WHITE PAPER

SECURITY RECOMMENDATIONS FOR PLATFORM DEPLOYMENT

CONTENTS

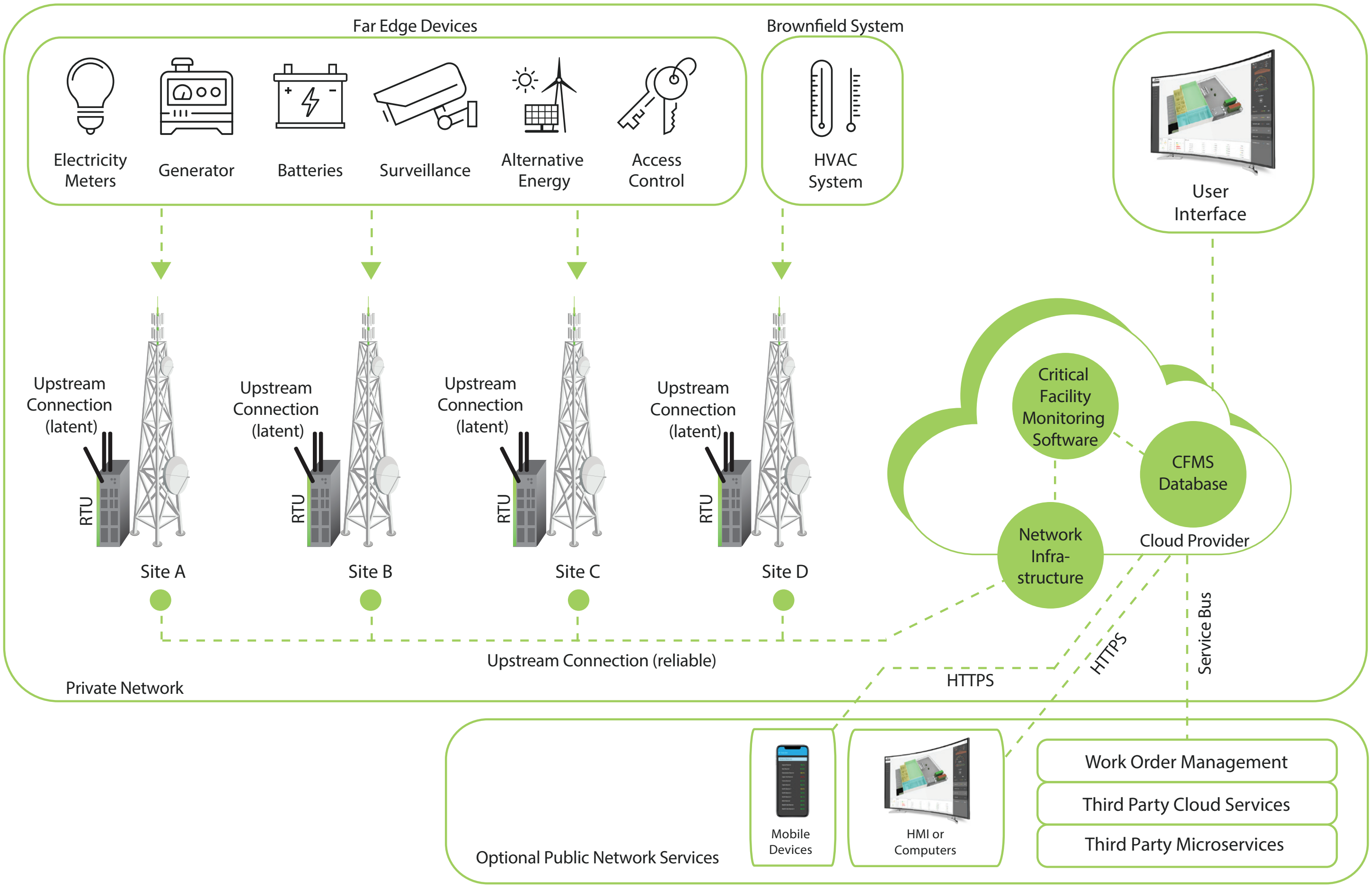
1.0 INTRODUCTION

Critical Infrastructure requires a unique blend of security provisions to accommodate comprehensive remote monitoring and management. In a multisite scenario, this is especially important because the security of all installations can be compromised by the weakest link –wherever that is in the network.

This guide provides recommendations on security strategies and best practices for installing Radix IoT solutions in greenfield and brownfield environments.

A complete security solution requires attention to each component of the network. This guide defines the components that comprise a typical network and provides recommendations on securing each component as well as the overall network.

The following diagram describes a typical IoT solution layout. The following sections of this document detail each component and generalized recommendations for each.



2.0 NETWORK COMPONENT/ SEGMENT DEFINITIONS & RECOMMENDATIONS

Private Network

A private network is a network environment of edge remote terminal units (RTUs), far edge devices, core network infrastructure components, containers, and/or virtual machines that comprise an IoT solution. For the purposes of this document this solution is intended to be a critical facility monitoring software (CFMS). A private network is a firewalled infrastructure that is segregated from the internet. Though internet connectivity may be bridged into the private network in some cases, it is considered managed access and is carefully monitored and controlled.

Security Information & Recommendations
A private network should exist encompassing ideally all of the far edge TCP/IP enabled devices, RTUs, and cloud infrastructure if possible. In general, the vector of attack for vulnerabilities from the outside would be through the user interface (UI) given it would be most likely to have an open port. Trusted clients that need access to the UI should connect through the network via a virtual private network (VPN) with a two-factor authentication (2FA) scheme in place. Should external clients be necessary without the deployment of a VPN it is recommended that the webserver running on the CFMS be deployed at a minimum using:

- An SSL Certificate to deploy SSL/TLS encryption allowing HTTPS to the Mango webserver. Further information can be found at https://docs-v4.mango-os.com/ssl on SSL encryption installation
- Configured firewall allowing port 443 to the CFMS
- Router and firewall provisioning to address brute force attacks using automated IP address banning

Optional Public Network Services
Often private networks are required to port to public networks for access to either 3rd party integration or to allow mobile connectivity. Specific port references are described below to allow for this connectivity.

Critical Facility Monitoring Software (CFMS)

A cloud and Edge based solution that allows for aggregation of data, monitoring, diagnostics, and remote control of far edge device information allowing remote management of many facilities from a single or centralized location. This software often connects to a database (either internal or external) to allow long-term storage of Far Edge Data. For the context of this document Mango and CFMS will be used interchangeably.

Security Information & Recommendations
The Mango CFMS is built and maintained by Radix IoT with security at the forefront of development using the Spring Security library of components which are updated in each release. As such, updates and patches are regularly issued and should be installed when available. Mango can easily be updated via the modules section of the UI. An important but often overlooked component is the OS that the Mango instance is running. This should be updated regularly and kept current with all security updates. Beyond this the following practices will help keep the CFMS secure:

- Strong User password requirements within Mango user management, and preferably single sign on (SSO) integration. Further information on user management can be found at https://docs-v4.mango-os.com/users
- Careful management of file permissions. Never make the Mango env.properties file read/write by "others". (Protection was built into Mango in v4 to prohibit Mango from starting if this is set)
- Careful planning of user rights management with particular attention to granular permissions to ensure that role-based access is allocated appropriately. Mango supports inheritance and enhanced access control that can require more than one role for access
- Whitelisting of all safe IP connections to the cloud is also recommended.

Cloud Provider

A provider of virtual computer resources, database technology, networking and often security apparatuses that mitigate the need for hardware while also offering scalability in a virtual software-as-a-service environment. Common cloud providers are Amazon (Amazon Web Services), Google (Google Cloud Platform), Microsoft (Azure), and Digital Ocean.

Security Information & Recommendations

Cloud platform operations and naming conventions vary greatly by vendor. Typically, Mango is run in the cloud, with a database connection and an optional connection to a secondary data lake of the customers' choosing. Depending on the cloud vendor, security and technology choices can greatly impact the operation and security of the overall solution. The following should be considered:

- Public network ports should be limited to the required CFMS ports. With limited exception this would only be 443 if external access is required.
- Ports on the private network side should be restricted to an 'as need' basis, and are somewhat dependent upon whether you are deploying cloud connect to edge RTUs (Which default to 9005, but can be changed if desired). In cases where direct connections are being made to devices via TCP/IP, applicable ports should be opened to allow communication, and all devices should exclusively reside on the private network and should be verified to not have a field bridge to a public network at the Edge. (Effectively creating an outside entry vector).
- If an independent CFMS database is deployed instead of the integral database provided by the Mango installer, this database should not reside on the same VM as the Mango runtime. Also, it should utilize virtual private cloud (VPC) to communicate with the database to avoid any requirement to open public ports. At no time should any public port be made available to a database.

CFMS Database

A location where data collected from far edge devices, and optionally an edge RTUs is organized for later analytical use. Typically, this will reside within a cloud provider's managed database structure. This is not to be confused with situations where external data lakes also are connected to the cloud provider to allow for broader data storage for other purposes.

Security Information & Recommendations

Mango's default database is mySQL. It can be installed on the same VM as Mango or in a separate environment. For scalable solutions and larger projects a managed service database environment from a major cloud provider is recommended. This will allow a simple and effective mySQL managed database solution to be created, replicated, and maintained separate from the Mango runtime environment. This is especially important for Cloud instances of Mango where many 'downstream' instances of Mango may be feeding data to the Cloud instance for long-term storage.

Edge RTU

A computing device (typically Linux based) that sits at an edge location as an instance of a site that functions to communicate with far edge devices and offers a consolidated translation of common protocols to enable data to be transferred to and from the CFMS. Edge RTUs handle not only communication with the far edge devices that may support many different protocols. They also communicate upstream with the CFMS which often lives within a cloud provider. This upstream connection may be a hardline connection to the internet, a cellular connection, or a satellite connection via a provider such as Starlink or Inmarsat.

Depending on the RTU design, the Edge RTU can function for days, weeks or months without a cloud connection, should the primary and secondary upstream connection be lost. Most RTUs allow for retention of data, and contain local logic to facilitate this offline operation in case of backhaul outages. It should be noted that not all site locations will employ edge RTUs. Depending on the far edge technology, it is sometimes possible – and financially advantageous – to directly connect far edge technology to the CMFS. Carefully consider the private network setup to ensure security in this type of solution.

Security Information & Recommendations
Radix IoT offers several edge RTUs that allow simple installation. However, customers may also install Mango on their own hardware. Specific requirements exist at radixiot.com for minimally viable hardware sets. The architecture of Mango in a networked solution is such that an Edge RTU is a full instance of Mango and communicates to other instances of Mango through a module known as Cloud Connect. https://docs-v4.mango-os.com/mango-cloud-connect-module.

In a critical facility solution with many sites, the architecture typically has locations that each have an edge RTU with Mango running, and connects upstream to a cloud instance of Mango on a VM. In this type of solution, both the edge RTU and cloud VM should reside in the same private network.

Cloud Connect defaults to using TCP Port 9005 and provisioning of any internal firewalls should accommodate this, including instances where a firewall (such as ifw) is installed on the RTU operating system.

Given that Mango runs identical software both at the edge RTU and in the cloud, it is theoretically possible to connect to native TCP/IP devices at the edge without the need for an RTU by setting up edge TCP/IP devices as data sources in the cloud instance of Mango. In such cases care should be taken that all devices and the VM are on a private network. Should this not be possible a VPN should be used to facilitate a safe connection to the edge with the fewest number of open ports.

Network Infrastructure

A collection of virtual or physical networking components including routers, switches, firewalls, DHCP servers, cellular modems, etc. that facilitate Ethernet traffic between devices in a private or public network.

Security Information & Recommendations
A network infrastructure solution should be planned out prior to any deployment and it should use standards that fit the needs of the business while offering a secure environment. Though Radix IoT offers a fully managed solution that builds this infrastructure for a customer, often there is a requirement to deploy into existing architecture. In this case it is the responsibility of the I.T. organization to provision servers and security policies to meet the needs of the solution.

Far Edge Device

A device with which an RTU can communicate, or a brownfield system that offers meaningful data or acts as a control point for the CFMS. These devices can natively communicate via TCP/IP, or a protocol that the RTU can supports. Such devices may also connect to a brownfield system via a gateway. Common far edge devices include motion sensors, temperature sensors, generators and security cameras.

Security Information & Recommendations

Careful consideration should be given to far edge devices, particularly those that communicate via TCP/IP. This is particularly important when no RTU is present. Firewall restrictions on the private network should only allow traffic on an 'as-need' basis and on specific ports. Additionally, thought should be put into how the device firmware is upgraded for security patches, as well as into access control for any software or embedded webserver that allows for configuration changes.

With an RTU in place, a dual NIC approach should be used to allow one ethernet controller to be dedicated to upstream communication, and a secondary NIC dedicated to local onsite TCP/IP traffic.

Brownfield System

A system in an edge location (or at a site) that functions with its own logic engine and connects often to proprietary devices to perform a function. Brownfield systems often have a gateway via which they communicate with an RTU using standard protocols. Common brownfield systems include network lighting systems, building management systems (BMS) and fire alarm and suppression systems.

Security Information & Recommendations

The recommendations for brownfield systems are similar to that of far edge devices. However, typically a brownfield system will employ a gateway that facilitates a translation between a proprietary protocol (or wire plant), and Ethernet protocols. Most commonly, these are single NIC devices with proprietary firmware, and often custom programming is required to facilitate mapping of objects and functions. Sometimes these devices may communicate via ModBus/TCP, or Bacnet/IP; however, when possible (and when the gateway supports it) a RestAPI that uses a strong authentication and authorization solution is preferable.

For API integration:

- When feasible, use solutions based on solid, proven authentication and authorization mechanisms such as OAuth2.0
- Practice the principle of least privilege verifying that you are only granted the minimum necessary to complete the required functionality
- Ideally encrypt payload traffic using TLS
- Employ rate limiting in the network infrastructure to reject subsequent requests at a threshold (10,000 requests a day or lower) to prevent DOS attacks

Upstream Connection (Reliable)

A TCP/IP based connection to the location where the critical facility management software resides and operates. The upstream connection is considered reliable when there is a copper or fiber connection facilitating this connectivity.

Security Information & Recommendations

A reliable upstream connection is preferred for all edge locations to connect to cloud instances. When possible these connections should be part of the private network only.

Upstream Connection (Latent)

A TCP/IP based connection to the location where the critical facility management software resides and operates. The upstream connection is considered latent when there is a degree of unreliability in the upstream stability as is the case in cellular technology, satellite, and Wifi. Typically, latent connections are only to be used as backups to reliable upstream connections.

Security Information & Recommendations
Though not recommended for primary communications to the Edge, cellular is a viable option for some applications as a primary and more commonly a backup connection to the cloud. When using cellular technology as a backhaul to the cloud the most secure path is via a private APN from the service provider. Though this is not always possible, public APNs can be used so long as a firewall exists on the RTU.

Service Bus

Defined as an authenticated RestAPI that allows third party software and analytics to use the data (both current and historical) stored by the Critical Facility Monitoring Software and/or allows external access to the CFMS Database typically for external analytics purposes.

Security Information & Recommendations
Mango supports a configurable RestAPI to allow data to be used by external applications. Common practices should be followed including:

- When feasible, use solutions based on solid, proven authentication and authorization mechanisms such as OAuth2.0 or key exchange for external authorization to the Mango API
- Practice the principle of least privilege verifying that you are only exposing pertinent information to the foreign entity via the RestAPI
- Utilize TLS for transport
- Employ rate limiting in the network infrastructure to reject subsequent requests at a threshold (10,000 requests a day or lower) to prevent DOS attacks

User Interface

The method by which a user or group of users visualizes and uses the CFMS. This is commonly through a web-browser on a computer, tablet, or cellular phone. The user interface often contains all the setup, and runtime features that enable the user to interact with the CFMS. User Interfaces are often provided in a graphical form.

Security Information & Recommendations
The webserver in the case of Mango is Nginx. Like any website, it is important to employ HTTPS with a valid certificate. Though it is typical to expose the webserver on a public network, for customers that are able, it is recommended to deploy the webserver on a private network and employ a VPN for access.

3.0 GLOSSARY OF TERMS

List of Acronyms

2FA: Two-Factor Authentication is an electronic authentication method in which a user is granted access to a service only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. This can be through several methods including a third-party authenticator app, an SMS based code, or several questions beyond just a single password. (Authentication shouldn't be a hyperlink.)

API: Application Programming Interface is a connection between computers or between computer programs to allow the exchange of information upon request. When used in the context of web development, an API is typically defined as a set of specifications, such as Hypertext Transfer Protocol (HTTP) request messages, along with a definition of the structure of response messages, usually in an Extensible Markup Language (XML) or JavaScript Object Notation (JSON) format. There are two primary models for API design: RPC and REST.A REST API (also known as RESTful API) conforms to the constraints of REST architectural style and allows for interaction with RESTful web services. gRPC is a technology for implementing RPC APIs that uses HTTP 2.0 as its underlying transport protocol. (No hyperlinks.)

APN: An Access Point Name (APN) is the name of a gateway, generally run by a cellular carrier between aGSM, GPRS, 3G, 4G/LTE, and 5G networks. Frequently this is the gateway to the internet, however, the concept of private APNs can exist which are issued by carriers that allow only intercompany information exchange, which could optionally restrict partially or fully access to the public Internet.

DOS: Denial of Service, (DOS, or DDOS referring to a distributed denial-of-service) is an attack on web services by flooding the targeted machine or resource with requests in an attempt to overload the system and prevent legitimate requests from being possible.

RTU: Remote Terminal Unit. Though it has a different historical context in I.T., RTU is a widely accepted term for a device that is used generally at the edge or remote locations to gather, consolidate, and then securely transfer data to an alternative location. (Typically, a Cloud Service.)

SSO: Single Sign On is an authentication scheme that allows a user to log in to one or several systems with a single ID credential set avoiding the need to re-enter authentication factors across several services.

VPC: Virtual Private Cloud (VPC) networks are private networks with alternative addresses that typically contain collections of resources that need to communicate together, but from a security perspective are better not exposed to the public internet. Typically VPC networks are set up within a cloud service to allow for coupling of resources required at the datacenter level, without requiring the need for publicly accessible addresses and associated firewall rules which could theoretically lead to security risks.

VPN: A virtual private network (VPN) extends a private network to remote locations by the means of using public networks. VPNs are commonly used to increase the security, and management of remote operations, while obfuscating data (typically via encryption) over the public network.

Published by
Radix IoT 2022

Radix IoT, LLC
14555 N. Dallas Parkway #125
Dallas, TX 75254
United States

For more information, please contact
our Customer Support Center.
(Charges depending on provider)
Email: info@radixiot.com

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

radixiot.com