Lightning Sensor & Analyzer

User manual

- December 9, 2024 -
Valid from software release 2.0.11929

Contents

1 Introduction to the Lightning Sensor & Analyzer

1.1 The LSA at a glance

The Lightning Sensor & Analyzer (LSA) is a compact lightning detection system for wind turbines designed to detect and process lightning strike characteristics, including reporting on all Lightning Protection Level I thresholds, being Class I compliant across all metrics specified by IEC 61400-24/AMD1 ED2. This functionality is key to determine lightning damage risks, prolong equipment lifetime, as well as ensure timely equipment maintenance.

The LSA can be installed on any wind turbine by placing the sensor box on the exterior of the turbine tower, typically 1m above the door frame. A single IP67 Ethernet cable is used for power and communication.

The distinguishing features of the LSA include:

- Simple retrofit options on existing wind turbines
- Designed from the ground up with long term reliability as a key focus
- Highly accurate charge measurement, due to extremely low sensor noise floor
- Relay as well as multiple communication protocol support for interfacing
- Support for detection of which blade is struck by lightning
- Multiple plug-and-play cloud based data retrieval and configuration options

For documentation and software, visit the LSA support web site at http://jomitek.dk/en/support/lsa

1.2 First time quick start guide

1. Attach the LSA to a PoE enabled interface. A DHCP server is needed to assign an IP address to the sensor.
2. Determine the sensor IP address by looking into the DHCP servers client allocation table or by using the Jomitek Device Locator software which can be downloaded from http://jomitek.dk/en/downloads/tools/.
3. Access the graphical user interface through a web browser by navigating to the IP address of the sensor.

1.3 Interface options and requirements in brief

Using a single Ethernet connector for both communication and power supply, the sensor may be powered by either a Power over Ethernet (PoE) class 2 device or through 24V or 48V DC power supplied via the Ethernet cable. Power must be fed via an Uninterruptible Power Supply source, to ensure that lightning strikes affecting the external power supply will be recorded. When connected via Ethernet, it can be accessed through a graphical web interface, IEC 60870-5-104 protocol, FTP, WebDAV, or a Lua or Telnet client, e.g. Putty. Additional web service options can easily by tailored to suit SCADA needs, e.g. using JSON-queries to extract sensor status, lightning event lists, etc.. The sensors are preconfigured with functionality allowing the sensor to push information to a web or InfluxDB server, see Section 8.

Using an optional separately sold Power and Interface Box (PIB), basic relay-type interfacing is supported, also providing backwards compatibility to the Classic Lightning Sensor system offered by Jomitek. The PIB provides multiple power redundancy options, including an integrated battery, visual display of active lightning alarm, alarm test, clearing of alarms, and an alarm relay output similar in functionality to that of the Classic system.

The LSA may be ordered with either an M12 connector, or an RJ45 connector as the physical interface for the Ethernet cable. Jomitek recommends the M12 option for future design-in work.

1.4 Cyber security in general

The Lightning Sensor & Analyzer (LSA) uses Ethernet for communication. The sensor is an open device for most of the protocols available. The communication is generally not encrypted. For these reasons it is strongly recommended to use a firewall or similar measures, to protect critical parts of the turbine Ethernet network. See additional cyber security options described in section 6.3.

2 System installation & maintenance

The typical installation of the LSA is simple and requires no calibration. It is attached directly to the outside of the wind turbine tower with permanent magnets ensuring a strong adhesion to the tower. Do ensure that the tower surface is clean before attaching the sensor. Mount a grounding wire to the grounding bolt, if required by the wind turbine vendor, and finally connect the Ethernet cable. Proper grounding may also be obtained using the optional mounting bracket and cable conduit installation kit detailed in section 2.3.

Note that the Ethernet interface on the LSA must be sealed at all times, either by a termination/blind plug, or by the matched IP67 Ethernet cable included with the sensor. By default, the LSA will be delivered with 4x permanent magnets fitted to the sensor using M6 mounting points, providing a good fit to circular structures with a diameter in the 5-10m range.

Another mounting option is to use the same M6 mounting points to fix the sensor box in place using M6 bolts - note that these bolts must be A2 or A4 class stainless steel. This option is important if the mounting place does not feature a magnetic surface, e.g. if it is a concrete tower.

When using the magnet mounting option, it is recommended to add an adhesive sealant around the magnet pad perimeter. This will guarantee a long term fixed placement. A suggestion for an appropriate sealant is the Sikaflex 291i, typically in the white variant, or a sealant with similar properties. The particular sealant used must be verified with the vendor of the wind turbine.

To ensure measurement accuracy in post-processing, the system must be configured before use. Read about configuring the sensor in section 2.4.

2.1 Installation considerations

The Lightning Sensor & Analyzer measures the magnetic field generated by the lightning current running through the wind turbine tower when struck by a lightning. For proper sensor performance, it is important to minimize magnetic disturbances close to the sensor. In general, this means that iron and other ferromagnetic materials extending or nearby the tower surface should be avoided within 20 cm of the sensor box in the vertical direction, and at least 100 cm in the horizontal direction along the tower surface. The tower cylinder itself is not a concern in this regard.

Ideally, the point of installation for the LSA is 0.5-1m above the door frame, in the case where cable entry is targeted via the door frame. As an alternative, catering for avoidance of ladders, scaffolding or similar during installation, the sensor may be installed at a vertical level overlapping with the door frame, however no closer than 60° from the center of the door. This separation corresponds to at least 0.5 times the tower diameter, measured along the circumference of the tower.

A lightning current may be led through a lightning down conductor inside the wind turbine, placed away from the center axis of the tower, see figure 1. In this case the current peak measurement will only be within the specified measurement accuracy if the LSA is placed in the indicated range, i.e. 45-55 degrees away from the line that can be drawn from the center of the tower out through the lightning down conductor. This translates to 0.44 times

the tower diameter. As an example, for a tower with a 6 meter diameter at the height of the sensor installation, this leads to a proper installation point being 2.64 meter either to one or the other side along the perimeter of the wind turbine tower, measured from the point of the tower surface closest to the lightning down conductor. Note, only 1 sensor is needed per tower - but due to tower geometry there are 2 valid options for installation points. It is suggested to use the one closest to the cable entry into the wind turbine.

The Ethernet cable for the LSA will often be routed from the inside of the turbine, to the outside position of the LSA. The cable may be subject to inductance phenomena, due to lightning strikes, leading to excessive voltage levels. The LSA is hardened against overvoltage events, however the following precautions should still be taken:

- If the Ethernet cable is coiled up at any point, fix the coil horizontally, i.e. as if placed laying on a table.
- In support of the previous point, to the extent possible, avoid using an Ethernet cable longer than is needed.
- Avoid routing the Ethernet cable vertically or coiled up in the immediate vicinity of the lightning down conductor inside the tower, i.e. at least with 1m separation.

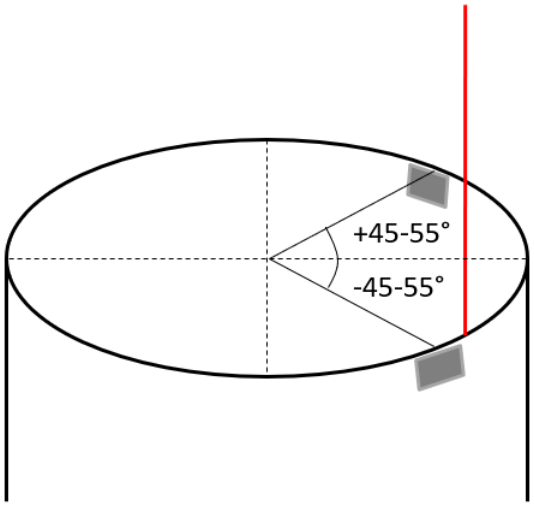


Figure 1: Cross section of a wind turbine tower, indicating proper placement of the LSA , with respect to an off-center internal lightning down conductor

In particular for retrofit installations where sensor connectivity is established using e.g. a cellular modem, the only external dependency for the sensor system is the power supply. The power cable shape and size as well as no need for a pre-fitted terminating connector, will allow for a considerably more flexible range of installation options, see section 2.3.3 for further examples in this regard. Note that the cable routing precautions mentioned for the Ethernet cable applies similarly to a power cable in the retrofit installation case.

2.2 Power supply and Relay Option

The LSA is powered by Power over Ethernet (IEEE 802.3). The PoE standard specifies two options for selection of wire-pairs with the LSA supporting both options, refer to figure (3) for details. The LSA is characterized as a Class 2 device, drawing power in the range 3.84W-6.49W. Note that the PoE supply must be tested to remain active (supply power) down to 1W power consumption, or be set manually active to ensure sustained PoE. This includes use of PoE injectors.

If the installation does not offer a PoE power supply, an external 24/48VDC supply may be used. This supply has to enter through the Ethernet cable. A special splitter cable making use of the mode B pins 4/5 (DC+) and pins 7/8 (DC-) can be ordered from Jomitek. However, in case of the use of a DC power supply it is recommended to use the Jomitek Power and Interface Box, which will also ensure proper conditioning and isolation of the power input to the LSA .

Note that the power supply for the LSA requires a minimum level of redundancy, ensuring supply for an absolute minimum of 2 minutes after a power failure of the mains supply of the wind turbine. If this criteria is not met, a lightning strike which interrupts the mains supply of the wind turbine will not be recorded, leaving the LSA ineffective. The Jomitek PIB supports the required Uninterruptible Power Supply (UPS) need. It may alternatively be met using a third party UPS / battery bank. For battery dimensioning purposes, note that while the LSA is configured as a Class 2 device, the average power consumption will be less than 2W.

The LSA may be ordered having a relay output for presenting alarms. The relay option uses 2 of the wires, pin 5 and pin 8. In this situation the sensor can get power from either the signal wires (1+2 and 3+6) or the direct wire (pin 4 and pin 7). The power wires used depends on the PoE switch used, whether it uses mode A or mode B. This implies that a special wire splitter is needed in case of relay output and use of a mode B PoE supply. By using the Jomitek Power and Interface Box, interfacing to the relay wires is simplified during installation, and this is the recommended approach. Please observe that the relay output is closed during normal operation. This means that if the interface cable is broken or disconnected, the receiving device (Jomitek PIB or other interface) will see this as a lightning alarm.

The power supply circuit is electrically isolated from the sensor electronics by a 1500V isolating transformer, and is also otherwise EMC hardened using best industry practices.

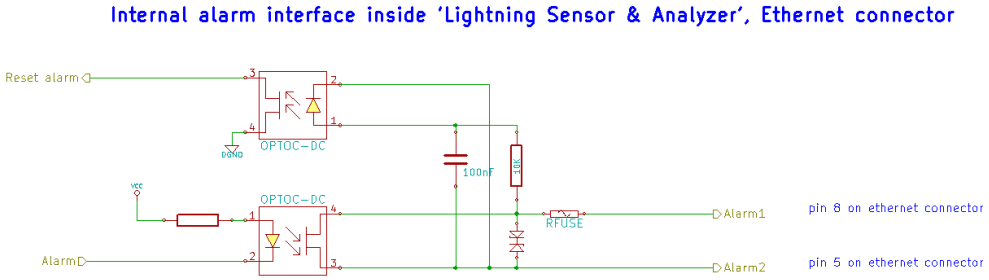


Figure 2: LSA Alarm Interface via Ethernet cable

802.3af Standards A and B from the power sourcing equipment perspective

Pins at switch	T568A color	T568B color	10/100 mode B, DC on spares		10/100 mode A, mixed DC & data		1000 (1 gigabit) mode B, DC & bi-data		1000 (1 gigabit) mode A, DC & bi-data	
Pin 1	White/green stripe	White/orange stripe	Rx +		Rx +	DC +	TxRx A +		TxRx A +	DC +
Pin 2	Green solid	Orange solid	Rx –		Rx –	DC +	TxRx A –		TxRx A –	DC +
Pin 3	White/orange stripe	White/green stripe	Tx +		Tx +	DC –	TxRx B +		TxRx B +	DC –
Pin 4	Blue solid	Blue solid		DC +	Unused		TxRx C +	DC +	TxRx C +	
Pin 5	White/blue stripe	White/blue stripe		DC +	Unused		TxRx C –	DC +	TxRx C –	
Pin 6	Orange solid	Green solid	Tx –		Tx –	DC –	TxRx B –		TxRx B –	DC –
Pin 7	White/brown stripe	White/brown stripe		DC –	Unused		TxRx D +	DC –	TxRx D +	
Pin 8	Brown solid	Brown solid		DC –	Unused		TxRx D –	DC –	TxRx D –	

Figure 3: PoE IEEE802.3 Standards A and B. Image source: https://en.wikipedia.org/wiki/Power_over_Ethernet

2.3 Installation materials and practical installation guides

In support of easing the physical installation of the sensor system, the following installation materials and guidelines are provided. These are also meant to assist in making the correct ordering choices, as well as create awareness of turbine model specific restrictions which the installation must accommodate. The guide is presented in 3 sections, with an initial listing of relevant installation materials, followed by a step-by-step installation guide for an integrated solution (sensor communication terminated inside the turbine), and finally a step-by-step guide of a typical retrofit solution (communication via an external cellular modem).

The materials will be pre-assembled to the extent possible, when supplied by Jomitek.

2.3.1 Materials listing

Product ID	Product name	Description
J30000001001	LSA-RJ45	LSA sensor box with RJ45 connector, fitted with 4 magnets and connector blind plug
J30000001002	LSA-RJ45-RELAY	LSA sensor box with RJ45 connector, relay version (only mode B PoE support), fitted with 4 magnets and connector blind plug
J30000061003	LSA-M12	LSA sensor box with M12 connector, fitted with 4 magnets and connector blind plug
J30000062004	LSA-M12-RELAY	LSA sensor box with M12 connector, relay version (only mode B PoE support), fitted with 4 magnets and connector blind plug
J73000059001	LSA-BRACKET	LSA multipurpose installation bracket, fitted with 2 magnets and a 12mm pipe brace, delivered mounted on the LSA when it is part of the same order
J90000067070	SIKAFLEX-291I-WHITE	Sikaflex 291i, 70ml tube (Mini Unipack), white. Delivered in the same package as the LSA, when part of the same order
J30100019001	LSA-GENERATOR	LSA lightning test generator, incl. 1x pre-installed 9V battery
J30100030002	LSA-GENERATOR-REMOTE	LSA lightning test generator fitted to 2m extension rod, incl. 1x pre-installed 9V battery
J31000002001	LSA-PIB	Power and Interface Box, including integrated LSA UPS support (not suitable for cellular modem UPS)
J71000038003	C13-AC-POWER	Cable kit with IEC C13 connector at one end, open ended at the other, 1m length
J74000056030	M12-DC-POWER-RELAY	Cable kit with M12 connector at one end, open ended at the other, 3m length, can be used for PIB DC power in and/or alarm relay signal out
J71000064001	LSA-CABLE-CONDUIT	Standard cable conduit assembly, stainless steel, 5 magnets /w pipe braces, grounding clamp, 135cm vertical, 25cm flex hose, 50cm end pipe. Lengths can be customized
J73000036001	MAGNET-CABLE-TIE	Magnetic fixture for cables, including cable ties, 5 units
J70000048xxx	LSA-ETH-RJ45IP67-RJ45IP20	Cable with RJ45 IP67 connector at one end, RJ45 IP20 at the other. Replace product ID x's with length in decimeter. J70000048050 is a 5m cable.
J70000037xxx	LSA-ETH-RJ45IP67-RJ45IP67	Cable with RJ45 IP67 connector at both ends. Replace product ID x's with length in decimeter. J70000037050 is a 5m cable.
J70000060xxx	LSA-ETH-M12-RJ45IP20	Cable with LSA M12 connector at one end, RJ45 IP20 at the other. Replace product ID x's with length in decimeter. J70000060050 is a 5m cable.
J70000080xxx	LSA-ETH-M12-RJ45IP67	Cable with LSA M12 connector at one end, RJ45 IP67 at the other (Phoenix 1656990, VS-08-RJ45-5-Q/IP67). Replace product ID x's with length in decimeter. J70000080050 is a 5m cable.
J71000064xxx	LSA-ETH-M12-M12	Cable with LSA M12 connector at one end, M12 at the other (Phoenix 1543236, SACC-M12MS-8Q SH). Replace product ID x's with length in decimeter. J71000064050 is a 5m cable.
J91000058101	LSA-CELLULAR-MODEM	Mikrotik LTE-M / NB-IoT outdoor cellular modem, incl. GPS, fitted with 2 magnets, including customized script/configuration for LSA use
J75000063xxx	MODEM-DC-CABLE	2 wire cable for 24-48VDC to supply the Mikrotik modem. The modem then supplies power to the LSA. Replace product ID x's with length in decimeter

Table 1: LSA installation materials

2.3.2 Installation instructions for the LSA, using the turbine network

The instructions for an LSA installation, where communication is supported via existing turbine communication infrastructure, follow 3 typical use cases (or a combination of those) with varying degrees of integration; Relay-only, limited (local) Ethernet connectivity via MODBUS TCP or IEC-60870-5-104, or full Ethernet connectivity with the sensor.

This guide assume the need for Ethernet connectivity (i.e. support of limited or full Ethernet communication), and the availability of a UPS powering a PoE switch used for the direct connection to the LSA. Furthermore the guide will focus only on the physical installation requirements, assuming the software configuration of the sensor (see section 2.4 or section 7.2) has been done in advance, or will be performed remotely as part of the commissioning process.

It is recommended to execute the physical installation work in a single continuous process. With proper preparation and experience, the installation work as described in the following is estimated as a <2 hour on site task, all included.

In some cases the cable installation through the tower wall, e.g. via a Roxtec enclosure, may be a requirement as an initial installation step. In such scenarios, proper protection of the cable connectors is important. In support of this protection, the cable kit with M12 connectors on both ends will feature blind plugs ensuring IP67 is maintained until final connectivity is established.

The relevant Jomitek installation materials are listed in table 2.

WARNING: The LSA sensor box itself, the LSA-BRACKET, and the LSA-CABLE-CONDUIT contain strong permanent magnets. All relevant health and safety precautions should be considered by the responsible installation technician, including use of gloves, and avoiding getting anything trapped between the turbine tower surface and the magnets during application.

Product ID	Product name	Description
J30000061003	LSA-M12	LSA sensor box with M12 connector, fitted with 4 magnets and connector blind plug
J73000059001	LSA-BRACKET	LSA multipurpose installation bracket, fitted with 2 magnets and a 12mm pipe brace, delivered mounted on the LSA when it is part of the same order
J90000067070	SIKAFLEX-291I-WHITE	Sikaflex 291i, 70ml tube (Mini Unipack), white. Delivered in the same package as the LSA, when part of the same order
J71000064001	LSA-CABLE-CONDUIT	Standard cable conduit assembly, stainless steel, 5 magnets /w pipe braces, grounding clamp, 135cm vertical, 25cm flex hose, 50cm end pipe. Lengths can be customized
J70000060xxx	LSA-ETH-M12-RJ45IP20	Cable with LSA M12 connector at one end, RJ45 IP20 at the other. Replace product ID x's with length in decimeter. J70000060050 is a 5m cable.
J70000080xxx	LSA-ETH-M12-RJ45IP67	Cable with LSA M12 connector at one end, RJ45 IP67 at the other. Replace product ID x's with length in decimeter. J70000080050 is a 5m cable.
J71000064xxx	LSA-ETH-M12-M12	Cable with LSA M12 connector at one end, M12 at the other (Phoenix 1543236, SACC-M12MS-8Q SH). Replace product ID x's with length in decimeter. J71000064050 is a 5m cable.

Table 2: LSA typical installation materials for turbine integration

Ordering for the cable assembly should include the LSA-CABLE-CONDUIT, and only one of the three LSA-ETH-M12 options, according to the type of terminating connector targeted on the inside of the turbine.

The installation location is preplanned (ideally confirmed by Jomitek), according to the guidelines of section 2.1.

The LSA-CABLE-CONDUIT is shipped from factory with the selected choice and length of LSA-ETH-M12 cable prefitted, in the same packaging. The package in its default configuration consists of 50mm diameter grey PVC parts (normally used for plumbing), assembled into a 2.2m long sealed straight pipe. The parts include a flexible joint (at the point where the flexible hose is placed inside the package), which can be adjusted in the range 0-90°.

The flexible joint is meant to improve storage options on site, and the straight pipe packaging parts may be used for impact protection of the connectors in the case where installation is not completed in a continuous process.

The LSA box and LSA-BRACKET are joined from factory, and should remain so. The box, bracket and Sikaflex are shipped in the same container.

The installation steps for these materials are listed in the following. During all steps, handle materials with care.

1. Ensure a clean tower surface in the area targeted for application of the sensor, bracket and cable conduit magnets. Consider use of a whiteboard marker, to mark up the intended point of sensor box installation, pipe, etc..
2. Remove any tape used to secure the flexible PVC joint during transportation of the LSA-CABLE-CONDUIT. Open the PVC pipe at one end of the flexible joint. Extract the cable and pipe assembly from the packaging (note the magnets inside).
3. The M12 connector at the end of the long fixed pipe (the pipe meant to be vertical, see figure 5), is placed on the ground ready for mating with the LSA and bracket.
4. Extract the LSA and bracket assembly from its shipping container. Avoid magnetic materials nearby the now exposed magnets. Loosen both M5 hex bolts and remove them, including the pipe brace. Be careful not to loose these items.
5. Remove the blind plugs of the male external M12 LSA connector, as well as the female integrated connector.
6. Insert the M12 LSA connector through the rectangular bottom hole of the bracket, and place the pipe end as illustrated in figure 4. Apply the doublesided brace back to its original position (now including the pipe), and firmly fix both M5 hex bolts with a torque setting of 4 Nm. Verify a secure fit is obtained.
7. Place the LSA face down, magnets up, on a protected surface. The package container may be used if nothing else is available. Note the pin alignment and mating notch of the LSA connector vs. the external M12 connector. Only one orientation is correct. When mating the connectors correctly, they will sink in until the threads reach each other. Tighten the mating screw of the external connector, to establish the IP67 sealed connection. Tighten manually / by hand. For reference, about 4 full revolutions are required. Tighten until resistance is met, and no further movement is possible by hand.
8. Flip the LSA and bracket around again (magnets down). Adjust the 3 magnets running along the long pipe, such that they point up / away from the attachment plane of the LSA and bracket magnets, i.e. so they don't get in the way for the next step.
9. Hold the assembly by the bracket flaps, and lift it up in the mounting orientation, with the bracket and pipe facing down and the sensor box up. Steady the pipe to avoid strain on the double sided pipe brace. Tilt the top end of the LSA forward, such that it contacts the tower wall only at the top end of the top magnets. Move the assembly about until the targeted installation position is reached. It is important to ensure a level (horizontal) orientation, using e.g. the middle black strip of the LSA box as a reference. When in position, CAREFULLY lower the bracket towards the tower wall, until the magnets take hold. At the end, the assembly may attach quite forcefully, so ensure that nothing is stuck between the magnets and the tower wall.
10. Flip the three magnets of the long pipe into position, locking them to the tower one by one.
11. Adjust the two magnets of the short pipe magnets as required for the final fit, and flip them into position. It is assumed that the pipe is terminated inside a protective cover before the cable enters e.g. a Roxtec entryway to the inside of the tower.
12. In cases where grounding (earthing) is required, the cable conduit assembly, bracket and sensor box itself shares a galvanic connection. A grounding wire connected to the grounding clamp at the end of the bottom pipe will hereby ensure full and proper grounding of the entire sensor system, with no need for further cabling. Note that the galvanic connection will include the cable shield of the Ethernet cable. As such, it is important that grounding at the opposite end of the Ethernet cable shares the voltage potential used for the cable conduit grounding, or that it is actively chosen not to terminate the Ethernet shield ground at the opposite end.

13. Further routing of connector and cable at the opposite end of the LSA depends on specifics of the type of entryway and internal routing options. Note the comments regarding cable routing in section 2.1.
14. Once full physical connectivity is obtained, and the sensor is powered up, it is suggested to follow the steps detailed in section 2.6, or as a minimum verify sensor connectivity as part of a local Ethernet network diagnostic, via detection in a remote turbine operations center, or similar.
15. When connectivity has been confirmed, the installation can be fixed in place using the Sikaflex sealant around the accessible parts where the magnet edge meets the tower wall. Note the recommended application temperature of 10-40℃. See figure 6.

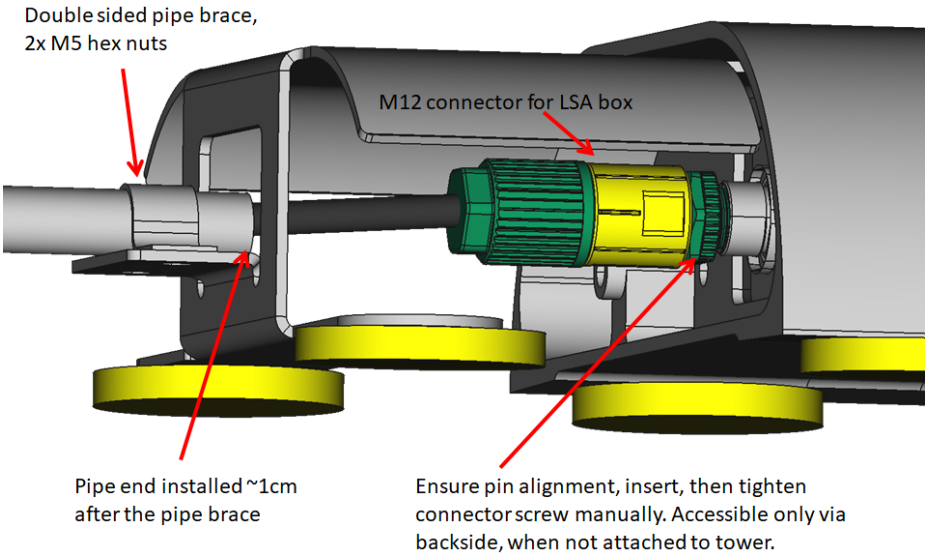


Figure 4: Side view of the cable conduit pipe fixed to the bracket pipe brace, with M12 connectors mated.

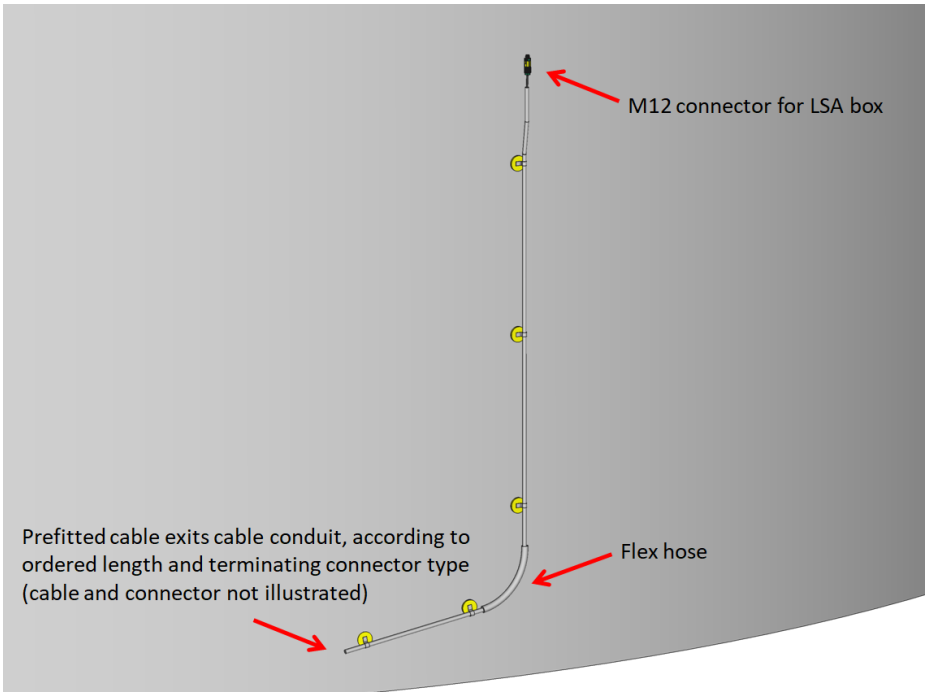


Figure 5: Example view of the cable conduit mounted on a tower wall. The top part is vertical, the bottom pipe tilts downward to drain out any water/moisture from the pipe. The LSA+bracket is not illustrated, but should be fitted before installation to the top part of the assembly.

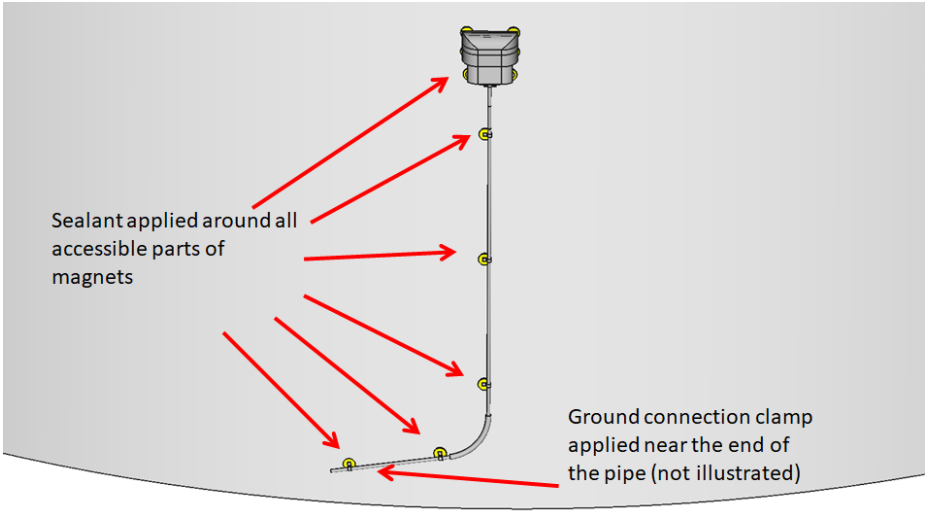


Figure 6: Example view of the cable conduit, LSA and bracket mounted on a tower wall. It is recommended to confirm full sensor connectivity before the assembly is locked in place with sealant. Note that all metallic parts of the assembly share a galvanic connection, which may be used for grounding (earthing) purposes.

2.3.3 Installation instructions for the LSA, using a cellular modem

The instructions for an LSA installation, using a cellular modem, assume use of the preconfigured outdoor modem offered by Jomitek. Use of other wireless backhaul solutions are possible, but will likely require additional engineering effort to obtain the robustness features offered by the Jomitek solution. Stability, security and low bandwidth use are key aspects of such a solution.

Prior to selection of a cellular modem as transmission backhaul for a retrofit LSA installation, it is important to verify the availability of a 4G network cell site near the intended location for installation (typically <5km away - possibly less depending on terrain). This includes determining the relevant provider(s) offering service, and that the service include NB-IoT or LTE-M support. The Jomitek modem supports both of these low bandwidth, extended coverage cellular services.

The cellular network coverage may as a first step be verified using coverage maps provided by the service provider, but should preferably include confirmation of the ability to set up a voice call using a regular handset on site. While NB-IoT or LTE-M enable coverage superior to that of a regular handset, the mentioned voice call test is a simple way to ensure that cellular coverage is sufficient.

In a future release, targeting Q1 2025, an option to verify cellular connectivity via the LSA web interface will be added.

Note that offshore wind turbine farms situated more than 5km from land will likely not have a cellular service available, except in cases where a cell site dedicated for the wind farm has been established. In such cases, it becomes even more important to determine the relevant provider, and support for NB-IoT or LTE-M, as it is likely to be a cell site offered via a single provider.

Especially in areas on the edge of cellular coverage, it is crucial to install the modem on the tower facing the direction of the nearest cell site. This is a practical consideration that must be taken into account in addition to relevant aspects of section 2.1.

This guide assume the availability of a UPS backed DC or PoE supply used for the direct connection to the cellular modem. Furthermore the guide will focus only on the physical installation requirements, assuming the software configuration of the modem and sensor (see section 2.4 or section 7.2) has been done in advance, or will be performed remotely as part of the commissioning process.

It is recommended to execute the physical installation work in a single continuous process. With proper preparation and experience, the installation work as described in the following is estimated as a <2 hour on site task, all included.

The relevant Jomitek installation materials are listed in table 3, assuming use of a DC supply to the cellular modem. As mentioned, an Ethernet cable may also be used to feed power to the cellular modem, however a cable with DC supply presents the greatest flexibility and ease of installation.

WARNING: The LSA sensor box itself, the LSA-BRACKET, the LSA-CABLE-CONDUIT, and the LSA-CELLULAR-MODEM contain strong permanent magnets. All relevant health and safety precautions should be considered by the responsible installation technician, including use of gloves, and avoiding getting anything trapped between the turbine tower surface and the magnets during application.

Product ID	Product name	Description
J30000061003	LSA-M12	LSA sensor box with M12 connector, fitted with 4 magnets and connector blind plug
J73000059001	LSA-BRACKET	LSA multipurpose installation bracket, fitted with 2 magnets and a 12mm pipe brace, delivered mounted on the LSA when it is part of the same order
J90000067070	SIKAFLEX-291I-WHITE	Sikaflex 291i, 70ml tube (Mini Unipack), white. Delivered in the same package as the LSA, when part of the same order
J71000064001	LSA-CABLE-CONDUIT	Standard cable conduit assembly, stainless steel, 5 magnets /w pipe braces, grounding clamp, 135cm vertical, 25cm flex hose, 50cm end pipe. Lengths can be customized
J73000036001	MAGNET-CABLE-TIE	Magnetic fixture for cables, including cable ties, 5 units
J70000060xxx	LSA-ETH-M12-RJ45IP20	Cable with LSA M12 connector at one end, RJ45 IP20 at the other. Replace product ID x's with length in decimeter. J70000060005 is a 0.5m cable, which is default for retrofit.
J91000058101	LSA-CELLULAR-MODEM	Mikrotik LTE-M / NB-IoT outdoor cellular modem, incl. GPS, fitted with 2 magnets, including customized script/configuration for LSA use
J75000063xxx	MODEM-DC-CABLE	2 wire cable for 24-48VDC to supply the Mikrotik modem. The modem then supplies power to the LSA. Replace product ID x's with length in decimeter

Table 3: LSA typical installation materials using a cellular modem

Ordering for the cable assembly may include the LSA-CABLE-CONDUIT for physical security and long term endurance. Especially for pilot projects or similar test campaigns, a more simple alternative approach using magnets fitted with cable ties, the MAGNET-CABLE-TIE, may be used to secure the power cable.

The installation location is preplanned (ideally confirmed by Jomitek), according to the guidelines of section 2.1.

The LSA box and LSA-BRACKET are joined from factory, and should remain so. The LSA box is prefitted with the LSA-ETH-M12-RJ45IP20 of the chosen length (default is 0.5m) connected with the LSA-CELLULAR-MODEM. The MODEM-DC-CABLE of the chosen length is prefitted in the LSA-CELLULAR-MODEM as well. This allows for all sealed cable connections to be prepared from factory, removing risk in the installation process.

The Sikaflex is shipped in the same container as the combined box, bracket, cellular modem, Ethernet cable and DC power cables.

The LSA-CABLE-CONDUIT is shipped from factory with no cabling. The package in its default configuration consists of 50mm diameter grey PVC parts (normally used for plumbing), assembled into a 2.2m long sealed straight pipe. The parts include a flexible joint (at the point where the flexible hose is placed inside the package), which can be adjusted in the range 0-90°.

The installation steps for these materials are listed in the following, assuming use of the LSA-CABLE-CONDUIT. It is straight forward to adapt the procedure for the alternative use of the MAGNET-CABLE-TIE option. During all steps, handle the materials with care.

1. Ensure a clean tower surface in the area targeted for application of the sensor, bracket, cellular modem and

cable conduit magnets. Consider use of a whiteboard marker, to mark up the intended point of sensor box installation, pipe, etc..

2. Extract the LSA and bracket assembly connected with the modem from its shipping container. Avoid magnetic materials nearby the now exposed magnets.
3. While avoiding strain on the Ethernet cable, place the LSA, bracket and modem assembly as planned for on the tower wall. This is most easily done by placing the modem on the tower wall first with one hand, while holding the LSA and bracket assembly with the other hand. Then, using both hands, tilt the top end of the LSA forward, such that it contacts the tower wall only at the top end of the top magnets. Move the assembly about until the targeted installation position is reached. It is important to ensure a level (horizontal) orientation, using e.g. the middle black strip of the LSA box as a reference. When in position, CAREFULLY lower the bracket towards the tower wall, until the magnets take hold. At the end, the assembly may attach quite forcefully, so ensure that nothing is stuck between the magnets and the tower wall.
4. Loosen both M5 hex bolts and remove them, including the pipe brace. Be careful not to loose these items.
5. Remove any tape used to secure the flexible PVC joint during transportation of the LSA-CABLE-CONDUIT. Open the PVC pipe at one end of the flexible joint. Extract the assembly from the packaging (note the magnets inside).
6. Starting with the cable end opposite to the modem, guide the DC cable through the cable conduit, inserting it into the long / vertical part of the conduit. Adjust the 3 magnets running along the long pipe of the conduit assembly, such that they point up / away from the attachment plane of the LSA and bracket magnets.
7. Pull the DC cable through until the top of the pipe is possible to fit with the double sided pipe brace. Install the pipe brace again with the M5 hex bolts, see figure 7. Firmly fix both M5 hex bolts with a torque setting of 4 Nm. Verify a secure fit is obtained.
8. Flip the three magnets of the long pipe into position, locking them to the tower one by one.
9. Adjust the two magnets of the short pipe magnets as required for the final fit, and flip them into position. It is assumed that the pipe is terminated inside a protective cover before the cable enters e.g. a Roxtec entryway to the inside of the tower.
10. In cases where grounding is required, the cable conduit assembly, bracket and sensor box itself shares a galvanic connection. A grounding wire connected to the grounding clamp at the end of the bottom pipe will hereby ensure full and proper grounding of the entire sensor system, with no need for further cabling.
11. Further routing of the power cable at the opposite end of the modem depends on specifics of the type of entryway and internal routing options. Note the comments regarding cable routing in section 2.1.
12. Once full physical connectivity is obtained, and the sensor is powered up, it is suggested to follow the steps detailed in section 2.6, or as a minimum verify sensor connectivity as part of a local WiFi network diagnostic, via detection in a remote turbine operations center, or similar. Note that the LSA web interface can be accessed using a WiFi hotspot hosted automatically by the modem, with SSID, password, IP address and port use as specified on the label of the modem. NOTE: After initial commissioning, it is strongly recommended to make use of the web interface security features, as detailed in the security paragraphs of section 6.3. If the sensor make use of Jomitek Cloud services, the relevant security measures will be applied remotely.
13. When connectivity has been confirmed, the installation can be fixed in place using the Sikaflex sealant around the accessible parts where the magnet edge meets the tower wall. Note the recommended application temperature of 10-40℃. See figure 8.

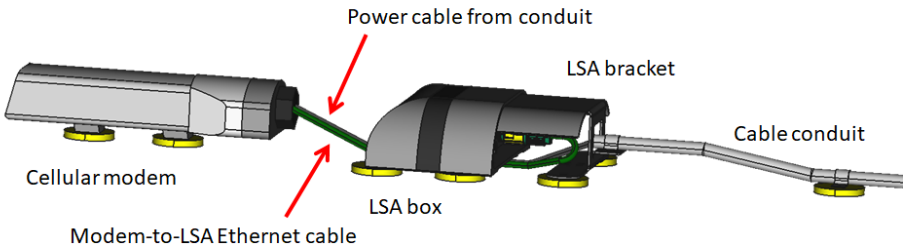


Figure 7: Side view of the modem, LSA, bracket and cable conduit. Note a single power cable via the conduit, and the Ethernet cable connectivity between modem and LSA.

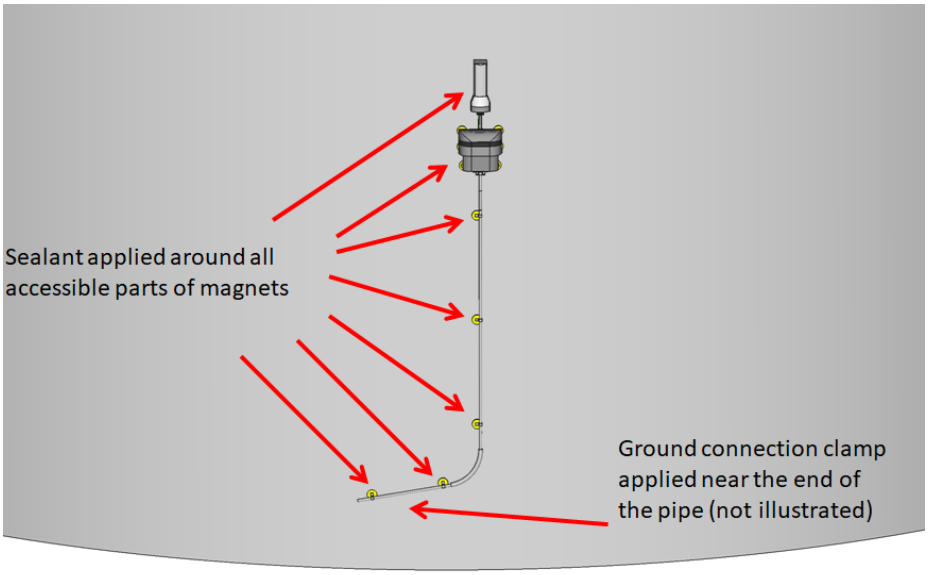


Figure 8: Example view of the cable conduit, LSA, bracket and cellular modem mounted on a tower wall in a retrofit configuration. It is recommended to confirm full sensor connectivity before the assembly is locked in place with sealant. Note that all metallic parts of the assembly share a galvanic connection, which may be used for grounding (earthing) purposes. An alternative retrofit solution would make use of a cable entryway via the tower door opening, which opens the option to simplify or entirely skip the cable conduit.

2.4 Scaling of measurements

To ensure correct scaling of the lightning current measurements, the wind turbine tower geometry must be configured. This is used as input for the post processing, which convert the measured magnetic field to an equivalent lightning current. The parameters to be configured for the structure can be found in the **tower** section, either via the web interface, or in the settings.conf file within the /conf folder using FTP or WebDAV. Note that **especially the tower radius is crucial to set correctly**, so the radius at the point of installation must be determined with diligence:

- height [m]: The height of the wind turbine tower from the tower base (ground or sea level) to the tip of the blade at its highest point during operation.
- sensor_mount_height [m]: The height of the sensor mounting point above ground or sea level.
- radius [m]: The radius of the wind turbine tower.

Additionally, as part of the **measurement** configuration, the following parameters can be adjusted to suit user requirements:

- trigger_level [kA]: The lightning current level used as threshold for triggering the alarm indication, and recording a lightning current time series, including post-processing. The default setting of 4kA is proposed as a reasonable trigger point, which will generally avoid detection of lightning leaders (the early build up phase of a lightning channel), in the cases where the lightning is never fully initiated.
- time_series_length [ms]: The length of the lightning current time series to record specified in milliseconds. It can be specified from 100 to 1000 milliseconds. It is recommended to keep the default setting of 1000ms.

The entity responsible for servicing the turbine may insert service alarm levels (**service_alarm_levels**), to indicate at which level of lightning strike severity a service visit should be triggered. These levels are not actively being used by the sensor post processing. They are intended as a way to indicate such service visit needs in addition to the levels defined as part of the Lightning Protection Level I severity rating of a lightning event. This collection of metrics is intended to support focused service visits, as well as halt of turbine electricity production, only when needed, and in this way lower the overall cost impact of lightning strikes.

2.5 Time synchronization for accurate event time stamps

While the LSA supports a basic time synchronization option, which updates the time of the LSA automatically whenever the web interface is opened, this option is primarily meant for initial setup and test purposes. Relying on this method, should the sensor lose power, the time stamp will not be correct afterwards.

To secure correct time stamps continually, the sensor must have access to an SNTP/NTP server. See section 6.3 for details on NTP server address configuration. In the web interface, the SNTP synchronization state will be clearly marked in the bottom right corner. A red light indicates no connection, while a green light confirm that synchronization via SNTP has been obtained. Note that immediately after rebooting or powering up the LSA , the SNTP indication will remain red for up to 30 seconds. Reload the web page in such case, to confirm that synchronization is obtained. Note that the synchronization state can also be determined based on MODBUS or IEC 104 readouts.

The sensor may operate without an SNTP synchronization source, however this will pose a significant risk of having untrustworthy time stamps of any lightning event recorded.

2.6 Full lightning sensor system test

As a final step during LSA installation, it is strongly recommended to conduct an end-to-end system test. This can be achieved using the Jomitek Lightning Pulse Generator, see figure (9).

The pulse generator is powered by a 9V battery. Always remember to bring a spare 9V battery and a screwdriver to exchange the battery. Remember to power off the device after use, to extend the battery life. If used with care, several hundred lightning discharges can be generated before the battery is drained.

The Lightning Pulse Generator features an On/Off button, LEDs indicating the charge state, and a red button which triggers a current pulse shaped like a standard lightning discharge.

Step-by-step instruction for triggering a lightning test pulse using the Jomitek Lightning Pulse Generator:

- Place the Lightning Pulse Generator centered and immediately above the LSA box, see figure (9)

- Turn it on using the On/Off button. A red LED will then be lit, and after a few seconds it will be replaced by a green LED, indicating that generator is fully charged.
- Perform the test by pressing the red button, which will release a current pulse similar to a lightning.
- Turn off the generator using the On/Off button again.
- Verify that the LSA recorded the pulse - depending on the configuration you may also verify if a physical relay was tripped, or if the wind turbine control was alerted using e.g. Modbus TCP or IEC-60870-5-104. Note that a lightning alarm will be triggered almost instantly, but the key parameter readout, as well as time series measurement will first be available after 2 minutes.

Figure 9: The Jomitek Lightning Pulse Generator must be placed centered and on top of the LSA box, to allow for correct detection of the test pulse.

2.7 Maintenance

The LSA is designed with a focus on very low maintenance requirements. The factory calibration applied lasts the lifetime of the sensor. As part of the continuous measurement flow being processed by the sensor, the sensor confirms the operational state of the internal measurement chain automatically. Should this confirmation fail, an error state warning is flagged e.g. via MODBUS or IEC 60870-5-104 (default address 1102).

The implication of this automatic check, is that scheduled maintenance visits, verifying the operational state of the LSA, can be avoided. This can be a significant factor, when considering the Total Cost of Ownership (TCO) of the sensor system.

3 Lightning strike detection and measurement

3.1 Theory of operation

A lightning striking a tall structure will cause an electrical current to run through the structure. For a wind turbine tower constructed from steel, this lightning current either use a lightning down conductor designed for the purpose, or it may find a way through the tower structure, as this is often the path of least resistance.

Electric current running in a conductor produces a magnetic field arranged in a circular pattern around the conductor. The LSA works by continuously measuring and monitoring the magnetic field strength at the surface of the wind turbine tower. If a lightning strikes the tower, the associated lightning current and magnetic field will be detected by the LSA which will trigger an alarm either via relevant Ethernet protocols, or via the Jomitek Power and Interface Box as a relay signal, and record a timeseries of the magnetic field which will be converted to an equivalent lightning current during post processing within the sensor.

Note that during a lightning event recording (maximum 2 consecutive measurements of 1 second duration each), the sensor enters a dedicated measurement state, which also means that the sensor will halt any Ethernet communication. I.e. if the sensor is being polled continuously e.g. using IEC-60870-5-104 or MODBUS, a pause in the data flow may be detected. To be clear, the sensor will respond to Ethernet communication during the post processing phase, but not during the actual time spent recording a lightning event.

3.2 Detection of which blade is hit by lightning

The LSA support detection of which blade is struck in 3 different ways with various pros and cons, as highlighted in the following:

1. Relay based
2. Based on MODBUS or IEC 60870-5-104 polling
3. Based on timestamp comparison

- Using a direct analog relay signal from the LSA , and interfacing this to the local turbine control, the turbine control logs the position of the blades at the time the lightning initiates (relay signal is raised within 1 milisecond of the rising edge of a lightning event), to determine which blade is pointing up towards the sky.
- Using the Ethernet connection, the turbine control is configured to poll the LSA on the alarm status using either MODBUS or IEC 60870-5-104, e.g. at an interval of 100ms, resulting in a detection accuracy <150ms, which is sufficient in all practical scenarios.
- Using the Ethernet connection, and based on a local NTP server providing time synchronization between the turbine control and the LSA , the lightning event time stamp is compared to a time stamped log from the wind turbine control, to determine which blade was struck. This method requires that the lightning event data processing is complete, and the time stamp comparison will therefore be delayed by up to 2 minutes (typically 30-40 seconds) from the time of the lightning event.

Using any of these options allow for detection of which blade - or blades, in the case of long duration lightning strikes - are struck. Such detection requires a one-time integration effort with the wind turbine control system, and can therefore be much more cost efficient than the cost of a dedicated sensor system mounted on each blade, including the higher installation cost of such sensors.

The rationale for blade detection - or lack thereof

As a general comment on blade detection, note that the value of such detection of lightning strikes lie mainly in cases with rare and powerful strikes, where it is reasonable to focus inspection efforts on the specific blade affected. This can likely reduce some of the inspection cost, compared to inspection of all 3 blades - though the main cost usually lies in getting on site.

In general, statistically speaking, the majority of cases will see a high likelihood of multiple minor-to-medium strikes on all blades, and it is either the aggregation of lightning events or a single powerful strike which prompts the need for on site inspection. In such cases, while blade specific detection is a nice-to-have, it is prudent to inspect all blades while on site. As such, there is little-to-no effective cost reduction tied to blade specific detection.

In addition, a lightning detection system dedicated to blade specific detection (i.e. one sensor per blade), beside the added cost and installation complexity of such sensors, often lack the fundamental ability to detect lightning strikes which partially or wholly avoid being directed through the blade lightning down conductors. Jomitek simulation estimates, based on real world charge influx measurements on wind turbines, suggests 10-15% of lightning strikes being partially or wholly conducted on the outside of the blade, or directly into the hub or nacelle structure. These cases are equally important to detect, and are supported by the measurement principle of the Jomitek LSA.

3.3 Key lightning parameter output

When the LSA detects a lightning current strength above the user configured threshold, a full lightning current time series is recorded at 1us resolution (1MHz). When the time series has been recorded in internal memory, the data is post processed and related parameters are calculated. The full time series data is converted from the recorded magnetic field strength to the equivalent lightning current and stored in a .wav formatted file. The lightning parameters are stored in a log file, alongside with all past lightning events. The post processed parameter readout include:

- Main stroke peak current [kA]
- Main stroke rise time [μs]
- Main stroke average steepness [kA/μs]
- Main stroke specific energy [kJ/Ohm]
- Subsequent stroke(s) maximum peak current [kA]
- Subsequent stroke(s) minimum rise time [μs]
- Subsequent stroke(s) maximum average steepness [kA/μs]
- Pulse count [#]
- Charge, flash [C]. The total charge delivered by the lightning.
- Charge, long [C]. The maximum charge of any lightning pulse lasting >2ms
- Charge, short [C]. The maximum charge of any lightning pulse lasting <=2ms
- LPL I severity [%]. Relative size of the parameter closest to exceeding LPL I thresholds.
- Inductive energy index [$\propto$J]
- Total specific energy [kJ/Ohm]
- Receptor mass loss [g]
- Polarity of the lightning pulse. Positive or negative.

Each recorded lightning strike has a timestamp adhering to the nearest $\pm 500\mu$s of the first sequence of three consecutive samples that crosses the user defined threshold in Settings $\Rightarrow$ lsa $\Rightarrow$ measurement $\Rightarrow$ trigger_level. The timestamp is expressed in both local time using the iso8601 format and in UTC time with a relative precision in nanoseconds. Note that the absolute precision of the sensors time stamp is limited by the time-server precision and the method used to synchronise the absolute time with the sensor, usually the absolute time precision is in the 50-100 milisecond range for NTP time synchronisation.

Note that the relative time precision can be used when comparing the time of two lightning events recorded by the same sensor.

- iso [YYYY $-$ MM $-$ DDThhmmss.sss $\pm$ hh : mm]. The local time of the strike in iso8601 format including time zone information
- sec[s]. The time expresses in elapsed seconds since January 1, 1970.
- nanoSec [s $\cdot$ 10^9]. The nanoseconds part of the timestamp.

Both the time series data and the key parameters can be viewed or downloaded directly from the web interface or by FTP/WebDAV transfer.

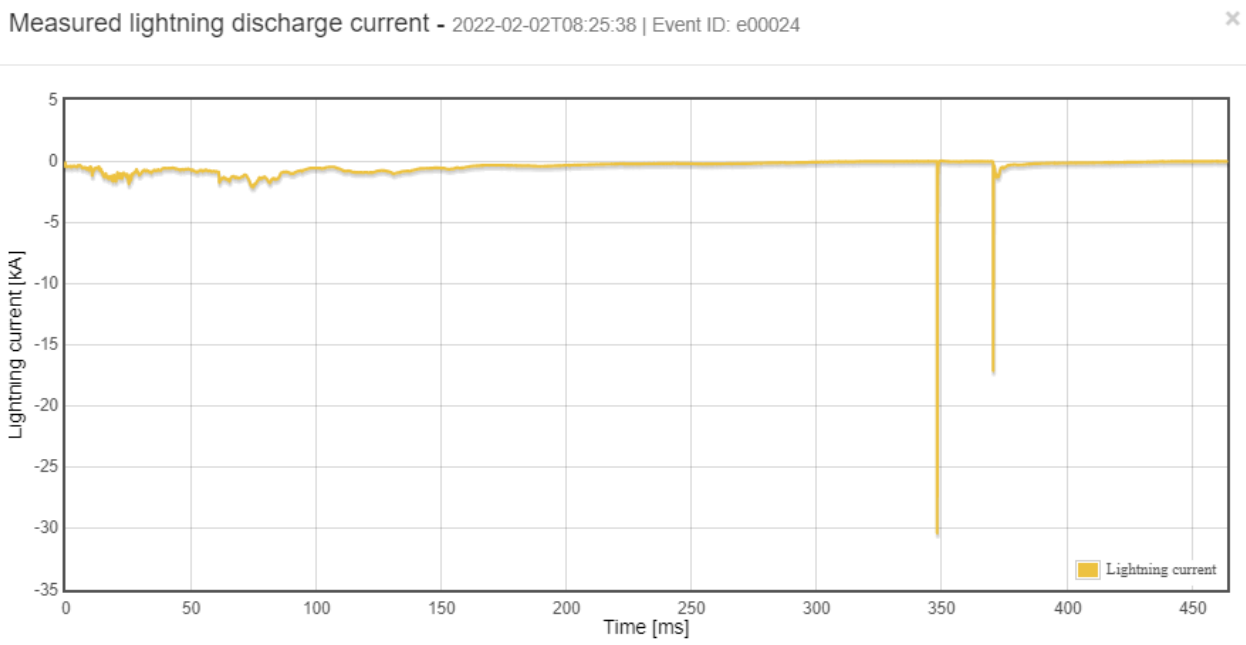
3.4 Receptor damage and replacement need

Based on the key lightning parameters, and as part of this the Jomitek sensor technology properties of a very low signal-to-noise ratio for time series measurements, an additional parameter is produced in the evaluation of a lightning event; Lightning receptor damage. See figure 10 as an example of this feature, in a case where no mass loss is expected.

With a number of base physical properties for stainless steel receptors, in terms of shape, size, heat capacity, melting point, eddy current phenomena etc., the sensor can produce a good estimate for the amount of receptor material which has disappeared due to a combination of resistive heating and atmospheric pressure during a lightning event. Importantly, the evaluation model reflects the fact that relatively 'small' lightning will have no measurable effect on receptor damage, which is a critical aspect of ensuring a good estimate.

The output of the receptor damage assessment is presented as removed mass from the receptors in gram. Customization of the model can be provided on request, in the case of non-standard lightning receptor layout, different metals, different output units or similar.

This output parameter presents the opportunity to lower wind turbine service costs, by avoiding or delaying scheduled receptor inspections, and instead target inspections for those wind turbines where significant receptor damage is detected based on LSA measurements.



Reset zoom | Full recording | Save full recording | Save visible recording

LPL I parameters	Measurement	LPL I limit
Peak current	-30.37kA	*±200kA*
Specific energy	26.7kJ/Ω	*10MJ/Ω*
Maximum peak current	-17.11kA	*±50kA*
Average steepness	-9.81kA/µs	*±200kA/µs*
Charge, flash	191.74C	*300 / 600C*
Charge, long	0.0C	*200C*
Charge, short	1.84C	*100C*

Additional parameters	Measurement	Service limit
Polarity of main stroke	Negative	-
Total specific energy	190.05kJ/Ω	*5000kJ/Ω*
Receptor mass loss	0.0g	-
Inductive energy index	∝3.78J	*∝5J*
Pulse count	2	-
Shortest rise time	3.09µs	-
LPL I severity	63.9	*100.0*

Figure 10: Example recording of a real world lightning event. The recording include a listing of the key lightning parameters, as well as the estimated loss of receptor mass caused by the event.

3.5 Lightning strike summary

While individual lightning strikes can be solely responsible for a given type of damage to occur, it is equally important to consider the damage incurred by multiple separate lightning events. The LSA provides a summary overview of past events based on (and including) *Settings->lsa->measurement->event_summary_start_number* up to and including the latest event. The event summary start number can be configured similar to other parameters hosted in the *settings.conf* file (see sections 6.3 and 7.2), as well as via the MODBUS protocol, see section 10).

The summary include the following list of parameters, where 'maximum' imply the highest (as an absolute value) entry across all events in scope, similarly the smallest entry for 'minimum', with 'sum' and 'count' being self explanatory.

- Maximum main peak current [kA]
- Maximum subsequent peak current [kA]
- Maximum main average steepness [kA/μs]
- Maximum subsequent average steepness [kA/μs]
- Maximum charge, flash [C]
- Maximum charge, long [C]
- Maximum charge, short [C]
- Maximum main specific energy [kJ/Ohm]
- Minimum main rise time [μs]
- Minimum subsequent rise time [μs]
- Sum charge, flash [C]
- Sum inductive energy index [$\propto$J]
- Sum total specific energy [kJ/Ohm]
- Sum pulse count [#]
- Sum receptor mass loss [g]
- Count negative main stroke polarity events [#]
- Count positive main stroke polarity events [#]

The parameters are meant to provide an easy option to assess if any LPL I metric was exceeded within the summary event scope, as well as provide primary metrics to assess the need for a maintenance visit based on the cumulative metrics. Following a service visit, an option would be to 'reset' the list, by updating the *event_summary_start_number* to the latest event + 1. Additional metrics can easily be added on request.

The summary will be updated based on either of the following trigger criteria.

- At the conclusion of a new event being recorded
- During reboot
- By writing to the event summary start number MODBUS register, see section 10

In the LSA web GUI, the summary parameters can be found in a user friendly format as part of the event page view, see figure 14.

4 Lightning parameter analysis

4.1 How to interpret the lightning parameter output

The core value of the LSA lie in the ability to assign responsibility for lightning related damage or faults, and to significantly optimize the operational costs associated with lightning strikes.

In relation to the question of responsibility, the cost of component failures are most often defined using IEC 61400-24, with the design criteria being the ability to withstand lightning strikes within Lightning Protection Level I limits. If a failure occurs, with LPL I limits exceeded, then the responsibility (cost) most often falls back to the owner of the turbine, whereas faults incurred below these limits are a subject to insurance claims and/or turbine vendor responsibility.

For the purpose of optimizing cost, consider the following aspects of a lightning detection system.

1. Avoidance of wind turbine component failure leading to a prolonged energy production halt
2. Avoidance of halting a wind turbine, when lightning detection is below concerning limits
3. One-off cost of the lightning sensor system itself, as well as for installation and integration
4. Maintenance cost of the lightning sensor system

Items 3 and 4 are addressed by the design principle and functionality of the LSA itself. Items 1 and 2 reflect a need to not only have reliable lightning detection, but also the ability to accurately differentiate between lightning levels of concern, and those that are not a concern. There are real world cases where a turbine on average is struck by lightning more than 10 separate days during a year, which is obviously unsustainable if site visits are triggered every time - in particular when the strikes are not necessarily of concern.

Unfortunately Jomitek has found that the IEC 61400-24 LPL I metrics are not presenting a reference frame easily translated to risk of wind turbine component failure or degradation. As such, additional parameters are introduced for this purpose. The following sections detail both the parameter output in relation to LPL I, as well as the added parameters which may be used to optimize the need for production halt and related service visits.

4.2 Reporting of parameters in relation to Lightning Protection Level I

IEC 61400-24 categorize parameters according to specific parts of a 'standardized' lightning discharge. However, real world lightning discharges exhibit properties which are not always directly translatable to these categories, introducing the need to clarify how real world events are mapped to the limits of Lightning Protection Level I.

First stroke vs. main stroke

Using figure 10 as a reference, a lightning strike event will often include an initial phase which may span several 100ms indicative of lightning leaders building up an ionized channel for more significant lightning discharges to conduct through later on. As part of this, there are some times minor discharge pulses with rise times in the 1-100us range included as part of the lightning leader phase. LPL I impose limits on the 'first stroke', with different limits and parameters for positive and negative strokes respectively.

Looking at the context of the term 'first stroke', it is evidently not meant to reflect lightning leader discharges. As such the LSA reporting use the term 'main stroke', defined as the discharge reaching the highest absolute peak current value within the time series recording of the lightning. The 'first stroke' limits are related to the LSA 'main stroke'. All other discharge pulses are treated as 'subsequent strokes', even though such a stroke may in some cases include a discharge pulse occurring before the main stroke.

Positive vs. negative stroke

As for the difference in parameters used when the first/main stroke is positive vs. negative, the LSA reports the specific energy and average steepness in both cases, and apply the same limits. The background for this is, that while a positive strike has the highest risk of a significant specific energy output, and the negative the highest risk of a high average steepness, these limiting factors are equally relevant for either stroke polarity.

Time parameters

While the rise time and time parameters in general are part of the LPL I limits, they are to be treated as defining for the pulse time characteristics for lab testing, and not a physically meaningful limit to be evaluated for real world lightning discharges. As such, the rise time is reported, but not used in active evaluation of the LPL I severity level. The physically limiting (damaging) factor in this context is the average steepness.

Charge

The topic of charge measurement and measurement frames is treated on a number of levels for LPL I, of which some are potentially overlapping. It is also the measure which has the highest risk of being exceeded, as long duration low current discharges, which can stack up to levels above the LPL I limits, are fairly common. While the charge of the individual first positive short stroke has a limit of 100C, this criteria is for the LSA being treated for any pulse with a duration <2ms, referred to as 'charge, short'. Any pulse with duration >2ms is treated with the limits of a long stroke, referred to as 'charge, long'. Finally, the charge of the recorded lightning event as a whole is reflected in 'charge, flash', using 300C as the reference limit. Note that this limit may also be set as 600C or higher, depending on the specifications agreed for a particular turbine / turbine model / contract.

Lightning Protection Level I severity

The Lightning Protection Level I parameters, as applied according to the description of the past paragraphs, are evaluated one by one against the limit in question for that parameter. The parameter with the highest relative value to the LPL I limit is used as the LPL I severity indication. The rationale for this parameter, is to present the severity of a lightning event as a single summarized value. In the example of figure 10 the LPL I severity ends up being defined by 'charge, flash' reaching 63.9% of the limiting value.

In summary, all relevant parameters for Lightning Protection Level I is presented as part of the LSA output.

4.3 Parameters supporting optimized need for site visits

The need for halting production and/or triggering a site inspection visit rely on an evaluation of the fundamental physical phenomena leading to component failure or degradation. Jomitek operate with 3 main metrics in this context.

1. Absolute peak current
2. Total specific energy (and related receptor mass loss)
3. Inductive energy index

Note that the charge is not included in this list, as it is presently not clear if specific types of lightning damage scale proportionally with the charge. Nonetheless, from an operational viewpoint the amount of charge must still be reacted upon, in relation to the Lightning Protection Limit I criteria.

Absolute peak current

Damage due to the peak current relate to the maximum force exerted on materials due to the Lorentz force, where a force proportional to the current is generated, and depending on the current path and layout of the turbine may

rip out, crush, or otherwise compromise the structure of conductors or supporting materials. Also associated with a high peak current, is a high voltage potential leading to arching phenomena, which may burn through materials, or make them brittle, increasing the risk of structural failure.

The nature of damage to look for is equivalent to applying hammer blows or a blow torch to the immediate surroundings of the conduction path, and therefore the state of the lightning down conductor and the blade around the receptors is of particular interest, with less visible areas of interest being the generator or transformer (depending on the turbine layout).

Total specific energy

The specific energy represents the charge squared, integrated over time, which has the unit of Joule per Ohm. In other words, it is a metric for energy dissipation related to a given impedance. The amount of resistive heating of the current path is proportional to the specific energy. The Lightning Protection Level I specification only mention specific energy in the context of the first positive stroke. However, the heat dissipated within a few 100ms is quite limited, and as such, in case of a multiple discharge event, a more meaningful metric is the specific energy of the full lightning discharge recording, i.e. the total specific energy. The total specific energy is used to determine the approximate amount of lightning receptor mass loss as described in section 3.4, which emperically is found to be the type of component seeing the greatest direct impact of the specific energy released during lightning events.

The nature of damage to look for is related to the state of the blade receptors in particular, where molten droplets may also have caused damage to the blade material in the immediate vicinity. Note that degradation is more likely to be caused by multiple lightning over time, than a single lightning event.

Inductive energy index

Lightning Protection Level I treat damage caused by inductive phenomena, as a consequence of the Electromotive force, in the form of the average steepness. Considering lightning events can include 10s of individual strokes, the average steepness as a metric for damage caused by induced energy can easily be off by an order of magnitude, comparing an otherwise similar average steepness of a single stroke lightning, to one with many strokes. As a consequence the LSA presents a more meaningful additional metric, which is the integration of abs(dI/dt) across the entire lightning event. It can be shown that this metric is proportional to the induced energy. The amount of this type of damage can vary widely across turbine models, as it is highly dependent on the placement and orientation of sensitive electronics nearby the conduction path.

The nature of damage to look for is related to low voltage electronic components failing or operating erratically. In particular components containing PCBs, which are otherwise considered well shielded from an EMC viewpoint, will still be subject to induced energy, as the magnetic field is not possible to effectively shield for, apart from distance and orientation with respect to the conduction path.

4.4 Time series event data

All time series data files recorded on the LSA are saved as WAV files (file extension .wav). The WAV file format is in itself a lossless and uncompressed format that holds time series meta data such as sampling frequency and sample bit depth as well as the time series measurements stored in a single file. To cater for low bandwidth scenarios the WAV files are furthermore compressed using Gzip, using the full file extension .wav.gz

Additional information describing the type of measurement, scaling, time stamp and similar is contained in the event .log file.

The format structure itself is simple and widely compatible with many software tools relevant for in depth analysis, e.g. Matlab and SciLab. Further information on the format can be found at https://en.wikipedia.org/wiki/WAV.

The web interface of the LSA includes a powerful way to graphically evaluate and analyse lightning recordings, independent of external tools. This option requires web access to the sensor in question.

5 Software and firmware structure

5.1 Microcontroller platform and RTOS

The Lightning Sensor & Analyzer features hardware tailored to meet the measurement capability and processing required to accurately report on any type of lightning discharge event, as well as the component resiliency required to withstand the harsh environment on the outside of an offshore wind turbine, for the lifetime of the turbine. In addition to the computational capabilities based on a custom RTOS (Real Time Operating System), the LSA feature a large onboard memory, designed for event logging during the entire lifetime of the sensor.

The firmware used in the microprocessor can be securely updated over the air using encrypted firmware images, enabling feature addition and improvements after installation.

The LSA firmware include the Lua scripting language which allows for a wide range of customization, including dynamic reconfiguration of the sensor on the fly. This enables easy interfacing to reports, event summaries, etc.. Requests for customization beyond the default capabilities are welcome.

5.2 File system

The LSA platform features storage of non-volatile data on an eMMC with integrated wear leveling. These data include software in the form of Lua scripts and web server content, as well as configuration files, time series recordings in the form of .wav files and other measurement data such as .log files. The eMMC is by default delivered with an 8GB size, which effectively will outlast the lifetime of the sensor and wind turbine. This is based on a lightning event usually consuming <1MB of storage space (automatically .gz compressed). In the unlikely event that the full memory allocation is consumed, the oldest time series data will be deleted, while the corresponding log files will remain, and in this way ensure that the key lightning parameters are retained.

- `/service` - The main folder containing user relevant data, accessible via FTP or WebDAV, see 12.2, 12.3.
- `/service/conf` - System configuration files.
- `/service/log` - Sensor log files.
- `/service/software_update` - Folder for uploading firmware and software updates.
- `/service/data` - Measurement data such as time series and event logs, stored in the /event subfolder.

6 Web interface

6.1 General structure

The web interface is structured around four main components as shown in figure 11, with the following description:

- The *tab menu* for navigating between sub pages.
- The *main content area* for displaying sub page content.
- The *page context menu* for interacting with the currently selected sub page. This menu may not be available on all sub pages.
- The *notification area* for displaying messages as feedback to user actions and input. Notifications will be queued, with the newest notification appearing at the top of the notification area. Notifications will automatically disappear after 20 seconds, or can be manually dismissed. The notification area displays the SNTP (time synchronization) status in the right hand side. A green light confirms synchronization, while a red indicate no synchronization obtained.

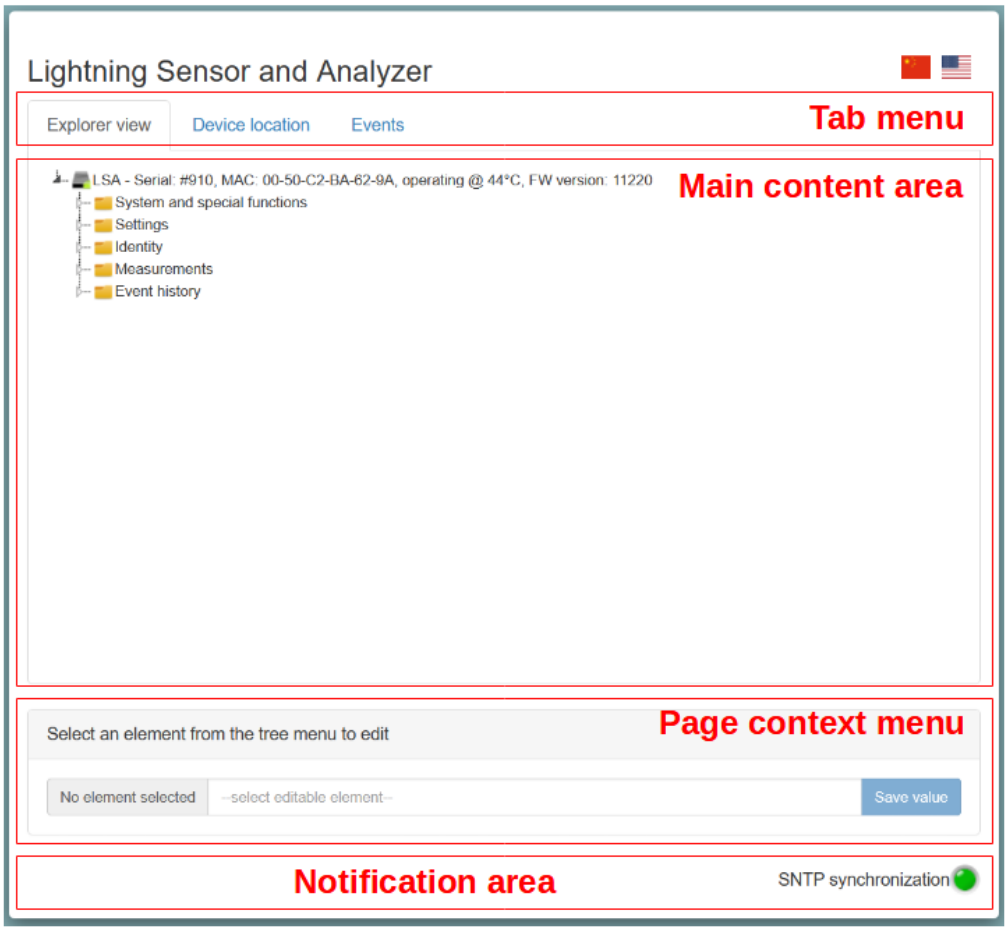


Figure 11: Overview of the web interface showing the layout of the four basic components.

6.2 Sub pages

6.2.1 Explorer view

The *Explorer view* page provides a quick and direct access to most LSA settings, functions and measurements. All items are arranged in a hierarchical folder structure that can be expanded when clicked. See figure 12.

When a node in the tree is clicked, the *page context menu* will show the node key and value, and if the value is editable, let you enter a new value which can be saved by clicking the *Save value* button.

Depending on the information type, the lowest level expansion will either act as a button executing a command, a link for file download, a link which expands the bottom part of the main page with the requested content or in a pop-up window, or in case of specific parameter values, the value is inserted in an editable text box.

The **main folder** (top level icon) represents the LSA sensor device itself, including a few main status and identification parameters.

The **System and special function** features **Reboot sensor**; A reboot command is sent to the sensor. The web client will automatically reload the page when the sensor should be up and running again. If this is not the case, please reload the page again, and remember to check that the IP address targeted is still correct after the reboot, as the address may have been manually changed by the user, or reassigned by the DHCP server.

The **Settings** information folder presents a database table as defined by the '*conf/settings.conf*' file. Any web based modication of the parameters will be directly updated in the '*.conf*' file itself. Note that some parameter changes will require a reboot to take effect. This folder (see section 6.3), along with the **Identity** folder (see section 6.4), is a direct mapping of a corresponding data table in Lua. This is the reason why there are no special characters in the subfolder and parameter names.

Note that the majority of the parameters in the **Settings** folder are described by placing the cursor above the parameter in question. The same is the case for many of the parameters included in the other folders.

The **Measurements** folder reflects the relevant parameters of the latest lightning event, as also accessible via the MODBUS or IEC-104 protocols.

The **Event history** provides a full listing of all lightning events, including option for view of the time series and main lightning parameters for the individual events, see the subfolder *eventFiles*. Note that section 6.2.3 describe a more easily accessible overview of the same information using the LSA web interface. Included at the bottom of the event history listing, note the *event_count* parameter which tracks the number of events recorded. Irrespective of specific (or all) events being manually deleted, the *event_count* will remain, to avoid any possible confusion regarding overlapping event IDs from the same sensor.

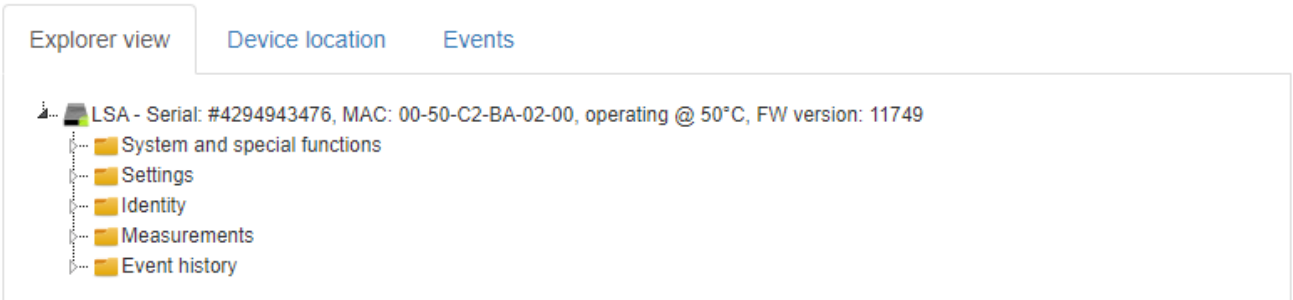


Figure 12: Screen shot from the *Explorer view* sub page listing the main folders.

6.2.2 Device location

The *Device location* page visualizes the geographical sensor installation location on an interactive map. The location coordinates can be edited by clicking the map to place a new marker. Once the new mark has been placed at the desired position, the location coordinates can be saved by clicking the *Save coordinates* button in the *page context menu*.

The device location coordinates can also be set through the *Identity->wgs84_coordinate* node in the *Explorer view* sub page. Note that the map will only load, if the client browser has internet access.

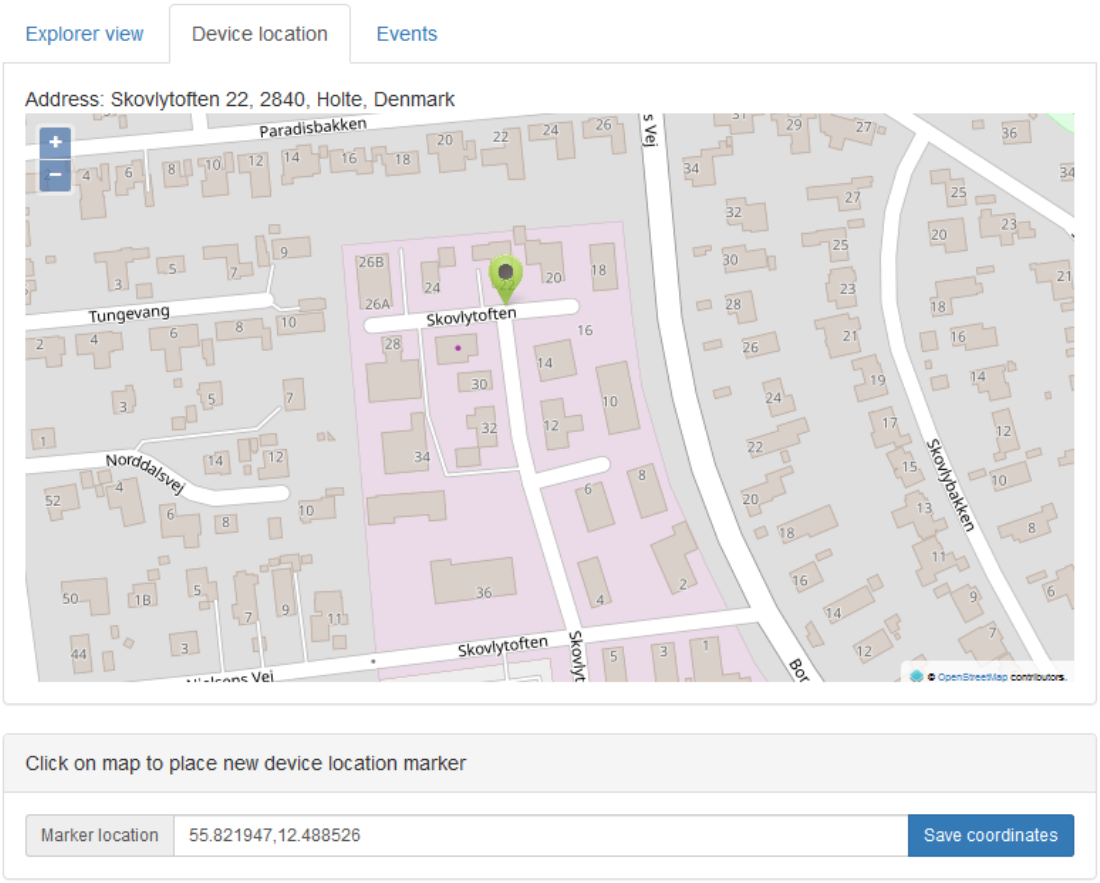


Figure 13: Screen shot from the *Device location* sub page presenting a marker location ready to be saved.

6.2.3 Events

The *Events* page provides an easily accessible overview of the strikes recorded by the LSA, including a graph at the top in chronological order of all recordings, with the size of each circle scaled according to the peak current, the event severity (Y-axis) scaled according to the lightning parameter closest to the respective Lightning Protection Level I level, and a custom log-scaling for the X-axis distance in time between events. See figure 14.

Either by clicking on a circle, or by clicking on the *Graph* link button on the right hand side of the table listing below the graph, an event presentation like shown in figure 10 is shown. With this view, it is also easy to inspect the time series behaviour of individual events using the zoom in and graph reset functionalities.

Using the *Download log of all events*-button, all key lightning parameters of all recorded strikes can be downloaded in a csv file, for easy filtering and analysis.

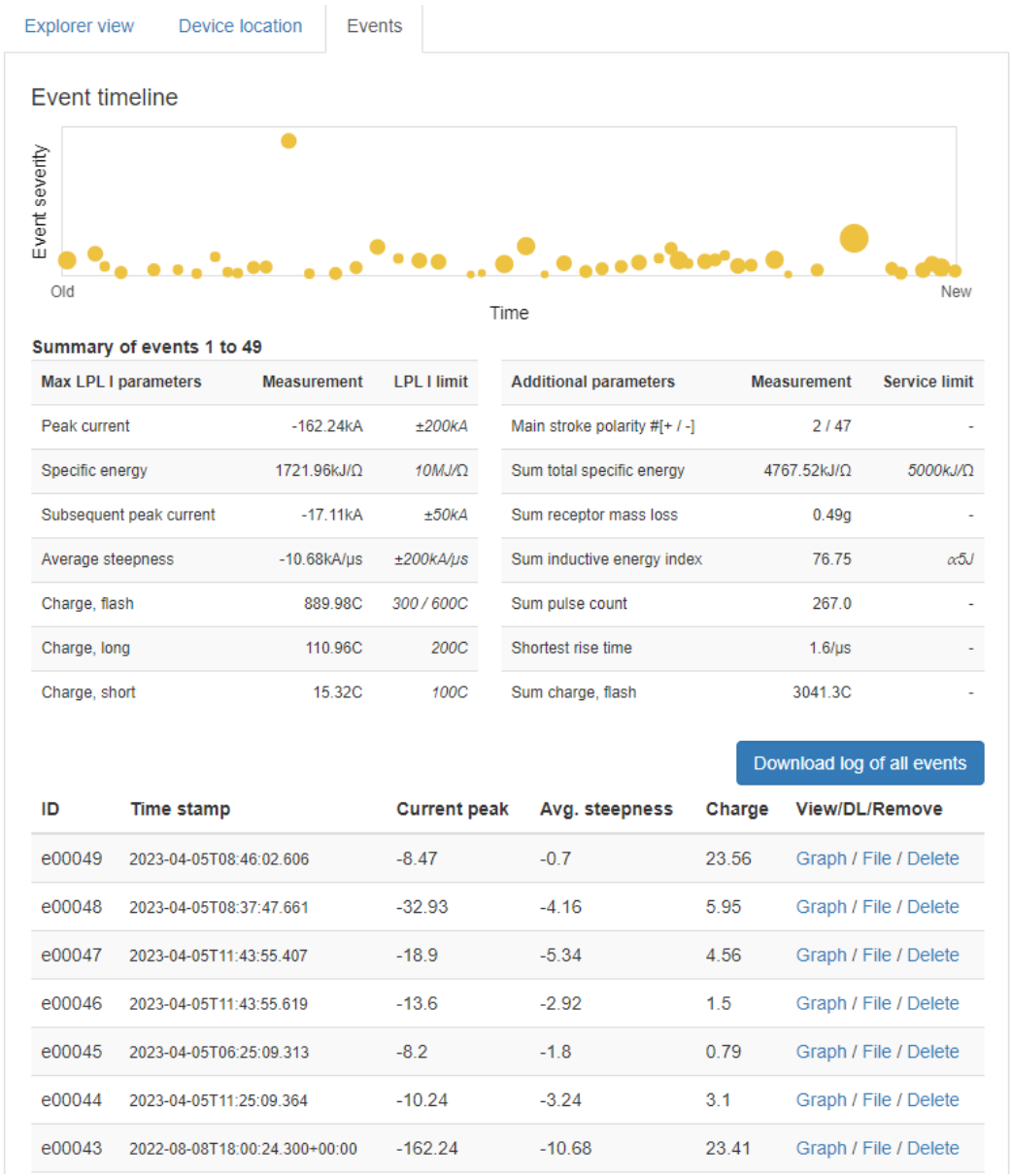


Figure 14: Screen shot from the *Events* sub page listing the lightning events registered by the sensor.

6.3 Settings

Below is a description of the different subfolders in the Settings folder, in alphabetical order.

clouddb
Parameters in the clouddb allow for configuration of up to two web servers set up to receive multipart/form-data POST file transfers initiated by the LSA. The parameters specify the host server address using either ***cloud_1*** or ***cloud_2***. The service is enabled when the respective ***enable_push_1*** or ***enable_push_2*** parameter is set to true. See additional detail in section 8.

iec104
The iec104 subfolder lists all main parameters used for the IEC 60870-5-104 protocol configuration. See section 9 for additional details.

influxdb

The sensor supports push of predefined datasets from the sensor to an InfluxDB server (verified to work with InfluxDB 2.1.1). The Influx data streams target two transmission modes enabled by setting ***enable_push*** and ***enable_interval_push*** to true. The interval push will send a dataset defining the sensor location and operational state, allowing for automated 'discovery' and health state monitoring of a sensor. Data fields include: Serial number, latitude, longitude, processor temperature, software version, SNTP synchronization and sensor error state.

The other mode, activated via ***enable_push***, targets transmission of lightning event key parameters in a similar fashion to the event log file content transfer described in section 8.

Additional customization options may be added in future updates. Should you have a specific request for an InfluxDB configuration or troubleshooting, please contact Jomitek for support.

lsa
The lsa subfolder contains a number of LSA sensor specific configuration options:

- **alarm_relay** define the settings for the output alarm relay signal used as an indication to external systems that a lightning strike has been detected.
- **measurement** define parameters related to the lightning current trigger level, the length of the time series to be recorded when a strike is detected, and the event number used as the starting point for summary lightning event metrics, see section 3.5.
- **service_alarm_levels** lists a set of parameter thresholds for when service visits are warranted. The intent of these parameters are for a wind turbine operator - in particular when a turbine is out of warranty - to determine if an inspection visit is required, based on emperical knowledge. To be clear; The LSA will raise a lightning alarm whenever a lightning event exceeding the ***trigger_level*** is detected. The ***service_alarm_levels*** serves as a series of parallel alarms indicating if specific event parameters exceed such empirically determined levels. It is entirely the responsibility of the turbine operator to determine what the levels should be (i.e. what level of risk vs. operational cost is acceptable). Jomitek is very open to support an expansion and refinement of this approach in terms of LSA functionality. Jomitek provides a default configuration for the service alarm levels, but takes no responsibility for the applicability and use of these default values. Furthermore, note that the functionality of these alarms may just as well be configured in a centralized manner, with the evaluation logic being applied by the SCADA system, or similar.
- **tower** define parameters describing the physical geometry of the wind turbine on which the LSA is mounted. Together, these parameters define the magnetic-field-to-lightning-current conversion model. It is important to specify these parameters in order to get the highest level of precision in the post processing, with a particular emphasis on the tower radius at the point of installation.

security
As mentioned in section 1.4 the LSA is generally speaking not able to provide end-to-end encryption, as the sensor makes use of a microprocessor without such capability. Nonetheless, a number of important security measures are supported by the LSA . Part of this security is highlighted in section 5.1, in that only encrypted firmware files created by Jomitek can be used to update the microprocessor. The processor has the hardware pins used for direct programming or program readout disabled. As such, the firmware and any update of this is considered a fully secure aspect of the sensor.

As for the various communication protocols supported by the LSA most of these offer no inherent security features. The exception being the web interface access, which supports login with credentials at several levels. Credential verification happens within the microprocessor (where the firmware is inacessible, even for an attacker with physical access). As one of several measures the credentials are SHA-256 encrypted client side, before being sent to the LSA , based on a time dependent key governed by the LSA .

The security concept of the LSA is built on the option of secure access via the web interface, with the *security* section of the Settings folder providing configuration of all relevant security settings. By default none of these options are enabled, to allow ease of initial configuration and integration tests of the sensor.

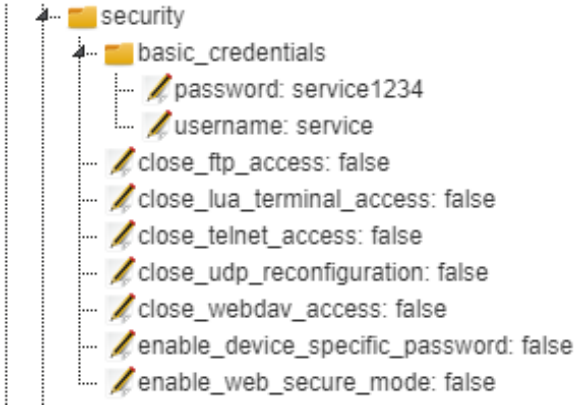


Figure 15: Overview of the web interface showing the security settings.

The credentials are supported in two ways; basic credentials, with full customization option, or using a device specific password, with a static password locked to the LSA hardware.

- **basic_credentials->password** is the password used for FTP access in all scenarios. It is also used for login to the web interface, when ***enable_web_secure_mode = true*** and ***enable_device_specific_password = false***. The input is limited to characters a-z, A-Z, 0-9, period and dash, and text length 4 to 24 characters.
- **basic_credentials->username** is the username used for FTP access in all scenarios. It is also used for login to the web interface, when ***enable_web_secure_mode = true***. It is used as username irrespective of the setting of ***enable_device_specific_password***. The input is limited to characters a-z, A-Z, 0-9, period and dash, and text length 4 to 24 characters.
- **close_ftp_access** when set to true, will disable FTP access.
- **close_lua_terminal_access** when set to true, will disable the Lua terminal access.
- **close_telnet_access** when set to true, will disable the Telnet access.
- **close_udp_reconfiguration** when set to true, will disable the Jomitek Device Locator functionality of re-configuring/recovering the LSA IP settings via UDP.
- **close_webdav_access** when set to true, will disable the WebDAV access.
- **enable_device_specific_password** when set to true, will allow login to the web interface only using the device specific password supplied by Jomitek, when ***enable_web_secure_mode = true***
- **enable_web_secure_mode** when set to true, will require login to the web interface using either basic credentials, or credentials using the device specific password. The device specific password will work in both scenarios, with basic credentials working only if ***enable_device_specific_password = false***.

Note that as a general measure for the security settings, as well as all other reconfiguration of settings, the LSA should be restarted, as many of the changes are put into effect only during boot up.

tcpip (TCP/IP and NTP)
The tcpip setting provides configuration of TCP/IP and (S)NTP settings. The following parameters are available, see figure 16.

- ***dhcp*** a boolean flag for enabling/disabling use of DHCP.
- ***gateway*** The forwarding host e.g. router to other networks used when no other route specification matches the destination IP address of a packet.
- ***hostname*** The hostname of this device.

- ***icmp*** a boolean flag for enabling/disabling the ICMP ping utility for the device.
- ***ipv4*** the IPv4 address of the device, when the sensor is booted with the DHCP flag set to false.
- ***ntpserver*** the IPv4 address of the primary (S)NTP server when the DHCP flag is set to false, set ntpserver to 0.0.0.0 to disable.
- ***ntpserver_alt*** the IPv4 address of the secondary (S)NTP server when the DHCP flag is set to false, the ntpserver_alt address is only used when the ntpserver addess is not 0.0.0.0, set ntpserver_alt to 0.0.0.0 to disable.
- ***subnet*** the subnet mask used when the sensor is booted with the DHCP flag set to false.

The sensor supports SNTP in two ways: By default when the DHCP flag is set to true, the sensor queries the DHCP server for an NTP server address. When the DHCP flag is set to false, or the DHCP server does not respond with an NTP server address, the sensor rely on the user to provide a set of valid NTP server addresses. These addresses are to be typed into the ntpserver and ntpserver_alt fields. For wind turbine farms, an NTP server is often present locally which would then be the preferred source, and otherwise public NTP servers may be used.

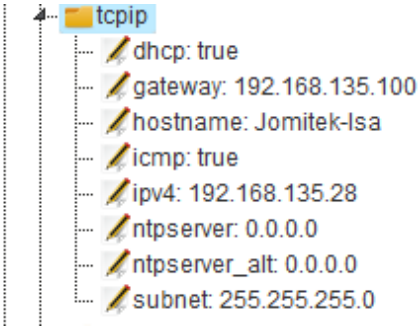


Figure 16: Overview of the web interface showing the TCP/IP settings.

As a default DHCP is set to true. The IP and gateway address and the subnet mask is also defined here and is only used when the sensor is booted with the DHCP flag set to false. Note that if the device experiences severe errors during startup, it will revert to the IP configuration defined in the '*conf/panic.ip*' file (default with *dhcp=true*), and if this also fails to load, hardcoded settings will apply, using *dhcp=true*. In DHCP mode, in the case where no DHCP server can be reached, the sensor will automatically choose a random IP address in the range 169.254.1.0 to 169.254.254.255 in compliance with RFC 3927 Section 2.1.

time->timezone
The timezone settings can be found in the **time** folder.

- ***utc_offset_hh*** sets the time offset with reference to UTC in hours.
- ***utc_offset_mm*** sets the time offset with reference to UTC in minutes.

web
The parameters in the web section define which port is used for the web service (default is '80'), and the start page when logging on to the device, with options including 'home', 'geolocation' and 'event'.

6.4 Identity

The Identity folder contains all the location and naming related information for a specific device. It should always be edited, or generated, on an individual basis. The parameters include *address*, *city*, *zip*, *country_state*,

location_name and *location_description* as identifying text for the location. The location_name could e.g. be the name or reference for a wind turbine, and the *location_description* could detail the wind turbine park name. Furthermore the location may be specified using WGS84 coordinates in a '<latitude>,<longitude>' decimal degrees format. The *serial_number* is the Jomitek device serial number and should not be edited. In this context, note that the only hardcoded identifier of a device is the uniquely assigned MAC address. The *type* parameter will, if left blank, be automatically set during bootup based on a device internal check of the accessible peripherals. Custom naming may be used as an alternative. Note that using the 'Device location' sub page enables manually/visually updating the coordinates of the LSA. When the marker location is saved, it is effectively overwriting the *Settings->wgs84_coordinate* parameter.

7 Support tools for LSA configuration and updates

On the Jomitek web site various tools are provided to support efficient initial configuration and continued operation of a large amount of sensors. See https://jomitek.dk/en/downloads/tools. Some of these tools, as well as scripting examples, are detailed in the following.

7.1 The Jomitek Device Locator

The Jomitek Device Locator (JDL) offers an all-in-one package in terms of detection and configuration of a Jomitek sensor, based on manual interactions via a GUI. It is a Windows program executable (.exe), tested to work using Windows 10 or later. As such, some organizations may have security policies restricting direct download, or in other ways hindering use of the software. Please reach out to Jomitek, to discuss possible solutions in such cases.

JDL overview

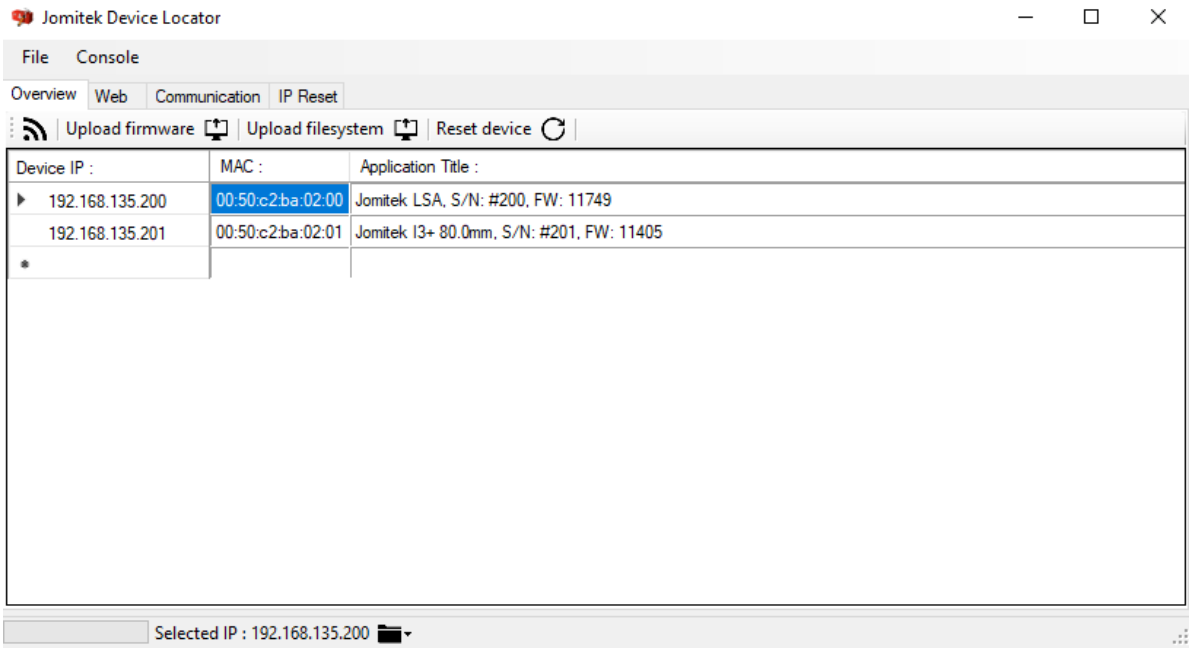


Figure 17: The Jomitek Device Locator overview tab.

Via the overview tab, using broadcast via UDP port 23, the JDL lists all Jomitek sensors reachable from the client PC, including identifying information such as the active IP address of each sensor, the corresponding MAC address, serial number information, type of sensor and the firmware (FW) in active use. See figure 17 for reference. In most cases the sensors use a DHCP server on the network it is connected to, to get an IP address assignment. In this context, the JDL is useful in easily identifying what address was assigned.

Note that use of UDP enables the Locator software to detect sensors that are outside of the IP range / subnet mask used by the client PC. As such, in order to be able to connect to a given sensor, it must be ensured that the client is reachable via the client IP address. This is usually the case if the same DHCP server is used for both sensor and client, and no custom rules are applied for IP assignments.

JDL communication

When marking a sensor in the overview tab, it is automatically selected as the target for the other JDL tabs. The communication tab provides a parallel view with access using Telnet on the left hand side (TCP port 23), see

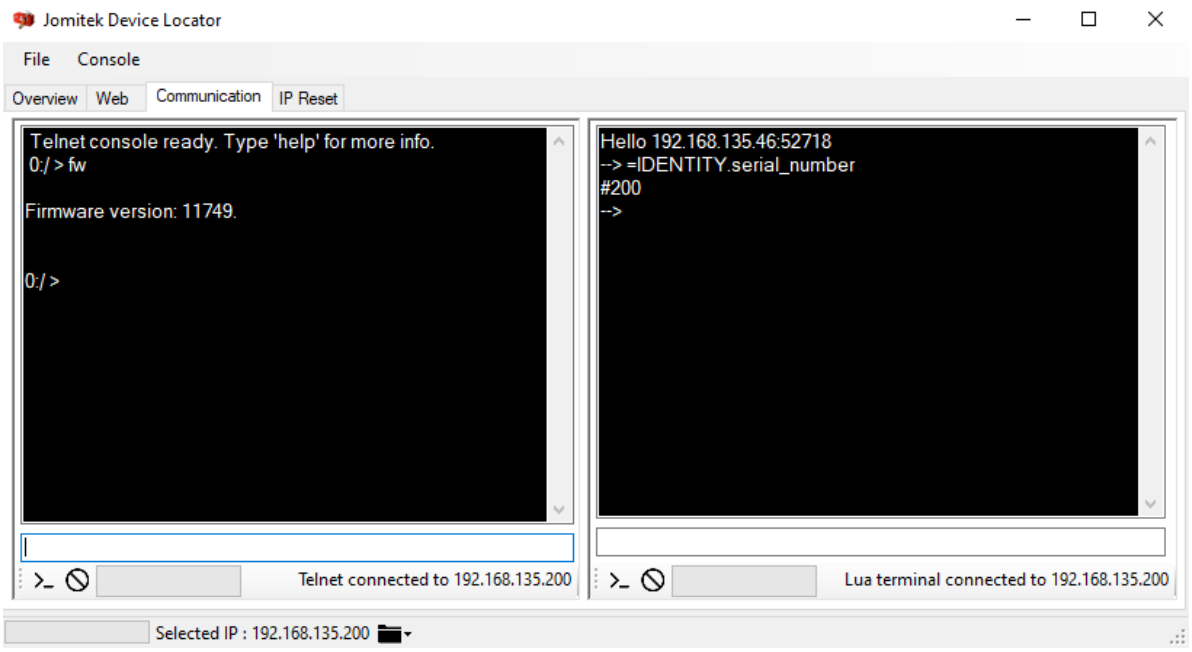


Figure 18: The Jomitek Device Locator communication tab.

connectivity alternatives in section 12.1. The right hand side provides Lua terminal access (TCP port 2840). Both of these access options are primarily meant for super users, and are as such not needed for normal operation.

JDL IP reset

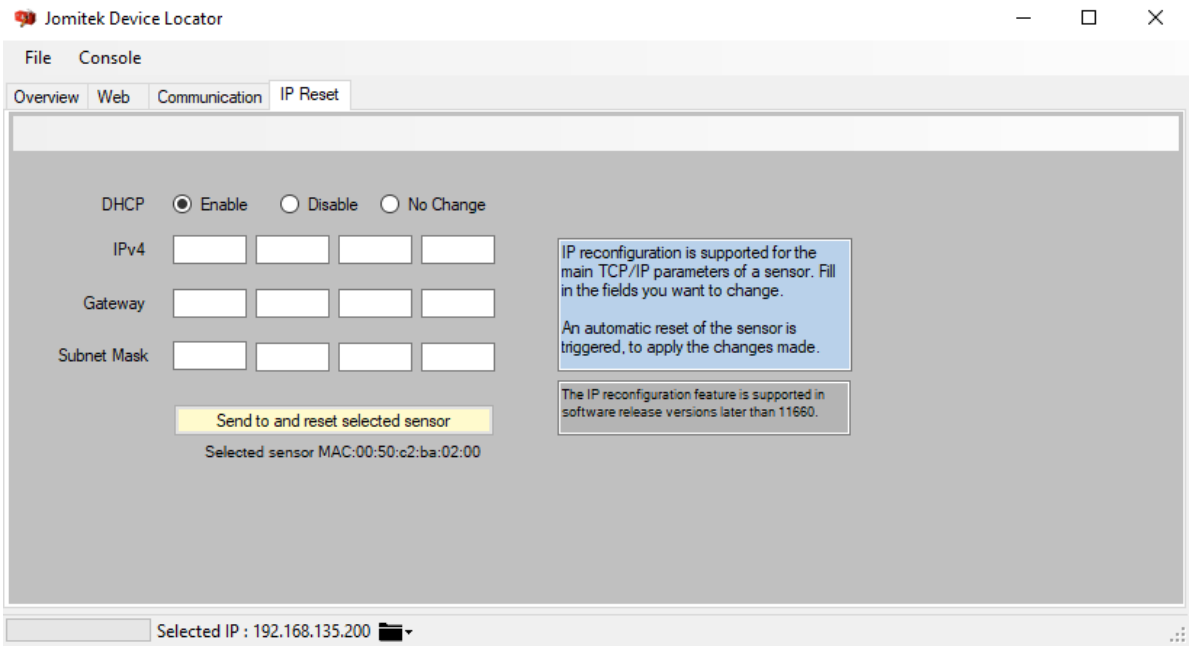


Figure 19: The Jomitek Device Locator IP reset tab.

The IP reset tab provides a reconfiguration option for the TCP/IP settings for Jomitek sensors, based on UDP port 1342. It is convenient in cases where the client IP settings do not allow direct access to a sensor, and rather than change the client settings, the sensor can be reassigned to be in a reachable IP range using this functionality.

7.2 Mass reconfiguration and updates

Jomitek offers custom configuration of sensors before delivery, with device specific settings if requested. Such custom configuration would usually apply to the parameters described in sections 6.3 and 6.4, which in the sensor is defined in the */conf/settings.conf* and */conf/identity.conf* respectively.

In some cases these parameters are first possible to configure after delivery, prompting the need for an efficient way to perform mass configuration changes of sensors. There are several possible ways to achieve this goal as exemplified in the following.

Reconfiguration via the web interface

While reconfiguration of parameters via the web interface is the most intuitive to use, provides on-mouse-over description of parameters, and feature client side validation of appropriate formatting of parameter input, it is also the least efficient and includes the risk of incorrect manual entries being made. Assuming a large volume of sensor updates (e.g. >10), the web interface is suggested to be used for initial tests only, to provide a valid template for the update need of additional sensors.

Reconfiguration using .reconf files

The *Mass reconf tool* macro enabled Excel document provided by Jomitek can be used as-is, or as an inspiration for similar scripting based sensor updates. See the 'User Manual'-sheet in the document for a detailed description of the functionality. The tool is based on the use of .reconf files (either settings.reconf and/or identity.reconf), which allows for incremental changes of parameters of the parent settings.conf and identity.conf files, without changing the rest of the .conf parameters. It is recommended NOT to overwrite .conf files directly.

The Excel document supports the generation of correctly formatted .reconf files, as well as generation of a transfer script based on FTP transfer via WinSCP.

A *settings.reconf* or *identity.reconf* file transferred to the */conf* folder (using WebDAV or FTP) will automatically be detected and incorporated in the respective .conf file by the LSA whereafter the .reconf file is automatically deleted. This process flow takes less than 10 seconds.

Before mass updates are initiated, it is important to ensure that there are no errors in the input provided, e.g. using a trial sensor, or other easily accessible sensor to validate full functionality. Jomitek is also available to support any validation needed in this context.

Note that updates to *settings.conf* will, in most cases, require a sensor restart before the changes take effect.

Reconfiguration using *curl*

Curl is a command line tool available across all major operating systems, which can be used to automate http interactions. However, note that there may be differences in the syntax used across various implementations. The examples provided in the following applies for Windows 10 with curl 8.4.0. The examples include the most common parameters required to update to configure and identify a sensor.

The parameter value in each case is underlined. To check what parameter values are valid, please test values using the web GUI as a first step. Note that the examples target a sensor with IP address 192.168.135.98. Change this to the relevant address to be updated.

Parameters specified in settings.conf; tower height, radius and sensor mount height respectively

- `curl -d "command=lua_table_update&file_name=settings&lua_table_path=CONFIG.lsa.tower.height&lua_value=80" http://192.168.135.98:80/backendhandler.lua`
- `curl -d "command=lua_table_update&file_name=settings&lua_table_path=CONFIG.lsa.tower.radius&lua_value=2.8" http://192.168.135.98:80/backendhandler.lua`
- `curl -d "command=lua_table_update&file_name=settings&lua_table_path=CONFIG.lsa.tower.sensor_mount_height&lua_value=7.5" http://192.168.135.98:80/backendhandler.lua`
- `curl -d "command=reset_device&reset_type=main" http://192.168.135.98:80/backendhandler.lua`

Note that parameters associated with the settings.conf file, will generally require a sensor reboot command in order to become active, which is included as the last command of the previous example list.

Parameters specified in identity.conf; location coordinates, location name and location description respectively

- curl -d "command=lua_table_update&file_name=identity&lua_table_path=IDENTITY.wgs84_coordinate&lua_value=55.821925,12.488535" http://192.168.135.98:80/backendhandler.lua
- curl -d "command=lua_table_update&file_name=identity&lua_table_path=IDENTITY.location_name&lua_value=T21" http://192.168.135.98:80/backendhandler.lua
- curl -d "command=lua_table_update&file_name=identity&lua_table_path=IDENTITY.location_description&lua_value=Wind farm name" http://192.168.135.98:80/backendhandler.lua

Software updates

Software updates, in the form of a *software.tar.gz* file, are applied by transferring the file to the */software_update* folder, and then triggering a reboot of the sensor. The update is usually completed within 2-3 minutes.

The transfer can be made in a number of ways, e.g. using FTP, WebDAV, and the 'Upload filesystem' button in the overview tab of the Jomitek Device Locator. The *Jomitek mass SW update tool* on the Jomitek website provides an example based on a macro enabled Excel document, which generates a script for software updates via WebDAV, using WinSCP. See the manual provided in the document for additional guidance on this approach.

An example using *curl* to perform a software update is provided in the following. It is assumed that a software file has been acquired, e.g. from the Jomitek software download page (see section 11.2), and that the curl script is being executed from the folder where the relevant software package is located. Note that the filename of the software package uploaded must be *'software.tar.gz'*. The example targets a sensor with IP address 192.168.135.98. Change this to the relevant address to be updated.

Software package upload and application via sensor reboot command

- `curl -d "command=getDeviceInfo" http://192.168.135.98:80/backendhandler.lua`
- `curl -T software.tar.gz http://192.168.135.98/dav/software_update/`
- `curl -d "command=reset_device&reset_type=main" http://192.168.135.98:80/backendhandler.lua`
- `curl -d "command=getDeviceInfo" http://192.168.135.98:80/backendhandler.lua`

The sensor should be expected to be unresponsive for 2-3 minutes during the update process, whereafter the last command can be executed. Note that the first and last commands in the example are optional checks of the pre and post sensor device info, which includes the firmware version in the response. This information can be used to confirm if the update was successful. For firmware prior to release 11773 the getDeviceInfo command will not work, and in such cases the upgrade can be confirmed by the command working post upgrade.

Reconfiguration and updates vs. security settings

As mentioned in section 6.3, no security measures are activated by Jomitek by default (unless specified so by the customer). The intention is to ensure full access for initial configuration and testing. If the customer choose to activate relevant security measures after commissioning of the sensor, note that scripted access, e.g. via FTP, WebDAV or curl commands may no longer work, depending on what has been disabled via the security settings.

The configuration of the security settings can be accomplished using curl commands, including setting *enable_web_secure_mode* to *true*. After a reboot, curl commands will no longer work. As such, to gain access to the sensor again, it must be unlocked manually using the web interface / GUI with appropriate credentials, whereafter scripted commands can be used again. The point of these comments is to make it clear that activation of the security features include a penalty on the complexity in regards to changes to the sensor configuration and software upgrades, as well as the ability to perform automated retrieval of measurement files, event logs, etc..

8 Automation for Cloud services

8.1 Cloud services in the context of the LSA

While 'Cloud' is a broadly used term, in the context of the LSA, it is meant to imply functionality supporting automated transfer of datasets via mainstream web services/protocols, allowing for centralized database storage, data presentation, and further data analysis.

This goal can be achieved using two main data retrieval approaches. In one case, the LSA will actively push data to a database, in the other a server will pull the data from the sensor, i.e. data polling.

Up to 3 separate servers may receive data in the push scenario, as some use cases will see multiple parties interested in direct access to the raw sensor data.

The descriptions in this chapter is meant to provide an understanding and example framework for Cloud automation allowing any party to set up such automation. Note that Jomitek offer Cloud services as well, based on the principles described, should that be of interest, see section 8.8.

For all transfers, from a cyber security perspective, it is assumed that the connection between the LSA and server is secure. This security may be supported by use of VLANs and/or VPN tunnels as primary examples. With cellular connections, use of a dedicated APN may also be part of the security solution.

The automated push transfers target two modes of operation:

- Discovery mode, pushed at regular intervals (typically on a 12-hour non-synchronous cycle)
- Event mode, pushed for each event that has not been registered as successfully transmitted to a given cloud server

These modes are further detailed in the following. The transfer schemes are built on the assumption that it should work well via a long range widely supported IoT cellular technology, with limited bandwidth available, i.e. in the order of 10-100kbps transfer speeds. NB-IoT and LTE-M / CAT-M LTE being prime examples of such networks. Continuous connectivity is not guaranteed, and the transferred data may come with a significant price tag scaled by volume - at least using commercial cellular network offerings. These requirements promote a transfer-when-needed philosophy, with the LSA actively pushing data, rather than the server using a polling scheme.

8.2 Trigger mechanism for Discovery mode

Discovery mode cover transfer of a pre-defined set of parameters, with the baseline including the following list.

- LSA serial number
- Location description (e.g. wind farm name)
- Location name (e.g. wind turbine identifier)
- Latitude, WGS84 decimal degrees
- Longitude, WGS84 decimal degrees
- Processor temperature, in Celcius
- LSA software version

- SNTP synchronization status
- Sensor error state

This data set is sent at regular intervals as a form of 'keep-alive' indicator, in support of an operational overview of the LSA installation base. In addition to indicating a working connection to a sensor, it identifies itself by coordinates, serial number and software version, and expose basic status indicators in the form of a temperature reading, the time synchronization status and whether the sensor measure the expected noise floor levels on the integrated analog sensors of the device, i.e. the sensor error state. Note that this information may allow avoidance of on site inspection of the LSA, bringing down the TCO.

On purpose, the push intervals are triggered in a non-synchronous fashion, which should help avoid a situation where all sensors in a wind farm attempt to transmit at the same time. The default interval is set to approximately 12 hours. The functionality is enabled via the ***enable_discovery_push*** parameter for each server destination.

8.3 Trigger mechanism for Event mode

Each LSA maintain an internal non-volatile log, which tracks which lightning event recordings have been successfully sent to a given server. The tracking applies for the InfluxDB server as well as the two ***clouddb*** defined servers, each with their own tracker.

Once the ***enable_event_push*** is set to true for a given server, automated transfers become active. If no other transfer is in progress, the LSA will evaluate the need to transfer the next queued event every 10 seconds. The tracker will move to the next event only at the completion of a transfer. If a transfer fails, a retry will be attempted 6 hours later.

If a server is defined and enabled after one or more events have already been recorded, all such events will still be transferred since the tracker will start with the first event and work its way up to the newest recording, where after it will remain idle until the next event is recorded. This behavior imply that a sizeable 'back log' may be transferred at the time of activating a given cloud server.

8.4 Example CloudDB server and database setup

The following example presents a framework which is open to copy and adapt according to end user needs.

Making use of an outdoor cellular IoT modem, which creates a VPN tunnel between a given LSA and the host web server, the server is made directly reachable by the LSA. The modem verifies connectivity via the VPN tunnel automatically every 23 hours. In case of no connectivity, the modem restarts. The modem will poll the LSA every 10 hours, to verify that the LSA is reachable. Should this fail, the modem will power cycle the LSA. As such, the ability to recover connectivity should be secured, as long as there are no outright hardware failures or a permanent power supply failure.

While Cloud hosted services are often referencing the major providers such as AWS, Azure or GCP, in this context it is equally applicable for a server setup with similar backup and redundancy targets as such providers.

An example of a baseline server setup - there are many possible combinations - is an enterprise-grade server with an Ubuntu installation, including Python with Flask (a web framework module), a PostgreSQL database using the TimescaleDB extension, and Grafana.

Flask is configured to listen to multipart/form-data HTTP POST messages on a given port and address. The relevant port and address is set up as e.g. the ***cloud_1*** address on the LSA. For the Event mode communication, the LSA will send the event .log file (clear text, Lua format), and .wav.gz file (timeseries data, compressed using

gzip, in wave-file format), according to the logic described in section 8.3. For the Discovery mode, a parameter list is sent as a status.dscvr file, clear text, Lua format.

When receiving such files, a Python script is created to parse the file data into the PostgreSQL database. From there, the data is available in an accessible format, where e.g. Grafana can be used for visualization.

An example of an event log file is presented in the following. Note that the syntax is in the form of a Lua table.

Listing 1: Event log file example

```
{
  eventParameters = {
    charge_flash = 56.72,
    charge_long = 0.00,
    charge_short = 0.35,
    polarity = "negative",
    current_peak = -4.53,
    subsequent_current_peak = -4.18,
    main_specific_energy = 1.02,
    specific_energy = 13.55,
    inductive_energy_index = 0.20,
    receptor_mass_loss = 0.00,
    pulse_count = 8,
    rise_time = 4.08,
    subsequent_rise_time = 2.68,
    average_steepness = -1.05,
    subsequent_average_steepness = -1.08,
    severity_lpl_I = 18.9,
    signal_noise_level = 35
  },
  eventType = "lightningStrike",
  eventFiles = {
    "e00003_211210_163617906.wav"
  },
  eventTimeStamp = {
    sec = "1639153566",
    nanoSec = "906374960",
    iso = "2021-12-10T16:36:17"
  },
  plotOptions = {
    "{'t':'Measured lightning discharge current','s':1,'u':'kA','y':'Lightning current [kA]',
    'x':'Time [ms]','l':['Lightning current']}"
  },
  sensor_id = {
    owner = "Jomitek",
    wgs84_coordinate = "55.69224,12.6706",
    type = "LSA",
    location_description = "Middelgrunden",
    city = "N/A",
    zip = "N/A",
    serial_number = "#1440",
    address = "N/A",
    location_name = "T10",
    country_state = "Denmark"
  }
}
```

Based on the event log file parsing, it is proposed to create 2 database tables:

serial_number	location_desc	location_name
1443	Middelgrunden	T13
1453	Tunoe Knob	T2

Table 4: 'lsa_identity' database table, including example entries

Based on the time series data in the wav.gz file, correlated with the log file information, it is proposed to create a third table, as follows:

global_event_id	event_id	serial_number	event_parameter	value	timestamp
1440000003	3	1440	charge_flash	56.72	2021-12-10 16:36:17.906 +0200
1440000003	3	1440	current_peak	-4.53	2021-12-10 16:36:17.906 +0200

Table 5: 'lsa_event_metadata' database table, including example entries

global_event_id	lightning_current	timestamp
1440000003	-10	2021-12-10 16:36:17.906001 +0200
1440000003	-9	2021-12-10 16:36:17.906002 +0200

Table 6: 'lsa_event_waveform' database table, including example entries

For the waveform table there are several options to consider on how to structure and store the data efficiently. The example shown is a bit 'brute force' in this context, but simple. As a note for the wave file format, it is a signed 24-bit integer value for each sample, scaled simply 1:1 in Ampere. I.e. 1kA would read as the value 1000.

A final 4th table ties to the Discovery mode information, as follows:

serial_number	location_desc	location_name	lat	lon	temp	sw	sntp	hw_error	timestamp
1440	Middelgrunden	T10	55.69224	12.6706	38	11873	1	0	2021-12-10 08:09:12.154 +0200
1440	Middelgrunden	T10	55.69224	12.6706	40	11873	1	0	2021-12-10 20:10:02.564 +0200

Table 7: 'lsa_discovery' database table, including example entries

For the event related tables, the timestamp is parsed from the log file time stamp info. For the discovery table the time stamp is created by the server, according to the time the information was received.

8.5 InfluxDB server description

The InfluxDB configuration provides a largely similar dataset to the specified destination server, compared to the CloudDB description, with the noteable exception that the timeseries data for lightning events are not included. I.e. Event mode data is restricted to the event parameters in the log file, as well as the timestamp and relevant sensor ID parameters.

For both Discovery and Event mode the InfluxDB line protocol is used. For Discovery data, the measurement tag 'lsa_discovery' is used, while Event data use 'lsa_event'. The InfluxDB functionality is verified compatible with InfluxDB 2.1.1.

8.6 JSON query pull based retrieval

While not ideal for continous monitoring purposes - as pulling data may generate a lot of network traffic - the LSA supports a polling scheme using the following HTTP queries:

`http://<insert-lsa-ip-address>/jsondata.lua?event_list=true`

The response will be a JSON formatted list of lightning events, see example in

Listing 2: List of lightning events, and event file path

```
{
  "e00005": "0:/root/service/data/event/e00001-e00100/e00005",
  "e00006": "0:/root/service/data/event/e00001-e00100/e00006",
  "e00012": "0:/root/service/data/event/e00001-e00100/e00012",
  "e00004": "0:/root/service/data/event/e00001-e00100/e00004",
  "e00009": "0:/root/service/data/event/e00001-e00100/e00009",
  "e00003": "0:/root/service/data/event/e00001-e00100/e00003",
  "e00001": "0:/root/service/data/event/e00001-e00100/e00001",
```

```
  "e00011": "0:/root/service/data/event/e00001-e00100/e00011",
  "e00010": "0:/root/service/data/event/e00001-e00100/e00010",
  "e00008": "0:/root/service/data/event/e00001-e00100/e00008",
  "e00007": "0:/root/service/data/event/e00001-e00100/e00007",
  "e00002": "0:/root/service/data/event/e00001-e00100/e00002"
}
```


8.7 Data visualization exemplified using Grafana

Using the open source monitoring and analytics tool Grafana, an example dashboard is presented in figure 20. The tool can be used to create a day-to-day operational overview, for alarm listings, and even for in depth analysis of time series data. It can also be easily integrated with other existing tools, e.g. work lists and other sources of data.

This will allow a direct understanding of which turbines should be prioritized for inspections, where there may be an option to skip inspections, and over time build a knowledge base supporting further operational optimization. E.g. in the form of practical experience that 'nothing breaks, if the average steepness is less than 5kA/us and peak current is less than 10kA' for a given turbine model, which could help reduce inspection downtime.

Figure 20: Example Grafana-based dashboard, presenting lightning event recordings for 2 separate wind farms - map view is zoomed in on only one of them.

8.8 The Jomitek Cloud service offering

While Jomitek will help support any automation effort for LSAs, as relevant for customers or 3rd party service providers, Jomitek offer such services as well. The offering may include the following elements, based on access to relevant sensors via a VPN tunnel to Jomitek:

- Remote commissioning / configuration / reconfiguration
- Software updates
- Cloud database export/integration towards external (customer) end point
- Discovery dashboard / availability overview / alarm notification service

- Event dashboard / lightning strike overview / alarm notification service

Note that the options include only remote services predicated on the LSAs in questions being reachable via Jomiteks VPN terminating end point. Please reach out to Jomitek for further detailing of the service scope.

9 IEC-60870-5-104 configuration

The IEC 60870-5-104 (abbreviated "IEC 104" or "104" in the following) application layer protocol can be used for transmitting sensor data from the sensor to a SCADA system or another data-aggregation device implementing the IEC 104 protocol. The TCP/IP protocol is used to ensure reliable data transfer. Additionally, the 104 protocol supports message sequencing on the application layer. A 104 client connects to TCP port 2404.

The sensor allows flexible configuration of the protocol settings, and of the data points. The data points can be transmitted based on a variety of triggers, including on-change, periodic, on manual request, or using interrogation commands requesting a larger set of data. The sensor can be configured to use all features defined in the IEC 104 standard, or the sensor can use a small subset for simpler applications.

The 104 protocol settings are found in the settings.conf file under the "iec104" section. These shall match the protocol settings defined in the SCADA client, and must be in compliance with the IEC standard. Interoperability requirements can be documented by a 104 client by filling out Chapter 9 in the IEC 104 standard. An overview of the parameters defined in the sensor is listed in table 8.

Setting	Meaning	Default
t1	Time-out of send or test APDUs.	16
t2	Time-out for acknowledges in case of no data messages, t2<t1.	11
t3	Time-out for sending test frames in case of a long idle state.	21
k	Maximum difference receive sequence number to send state variable.	8
w	Latest acknowledge after receive w I format APDUs.	12
common_address	IEC 104 address of sensor.	1
background_scan	Interval in seconds between transmission of digital data points.	1800
cyclic	Interval in seconds between transmission of analogue data points.	600
scan	Data change scan interval in milliseconds for sending event-triggered data.	500
clock_validity	Time-tagged client commands validity period in seconds.	600
redundancy	Max number of redundant connections as defined by IEC 104.	2

Table 8: IEC-104 parameters.

Three *.csv* files are used to map sensor measurements to data points accessible by an IEC 104 client. A macro enabled Excel file is used to generate these *.csv* files, and all changes to the data mapping should be applied in the Excel file. There are three sheets in the Excel file, and each generate one .csv file. The sheets are called "iec104_analogue", "iec104_digital" and "iec104_commands", which define analogue and digital measurement mapping to the IEC 104 protocol. An example snapshot of the "iec104_analogue" sheet is shown in figure 21. The "iec104_commands" is currently not used for the LSA , and will not be detailed further.

- **address** The address of the data point, [1-65535].
- **type** The IEC 104 type (see interoperability list in IEC 60870-5-104 chapter 9).
- **data** Internal sensor variable name.
- **interrogation** The interrogation group this data point belongs to. Can be "global" or "groupX", X=[1-16].
- **spontaneous** Set to true if data point should be transmitted on change.

	A	B	C	D	E	F	G	H	I	J	K
1	address	type	data	interrogation	spontaneous	cyclic	absmin	absmax	rel	interval	desc
2	100	M_ME_TE_1	measurements.alarm_state	global	TRUE	TRUE	0	0	0	0	The alarm state, 1=active (alarm), 0=inactive (alarm cleared)
3	1000	M_ME_TF_1	measurements.event_id	global	TRUE	TRUE	0	0	0	0	Reference ID for the discharge event
4	1001	M_ME_TF_1	measurements.current_peak	global	TRUE	TRUE	0	0	0	0	The maximum absolute current of the lightning, in kA
5	1002	M_ME_TF_1	measurements.rise_time	global	TRUE	TRUE	0	0	0	0	The rise time from 10% to 90% of the peak current, in microseconds
6	1003	M_ME_TF_1	measurements.charge_flash	global	TRUE	TRUE	0	0	0	0	The total charge released in the lightning, in C
7	1004	M_ME_TF_1	measurements.main_specific_energy	global	TRUE	TRUE	0	0	0	0	The specific energy of the main strike, in kJ/Ohm
8	1005	M_ME_TF_1	measurements.unix_s_HWORD	global	TRUE	TRUE	0	0	0	0	Latest event time stamp, UNIX format, high word
9	1006	M_ME_TF_1	measurements.unix_s_LWORD	global	TRUE	TRUE	0	0	0	0	Latest event time stamp, UNIX format, low word
10	1007	M_ME_TF_1	measurements.average_steepness	global	TRUE	TRUE	0	0	0	0	Average steepness of the rising edge of the main strike, in kA/us
11	1008	M_ME_TF_1	measurements.polarity	global	TRUE	TRUE	0	0	0	0	The polarity of the lightning event, 1=positive, -1=negative
12	1009	M_ME_TF_1	measurements.receptor_mass_loss	global	TRUE	TRUE	0	0	0	0	Estimated mass loss of blade receptors, in gram
13	1020	M_ME_TF_1	measurements.inductive_energy_index	global	TRUE	TRUE	0	0	0	0	Index for the inductive energy potential of the full lightning event, proportional to J
14	1021	M_ME_TF_1	measurements.specific_energy	global	TRUE	TRUE	0	0	0	0	The total specific energy of lightning event, in kJ/Ohm
15	1022	M_ME_TF_1	measurements.charge_short	global	TRUE	TRUE	0	0	0	0	The maximum charge of any lightning pulse with a duration greater than 2ms, in C
16	1023	M_ME_TF_1	measurements.charge_long	global	TRUE	TRUE	0	0	0	0	The maximum charge of any lightning pulse with a duration less than 2ms, in C
17	1024	M_ME_TF_1	measurements.subsequent_current_peak	global	TRUE	TRUE	0	0	0	0	The maximum current peak of the subsequent strokes, in kA
18	1025	M_ME_TF_1	measurements.subsequent_rise_time	global	TRUE	TRUE	0	0	0	0	The minimum rise time of the subsequent strokes, in us
19	1026	M_ME_TF_1	measurements.subsequent_average_steepness	global	TRUE	TRUE	0	0	0	0	The maximum average steepness of the rising edge of the subsequent strokes, in kA/us
20	1027	M_ME_TF_1	measurements.pulse_count	global	TRUE	TRUE	0	0	0	0	The number of lightning strikes (main and subsequent) within the measurement
21	1028	M_ME_TF_1	measurements.severity_lpl_I	global	TRUE	TRUE	0	0	0	0	Severity in percent, based on Lightning Protection Level I (IEC 62305-1) parameters
22	1100	M_ME_TE_1	state.processor_temperature	global	TRUE	TRUE	0	0	0	0	Temperature in degree Celcius of the processor core
23	1101	M_ME_TE_1	state.sntp_sync_active	global	TRUE	TRUE	0	0	0	0	Status for time synchronization via SNTP
24	1102	M_ME_TE_1	state.sensor_error	global	TRUE	TRUE	0	0	0	0	Status of the sensor operational state

Figure 21: iec104_analogue.

- **cyclic** Set to true if data point should be sent periodically.
- **absmin** Minimum absolute change in data value to trigger spontaneous transmission. This is useful for avoiding sending a data point too often when the value is low.
- **absmax** Maximum absolute change in data value to trigger spontaneous transmission.
- **rel** Relative change in percent of the data value to trigger spontaneous transmission. For example, setting rel = 10 for a data point with value 500 triggers transmission at 450 or 550.
- **desc** A short description of the data point and unit.

Refer to figure 22 for a graphical example of the transmission thresholds absmin, absmax and rel.

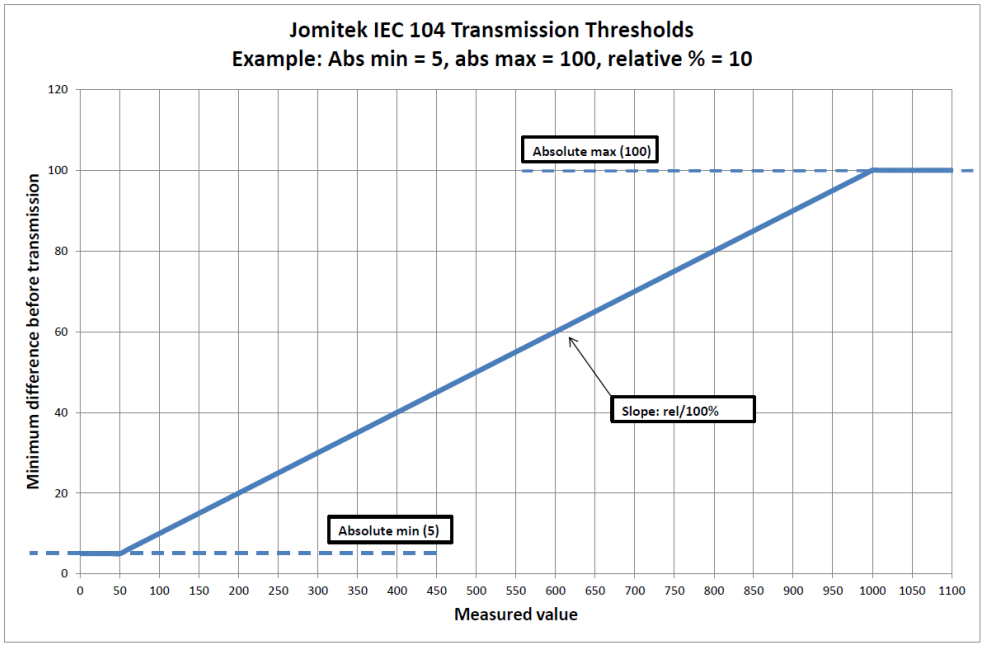


Figure 22: absmin, absmax and rel.

Any change in a digital value triggers transmission given spontaneous is set to true for this data point in the "iec104_digital" sheet. For this reason the "iec104_digital" sheet does not define absmin, absmax and rel

columns. Also, the "iec104_digital" sheet replaces the "cyclic" column found in the analogue sheet with "background". The use of the "cyclic" column for analogue values is similar to the use of "background" column because they are both used to trigger transmission at fixed intervals.

Since the IEC 104 protocol uses TCP/IP, it may in some cases be useful to look into the communication stream using Wireshark[1] for troubleshooting purposes.

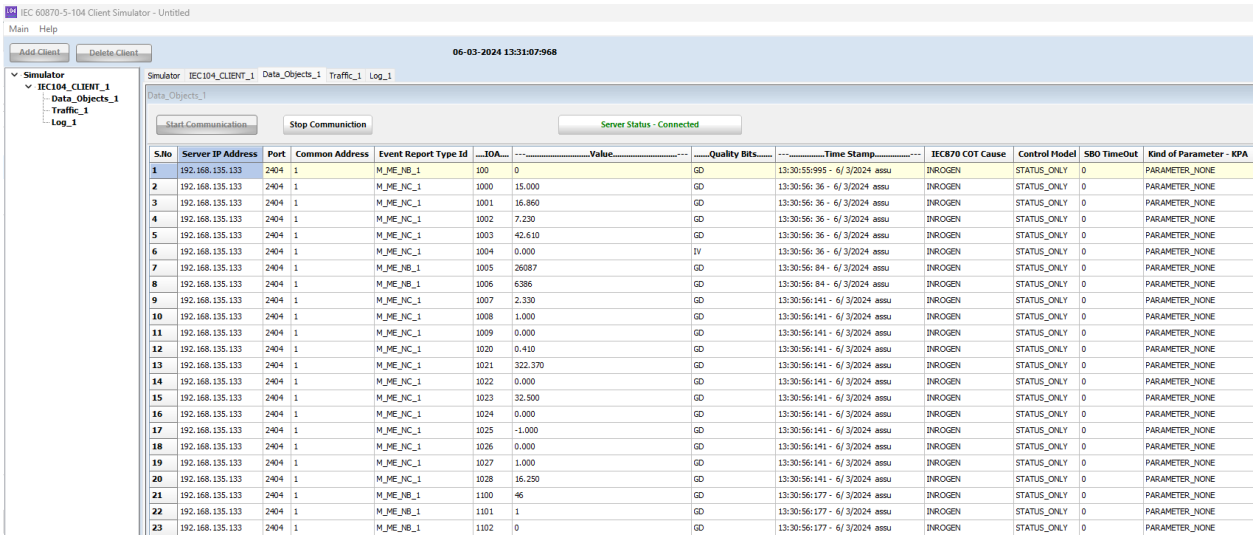
9.1 Time stamp readout and interpretation example

When a strike events occur, the details of the event is calculated (takes 1-2 minutes for a 1000ms recording) and the result can be seen in the web overview. See figure 14 as an example.

The IEC 104 read out always presents the latest recorded strike. As there may be a risk of 2 or more strikes being recorded without reading out the earlier strike via IEC 104, the user can follow the event number of the active strike being displayed on the IEC-104 readout. This makes it possible to check if a readout has been missed. The data can be read out using the web interface, or the full event log file via FTP or WebDAV.

Time is stored in UNIX time format. This is a 32 bit integer. As IEC 104 can read out 16 bit integers, the time is stored in 2 words, a high- and a low word. This is illustrated in the .csv file that defines the IEC 104 variables, see figure 21.

When performing a general interrogation command in IEC 104 the result is shown in figure 23. In this example, the read out of the high word (addr. 1005) is 26087 in decimal format or in hex format, 65E7. The low word (addr. 1006) is 6386(dec) = 18F2 (hex). The combination into a 32-bit hex number is 65E718F2, equal to the decimal number 1,709,644,018.



S.No	Server IP Address	Port	Common Address	Event Report Type Id	....IOA....	---.....Value.....---	.....Quality Bits.....	---.....Time Stamp.....---	IEC870 COT Cause	Control Model	SBO TimeOut	Kind of Parameter - KPA
1	192.168.135.133	2404	1	M_ME_NB_1	100	0	GD	13:30:55:995 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
2	192.168.135.133	2404	1	M_ME_NC_1	1000	15.000	GD	13:30:56: 36 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
3	192.168.135.133	2404	1	M_ME_NC_1	1001	16.860	GD	13:30:56: 36 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
4	192.168.135.133	2404	1	M_ME_NC_1	1002	7.230	GD	13:30:56: 36 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
5	192.168.135.133	2404	1	M_ME_NC_1	1003	42.610	GD	13:30:56: 36 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
6	192.168.135.133	2404	1	M_ME_NC_1	1004	0.000	IV	13:30:56: 36 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
7	192.168.135.133	2404	1	M_ME_NB_1	1005	26087	GD	13:30:56: 84 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
8	192.168.135.133	2404	1	M_ME_NB_1	1006	6386	GD	13:30:56: 84 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
9	192.168.135.133	2404	1	M_ME_NC_1	1007	2.330	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
10	192.168.135.133	2404	1	M_ME_NC_1	1008	1.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
11	192.168.135.133	2404	1	M_ME_NC_1	1009	0.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
12	192.168.135.133	2404	1	M_ME_NC_1	1020	0.410	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
13	192.168.135.133	2404	1	M_ME_NC_1	1021	322.370	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
14	192.168.135.133	2404	1	M_ME_NC_1	1022	0.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
15	192.168.135.133	2404	1	M_ME_NC_1	1023	32.500	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
16	192.168.135.133	2404	1	M_ME_NC_1	1024	0.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
17	192.168.135.133	2404	1	M_ME_NC_1	1025	-1.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
18	192.168.135.133	2404	1	M_ME_NC_1	1026	0.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
19	192.168.135.133	2404	1	M_ME_NC_1	1027	1.000	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
20	192.168.135.133	2404	1	M_ME_NC_1	1028	16.250	GD	13:30:56:141 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
21	192.168.135.133	2404	1	M_ME_NB_1	1100	46	GD	13:30:56:177 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
22	192.168.135.133	2404	1	M_ME_NB_1	1101	1	GD	13:30:56:177 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE
23	192.168.135.133	2404	1	M_ME_NB_1	1102	0	GD	13:30:56:177 - 6/ 3/2024 assu	INROGEN	STATUS_ONLY	0	PARAMETER_NONE

Figure 23: Generel interrogation command result

Entering this decimal number into a UNIX time calculator like: http : //www.onlineconversion.com/unix_time.htm the result shown in figure 24 is seen to match the title line time stamp as presented in the web read out in figure 25.

[1] https://www.wireshark.org/

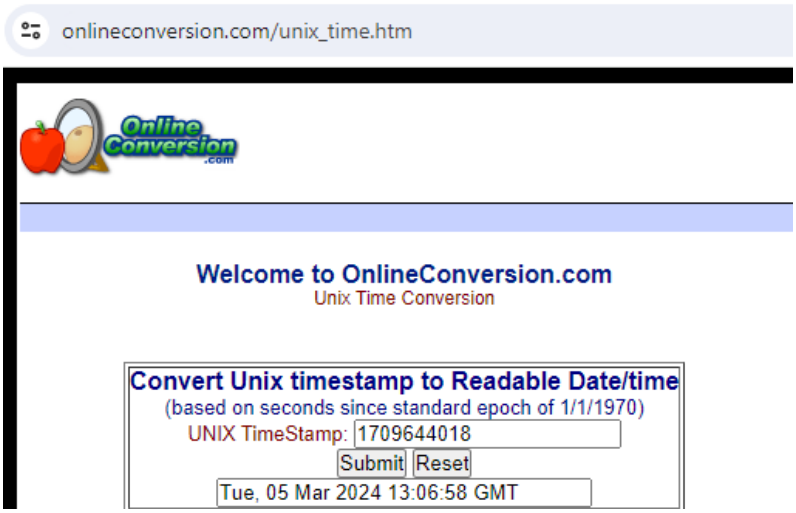
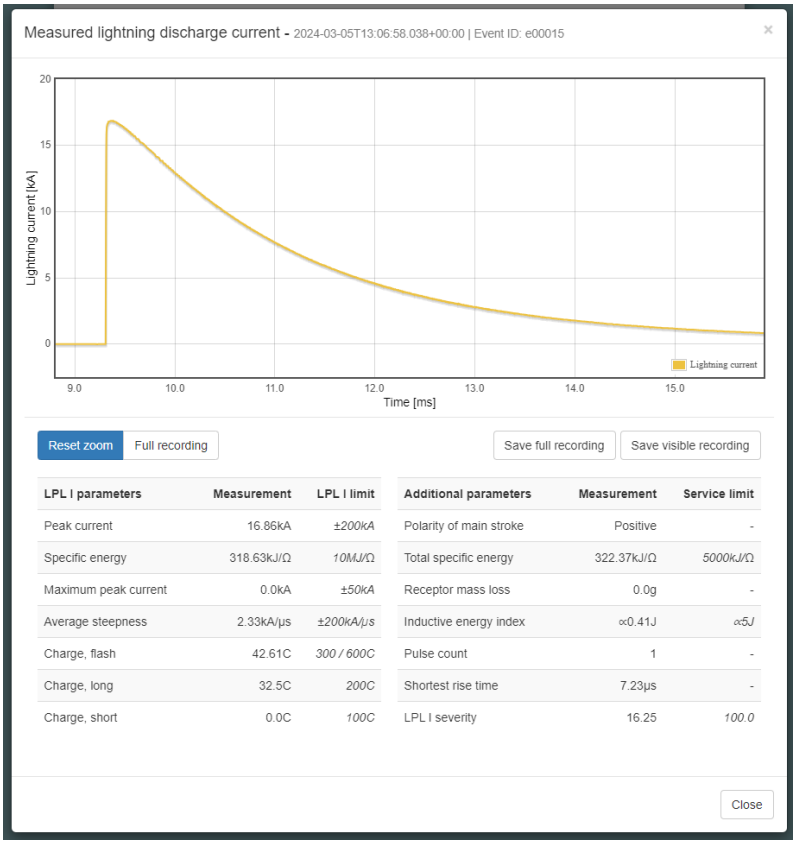


Figure 24: UNIX time conversion



LPL I parameters	Measurement	LPL I limit	Additional parameters	Measurement	Service limit
Peak current	16.86kA	*±200kA*	Polarity of main stroke	Positive	-
Specific energy	318.63kJ/Ω	*10MJ/Ω*	Total specific energy	322.37kJ/Ω	*5000kJ/Ω*
Maximum peak current	0.0kA	*±50kA*	Receptor mass loss	0.0g	-
Average steepness	2.33kA/µs	*±200kA/µs*	Inductive energy index	∝0.41J	*∝5J*
Charge, flash	42.61C	*300 / 600C*	Pulse count	1	-
Charge, long	32.5C	*200C*	Shortest rise time	7.23µs	-
Charge, short	0.0C	*100C*	LPL I severity	16.25	*100.0*

Figure 25: Example event viewed in the LSA web interface

10 MODBUS configuration

As an alternative to IEC 60870-5-104, MODBUS TCP is supported, using the address table below, see table 9:

Description	Unit	Range	Address	MODBUS fct. code
Software version	Number	0-65535	0	4 (read)
Serial number	Number	0-65535	1	4 (read)
Alarm status	Boolean (1=alarm)	0-1	100	4 (read), 6 (write)
Service alarm, peak current	Boolean (1=alarm)	0-1	101	4 (read)
Service alarm, main specific energy	Boolean (1=alarm)	0-1	102	4 (read)
Service alarm, subsequent peak current	Boolean (1=alarm)	0-1	103	4 (read)
Service alarm, average steepness	Boolean (1=alarm)	0-1	104	4 (read)
Service alarm, charge, flash	Boolean (1=alarm)	0-1	105	4 (read)
Service alarm, charge, long	Boolean (1=alarm)	0-1	106	4 (read)
Service alarm, charge, short	Boolean (1=alarm)	0-1	107	4 (read)
Service alarm, total specific energy	Boolean (1=alarm)	0-1	108	4 (read)
Service alarm, inductive energy index	Boolean (1=alarm)	0-1	109	4 (read)
Service alarm, general	Boolean (1=alarm)	0-1	110	4 (read)
Event number	Number	1-65535	1000	4 (read)
Latest peak current	kA	-32768-+32767	1001	4 (read)
Latest rise time	usec	0-65535	1002	4 (read)
Latest charge, flash	C	0-65535	1003	4 (read)
Latest main specific energy	kJ/Ohm	0-65535	1004	4 (read)
Latest event time stamp, HW	Unix time	0-65535	1005	4 (read)
Latest event time stamp, LW	Unix time	0-65535	1006	4 (read)
Latest maximum average steepness	kA/usec	-32768-+32767	1007	4 (read)
Latest polarity	1=pos., -1=neg.	-1 to 1	1008	4 (read)
Latest receptor mass loss	miligram	0-65535	1009	4 (read)
Keep alive counter	Seconds	0-65535	1010	4 (read)
Current time stamp, seconds, HW	Unix time	0-65535	1012	4 (read)
Current time stamp, seconds, LW	Unix time	0-65535	1013	4 (read)
Current time stamp, subsecond	msec	0-999	1014	4 (read)
Latest event time stamp, subsecond	msec	0-999	1015	4 (read)
Time since last alarm	1/10th seconds	0-65535	1016	4 (read)
Time since last alarm	milliseconds	0-65535	1017	4 (read)
Reserved for future use, returns 0	N/A	0	1018	4 (read)
Reserved for future use, returns 0	N/A	0	1019	4 (read)
Latest inductive energy index	$\propto$J	0-65535	1020	4 (read)
Latest total specific energy	kJ/Ohm	0-65535	1021	4 (read)
Latest charge, short	C	0-65535	1022	4 (read)
Latest charge, long	C	0-65535	1023	4 (read)
Latest subsequent current peak	kA	-32768-+32767	1024	4 (read)
Latest subsequent rise time	usec	0-65535	1025	4 (read)
Latest subsequent avg. steepness	kA/usec	-32768-+32767	1026	4 (read)
Latest pulse count	#	1-65535	1027	4 (read)
Latest LPL I severity	%	0-65535	1028	4 (read)
Temperature inside box	Degree C	-200 - 200	1100	4 (read)
SNTP time synchronization	Boolean (1=sync.)	0-1	1101	4 (read)
Sensor error state	Boolean (1=error)	0-1	1102	4 (read)
Event summary start number	Number	1-65535	2000	4 (read), 6 (write)
Summary, maximum peak current	kA	-32768-+32767	2001	4 (read)
Summary, maximum subsequent peak current	kA	-32768-+32767	2002	4 (read)
Summary, maximum average steepness	kA/usec	-32768-+32767	2003	4 (read)
Summary, maximum subsequent average steepness	kA/usec	-32768-+32767	2004	4 (read)
Summary, maximum charge flash	C	0-65535	2005	4 (read)
Summary, maximum charge long	C	0-65535	2006	4 (read)
Summary, maximum charge short	C	0-65535	2007	4 (read)
Summary, maximum main specific energy	kJ/Ohm	0-65535	2008	4 (read)
Summary, minimum rise time	usec	0-65535	2009	4 (read)
Summary, minimum subsequent rise time	usec	0-65535	2010	4 (read)
Summary, sum of charge, flash	C	0-65535	2011	4 (read)
Summary, sum of the inductive energy index	$\propto$J	0-65535	2012	4 (read)
Summary, sum of specific energy	kJ/Ohm	0-65535	2013	4 (read)
Summary, sum of pulse counts	Number	0-65535	2014	4 (read)
Summary, sum of receptor mass loss	gram	0-65535	2015	4 (read)
Summary, count of negative polarity events	Number	0-65535	2016	4 (read)
Summary, count of positive polarity events	Number	0-65535	2017	4 (read)

Table 9: MODBUS address table

The alarm register, 100, will be updated immediately after a strike is detected. The associated lightning event parameters and service alarms are updated when internal post processing is completed, which for a 1000ms event recording takes 1-2 minutes. Note that register 1016 is valid for 1.8 hours (65535/10 = 6535 seconds), while register 1017 equivalently is valid for 65.535 seconds, after which the register values are automatically reset to 0.

In order to clear an alarm event via MODBUS 0x4341 (17217 decimal) must be written to address 100. This command will also clear all service alarms.

The Unix time stamp should be interpreted similarly to the description in section 9.1. The meaning of 'Latest' in above table is a reference to the latest recorded lightning strike. Data for earlier strikes should either already have been retrieved, or they can be accessed via FTP, WebDAV or the LSA web interface, or in summary form presented in the 2000 address series.

An alternative to function code 4 (read register) is function code 3. Function code 16 (write multiple registers), may be used instead of function code 6 (write single register), by specifying a single register in the command.

11 Firmware and software updates

11.1 Boot loading sequence

During startup the LSA checks the `/service/software_update` folder for the presence of a **software update file** or **firmware image file**.

- A **software update file** (`software.tar.gz`) contains a folder structure image that, when unpacked, overwrites the LSA file system. The unpacked file system may include a **firmware image file** in the software update folder.
- A **firmware image file** (`image.bin`) is a binary file which contains the low level functionality needed to run the LSA device.

If a **software update file** is found, it is unpacked and installed automatically, during the next sensor reboot. Such a reboot will therefore often take 2-3 minutes, compared with a standard reboot time of approximately 30 seconds.

If a **firmware image file** is found, the boot loader will search for the presence of a **checksum file** (`checksum.txt`) which is used to verify the integrity of the firmware image. If the calculated checksums match, the firmware is decrypted and its binary instructions copied to the microprocessor which will reboot upon completion, thus finalizing the firmware update process. This process ensures all firmware updates are end-to-end secure, and only updates issued by Jomitek will be possible to load.

After boot loading completes, the system will proceed to initiate further low-level processes after which the Lua scripting engine and web server will be started. At this point the system will be fully operational.

11.2 Sensor updates

The software on the LSA can be updated in four simple steps:

1. Download the newest update file from `http://jomitek.dk/downloads/device_software_update`. The page is password protected, use username: *jomitek* and password: *jomitek*.
2. Connect to the LSA through FTP, WebDAV, using curl or the Jomitek Device Locator, see sections 12.2, 12.3, 7.2 or 7.1 respectively.
3. Transfer the update file, `software.tar.gz`, to the `/service/software_update` directory.
4. Reboot the LSA , e.g. via the web interface, and wait for the boot loading sequence to automatically apply the update.

The LSA will now restart and apply the software update.

For automated mass updates, please refer to `http://jomitek.dk/downloads/tools`, where an Excel and WinSCP-based tool is provided for reference. The mass updates are based purely on WebDAV, i.e. default port 80, which should help avoid many issues in relation to firewall configurations, and related security bottlenecks. Other scripting and file transfer tools may be used based on the example provided, or as otherwise suggested using curl in section 7.2.

12 Advanced user interfaces

12.1 Telnet command line interface

Meant primarily for super users, the LSA can be accessed and configured via a limited command line interface using Telnet. This interface is accessed by connecting to the sensor IP address on TCP port 23 using a standard Telnet client. It is recommended to use Putty[2] which is open source and free to use.

Be sure to enable the 'Implicit CR in every LF' and 'Implicit LF in every CR' options when configuring Putty.

A list of Telnet commands for the LSA is listed by typing 'help' in a terminal, when connected to a sensor.

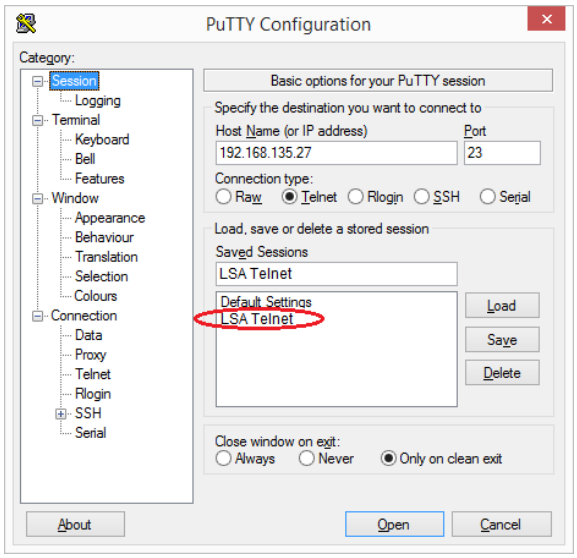


Figure 26: Putty Telnet Session configuration.

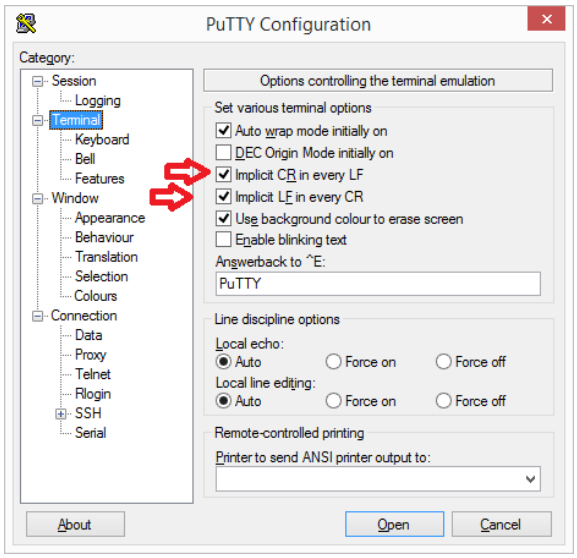


Figure 27: Putty Telnet Terminal configuration.

[2] `http://www.putty.org/`

Figure 28: The Telnet command line interface.

The Telnet access may be used for SCADA interface testing, as it is possible to issue a 'trig' command which initiates a lightning event recording, even though the configured trigger level is not exceeded.

As an alternative to a software based test, a simple manual test is to use a fairly strong permanent magnet (e.g. one of those used for mounting). Let it pass over the sensor box by hand, with the pass lasting less than a second. It should then create an event detection, if the trigger level is exceeded. A more controlled and well defined test can be obtained using the Jomitek Lightning Pulse Generator, as noted in section 2.6. Note that the trigger level setting should be <10kA for either the permanent magnet or Jomitek Lightning Pulse Generator to be detected.

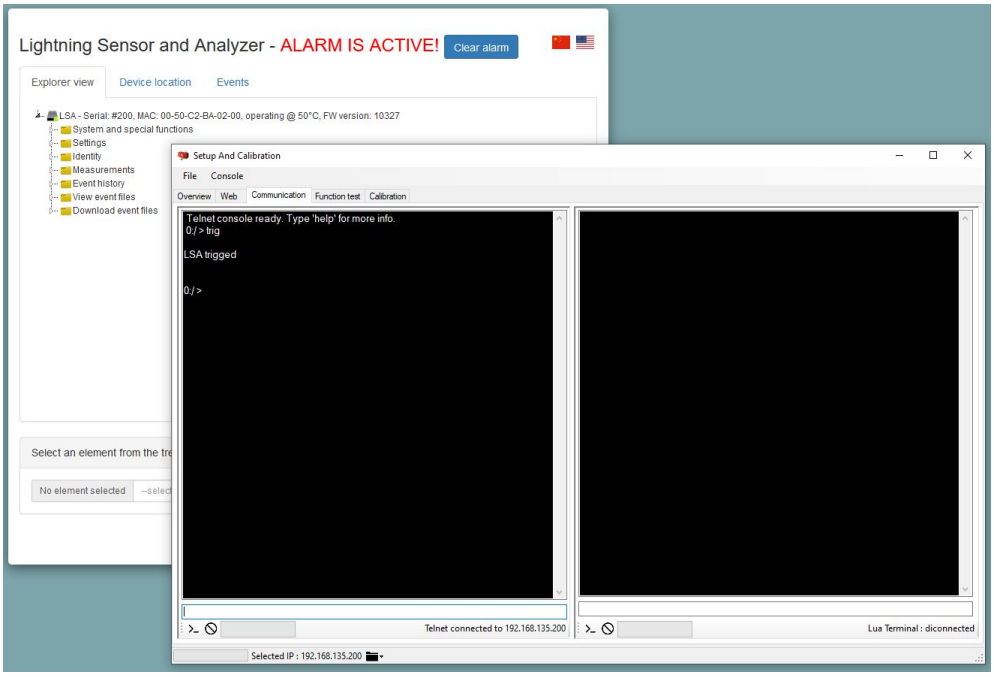


Figure 29: The Telnet 'trig' command.

12.2 FTP file transfer interface

The internal memory on the LSA can be accessed via the FTP protocol on TCP port 21. Use an FTP client program (e.g. FileZilla[3]) and log in with default username: *service* and password: *service1234*.

When connected you will have access to these folders.

- The `software_update` folder where software update files can be uploaded.
- The `log` folder where various log files are placed by the sensor system.
- The `data` folder where all stored measurement data are placed by the sensor system.
- The `conf` folder where configuration files and scripts are stored.

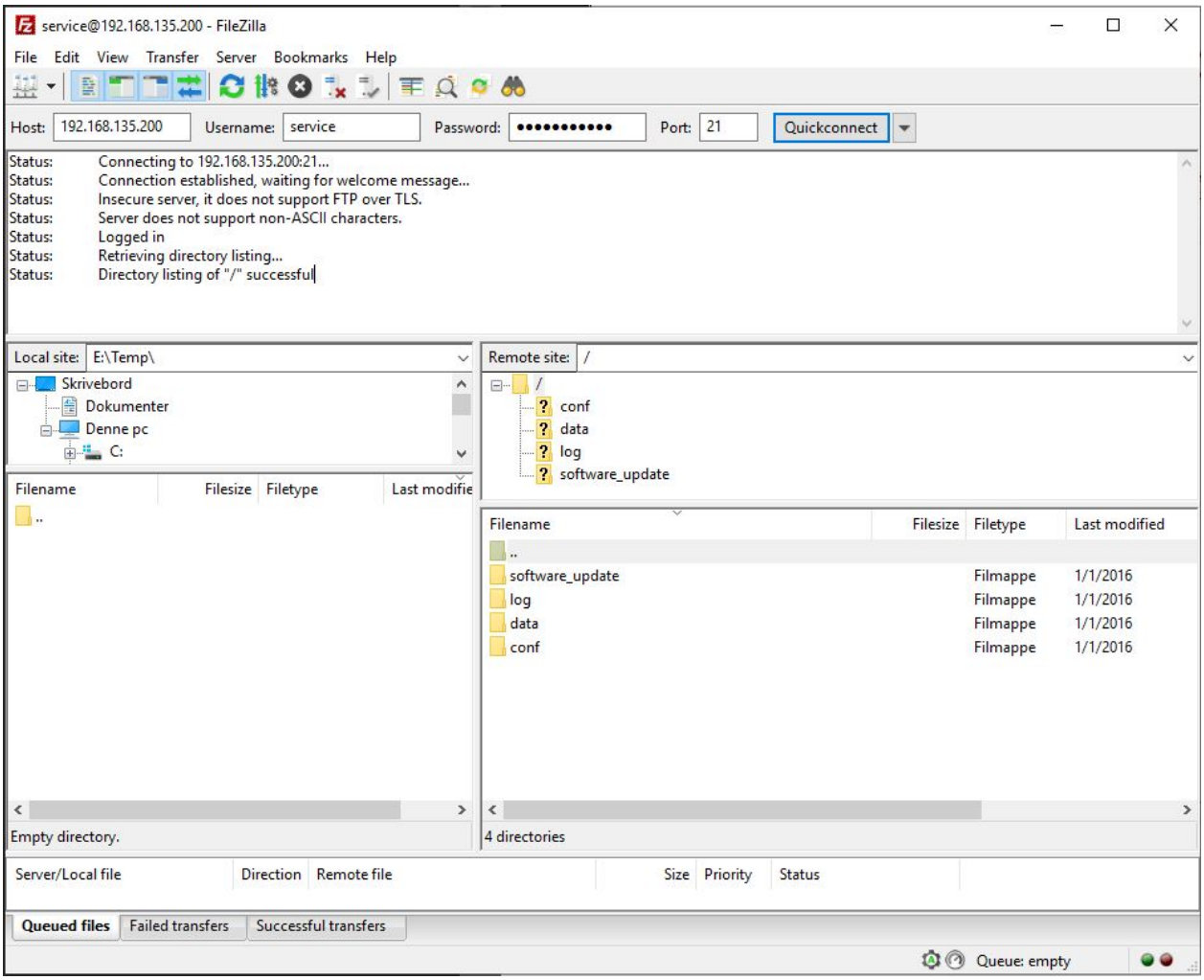


Figure 30: FTP connection to the LSA shown with the FileZilla FTP client.

[3] `https://filezilla-project.org/`

File Upload is supporting upload one file at a time, so set the sender to non-simultaneous file-transfer

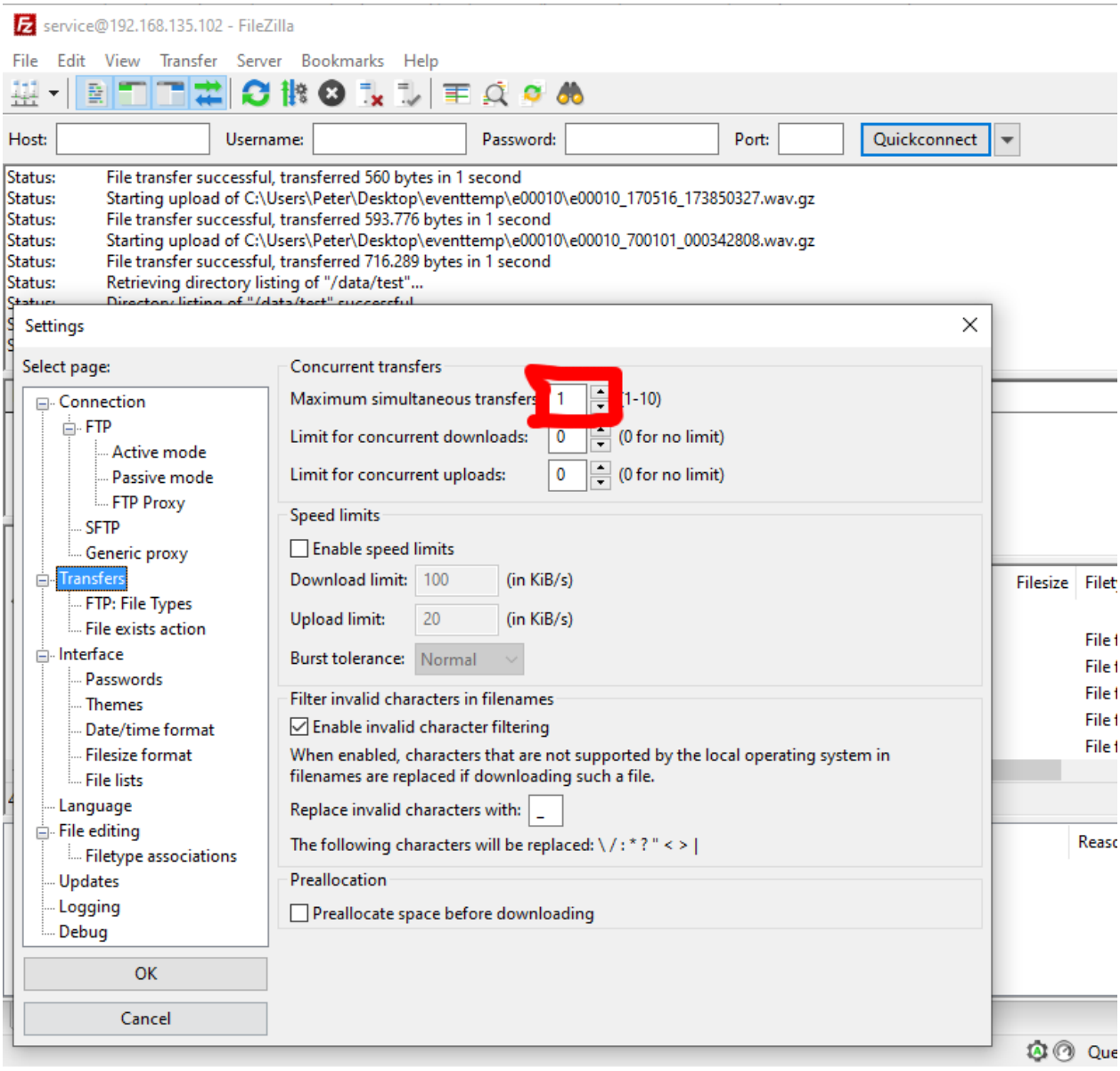


Figure 31: FTP configuration for file upload via FileZilla.

12.3 WebDAV file transfer interface

The LSA can be accessed via the WebDAV protocol on TCP port 80. This presents the advantage, compared to FTP, of using the same default port as is used for web browsing (it is an extension to the HTTP protocol) which simplifies firewall configuration requirements. Use a WebDAV client program (e.g. WinSCP) and log in with default username: *service* and password: *service1234*.

Note, that it is important to connect to the subfolder '/dav' as shown in the figure.

The file structure is equivalent to the description for FTP, see section 12.2.

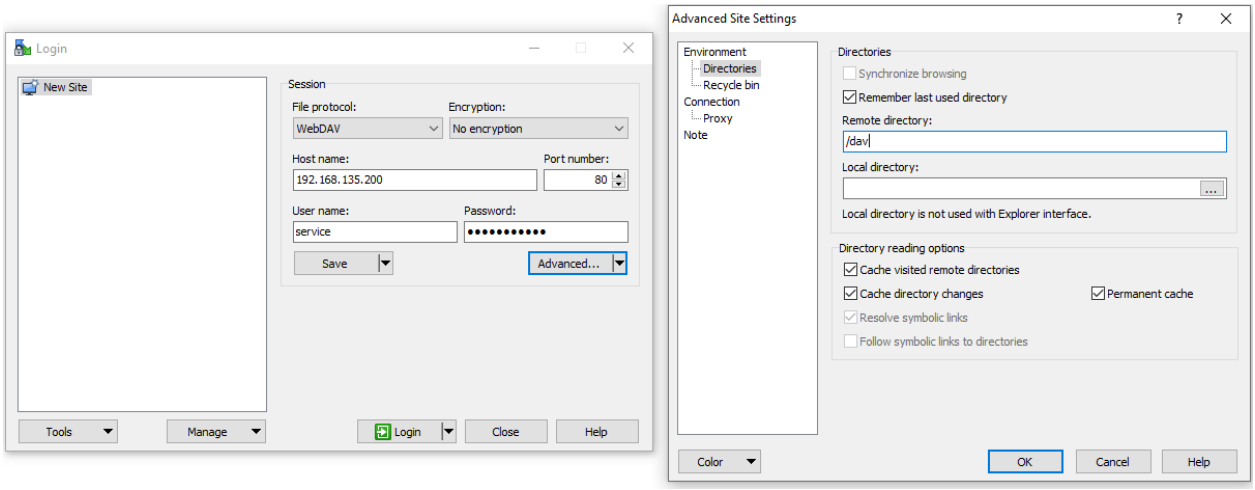


Figure 32: WebDAV connection setup to the LSA shown with the WinSCP client.