bandora

Bandora.OM

Security and Compliance Architecture

Ricardo Gomes, Márcia Pereira and Gregory King

Contents

Márcia Pereira
Co-Founder & CEO

Security and Compliance in Buildings

Buildings are no longer stand alone ecosystems running Building Management Systems (BMS) based on proprietary protocols. Smart Buildings technologies became a reality when BMS manufacturers started using standard protocols. Thanks to Internet, every system inside a building is connected and available everywhere.

Those technologies allow that a facility manager can connect and manage is building from anywhere using a web-based management console. Of course, as any other internet connected device, BMS are vulnerable to cyber-attacks, just like any other system.

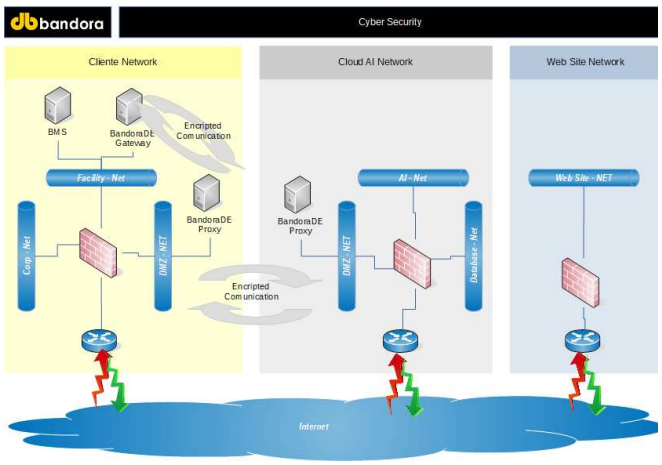
Those who develop solutions running over smart buildings technologies must be aware of threats, and develop secure architectures, assuring that mission critical BMS are not vulnerables to all kind of attacks.

It's not only about security. New Data Protection regulations, such as EU GDPR and California Consumer Privacy Act define new ways as data can be processed, with heavy fines for those who disrespect new rules. In Bandora Systems, we know that security and compliance are serious concerns. Our solution Architect and Data Protection experts developed secure architectures

Architecture

BandoraOM is a Cloud Based Artificial Intelligence Engine. Developed to help facility managers to better manage their buildings, increasing occupants' comfort and energy efficiency, BandoraOM is a software suite with 4 different software products.

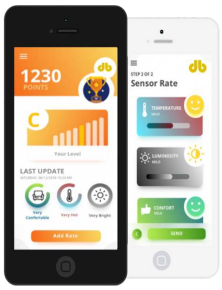
BandoraOM components runs on Bandora's hybrid cloud, except BandoraDE, which is installed in customer's building. BandoraDE is a software gateway that runs on customer network and assures communication with Building Management System.



BandoraOM suite Security Architecture

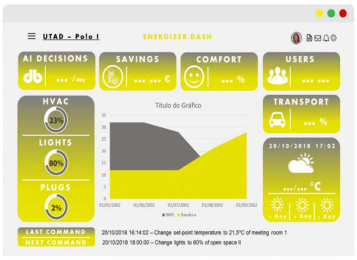
bandoraME

The app that occupants will use to give feed-back, regarding com-fort, temperature and lighting.



bandoraDS

The dashboard where facility managers or staff can analyze building data, as well as the decisions and commands executed by the AI engine.

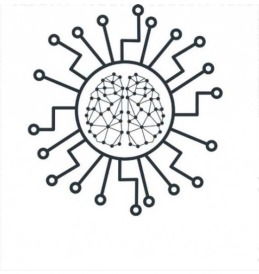


bandoraDE

Software Gateway that gathers data from BEMS and transmits it to BandoraOM system through VPN; assures transparent access to different BEMS vendors

bandoraOM

The Artificial Intelli-gence and Machine Learning Engines that analyze all building data, returning commands to setup up the Building Energy Management Systems.



BandoraOM Software Suite

Chapter 1

BandoraDE

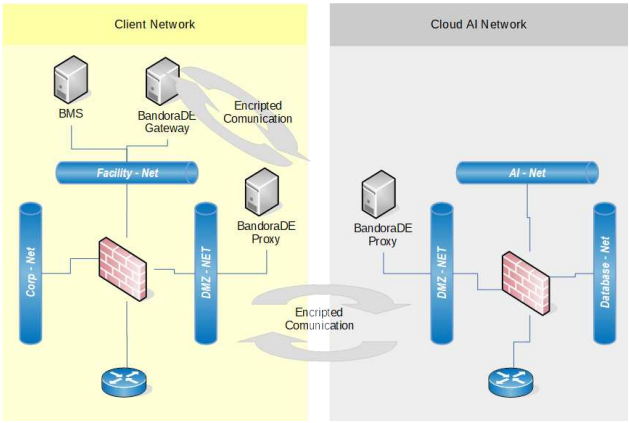
BandoraDE is the software component that assures the connection between Building Management System and Artificial Intelligence Engine hosted in Bandora's hybrid cloud. BandoraDE has two components: An application proxy (bandoraDE Proxy) that assures message transfer between bandoraOM AI Engine and a gateway (bandoraDE gateway) that assures connection to existing Building Management System.

Both systems can be installed in a Microsoft ™ Windows™ or Ubuntu™ hosts. We recommend that BandoraDE Proxy can be installed on DMZ, while BandoraDE Gateway requires connection to Building Management System. BandoraDE architecture is developed to avoid unwanted access to BMS.

BandoraDE roles are:

BandoraDE Proxy is an application proxy and VPN Server. It establishes a VPN tunnel to BandoraOM web Service to send logs and receive instructions from AI Engine to Building Management System. Hard coded rules included in BandoraDE proxy defines that only BandoraOM Web Services host is the only device that can exchange messages with BandoraDE Proxy.

BandoraDE Gateway assures connection to the Building Management System. Must be installed in at the same network than BMS, without internet access requisite. BandoraDE Gateway includes hard coded roles that defines that BMS and BandoraDE Proxy are the only allowed host to exchange messages. BandoraDE Gateway uses the BMS API to receive logs and send instructions to BMS. Messages are translated from BandoraOM schema to BMS vendor language using an HCL service.



BandoraDE Architecture

All messages exchanged with BandoraDE Proxy and BandoraDE Gateway uses HTTPS protocols, assuring data encryption. Using an internal developed schema, a HCL installed in BandoraDE Gateway manages messages translation to BMS's API, in order to assure the hardware agnostic feature of BandoraOM Solution.

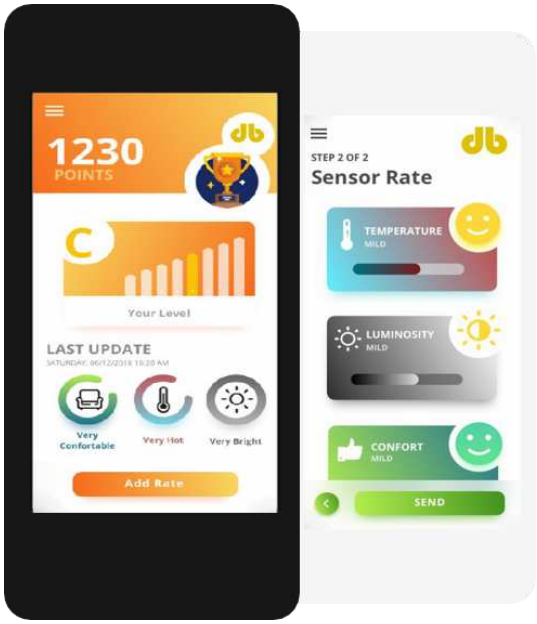
BandoraME

BandoraME is an app developed to run in a smartphone or tablet. It allows occupants to send feedback regarding comfort, temperature and luminosity. bandoraME sends data to bandoraOM Web Services using HTTPS protocol. No personal data is collected and exchanged.

BandoraME is available at Apple Store and PlayStore for IOS™ and Android™ devices, requiring internet connection and active Location Service.

BandoraME sends a data frame to BandoraOM AI Engine.

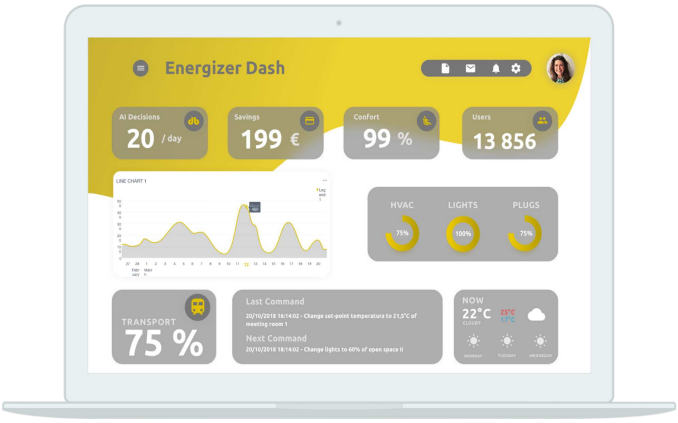
BandoraME runs on two modes: user mode, which requires a registration on first use, and a guest mode, usually to be available in shared spaces to collect visitors feedback.



BandoraME App

BandoraDS

BandoraDS is a web based Dashboard hosted in BandoraOM Cloud Service. It's a multi-instance service that uses LDAP authentication and allows the Facility Manager to view the status of his building in BandoraOM solution. BandoraDS doesn't include any kind of control features, only to view real time status and includes a report engine.



BandoraDS dashboard

BandoraOM

BandoraOM is the heart of our Autonomous Buildings Operations solution. BandoraOM architecture is distributed among three different locations with different roles :

BandoraOM Web Service communicates with BandoraDE Proxy hosted in customer's building, trough a VPN, in order to exchange messages with Building Management System. Messages can be incoming BMS status logs and outcoming instructions to BMS.

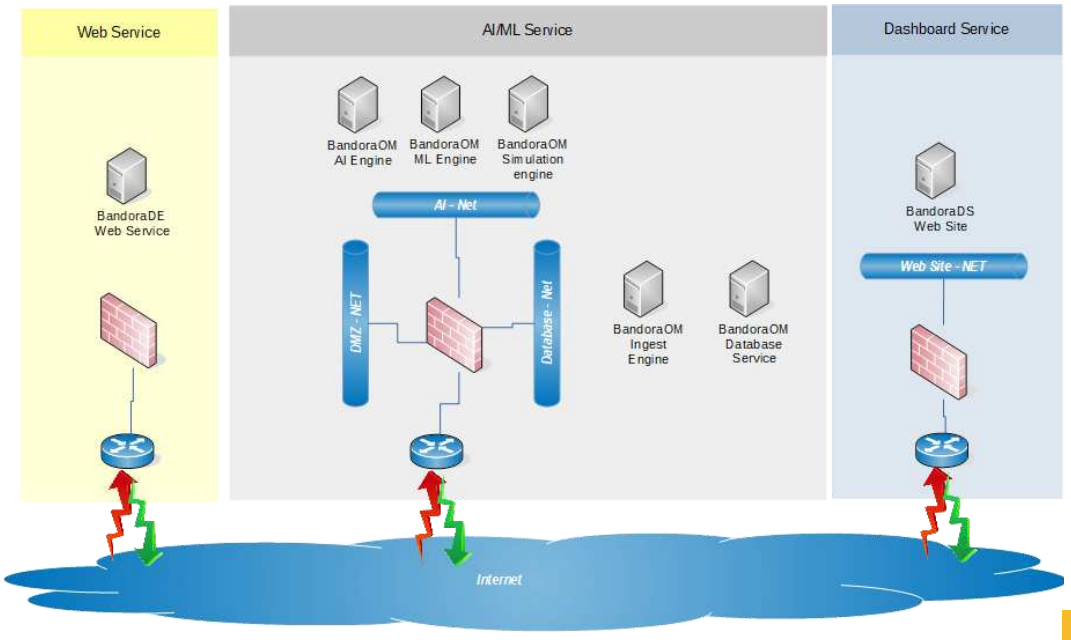
BandoraOM Web Service also receives information from BandoraME App regarding ocupant's feedback. BandoraOM Web Service is configured with a point-to-point role, allowing only access from BandoraDE Proxy and BandoraOM Ingest Engine. BandoraOM Web Service is hosted in a public network, accessible by BandoraDE Proxy through Internet connection.

BandoraOM AI/ML Service is the core of BandoraOM solution. It includes Bandora Ingest Service, who imports BMS and BandoraME logs into a Database to be analyzed by AI Engine.

Bandora AI/ML Service hosts the simulation service that applies ML Alghoritms.

BandoraAI/ML Service is hosted in a private cloud in Bandora's Datacenter. Security roles guarantees that only BandoraOM Web Service exchanges information with BandoraOM AI/ML Service.

BandoraOM Dashboard Service hosts BandoraDS System. BandoraOM Web Service sends data to BandoraDS which is available through internet connection to Facility Managers.



BandoraOM Architecture

Chapter 2

Data Privacy Regulations

New regulations about data privacy, such as European Union GDPR (General Data Protection Regulation) and California Consumer Privacy Act protect user's personal data. All companies and software vendors must be compliant with those regulations. BandoraOM suite doesn't exchange personal data, either in BandoraDE or BandoraME.

All data uses internal Bandora Schema with no references to any kind of personal information. Occupants feedback in BandoraME app.

doesn't send any kind of personal information, such as ID, mail address,etc. Only messages regarding feedback and a encrypted user ID are sent by BandoraME. BandoraOM doesn't process personal information, only statistical data to better understand and adapt Building behavior.

About BandoraDE, only data about Building Management System status will be exchanged with BandoraOM AI Engine. BandoraDE's data frame doesn't include any kind of information about Buildings location or identification, but only a internal building ID.

BandoraME Data Frame

BandoraDE Data Frame

Conclusion

In Bandora Systems, we are aware that for our customers, all data is sensitive and all facilities are critical. We also know a succeeded cyber-atack can compromise people and buildings security with serious consequences. All Bandora's solutions are built using the most recent best practices and reference architectures regarding security and compliance policies.

We know your data is critical
We keep you secure