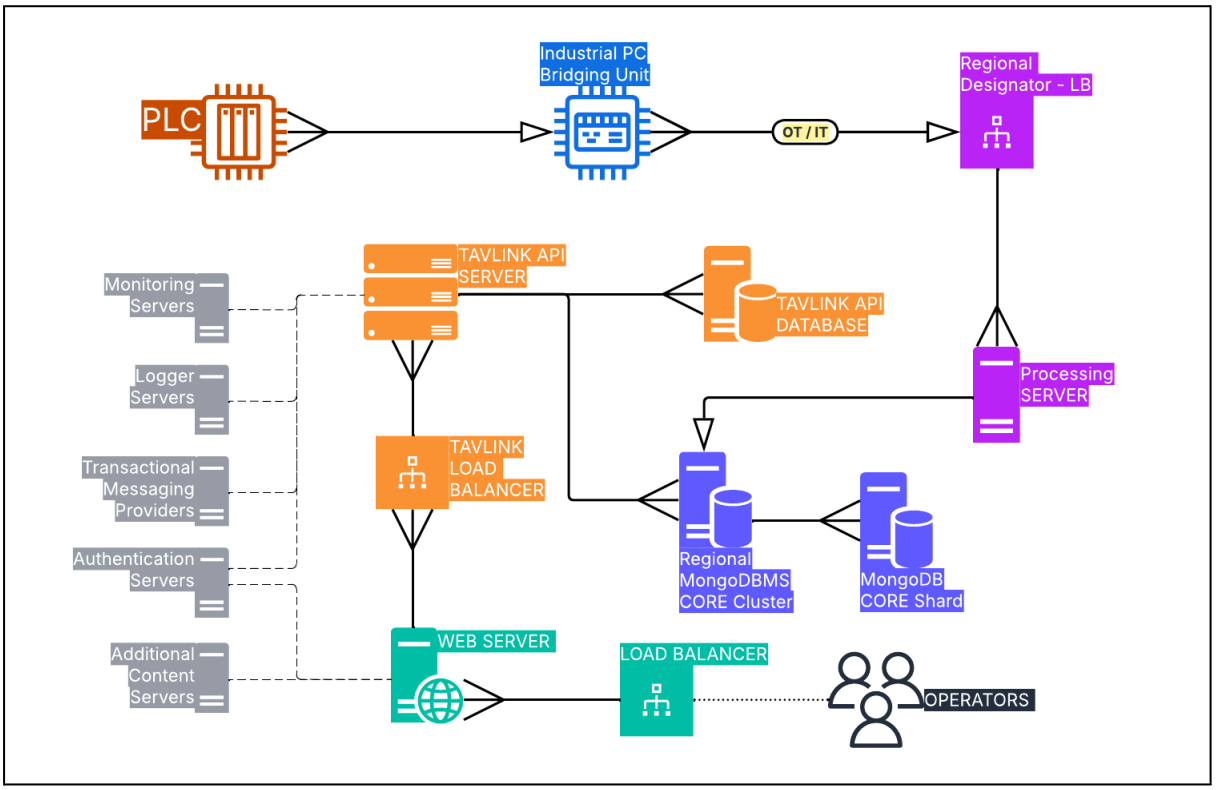
3.3. Dataflow Modelling

The system must enforce restricted and controlled data flow between components and zones. The current design follows an unidirectional data flow from the OT environments to the IT infrastructure. The IT infrastructure must process the data received from the OT devices into databases from which other microservices must be able to read out the information appropriately to display the data to the end-user. OT sites must incorporate extra bridging units to safely bridge the information between the two (OT and IT) domains. Data normalisation and validation must be performed during the database ingestion to ensure consistency and reliability.

4. System Architecture

The system architecture of Távlink consists of several layers, zones and components. While the highly modular design increases development and deployment complexity with a larger attack surface, it also has major efficiency, scaling and security advantages over traditional systems operating with fewer, larger multi-purpose components. The following subsections introduce each layer and component in detail.

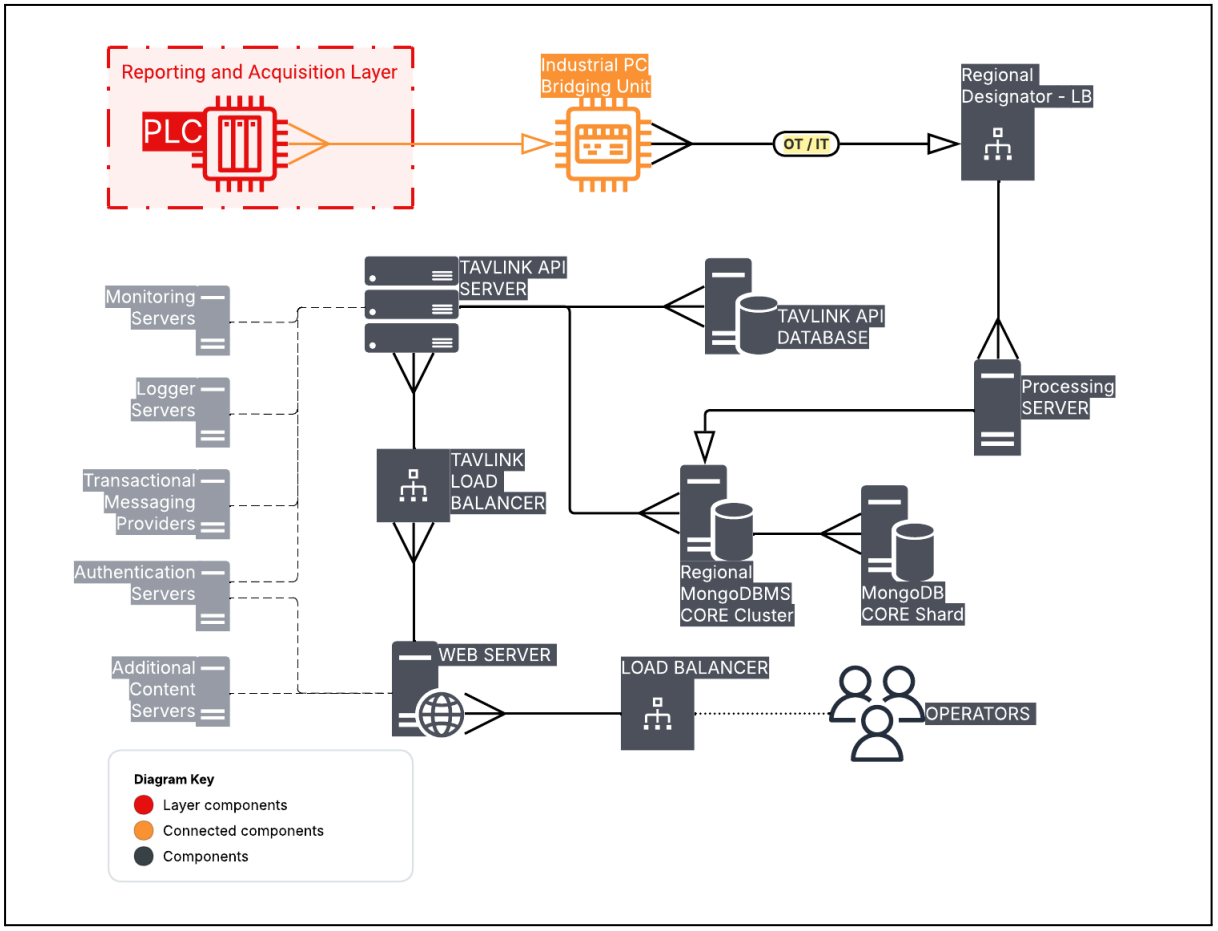
Figure 1. Távlink overview



4.1. Reporting and Acquisition Layer

The Reporting and Acquisition Layer represents the initial stage of the monitoring architecture. It is responsible for the collection of operational data from the monitored devices. This layer includes all data-producing components, such as industrial devices or other general-purpose IoT sensors. Devices at this level generally do not have a direct internet connection, and such exposure is even forbidden in critical infrastructure environments. As a result, a separate dedicated edge processing layer is required to securely bridge the collected data to the IT domain.

Figure 2. Reporting and acquisition layer



4.1.1. Programmable Logic Controllers (PLCs)

PLCs are deployed on-site and operate within the OT domain. To facilitate monitoring for these devices while maintaining isolation, PLCs communicate with a designated bridging unit on-site through a firewall. The bridging unit's responsibility is to pass the data forward to the IT domain.

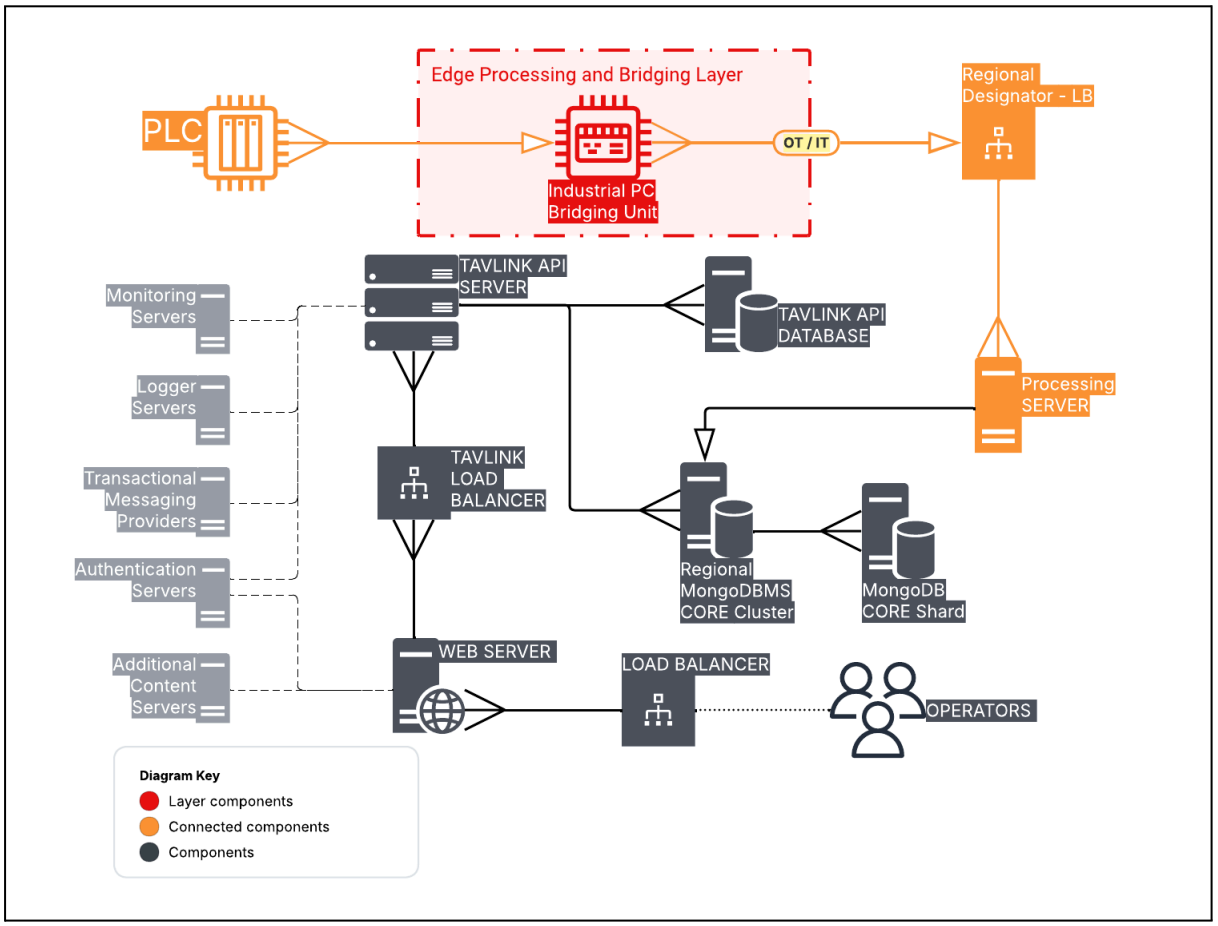
4.1.2. Internet of Things (IoT) Devices

The system is intended to support any devices (sensors) that are capable of producing operational data. Regardless of their communication method, if there is a way to configure them for reporting operational data, they can be implemented into the Távlink system. During development, such data can be simulated for testing purposes.

4.2. Edge Processing and Bridging Layer

The Edge Processing and Bridging layer is responsible for providing an interface between the isolated data sources and external networks. It is a convergence point of the OT and IT domains. It is responsible for securely transmitting the collected data from the reporting devices to the processing servers, where the data gets ingested into the IT system.

Figure 3. Edge processing and bridging layer



4.2.1. Bridging Unit - Industrial Computer

The Bridging Unit is generally implemented as an industrial computer deployed on-site in a controlled environment. Its purpose is to securely transfer monitoring data from the reporting devices to the ingestion layer. This unit is also responsible for preprocessing the data and aggregating it into batches. Deployment of such units is generally done manually. This unit is intended to run a lightweight server (daemon) that could be written in Rust to reduce risks of memory management.

4.2.2. Jump Server - Industrial Computer

The Jump Server is generally implemented as an industrial computer deployed on-site in the outer demilitarised zone (DMZ). It can provide controlled connectivity to other edge layer devices. Its primary purpose is to support maintenance operations to the Bridging Unit, which does not feature direct internet connectivity due to safety reasons. This ensures security isolation with defence-in-depth. The server can also act as an independent local monitoring component for health and metrics.

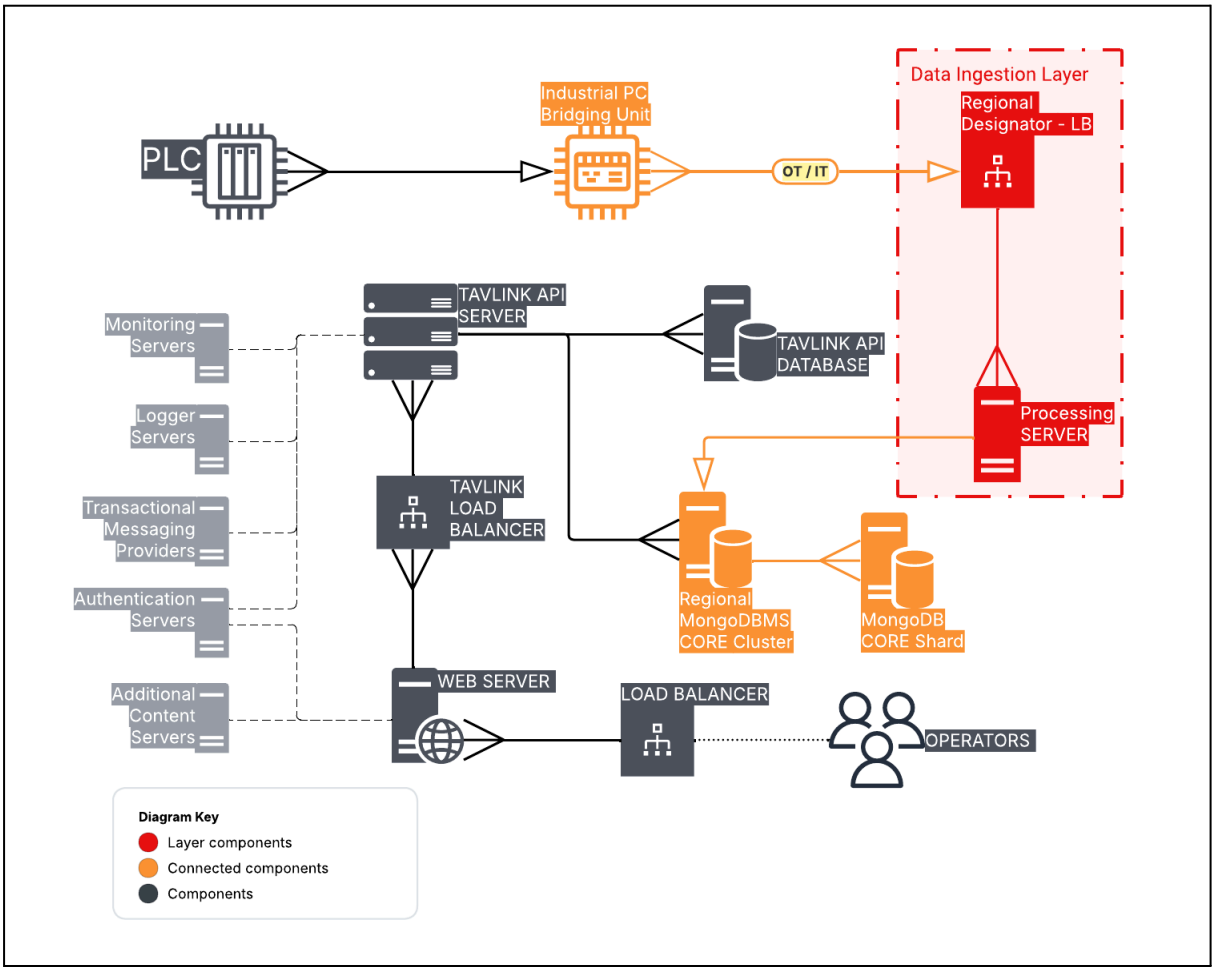
4.2.3. Firewalls

Firewalling is a baseline for all OT and IT systems, but especially at the convergence point of those two domains. Firewalls must be deployed at multiple boundaries where appropriate and feasible. Implementation may depend on site requirements, but generally includes at least one physical industrial firewall.

4.3. Data Ingestion Layer

The Data Ingestion layer is responsible for receiving, validating and persisting the monitoring data into databases. It is the data entry point in the IT domain.

Figure 4. Data ingestion layer



4.3.1. Ingestion / Processing Server

The Processing Server establishes a secure connection with the Bridging Unit and the regional database cluster. Its primary function is to receive the monitoring data, prepare it and then store it. This architecture adopts an event-driven API-based approach, where the Bridging Unit actively submits the data for ingestion. Upon receiving the data, the server performs validation and normalisation before saving the data into the databases. The ingestion service must be completely stateless for efficiency and scalability.

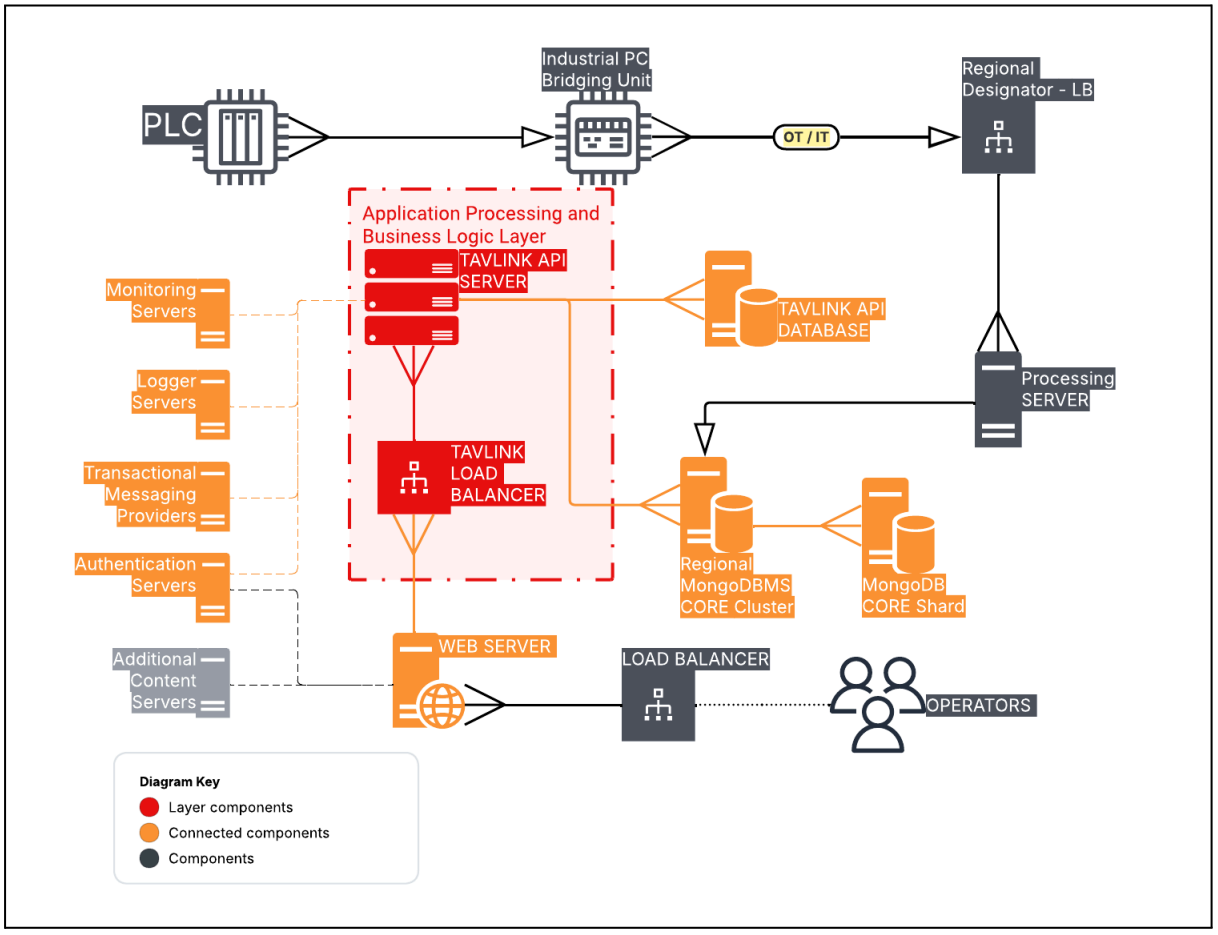
4.3.2. Designator (Load Balancer)

The Processing Servers are deployed behind a Designator component that acts as a load balancer. It has the responsibility of distributing incoming traffic across the available servers. This ensures availability and resilience in case of an individual server failure, allowing for uninterrupted data flow.

4.4. Application Processing and Business Logic Layer

The Application Processing and Business Logic Layer represents the core of the Távlink system. It is responsible for implementing the core system logic, allowing the management of system components and their communications. For end users, it also provides a comprehensive API for the monitoring system.

Figure 5. Application processing and business logic layer



4.4.1. Távlink API Server

The Távlink API Server serves as the central backend service of the monitoring system. It exposes a robust API (application programming interface) for administrators and end-users that can be used to manage the monitoring system. For end-users like operators, this is the initial medium for monitoring data retrieval. The API Server is designed to operate statelessly, enabling horizontal scaling and fault tolerance. A framework is needed for this service that supports efficient request handling, robust schema validation and integration with document-oriented databases (such as MongoDB). As an example, FastAPI has these features built in that complement this design. It also generates API documentation, and developers enjoy vast amounts of Python libraries, making it a suitable candidate.

4.4.2. Távlink Load Balancer

Traffic sent to the Távlink API Server is distributed through this load balancer. This component routes the incoming traffic to the available servers, utilising available resources efficiently. This layer is also designed to support auto-scaling to allow scale up or down on demand.

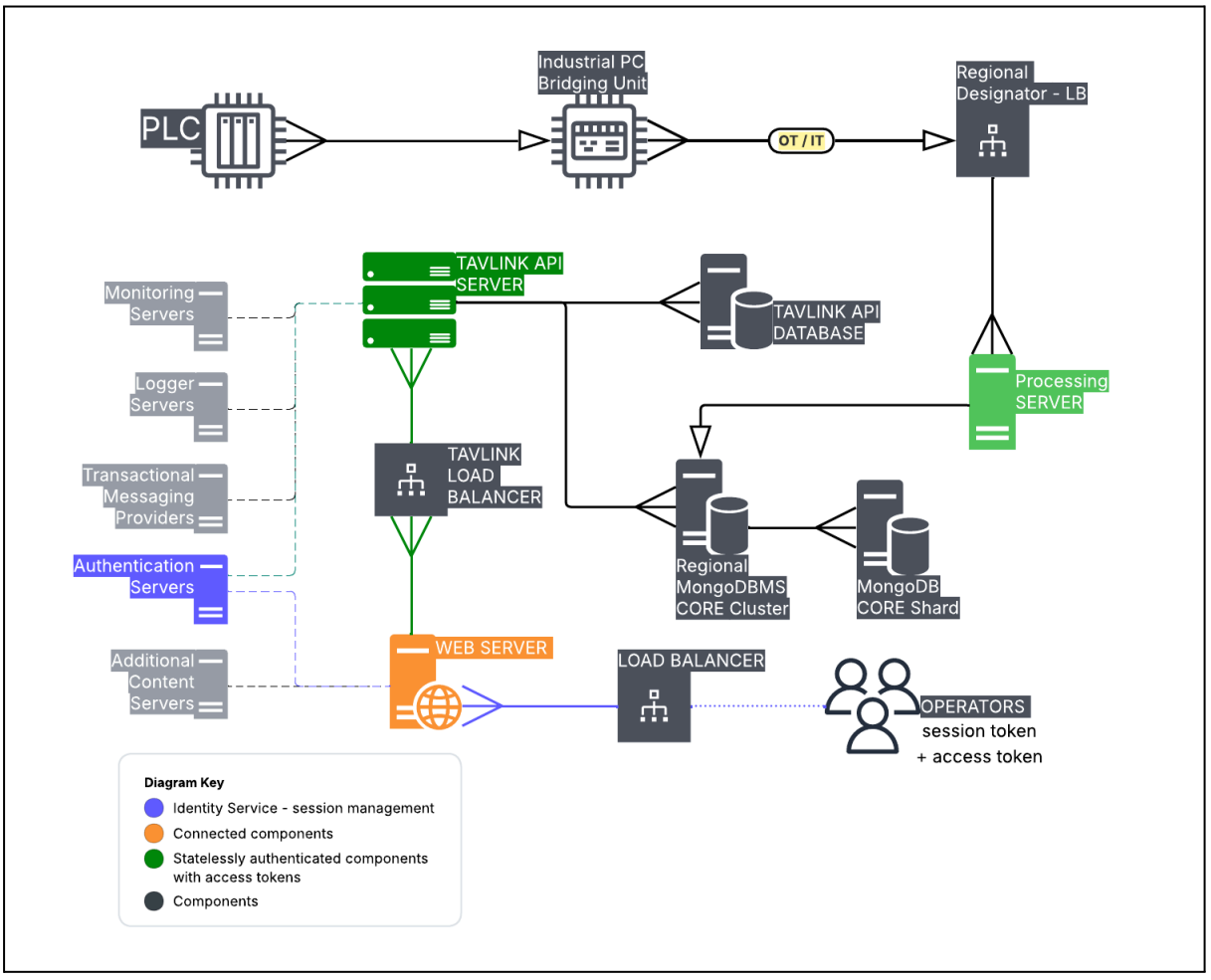
4.5. Identity, Access Management and Control Layer

The Identity, Access Management, and Control Layer is responsible for authentication, authorisation and the enforcement of access control across the entire system. Considering that operational data is sensitive, robust identity management is essential to ensure secure authorised access to resources.

Rather than implementing these mechanisms directly into the Távlink platform, the architecture integrates a trusted external identity service. This separates and outsources the responsibility of authentication and authorisation to a service that is specialised in that field. That way, access can be delegated, and while these authentication servers will handle session management, the monitoring system can incorporate a consistent and stateless authentication method across all components. This reduces complexity and minimises operational burden with the security implementation and maintenance.

The selected identity service must support advanced features, including multi-factor authentication (MFA) methods and robust session handling to minimise access threats. Several identity platforms are suitable, but one was particularly used to design the architecture around: the Rifstar AuthBridge API. It is an internally developed identity service which has not yet been made public. It handles session management and access control (RBAC) with appropriate authentication and authorisation mechanisms. The design does not depend on this identity service and can be substituted if needed.

Figure 6. Identity, Access Management and Control layer

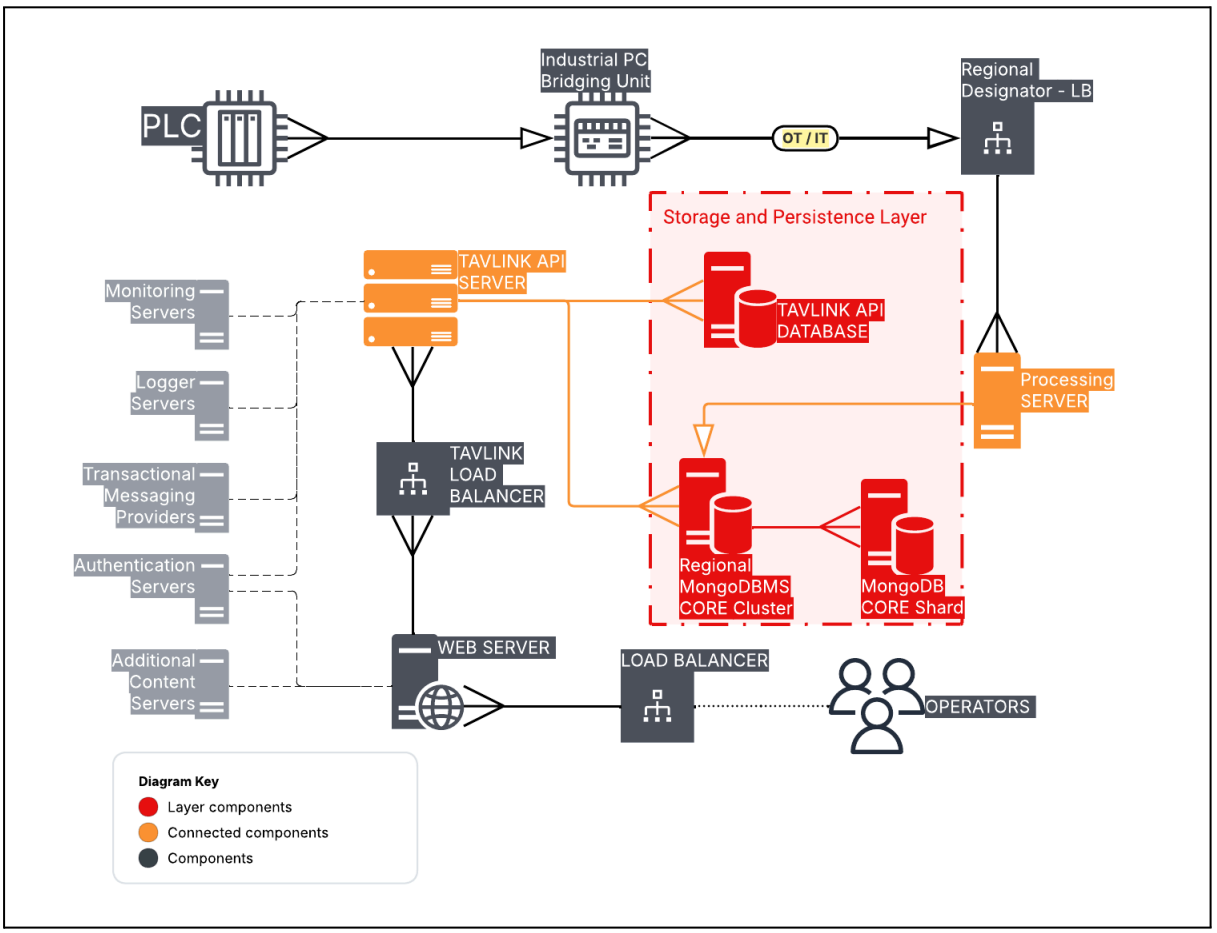


4.6. Storage and Persistence Layer

The Storage and Persistence Layer includes all major storage methods across the system. Business operational and monitoring data have to be stored, retrieved and managed reliably. At the core of the architecture is a document-oriented database technology such as MongoDB. It is selected for its robustness, speed and flexibility. Such flexibility is suitable to accommodate evolving schemas without the need to redesign the system, which can be a major advantage if reporting formats change over time.

To support the scalability of the system, a distributed database architecture must be adopted. A sharded deployment model enables the system to handle large volumes of monitoring data with scale. With this approach, the data can be distributed through a regional cluster, which also improves the performance of the system. The data placement and retrieval are the responsibility of the regional cluster itself. That simplifies design as the data ingestion servers operate statelessly and have only knowledge of the appropriate cluster to send the data to. Data replication can also be introduced easily for resilience and fault tolerance if needed.

Figure 7. Storage and persistence layer



4.6.1. Application Data Store (API Layer)

This data store is responsible for persisting application-level data required by the Távlink API. This includes configuration and system data.

4.6.2. Monitoring Data Store (Ingestion Layer)

The monitoring data store is dedicated to persisting data collected from the reporting devices through the ingestion layer. This component can have sharding and replication implementation through a database cluster. The data stored here is limited to the operational output of the monitored devices.

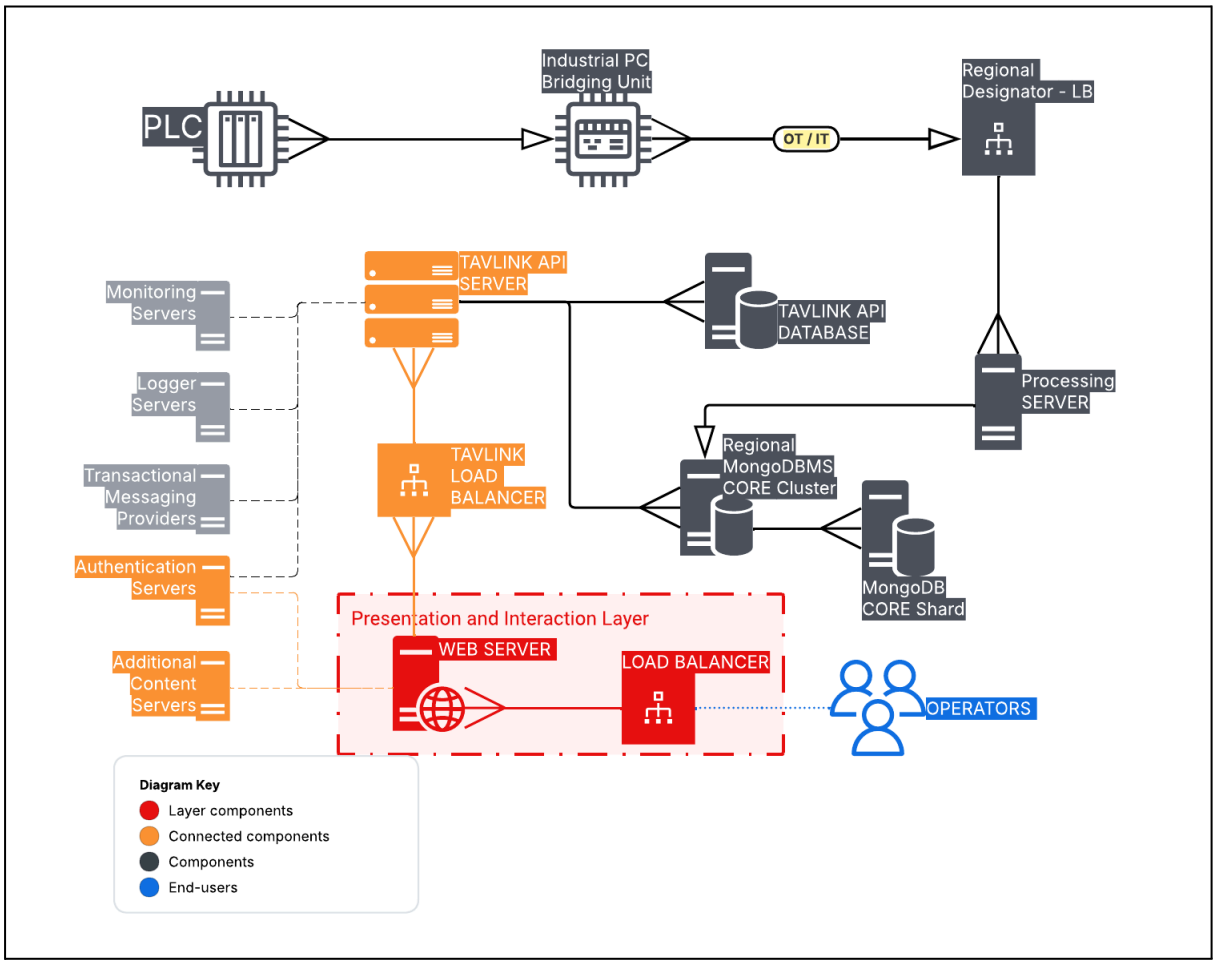
4.6.3. Regional Database Cluster

To ensure efficient data storage and retrieval while maintaining consistency, monitoring data is distributed across regional database clusters. Each cluster distributes data using sharding mechanisms, and it maintains information about data placement, allowing queries to be routed to the appropriate storage nodes.

4.7. Presentation and Interaction Layer

The Presentation and Interaction Layer serves as the primary user-facing interface to the Távlink system. It is responsible for presenting monitoring data and system management in a secure and user-friendly manner.

Figure 8. Presentation and interaction layer



4.7.1. Web server - Control Panel

The system can be accessed through a web-based control panel that communicates with the Távlink API to manage the monitoring system and retrieve monitoring data. This browser-based interface was selected to ensure platform compatibility across devices and operating systems.

This approach simplifies development and maintenance while still allowing future expansions towards other interfaces like mobile applications through the Távlink API if needed.

Modern extensive web application frameworks that support modular and responsive component design, like React, are perfect for this use case, combining with Next.js for server-side rendering. Additional features, such as localisation, may be integrated through other backend services to enhance usability.

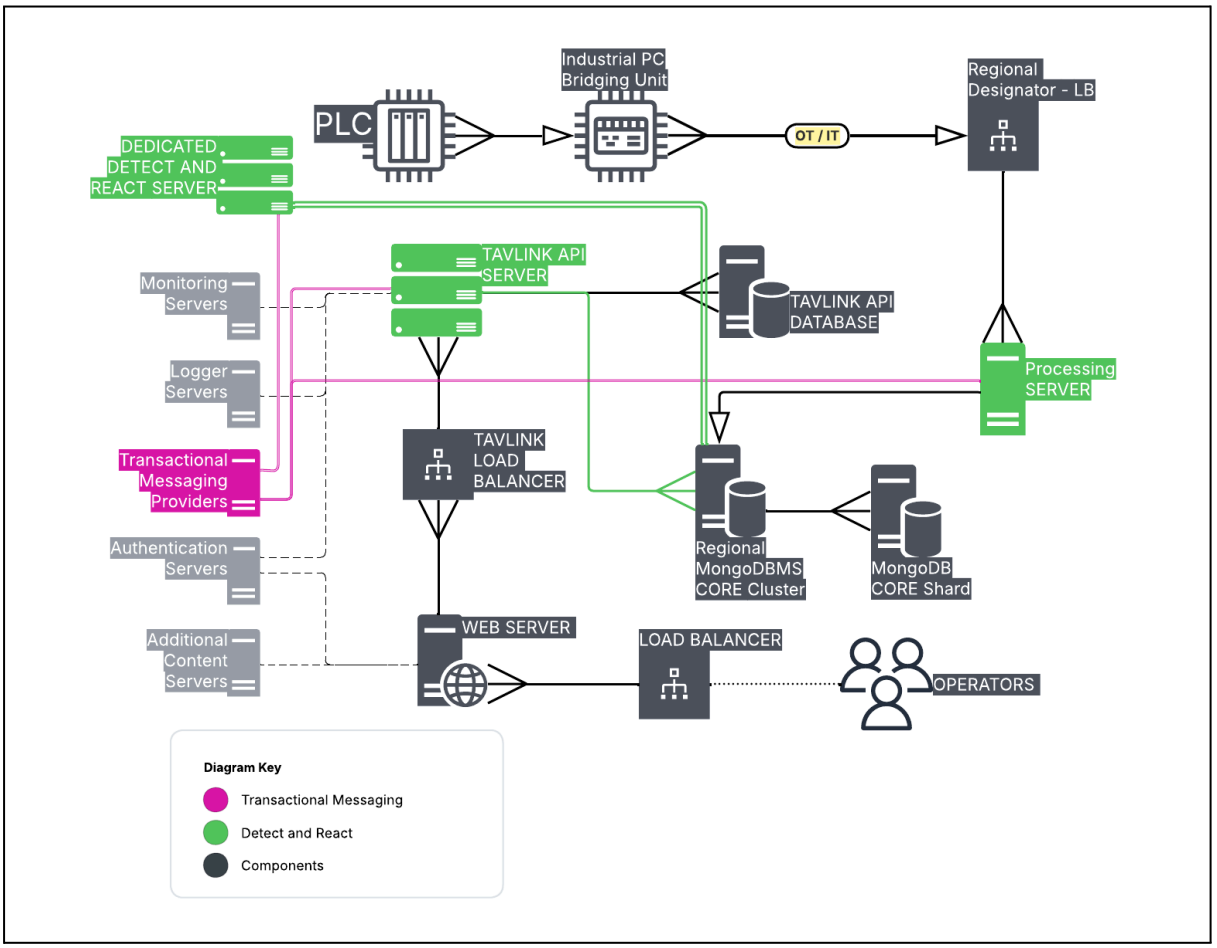
4.7.2. Load Balancer

Traffic to the web-based control panel is managed through a load balancer to distribute incoming traffic across the available web server instances. This ensures horizontal scalability while improving availability by preventing single points of failure. Instances under the load balancer are designed to be automatically provisioned and decommissioned based on demand for optimal performance and cost.

4.8. Monitoring and Reaction Layer

The Monitoring and Reaction Layer is responsible for detecting relevant conditions within the collected monitoring data and initiating appropriate response actions. This includes the generation of alerts and notifications based on defined thresholds, patterns and behaviours set by the operators. Message queuing can be implemented in various ways, one of which is using external services. Outsourcing it simplifies development, while transactional messaging services also include queuing out of the box. These services include, but are not limited to, email, short message service (SMS) and voice-based notifications. The detection can be implemented either in the business logic or the ingestion layer. For efficient and fast detection, it should be implemented within the ingestion layer, but that limits context. For larger context-aware detection, business logic level is suitable for implementation, in which case an extra separate detect and react component should be added that aggregates database content in a scheduled way. That way, the Távlink API server doesn't get overloaded with tasks. To get the best of two worlds, both can be implemented. The Reaction should consist of independent components or should be outsourced.

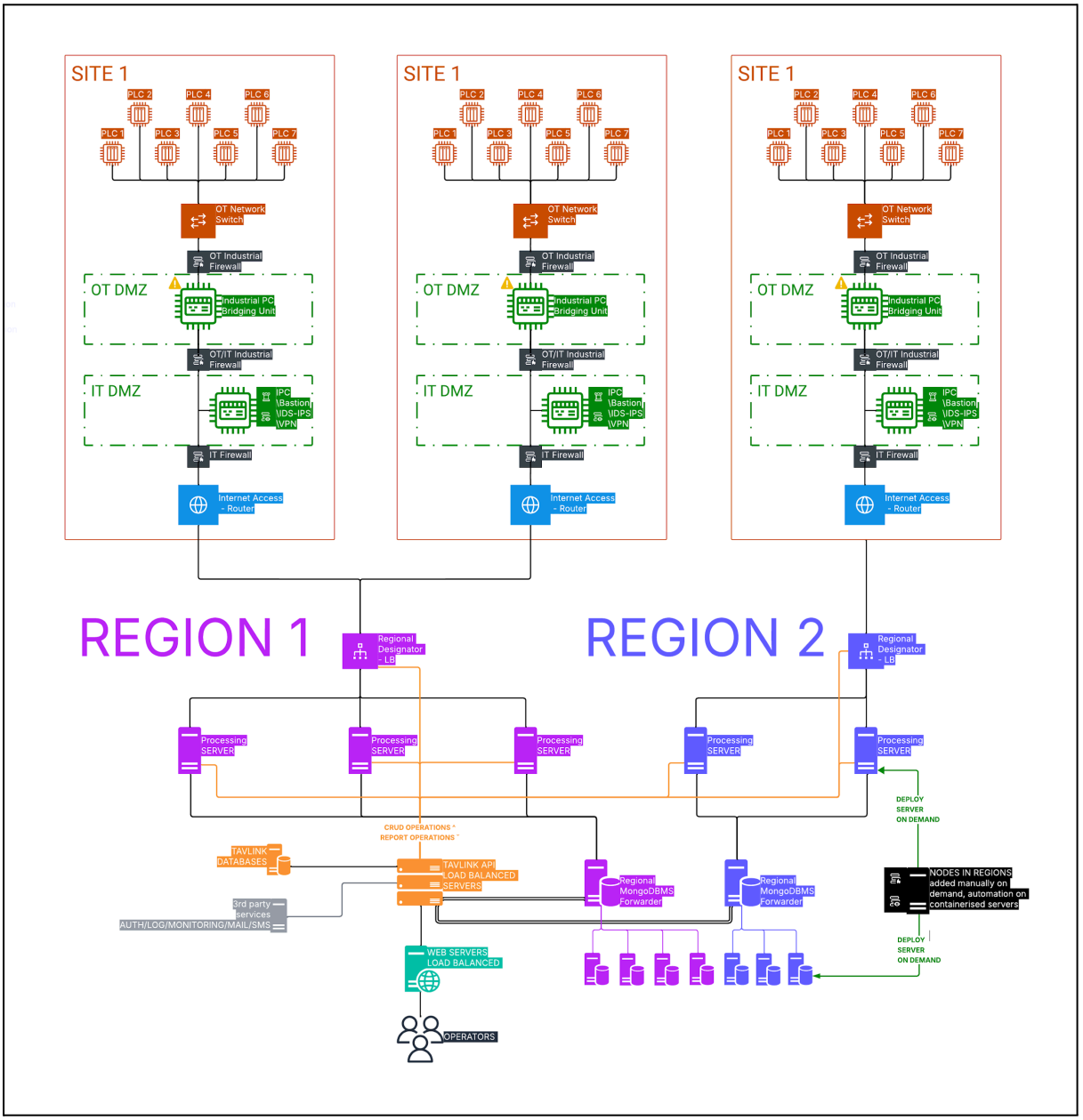
Figure 9. Monitoring and reaction layer



4.9. Example Deployment of Architecture

Figure 10 illustrates a simple example deployment of the proposed Távlink architecture for three industrial sites within two geographical regions. The deployment demonstrates how the layered and segmented design can be realised into practice and also showcases the clear separation of IT and OT domains.

Figure 10. Example deployment with three OT sites in two IT infrastructure regions.



5. Security Architecture

This section includes the basic security model of Távlink. Future documentation must also include threat modelling, disaster recovery, incident response and business continuity plans.

5.1. Identification and Authentication Model

Identification and authentication within the system are delegated using an external identity management service. This approach centralises authentication logic and session management. Upon successful authentication, the user receives a session token and a short-lived access token that can be used for stateless authorisation within the Távlink platform. Access tokens are signed by the identity provider, which can be validated using public-key (asymmetric) cryptography. These tokens can be refreshed through the identity provider using the session token. (see figure 11)

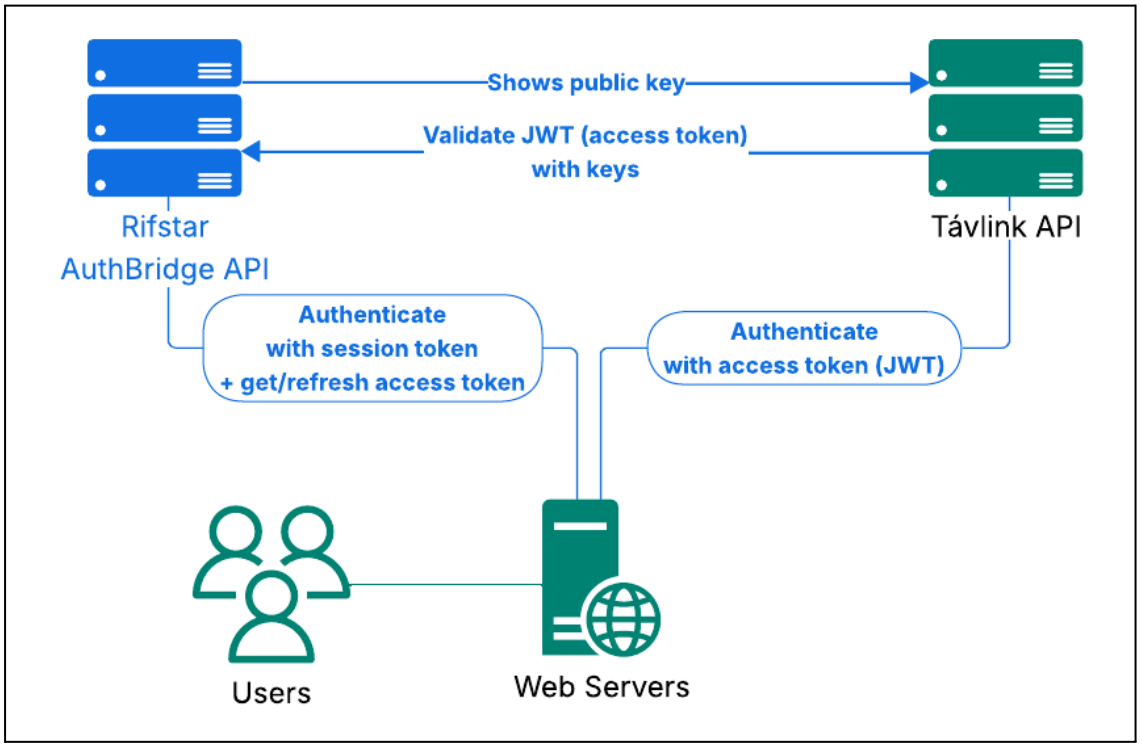
5.2. Access Control

The external identity provider has built-in access control, which can be used for efficient and fast permission evaluation. The access token (JWT) itself already includes the user info and permissions. The permission system is based on a role-based model with the principle of least privilege, and it can be configured using the external identity provider. [12]

5.3. Monitoring, Logging and Audit Controls

All systems are monitored and logged independently using external services. All major operations and security events must be logged. In case of audit and incident response, the system must have appropriate controls. [12]

Figure 11. Stateless authentication and authorisation (Távlink web panel)



6. Data Architecture

6.1. Data Model and Schema

The data model of Távlink is designed to be flexible to accommodate support for all kinds of devices. Although the databases are flexible in storage, the monitored device types must be defined in the system by their schemas and configurations, including field structure, data types and reporting intervals. Enforcing such requirements ensures reliability during ingestion and presentation while also allowing for accurate estimation of storage requirements. This is essential for capacity planning and allows for data retention calculation. For data that requires enhanced integrity, additional mechanisms can be put in place, such as cryptographic hash chaining, to ensure that data is not tampered with and is authentic. Monitoring data are generally processed in batches, which also reduces database overhead and promotes high throughput.

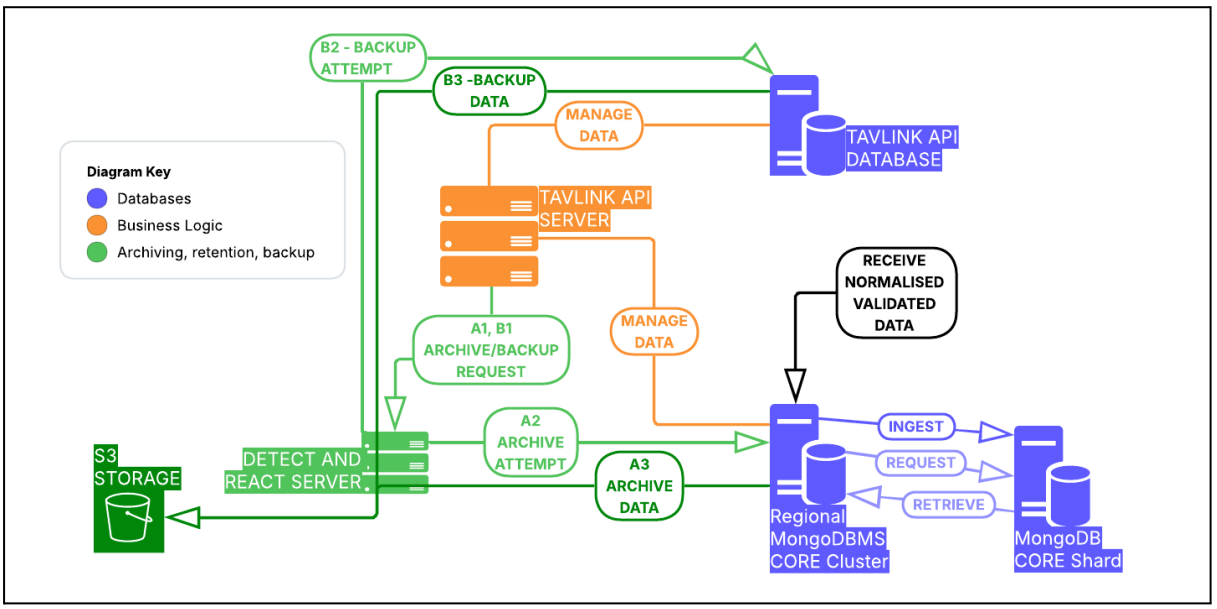
6.2. Normalisation

Data normalisation is performed during the ingestion of the data to ensure consistency. Incoming monitoring data is validated against its type's schema to ensure consistency.

6.3. Retention and Archiving

Data retention and archiving are based on predefined configurations and are subject to site and device-specific requirements. Older data may be archived using protocols such as S3 to free up database storage. This reduces costs and also retains information if needed. Backup procedures work similarly to archiving.

Figure 12. Data architecture



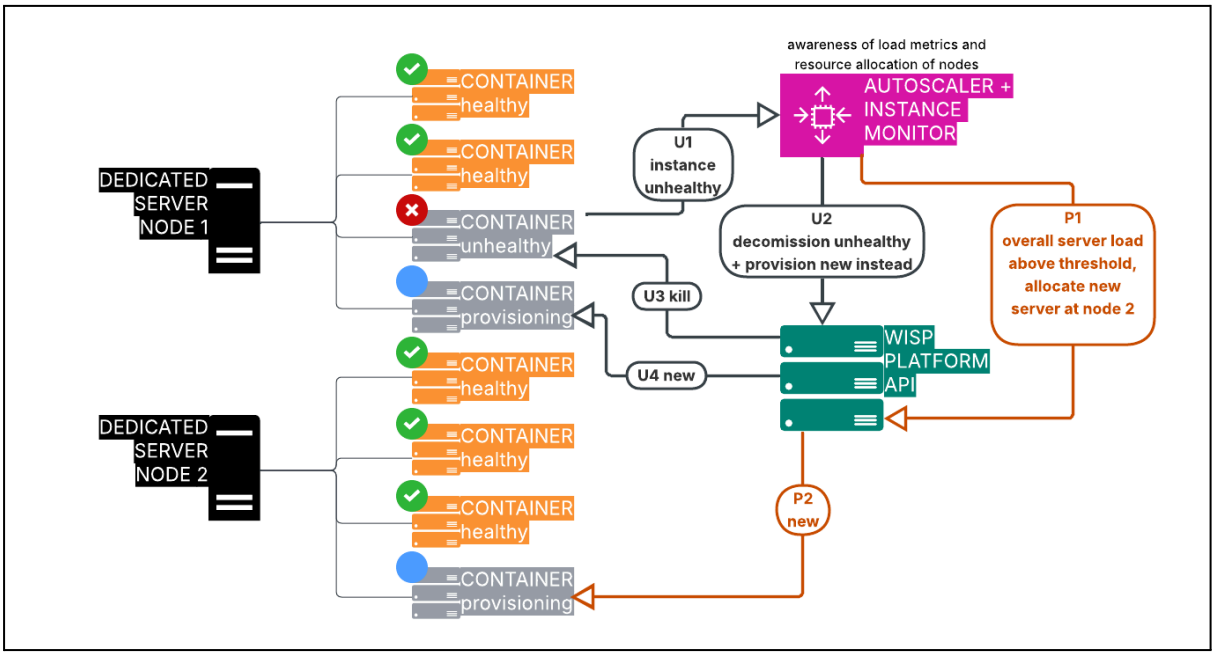
7. Deployment Architecture

This section describes the deployment strategy for the Távlink IT infrastructure.

7.1. Deployment Infrastructure

The deployment environment is based on a dedicated server infrastructure operating within a cloud. Containerisation technology is used to emulate cloud capabilities such as automated provisioning. A container orchestration platform or similar can be employed to create, manage and terminate instances on demand. This system was planned with WISP in mind, which is a Docker-based server management panel featuring RESTful API capabilities (see figure 13 for auto scaling with WISP). As a more straightforward approach, any cloud provider can be used to achieve this. Both enable horizontal scaling and load balancing across the available resources. However, deploying as a private cloud-like system maintains full control over the underlying infrastructure.

Figure 13. Auto scaling within the private cloud-like environment managed by WISP



7.2. Deployment Process

Components are prepackaged and deployed as containerised servers. Deployment actions are done through automated workflows via the platform API. For these features to work, there is also a need for a dedicated instance to handle these processes, as well as monitoring server metrics for appropriate scaling controls.

7.3. Separation of Deployment Levels

Deployment levels are completely separated logically. Each environment serves a distinct purpose, and additional environments can be added if needed.

7.3.1. Development

The development environment is an early-stage, experimental testing environment which is completely local. Once functionality is verified, components may be promoted to the appropriate next level.

7.3.2. Prototype

The prototype (or pre-production) level is a production-like testing environment. It is used for evaluation, benchmarking and testing for functionality, security and load. Once automated tests and the human evaluation pass the requirements, a final approval promotes the components to production. This ensures full testing in realistic conditions before production deployment.

7.3.3. Production

The production environment operates within the same private cloud-like infrastructure as the prototype but serves as the active business deployment. To ensure fast and reliable deployment, instead of updating running instances, new service instances are provisioned alongside the existing ones. This creates two separate versions running in production, and traffic would be gradually redirected to the newer version. The previous version can be switched off or even kept in a minimal state for warm rollback without major service interruption. While concurrent versions introduce potential data compatibility risks, the use of flexible database architecture ensures that data remains usable across versions.

7.4. CI/CD - Continuous Integration and Delivery

Automation is fundamental for reducing manual effort and minimising human error. A CI/CD pipeline can be used to automate build, test and deployment across all environments.

7.4.1. Automated Testing

Automated testing must include unit, functional, feature, security and benchmarking tests. Stress tests must also be applied to validate system behaviour under peak load conditions.

7.4.2. Manual Approvals for Production Deployments

Production deployment must always be approved manually by humans with predefined checklists. This serves as an additional safeguard as the system interacts with critical infrastructure and manages sensitive operational data.

8. Conclusion

The architectural design of Távlink attempts to address the challenges of monitoring industrial environments remotely. The design has a layered approach, and it aligns with well-known global industry standards of IEC 62443 and ISO 27001. Security, scalability and resilience were foundational principles followed while designing this system. While specific technologies and implementation choices may vary depending on deployment context, this paper serves as a general blueprint for a secure and robust implementation of an industrial remote monitoring system.

9. References

[1] Mitsubishi Power,
"Power plant cybersecurity in a globally connected world,"
White Paper, Mitsubishi Heavy Industries, Feb. 2023.
[Online]. Available:

https://power.mhi.com/service/tomoni/downloads/pdf/101512_MP_WhitePaper_Cybersecurity_Letter_FINAL_021523_LR.pdf

[2] International Society of Automation (ISA),
"ISA/IEC 62443 series of standards."
[Online]. Available:
https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[3] ISO/IEC,
"Information security, cybersecurity and privacy protection —
Information security management systems — Requirements,"
ISO/IEC 27001:2022, Oct. 2022.

[4] R. M. de Freitas, S. L. M. C. Titotto, A. A. de Andrade, and R. G. Lins,
"A five-step cyber-defence model for Industry 4.0 control systems
integrating IEC 62443 and ISO 27000,"
in Proc. 16th IEEE Int. Conf. on Industry Applications (INDUSCON),
São Sebastião, Brazil, 2025, pp. 743–750,
doi: 10.1109/INDUSCON66435.2025.11241757.

[5] IEC,
"Industrial communication networks – Network and system security –
Part 1-2: Master glossary of terms and abbreviations,"
IEC/TR 62443-1-2:2010, Nov. 2010.

[6] J.-H. Wang, C.-Y. Huang, H.-Y. Chou, C.-Y. Wang, H.-J. Kuo, and V. Ting,
"Security service architecture design based on IEC 62443 standard,"
in Proc. IEEE 3rd Int. Conf. on Electronic Communications,
Internet of Things and Big Data (ICEIB),
Taichung, Taiwan, 2023, pp. 483–486,
doi: 10.1109/ICEIB57887.2023.10169989.

[7] IEC,
"Industrial communication networks – Network and system security –
Part 1-1: Terminology, concepts and models,"
IEC/TS 62443-1-1:2009, Jul. 2009.

[8] IEC,
"Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program,"
IEC 62443-2-1:2010, Nov. 2010.

[9] IEC,
"Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels,"
IEC 62443-3-3:2013, Aug. 2013.

[10] IEC,
"Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements,"
IEC 62443-4-1:2018, Jan. 2018.

[11] C. Rajak, J. Bharti, A. Mateen, N. Mehndiratta, J. Chauhan, and R. Marndi,
"A roadmap to ISMS ISO/IEC 27001 implementation process,"
in Proc. 3rd Int. Conf. on Range Technology (ICORT), Chandipur, Balasore, India, 2023, pp. 1–5,
doi: 10.1109/ICORT56052.2023.10249115.

[12] IEC,
"Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems,"
IEC/TR 62443-3-1:2009, Jul. 2009.