OS6 Architecture Specification
Issue 13
OptaSense/ENG/1013

Meadows Business Park
Building 3, Second Floor – Suite 1
Camberley, Surrey GU17 9AB
United Kingdom

www.lunainc.com

Table of Contents

1. Introduction to OS6

1.1 Background

Luna are world leaders in fiber sensing. OS6 is our 6th generation of the Linear Asset Monitoring System using Distributed Acoustic Sensing.

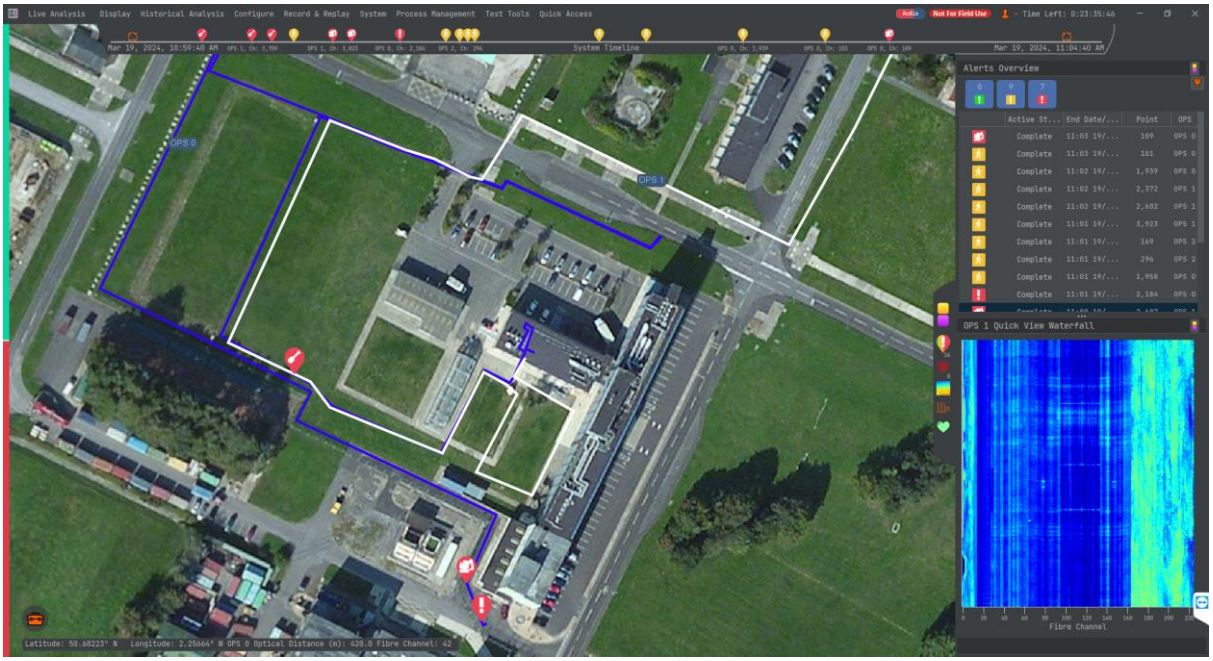


Figure 1 - OS6 Main Screen

1.2 Key Related Documents

Various documents relating to the use of OS6 are available. Please consult your Luna representative for access:

- Application Specifications – for each of our customer applications we have a dedicated specification document – e.g., Pipeline Leak, Pipeline TPI, Road, Rail, Power Cable, Perimeters. These detail the capabilities available for different applications and a baseline for the performance.
- Fiber Acceptance Specification – detailing the expectations for fiber installations.
- Cable Deployment Guides – application specific guides on cable selection and deployment requirements.

1.3 Keeping up to date

Please subscribe to the mailing list on our website for notifications on the latest Software and Hardware releases.

2. System Summary

2.1 Main Architectural Features

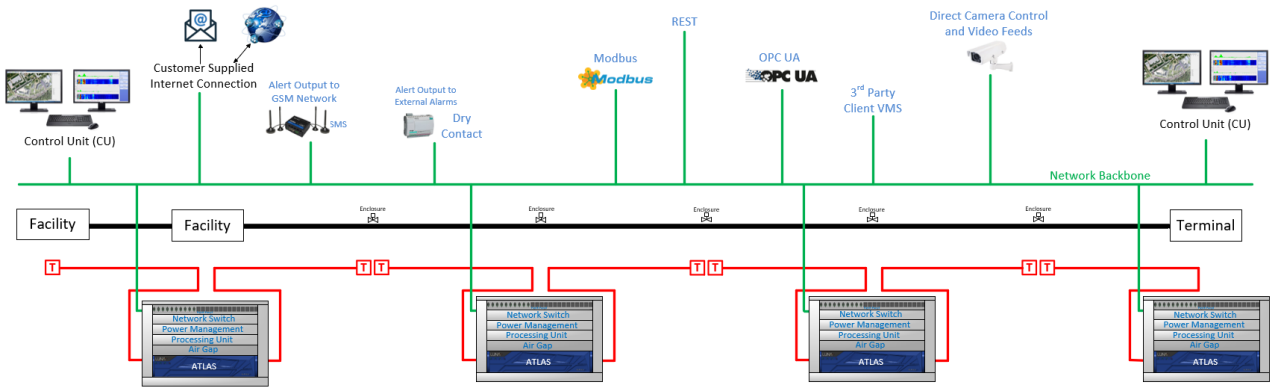


Figure 2 – (Example) System Architecture

- The current Distributed Acoustic Sensor (DAS) is known as 'ATLAS'
- Each ATLAS Interrogator Unit (IU) requires a Processing Unit (PU) to process the Time-Series Acoustic data.
- The PU runs the OS6 Detection Algorithms (such as Digging, Personnel Detector & Leak Detectors)
    - For information on data rates and maximum detector ranges please consult with your Luna representative.
- The PU has Data Recorders (FIFO) for storing the 'raw' Time-Series data and processed data.
    - This allows extraction of data, as well as a 'step back in time' feature to review events.
- The PU has by default an instance of the Distributed Database running on it.
- OS6 uses Distributed Architecture, which replicates and shares data across all PUs. This provides redundancy for:
    - System configuration
    - Alerts
    - Audits
- The Distributed Architecture provides the flexibility to exclude selected PUs from running the Distributed Database where network reliability or latency issues are present.
- If a PU and/or IU are no longer available on the Network (due to network issues, hardware failure etc.) the rest of the system will continue to function with the remaining PUs/IUs
    - All Alert data/configuration for the 'failed' PU/IU will still be accessible (up to the point of failure)
    - *This can help with diagnosing the reason for the failure.*
- Control Units (CU) host the GUI used to display information needed by installers and users.
- External Interfaces can be hosted on specific PUs with the ability to be deployed with redundancy.

2.1 Network Recommendations

- A latency of less than **30ms** (end-to-end) is recommended.
    - The maximum is **50ms**
- A network backbone of at least 1 gigabit is recommended.
- The OS6 architecture allows multiple Control Units (CUs) to simultaneously access the system.
    - The number of CUs that can be added is limited by network constraints i.e., bandwidth, latency.

2.2 Remote Processing (IU & PU not co-located)

In certain circumstances it may be necessary to locate the PUs remotely from the interrogator. This is not recommended due to high data rates of the IU data. This could be achieved with direct / dedicated optical fiber connections between the components. If this is required, please consult your Luna representative for more information.

2.3 Redundancy

The OS6 System Architecture has adopted several approaches to maintain a live operational system when failures occur with various components.

2.3.1 Data Redundancy

The following items are shared across all instances of the Database

- Alerts
- System Configuration
- Audits
- Process Metrics

If the originating PU is unavailable (H/W failure, Network failure), the above items which originated from that PU will still be available up to the point of failure.

The following items are NOT shared (and thus no redundancy is available).

- Time-Series Acoustic Data (IU raw data)
- Processed Data (e.g. 'Waterfall' data, Detector processed Data)

RAID configurations for these are also NOT available.

2.3.2 Fiber Redundancy (cut resilience) – ATLAS IU

Fiber cut resilience can be set up within an OS6 System by having a 2-Fiber configuration. This can be achieved with the following IUs

- Single ATLAS IU (2 fiber setup)

2.3.3 Fiber Redundancy (cut resilience) – Legacy IUs

- Single OLA2.2 (2 fiber setup)
- Two OLA2.1s (1 fiber setup per IU)

2.3.4 Cut Resilience – Perimeter example

Cut resilience for Perimeter setups are normally achieved by having the following

- Fiber 1 is set up to monitor the perimeter in a clockwise direction
- Fiber 2 is set up to monitor the (same) perimeter in an anticlockwise direction
- 2 separate fibers in the same cable are required

For cut resilience for linear assets (Pipelines, Borders etc.) the 2 fibers would need to be in separate cables.

2.3.5 IU Redundancy

IU Redundancy is achieved by having a multiple IU setup.

Please note that items Fiber Redundancy (cut resilience) & IU Redundancy cannot be combined into a single solution using a single IU (such as ATLAS). In this case it would require two ATLAS to satisfy the above scenarios. For example, if proposing to replace two OLA2.1s (IU Redundancy) with a single ATLAS (2 fiber setup) it will NOT result in IU Redundancy.

2.3.6 PU Redundancy

It is recommended to purchase spare PU(s). If a failure with a PU occurs, a spare PU can be installed manually on the System to replace the failed PU.

2.3.7 GUI Redundancy

The OS6 GUI is not required for a running System. Once the System has been configured using the OS6 GUI, the GUI can be powered off. Alerts/Status can be sent via an OS6 Interface running on the PU.

Please note that there is no maximum number of GUIs to a System (this is only limited by Network constraints)

2.3.8 Interface Redundancy

A number of Interfaces can have multiple instances running to achieve Redundancy

- REST (is run on all PUs)
- MQTT (multiple instances can be set up)
- OPC-UA (multiple instances can be set up)

Majority of other Interfaces can be moved to another PU via the System Install Scheduler.

2.3.9 Power Supply Redundancy

The PU has dual power supply as standard

A UPS is recommended in the event of power outages.

2.3.10 Network Redundancy

Manually configured - Bonded ethernet on the PU. Please contact your Luna representative for further details.

2.3.11 PU disconnected from the Network

Live Alerts will still be created, but will not be shared until PU is back on the Network

2.4 Operating Systems

- PU — Bespoke (read-only) version of Oracle 9, 64-bit Linux
- CU — Windows 11 (pro), 64-bit

3. Outline Major OS6 Features

OS6 consists of a range of processing and hardware implementations which incorporate various analysis modules and detectors supported by a range of software elements. The system is used by a wide range of customers and can be adapted to suit many requirements.

3.1 OS6 Detectors

OS6 has a suite of algorithms to detect, classify and locate a variety of events.

OS6 can be used for several scenarios, including:

- Pipeline Monitoring – Third Party Intrusion, Leak Detection and Pig Tracking
- Borders / Perimeters – Third Party Intrusion
- Power Cable Monitoring
- Road Monitoring – Traffic Flow, Congestion and Incident Detection, Vehicle Counting
- Railways – Train Tracking, Third Party Intrusion and Environmental Monitoring
- Each detector is licensed, and the system is flexible to allow additional detectors to be added later if required.

3.1.1 Detector Techniques

OS6 Detectors use various techniques to aid Detection of Activities. This includes:

- Self-adaption procedures to optimize sensitivity on every point along the fiber by 'learning' from the local environmental / seasonal conditions reducing Operator tuning
- Detector(s) developed using Machine Learning are supported in OS6

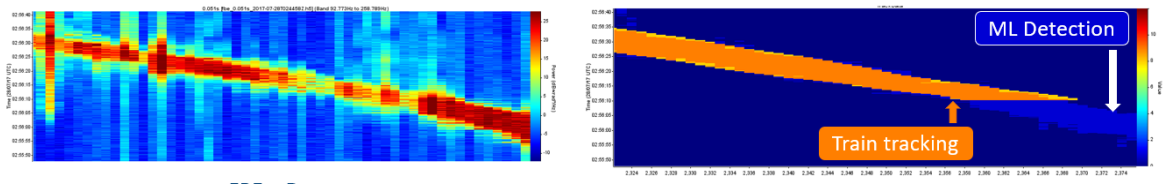


Figure 3 - ML Train Detector

3.2 OS6 GUI

3.2.1 Integrated Display

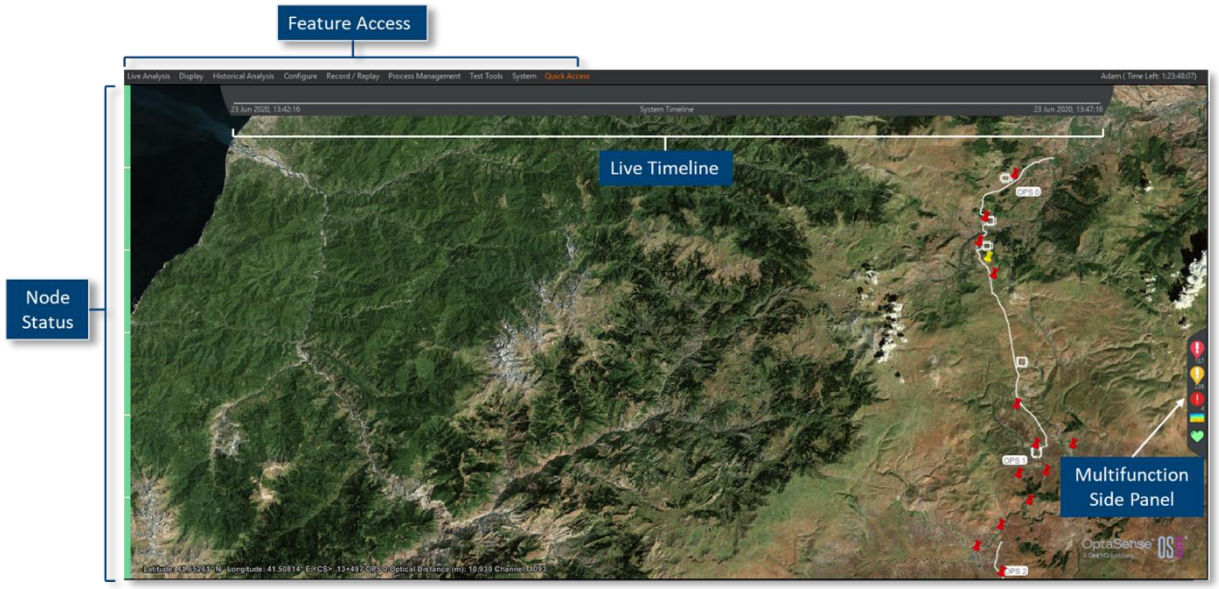


Figure 4 - OS6 Main Screen

OS6 features an integrated (thin client) GUI with the focus of the user being placed firmly on alerts in the context of their asset.

Separate displays can all be easily launched as needed from the integrated GUI, but the focus and most of the work can all be executed from the main display.

Integrated display features:

- **Main Map** displaying the Fiber route and any Alerts that are created
    - Alerts are displayed at the correct location on the Map with the associated Alert icon
- **Graphical Timeline** illustrating the last few minutes of activity in terms of alerts and system changes
- **Multi-Function Side Panel** integrated into the main display hosts several key features, such as mini waterfall and alert table. A split display within the side panel offers further customization
- **Node Status** bar provides a simple overview of the overall system health.

The system will automatically remember each user's last activity and reload to the same state when they log in.

3.2.2 Live Data (Map/Waterfall)

Alerts appear on the map and the waterfall display at the time/location of the ‘event’ that generated the alert. Moving alerts will track across the map and waterfall displays.

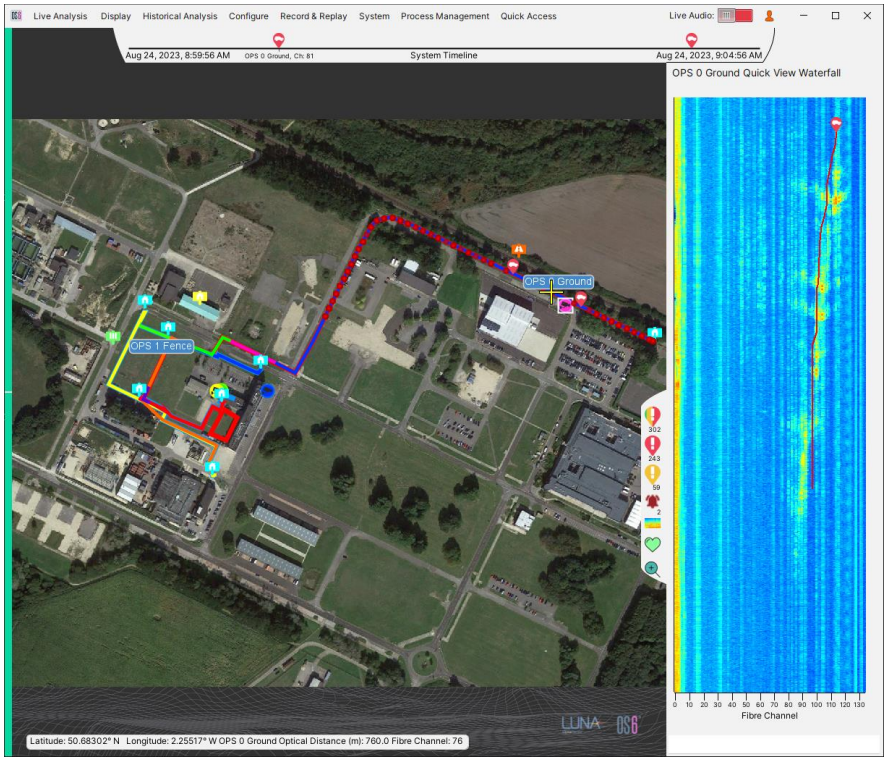


Figure 5 - Main Display

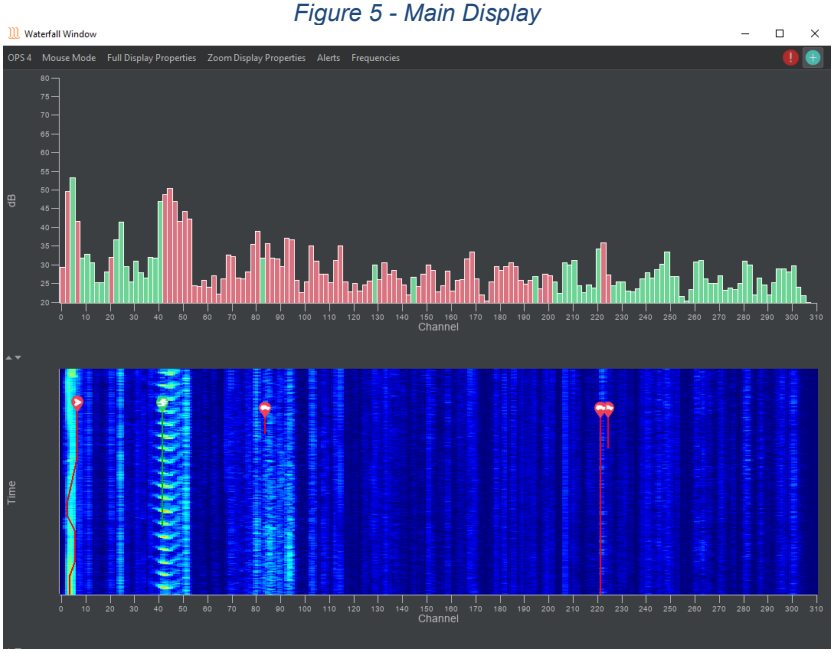


Figure 6 - Waterfall Display

3.2.3 Historical Alert Searching

Tools are available within OS6 to allow the user to search for and gain further information about individual alerts and associated historical data.

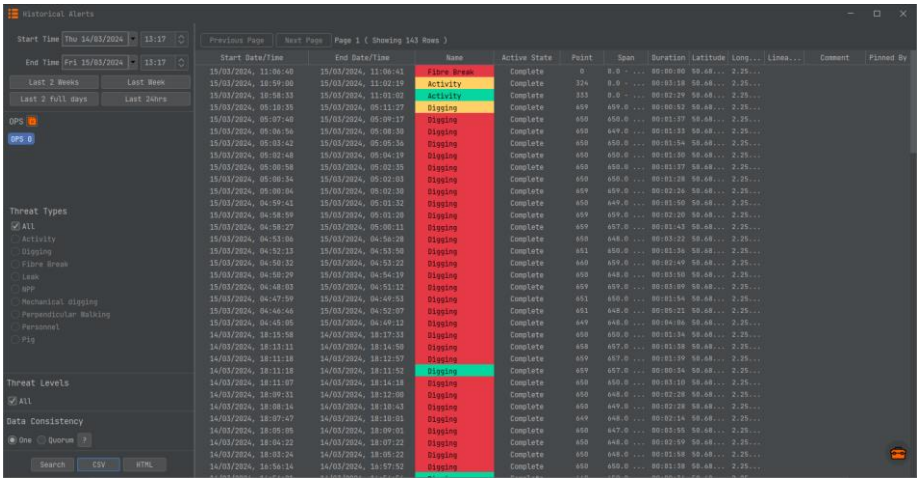


Figure 7 - Historical Alert Search

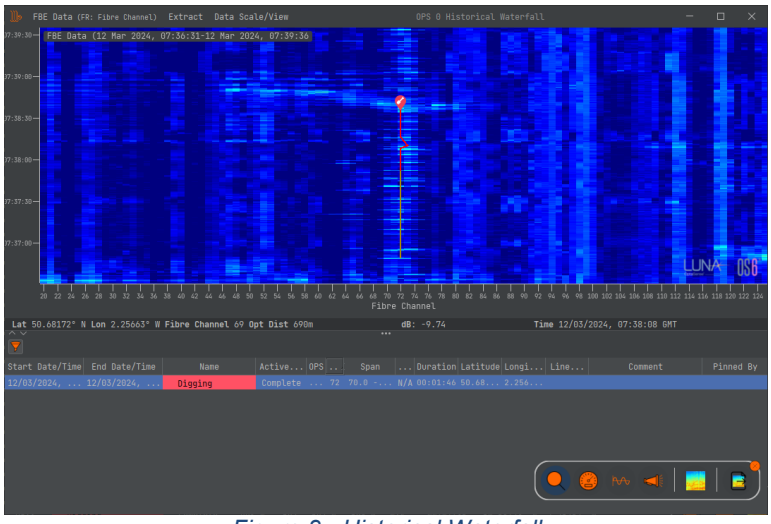


Figure 8 - Historical Waterfall

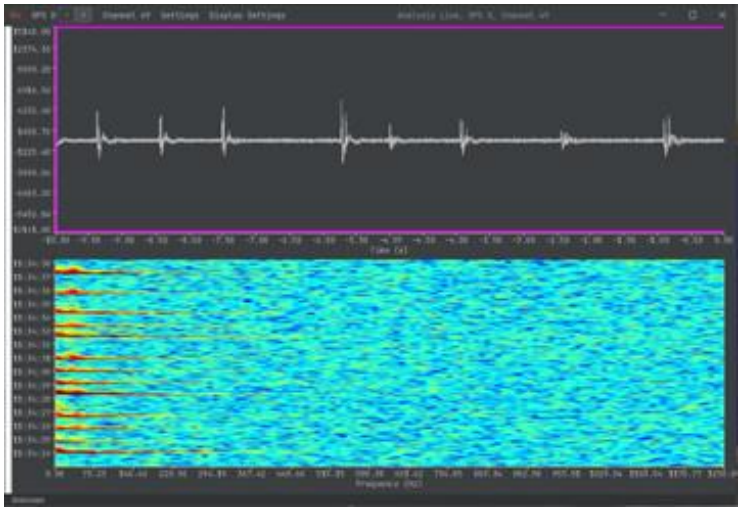


Figure 9 – Single Location (Point) Analysis

3.2.4 Extensive Auditing

Auditing activities can also be interrogated with detailed information supported on each entry.

OS6 offers 'System' auditing as well 'User' auditing against named accounts for forensic analysis purposes.

The auditing tool allows various search and export functions to aid forensic analysis. These include:

1. Detector changes
2. Area changes
3. Alert creation/updates
4. Alert Lifecycle changes (comments, Acknowledgement etc.)

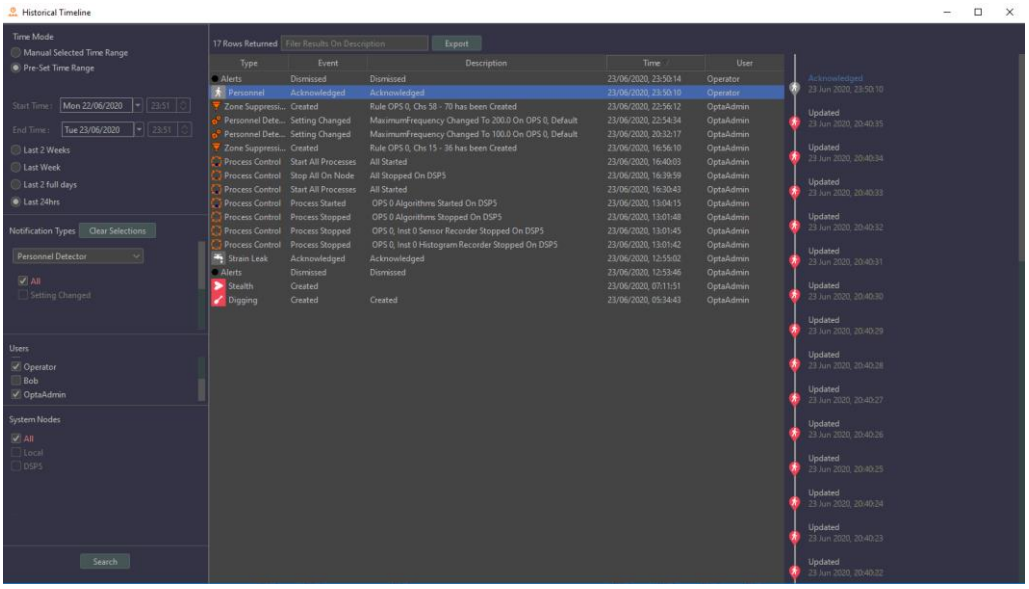


Figure 10 – Audits

3.2.5 Feature Search

The quickest way to access many features is to use the keyboard. Simply start typing the content you are looking for (e.g., waterfall) and the relevant options will pop up.

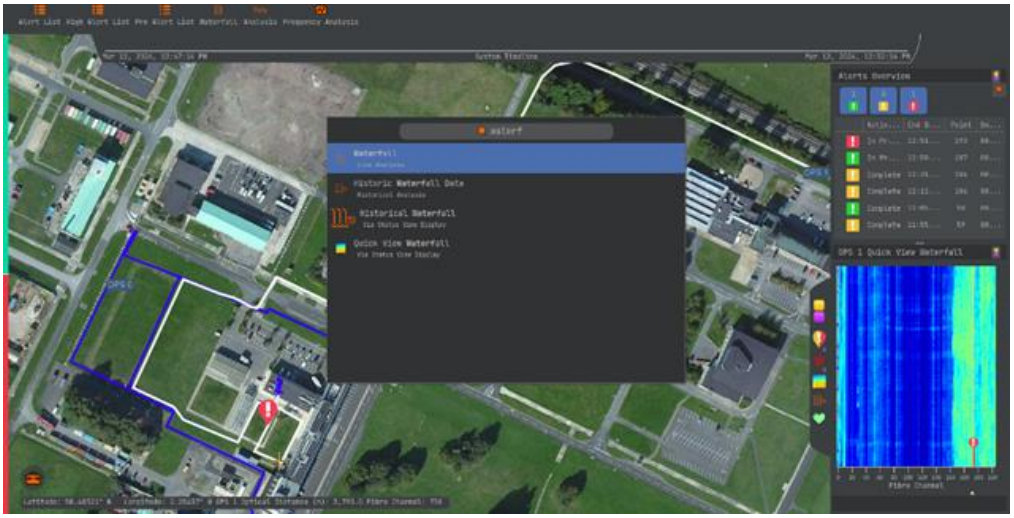


Figure 11 - Quick Search

3.2.6 System Health and Status Reporting

A suite of reporting and health tools are available in OS6:

1. Ability to view the health of all the major components that are part of the System.
   a. Software
   b. IUs
   c. Processing Servers
2. Ability to start/stop various components.
3. Ability to drill down to look at individual component's statuses (CPU loading/memory/temperature)
   a. Live & Historically
4. User Notifications are created when System is in an unhealthy state.
5. Ability to create custom reports in any area and have them exported in various formats.

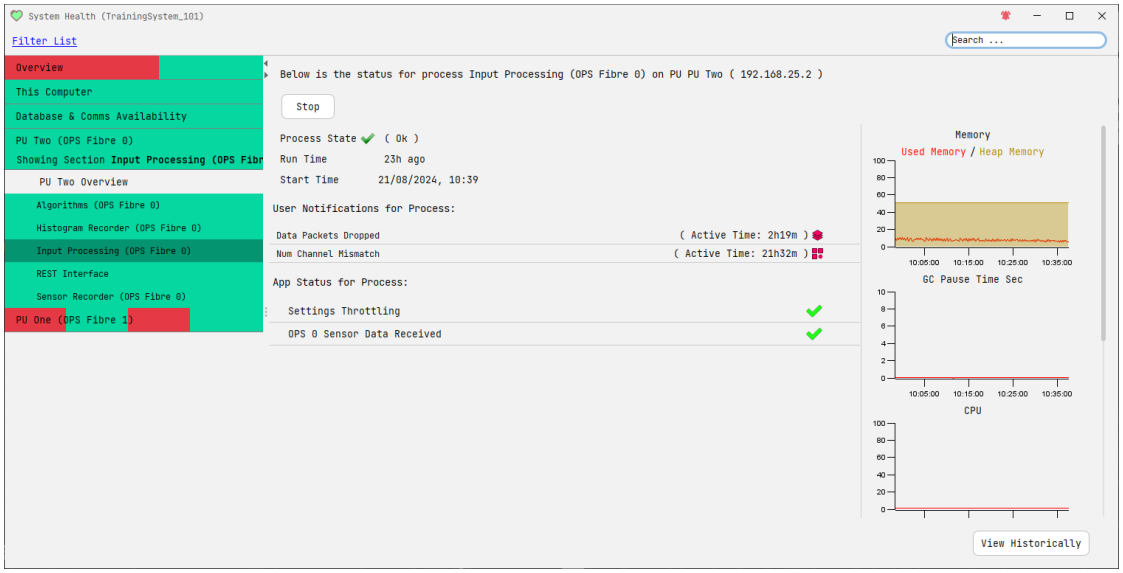


Figure 12 - System Health

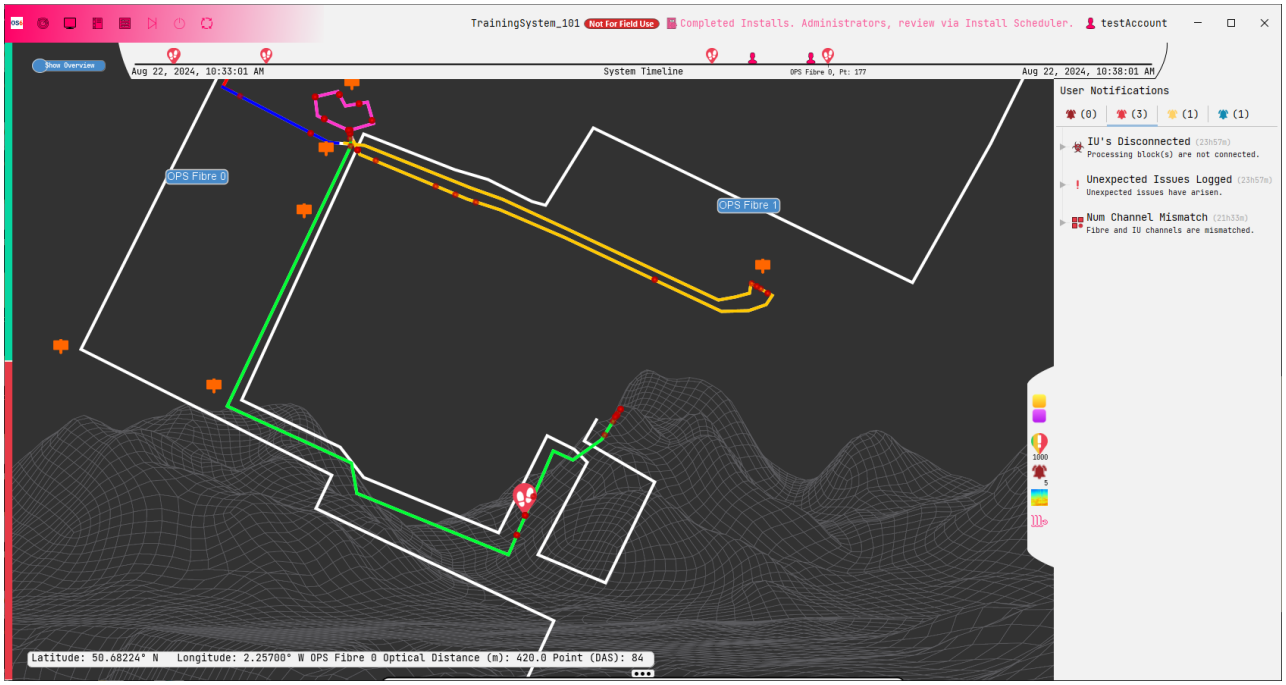


Figure 13 - User Notifications

3.2.7 Error Feedback and Support

The System provides a simple mechanism to generate a support ticket, which can be sent to the Luna support team.

3.3 User Setup

3.3.1 User Settings

Each user has their own display ‘settings’ such as default speed unit, waterfall color scaling.

3.3.2 Profile Management

Users can create a profile to open and arrange windows (and the content within) in a bespoke way. The system will remember the profile for each user and reload it on request. The last configuration will reload when a user logs in again.

3.3.3 Look and Feel

Users can choose from a range of themes for the software to change how the software looks.

3.4 Language Options

OS6 supports multiple language packs. Additional packs may be added as part of on-going development or as a bespoke client request.

4. System Components

4.1 ATLAS Interrogator Units (IU)

- Latest generation long-range quantitative IU
- Feature 1, 2 & 4 fiber options

Figure 14 – ATLAS

4.2 Legacy IUs

OS6 is compatible with certain Legacy IUs including OLA2.1+ & OLA2.2. For further information please consult your Luna representative.

4.3 Processing Unit (PU)

System processing is carried out on a Luna specified hardware running the OS6 software.

Figure 15 –Processing Unit (PU)

- A single PU is required to process ATLAS (time-series) data
- Each PU connects to a single ATLAS IU
- The PU receives, processes and stores ATLAS data
- The PU hosts the OS6 detectors
- By default, each PU hosts an instance of the distributed database.
  - The system provides flexibility over which nodes form part of the database cluster
  - System Configuration stored across all Database Nodes
  - Alert data stored across all Database Nodes
  - Audit data stored across all Database Nodes
- The PU incorporates large capacity rolling recorders which can be flexibly configured
  - Time-Series Acoustic data for analysis/replay/extraction
  - Processed data for historic visualization purposes
  - Detector specific rolling recorders
  - Separate manual recording disk storage
- The amount of data stored is configurable. The defaults are:
  - ~1 week of Time-Series data
  - ~3 months of Processed data

4.3.1 Virtualization

Virtualization of the PU is NOT recommended and is NOT supported. Virtualization would add a large level of uncertainty to the System. For further information, please consult with your Luna representative.

4.4 Control Unit (CU)

Figure 16 - All-In-One CU

OS6 requires at least one CU to configure the system. Once configured, the system can continue to operate in a 'headless' state with the CU powered off, if required.

OS6 employs a bespoke version of Windows 11 that has had redundant and unused features/drivers/applications removed.

The OS6 CU is normally provided with a second high-resolution monitor to provide more screen area for an operator to monitor the system with.

By default, the CU is available as a fully featured All-In-One PC, but it can also be delivered as a tower PC or rack-mountable unit if required.

4.5 Field Rack Option

The OS6 System (IU, PU, and CU) can be packaged into a field-ready, portable, ruggedized case. Detailed specifications are available by request.

4.6 Uninterruptible Power Supply (UPS)

It is highly recommended that UPS units are used to allow PUs and IUs to keep running for a specified time if the power supply is interrupted. This also reduces the risk of (system) files being corrupted due to unexpected power loss (which could result in parts of the system being in an unhealthy state).

The Eaton 5P 'managed' UPS is recommended

Figure 17 - Recommended UPS

Once power is interrupted, the UPS will use its built-in battery. If the battery reaches a pre-defined level, the UPS will perform a managed shutdown of the PUs and IUs, thus reducing the risk of file corruption.

The following network card is required: Network Card details to be installed in the UPS.

4.7 Ancillaries

4.7.1 Network Time Protocol (NTP)

As part of the OS6 system, an NTP time source is required.

Luna can provide a GPS unit for this purpose if customers do not already have one.

Figure 18 - NTP unit

4.7.2 Remote Power Cycling

An Ethernet Controlled Power Supply (ECPS) is included in the system ancillary pack to allow the power feeds to the Hardware to be remotely power cycled.

All processing hardware also supports IPMI (Intelligent Platform Management Interface), which offers an alternative network-based route to remote booting (and PU re-configuration). The IPMI requires an additional set of IP addresses. Both ECPS and IPMI are normally implemented.

Figure 19 - ECPS unit

4.7.3 Gigabit Ethernet

Figure 20 - Gigabit Ethernet Switch

For installations requiring a fiber optic network backbone, a GES with additional SFP modules is also available.

4.8 Termination Unit (TU)

A TU needs to be spliced onto the end of the sensing fiber to eliminate reflections from the end of the fiber. This is a preventative measure to protect the IU and to prevent detector saturation. The TU should be placed inside the patch panel.

Figure 21 - Termination Unit

5. Interfacing Options

OS6 supports a range of commonly used interfaces, each individually licensed.

5.1 MQTT Interface (Kalkitech SYNC 2000 Compatible)

OS6 has an MQTT Interface (Transport Layer Security is available). This Interface is compatible with the Kalkitech SYNC 2000. OS6 can send OS6 Alerts & OS6 Status to the Kalkitech SYNC 2000 (via this MQTT Interface).

Figure 22 – Kalkitech SYNC 2000

The Kalkitech Sync 2000 can convert to the following protocols:

- Modbus (slave)
- DNP3 (slave)
- OPC-UA (server)
- IEC61850 ed.2 (server)
- IEC60870-5-104 (slave)

5.2 REST Interface

The OS6 REST interface is a standardized way for external devices and systems to communicate directly with the system.

Our highly secure REST interface (Transport Layer Security is available) allows rapid integration with the system for visibility of data and alerts externally.

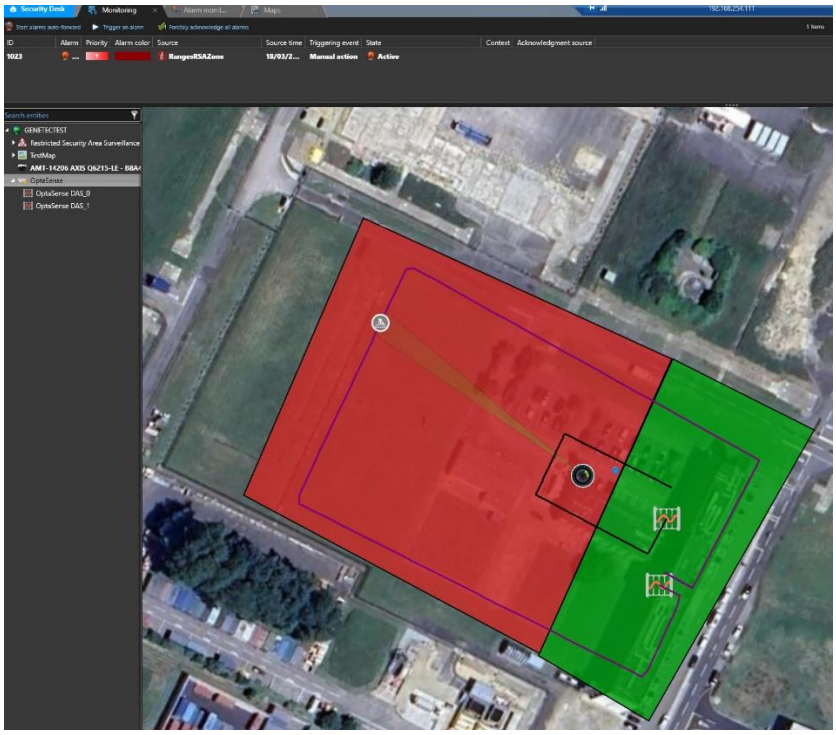
5.3 Camera Control & VMS Sub System

OS6 provides an interface to a Camera Control Subsystem to allow alerts to be transmitted to VMS systems.

5.3.1 Genetec Interface

OS6 has an official Genetec Certified Interface.

The OS6 IS Gateway driver has been developed by OptaSense and is integrated with the Genetec Security Center.



The OS6 IS Gateway driver allows:

1. OS6 Alerts to be forwarded directly into the Genetec Security Management Platform.
2. The Fibre route can be uploaded from OS6 and displayed on the Genetec Map
    a. This allows security operators to visualize events in the context with other Security Systems
3. Operators can dismiss OS6 alerts within Genetec once they have been reviewed
4. Users can configure whether Genetec intrusion acknowledgements are sent to OS6 as alert dismissals
5. OS6 also communicates OS6 **System Notifications and Warnings** to the Genetec Security Center
6. OS6 IS Gateway integration includes **configurable alert filtering capabilities**.
7. Users can select which OS6 alert types are forwarded to Genetec and define a **minimum alert level threshold** that events must meet before they are transmitted to the security platform.

5.3.2 Genetec Compatibility

Name	Version Number	Comments
Minimum OS6 Version	OS6.15	
OS6 Genetec Driver Version	1.0.2	
Genetec Security Centre Version	5.14.0	
Genetec RSA Plug-in Version	5.2.61	
Genetec IS Gateway Version	1.3.13	

5.3.3 Supported VMS Systems

Name	Version	Comments
Milestone X Protect Management Client 2018 R1	version 12.1a, Build 7115	
BVMS (Bosch)	build 10.0.1.375	using REST and Virtual Inputs

5.3.4 Supported Control Camera

An alternative to using a VMS is to have OS6 control cameras directly. This is most suited to small systems with only a few cameras and where a VMS is not actively being used by the operator. Cameras must be PTZ (pan-tilt-zoom) type, and the following specifications are supported:

Name	Version	Comments
ONVIF S	Version 1.1.1 March 2016	
Pelco	API Version 1.0	

Compliant video streams can be cued to display within the OS6 environment. H.264 over RTSP is the best tested video protocol, although other combinations should also work.

Figure 23 - OS6 Camera Display

5.3.5 3rd Party VMS Systems (NOT developed by Luna)

Additionally, some VMS software providers have created their own compatible interfaces by taking the HTTP output and reading it themselves. These Interfaces are not managed or supported by Luna, and as they are dependent on the now deprecated HTTP Interface, they are not available to new customers.

It is highly recommended to contact the 3rd Party to confirm status of the support/compatibility:

- Wavestore version 5.48.745
    - This will require the provision of an add-on license from Wavestore
    - Please speak with a Wavestore representative before proceeding

5.4 SMS Integration

The OS6 SMS feature allows OS6 Alerts and/or System Errors to be sent to specific telephone numbers. This feature is delivered through an internet-connected CU, so at least one CU must have reliable internet access for SMS notifications to be transmitted.

This new approach resolves many potential issues when using a Modem/SIM card; local mobile network coverage, signal strength, network availability, roaming agreements, and selected SIM plan (with some SIM tariffs blocking SMS, limit message volumes, restrict international destinations, or require specific APN or roaming settings).

5.5 Email Integration

The OS6 Email feature allows OS6 Alerts and/or System Errors to be sent to configured email accounts. This feature is delivered through an internet-connected CU, so at least one CU must have reliable internet access for email notifications to be transmitted.

5.6 OPC-UA Specification

OS6 can output OPC-UA messages to allow connection of system outputs to OPC compliant SCADA / DCS systems.

5.7 Dry Contact Integration

OS6 can be configured to trigger “dry contact” relays that can be used to trigger inputs on other connected alarm reporting systems. For example, when an OS6 Alert is raised, it can be used to trigger external alarms systems, control systems, public address systems, etc., subject to client requirements.

Dry contact alert outputs can be configured for OS6 Alerts, and a separate relay output can be activated for OS6 System errors. A wide degree of segmentation of alert types and locations can be achieved by using dry contract device(s) – multiple units can be supported.

5.8 Charon4 (DTS) Interface

OS6 can receive DTS temperature data and events via Luna Charon4 Software. The DTS data/events make use of the large number of features available to DAS data, including:

- Historical Waterfall Displays
- Live Waterfall displays
- Rolling recorders

DTS events are converted into OS6 alarms, allowing users to interact with them in the same fashion as a DAS alarm.

The DTS events are also compatible with most of the OS6 Interfaces.

5.8.1 DAS + DTS Leak Detector

The OS6 Leak Detector can now accept both DAS & DTS Alerts as part of the Leak Fuser. This will improve the Probability of Detection as well as reducing Nuisance Alerts

Please speak to your Luna representative regarding compatibility

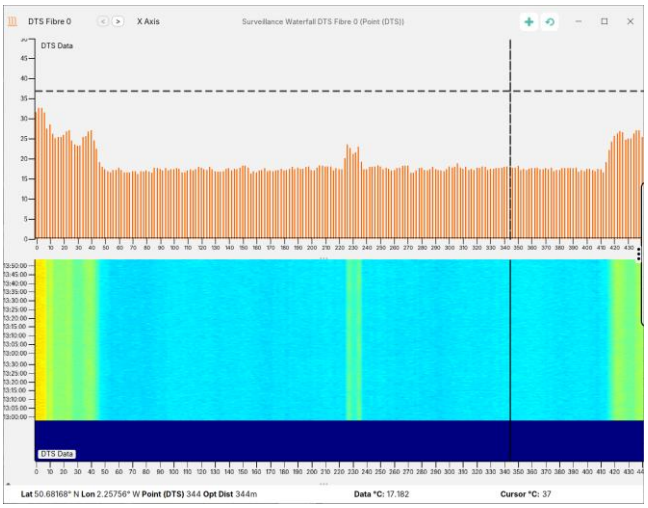


Figure 24 DTS Waterfall

6. Deprecated Interfacing Options (no longer available for new installations)

6.1 MODBUS Specification (no longer available to new customers)

The two OS6 MODBUS interfaces are being deprecated. These have been replaced by the OS6 MQTT Interface in conjunction with the Kalkitech Sync 2000.

These two MODBUS interfaces are not available to new customers. Existing customers should discuss an upgrade path with their Luna representative.

6.2 Published HTTP Specification (no longer available to new customers)

This interface is only available for existing customers who are upgrading from an older version of Software to OS6.

OS6 publishes an HTTP interface to allow 3rd parties to interface to OS6 to provide an output mechanism for alerts with full meta data, alert acknowledgment and dismissal, limited control and reporting as well as a duplex mechanism to inject alerts from external systems. An XSD schema document, full specification and developer's guide are available.

7. Security

7.1 Secure Product Development – IEC 62443-4-1

OS6 adopts the IEC 62443-4-1 standards for Software Development.

This addresses cybersecurity for operational technology in automation and control systems.

It is highly recommended that customers should always be on the latest version of the OS6 Software (as well as the latest associated Operating System) to ensure that any identified vulnerabilities have been resolved. Please contact your Luna representative for further details.

7.2 Software Source

- As part of the build process, the source code is obfuscated
- All OS6 executables have a Trusted publisher certificate
- A copy of each Software executable is securely held by Luna (for reference and backup)
- Each Software version has a unique identifier
    - OS6.X.Y
        - X – is classed as a Minor version update (normally new features, improvements, minor bug fixes)
        - Y – is classed as Critical release (normally major bug fix, where there is no work around)
    - Each increment of OS6 is normally compatible with previous versions
        - Any deviations from this will be described in the Release Notes (detailing how the update is dealt with)

7.3 Vulnerability Scans

- Regular Common Vulnerabilities & Exposures scans are performed using the latest versions of Software on in-house Test Systems
    - Subsequent Software (& Linux) updates are made available to all OS6 customers.
- Windows updates / scans for the CUs should be run by the customer to ensure that Windows version is up to date.

7.4 Users

- OS6 allows multiple user accounts.
- Administrators (Trained Users) are encouraged to only issue accounts with (unique) named users and not use “generic” logins as this circumvents the auditing process.

7.5 User Levels/Permissions

Different user access levels are offered:

User Level	Description
Light User	Read-only access with limited functionality
Standard User	Can acknowledge/dismiss alerts
Trained User	As per Standard user, with area editing and area suppression privileges
Super User	As per Trained user, but ability to modify the Detector & System Settings

7.6 User passwords

- Each user account requires a password
- Complexity rules are applied to all passwords
- Passwords are hashed and stored in the OS6 Database

7.7 Login Attempts

After a number of failed login attempts, the user is temporarily locked out of the System

7.8 Super User

Trained Users may login with Super User privileges via 2FA process. Super Users have advanced configuration access such as for the setup of detectors and to make system architecture changes. This privileged access times out after a number of days. Only Trained Users with Super User privileges can access this function to further enhance system security.

7.9 Installing/Upgrading Software

Only users with Super User privileges can perform an installation or upgrade of the System (Software and/or Linux Operating System)

7.10 (Distributed) Database Connection

Database connection is only possible with valid credentials

7.11 Data Replication (Distributed Database)

The Distributed Architecture replicates and shares data across all PUs. This provides redundancy for:

- System Configuration
- Alerts
- Audits

7.12 Config Backup (Automated)

There is also an automatic process that regularly backs up the configuration onto the CUs

7.13 Config Backup (Manual)

Users with the correct user level can manually export the configuration

7.14 Config Import

Users with the correct user level can manually import a (previously saved) configuration

7.15 Auditing

OS6 provides 'System' auditing as well 'User' auditing against named accounts for forensic analysis purposes.

Any change to the System is logged in the Database and can be reviewed using the OS6 Audit Tool.

7.16 Licensing

- A unique license file is generated for each OS6 installation
- A valid license file is required for an Operational System
- The license file is encrypted

7.16.1 CUs

- It is possible to set a limit to the number of CUs that can connect to the OS6 System

7.16.2 Detectors/Interfaces

- Each OS6 Detector and Interface require an entry in the license file for it to be enabled in the Software

7.17 Linux (Read-only)

- A bespoke (read-only) version of (Oracle 10) Linux is installed on each PU
- A valid username/password is required
    - It is highly recommended that the password is changed from the 'default'
    - Each PU can have a unique password
- Regular Common Vulnerabilities & Exposures scans are performed on the latest Linux version on the in-house Test Systems

7.18 End of Life Notifications

OS6 will display various Notifications regarding items such as 'End of Life' for Software & Operating System versions as well as any Deprecated features

7.19 Security Notices

If any critical vulnerabilities/issues are identified a Notification email will be created and sent to customers who have subscribed to our mailing list (scroll to the bottom of the page to sign up)

7.20Software bill of materials (SBOM)

A machine-readable SBOM (a detailed inventory of all the components that make up OS6 Software, including libraries, packages, and dependencies) is created for each release of Software.

8. Support Options

Luna has developed a specific customer-facing range of support options where support needs can be tailored. Options include:

1. Web-based support.
2. Dial up customer support line.
3. 24-hour engineering access
4. Replacement parts delivered anywhere in the world.

Our four global support centers cover a 24-hour time zone and are ready to ensure that your systems are kept working to the maximum effectiveness.
For more information, please head to the support pages on the internet

9. Contact Information

Contact our team of technical experts for further support and enquiries:

solutions@lunainc.com

Meadows Business Park
Building 3, Second Floor – Suite 1
Camberley, Surrey GU17 9AB
United Kingdom

www.lunainc.com