PHYSICUS
Silvanska 27, 841 04 Bratislava, Slovakia
tel: +421-905-852 073 email: physicus@physicus.eu

LogboxSE technical documentation.
RED compliance 2025. Confidential

Contents

1. Technical documentation

This documentation is produced for LogboxSE datalogger. It describes security operation of the product in detail. The final goal is to document all aspects of cyber security and conformance with RED Directive 2022/30/EU (Radio Equipment Directive).

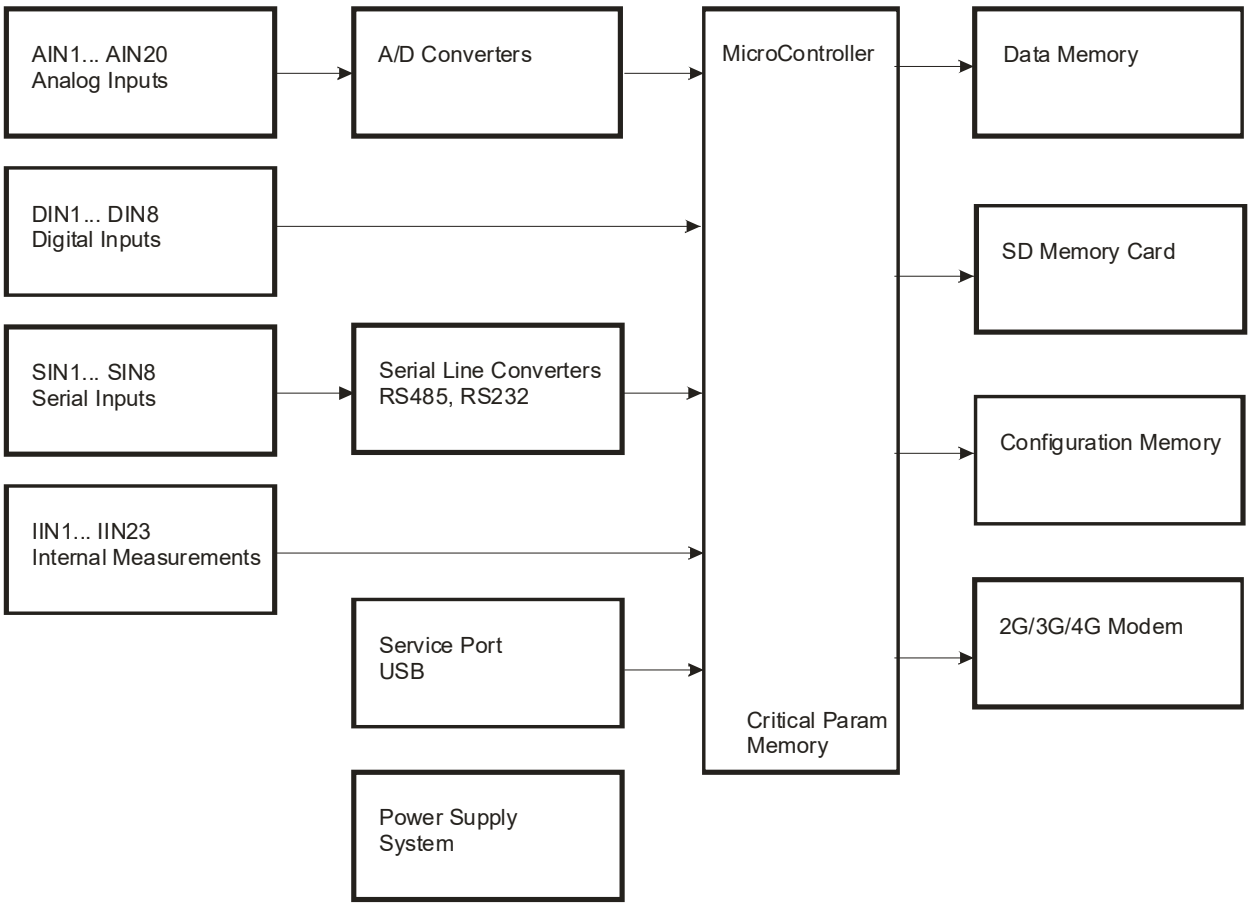
1.1 Product Description

LogboxSE datalogger is a custom built embedded device designed to measure, process and log measured parameters from external sensors. It can include temperature, humidity, global radiation, wind speed and direction and others. Device is fully user configurable and can measure almost any analog, digital or serial sensors. Data are stored in internal memory and further transmitted over the mobile network to user selected server (SMTP or FTP). It uses internal PLS63-W cellular modem module from Telit.

1.2 Intended use

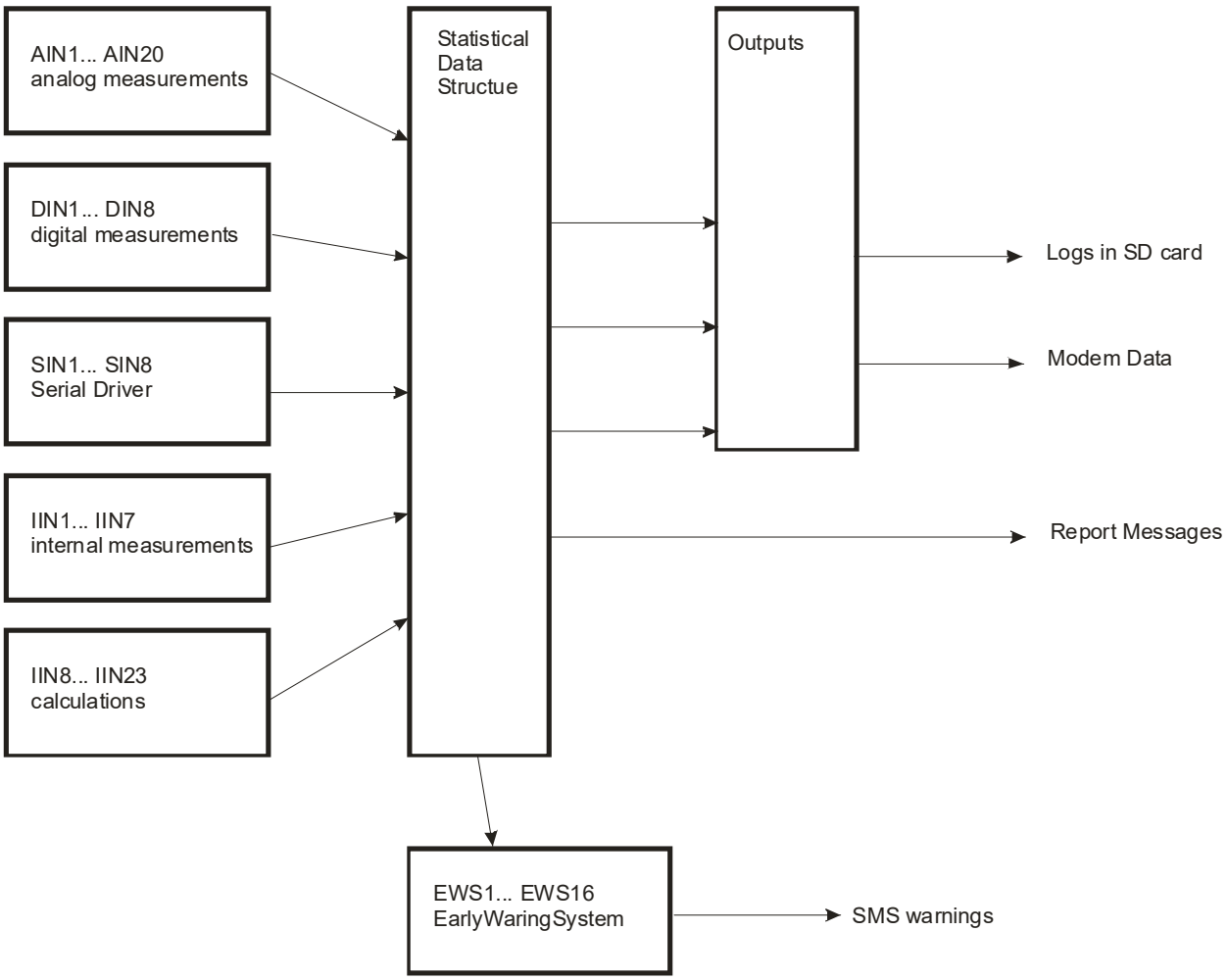
LogboxSE is used in environmental monitoring in outdoor locations. Periodically or on demand it can transmit data over the mobile network to the user selected server for further data storage and post processing or analyses. It is not intended for use in life critical applications.

1.3 Block Diagram



Datalogger block diagram shows most important blocks. In respect to security assessment, there are 4 communication ports available for the user: COM1 (RS485 or RS232), COM2 (RS232), USB service port and Modem. COM 1 is reserved to communication with external serial sensors and it is not possible to access datalogger service mode.

1.4 Data Architecture



All input data from sensors are recalculated to engineering units at the time of measurement. Then, saved in statistical data structure, which include min, max, …. At Logging interval all data are processed (calculated averages, min, max and stdev) and produced to output. Output format is string and is saved in internal memory (used in modem remote data transmission), saved in SD memory card and sent to COM2 as live data report. If Early Warning System (EWS) is configured, data are in parallel processed and warning are checked. Once any warning is activated, system can generate warning SMS message.

All of these options are user configurable.

1.5 Communication Channels

From block diagram it is obvious that datalogger provides following communication channels:

COM1 – it is hardware RS232 or RS485 (user configurable) serial line. It is designed for communication with external sensors. Thru this port it is not possible to enter into Service Mode, and therefore it is a safe communication channel.

COM2 – it is hardware RS232 serial line. Primary intention is for sending data to upper system (SCADA) or local observer. User can use this communication port to enter Service Mode and make configuration changes.

USB – it is hardware composite device, Mass Storage Device (SD card) and Virtual COM Port. It is designed for configuration changes in datalogger. Setup software is used to read, write and make new configurations.

Modem – 2G/3G/4G mobile network communication channel. Designed primary to send data over mobile network to user defined server. At the moment logger supports sending data over emails (SMTP, SMTPS) or FTP (FTP, FTPS). If configured to SMTPS or FTPS server, it uses TLS data encryption.

Secondary use of modem is to retrieve configuration file from server (FTP/FTPS only) remotely.

Alternatively, if configured, modem can act as server on port 10001. From remote site user can connect to this port and see either live data or enter Service Mode to make changes in configuration.

From security point of view, user can change setup parameters in Service Mode only. Every communication channel enabled for Service Mode is processed in firmware the same way. It does not matter if service command comes from COM2 or USB, or even from FTP downloaded file over mobile network. All of these attempts are handled and protected the same way, which will be in following text.

From RED Directive 2022/30/EU and EN 18031-1:2024 European Standard perspective logger can be user configured to maximum safety and protection from unauthorized attempt to change any configuration parameter. On the other hand, if the user does not require this kind of protection, logger can be configured to standard operation.

1.6 Firmware description

Firmware is based on real time operating system. It uses upto 50 tasks and upto 60 events. Firmware is optimized to low power consumption. If there is no active task, microcontroller is turning to low power mode.

All tasks are independent. It makes system more robust and immune to time sync issues.

Used third party software components are following:

- Salvo ver 3.6 - operating system
- FatFS ver 0.11a - file system for memory card
- USB ver 5.00 – composite driver for MSC and CDC

1.7 Security Features

Basic idea to protect datalogger from unauthorized configuration access is to provide password. In logger configuration parameter Security must be set. In this case once the logger enters Service Mode, user MUST enter SecPassConfirm parameter. Otherwise, any other command will be ignored. There is one exception – SetDefaultConfig command. It must be enabled, because if the user will forget SecPassword there must be a way how to return to factory default configuration. (Of course, factory default configuration does not contain any credentials and configures only basic operation for the device. Factory default is set with default password of serial number of the device.) Settings like Security and internal “flags” are stored in separate part of the memory. And it is not overwritten during firmware update procedure. All credentials are stored encrypted in configuration memory. As mentioned previously, all parameters are user configurable.

Datalogger still enables no security protection operation. It is a requirement from the users, because they can use the device in safe environment (personal access control to installation location, VPN networks, sometimes user does not user modem communication at all) and they control potential security risks on system level.

EXAMPLE 1: user does not use security. Using Setup software, user is able to read configuration, alter any parameter and write new configuration to the logger.

EXAMPLE 2: security is enabled. In Setup software user need to enter SecPassConfirm. Then read configuration from datalogger. If the password is not correct, logger will not response to the commands. If password is correct, logger will provide full configuration. Once the configuration is changed and finalized, Password MUST be entered correctly. Then user can send configuration to the logger. If Password is not correct, logger will not response to any entered command.

This principle applies to any of used communication channels. For example, if Security is enabled and logger is configured to download new configuration from server, in configuration file there must be first command SecPassConfirm. Otherwise, downloaded configuration will be ignored.

Summary of security features and options.

Security risk source	**Required operation**	**Note**
Service Mode unauthorized access	Security set SecPassConfirm entered Applies to COM2, USB, remote FTP config file download	If not correct Password, no response to commands and exit service mode. Only SetDefaultConfig command accessible
Credentials stored in memory	Encrypted	Stored in separate part of configuration memory on various locations
Data transfer	FTPS or SMTPS server used	TLS data encryption based on modem module implementation. TLS supports version 1.0. In the future there will be used PLS63 modem module, which supports TLS 1.1, 1.2 and 1.3 versions.
Remote access from network	The same as entering Service mode Using VPN	User can even disable remote access to the logger. Or it can be limited to short time over each day (10 minutes). Not accessible from public internet

1.8 Firmware update

Firmware update is made only occasionally. As a manufacturer we do not prefer firmware updates, as we believe testing our devices is extensive and released versions are always after several months of real operation on various testing stations.

Firmware update is necessary mostly only in the case of new Serial Driver was added to firmware. It has no impact on security features, as Serial Driver communication is on COM1 port and it has no access to Service Mode.

Firmware update image is supplied with additional file containing hash SHA256, which ensures file integrity. It us up to the user to use it.

USB interface is designed for firmware update. During this procedure, due to nature of memory capacity of microcontroller, all firmware memory is deleted and then new firmware is written to the same memory space. It is critical operation and therefore end user firmware update should be avoided, if possible. For firmware update there is small utility from microcontroller manufacturer. During firmware update, configuration parameters are not changed, as they are stored in different physical memory chip. If Security command is set, SecPassConfirm is required. This applies also to firmware update. Once the update is performed, user MUST enter SecPassConfirm again to enable datalogger full operation. This is one time procedure only.

There is no option of remote firmware update.

1.9 Compliance testing

Modem is RED compliant based on Manufacturer Declaration on Conformity. It applies to RF and EMC safety.

Cybersecurity is described in paragraph 1.8, 1.9.

2. Cyber Security Risk Assessment

Product:	LogboxSE
Manufacturer	Physicus
Date:	7.5.2025
Firmware version	15.0
Modem Module	PLS62-W, PLS63-W (Telit)
Network	2G/3G/4G
Protocol used	FTP, FTPS, SMTP, SMTPS

	Threat	**Description**	**Risk**	**Impact**	**Action**
1	Data interception	FTP/SMTP transmits data and credentials in plain text	High	Unauthorized access to data / credentials	Use of FTPS, SMTPS for encrypted transmission
2	Unauthorized access	Fixed default credentials can be guessed or leaked	High	Attacker can get access to the server or logger	User defined credentials

3	Device hijacking	Malicious party gains control and modifies data	Medium	False data	Use secure data transmission, disable remote access
4	Malicious firmware	Unauthorized firmware upload	Low	Non operative device	No remote firmware update option
5	SIM misuse	SIM card is outside the intended context	Medium	Financial costs, abuse of mobile data plan	Use VPN SIM card. Physical control of personal access
6	DoS attack on server	Device cannot connect to server	Low	No access to server	Protection on server level
7	Privacy violation	Sensitive info leak	Low	GDPR / data protection violation	Non personal data stored / transmitted

Summary

Area	**Control**
Data transmission	Transmitting data over secure FTPS or SMTPS
Credentials	Each device uses user defined credentials. No defaults. Stored locally in encrypted format.
Updates	Updates loaded locally only via USB connection. SecPassword required after firmware update.
Logging	Basic logging of modem communication possible – user configurable.
SIM protection	Use of VPN

3. EN 18031-1:2024 compliance list

(status: M – mandatory, R – recommended, C – conditional, F – feature)

Ref.	Status	Scope	Detail
5.0		**Reporting Implementation**	
5.0-1	M	A justification shall be recorded	Internal records
5.1		**No universal default passwords**	
5.1-1	MF	unique passwords or defined by the user	user defined
5.1-2	MF	pre-installed unique passwords secure	Unique default password per device, user defined
5.1-2A	R	Passwords should not be used in M2M authentication	user defined
5.1-3	MF	best practice cryptography used for authentication	Encrypted
5.1-4	MF	simple change of passwords	when identified, user can change it

5.1-5	MCF	resistance to brute-force attacks	no connection to the device from network
5.2		**Implement a means to manage reports of vulnerabilities**	
5.2-1	M	manufacturer should make vulnerability disclosure policy publicly available	in user manual
5.2-2	R	disclosed vulnerabilities action in timely manner	not applicable
5.2-3	R	manufacturer should monitor for vulnerability during support period	periodically
5.3		**Keep Software Updated**	
5.3-1	RF	immutable components should be securely updateable	N/A
5.3-2	MC	secure update mechanism	update with password
5.3-3	MF	simple update for the user	update with password
5.3-4A	RF	one secure update mechanism configurable to be automated	over USB
5.3-4B	RF	during initialization check updates	no automated update
5.3-5	RF	check for security updates	no automated update
5.3-6A	RF	user should enable/disable/postpone automatic updates	no automated update
5.3-6B	RF	if update notifications are enabled, user should be able to enable/disable	no automated update
5.3-7	MF	best practice cryptography used for updates	N/A
5.3-8	MC	security updates shall be timely	N/A
5.3-9	RF	device should verify the authenticity and integrity of sw updates	checking authenticity, supplied hash file for integrity protection
5.3-10	MV	if updates are over network, device should use trust relationship	no update over network
5.3-11	RC	user notified for security update is required	no update over network
5.3-12	RC	user notified when sw update will disrupt device functionality	no update over network
5.3-13	M	manufacturer shall publish support period	in user manual
5.3-14	RC	if no possible updates, manufacturer shall provide reason and period of hardware replacement	N/A
5.3-15A	RC	if no possible updates, device should be isolable	N/A
5.3-15B	RC	if no possible updates, device hardware should be replaceable	N/A
5.3-16	M	model should be available by user interface	reported in service mode
5.4		**Securely store sensitive parameters**	
5.4-1	MF	security parameters shall be stored securely	stored encrypted
5.4-2	MF	hard coded identity is resistant to physical, electrical or sw tampering	in special part of the memory
5.4-3	M	hard coded critical parameters shall not be used	no hard coded parameters
5.4-4	MF	critical parameters shall be produced to reduce risk	N/A
5.5		**Communicate securely**	
5.5-1	M	use best practice of cryptography	Encrypted

5.5-2	R	user reviewed or evaluated implementations	N/A
5.5-3	R	crypto algorithms should be replaceable	N/A
5.5-4	R	access via network shall be possible after authentication only	Password protected
5.5-5	MF	security changes over network only after authentication	Password protected
5.5-6	RF	encrypted parameters in transport over network	N/A
5.5-7	MF	protect critical parameters over network	N/A
5.5-8	MC	manufacturer shall follow secure management processes for lifetime	N/A
5.6		**Minimize exposed attack surfaces**	
5.6-1	MF	unused interfaces shall be disabled	Only selected interfaces are active
5.6-2	M	during initialization minimize disclosure	N/A
5.6-3	R	hw interfaces should not enable attacks	Time delay applied
5.6-4A	MF	debug interfaces disabled or protected	Not available
5.6-4B	RF	debug interfaced physically protected	Not available
5.6-5	R	enable only sw services that are required for function	OK
5.6-7	R	sw should run with least necessary privileges	OK
5.6-8	R	HW level access control for memory	OK
5.6-9	R	sw development of security	Implemented in design
5.7		**Ensure software integrity**	
5.7-1	R	device should verify secure boot mechanisms	Checks confirguration
5.7-2	RF	if unauthorized changes detected, device should notify user and no more connection	Password protection, no notification to the user
5.8		**Ensure that personal data is secure**	
5.8-1	RF	transmitted personal data best practice cryptography	No personal data
5.8-2	MF	communicated personal data best practice cryptography	No personal data
5.8-3	MF	external sensing capability documented to the user	N/A
5.9		**Make systems resilient to outages**	
5.9-1	R	resistance to outages of networks and power	OK
5.9-2	R	device operating if loss of data and should recover after loss of power	OK
5.9-3	R	connection to network in timely manner in respect with network usage	OK
5.10		**Examine system telemetry data**	
5.10-1	RF	data examined for security anomalies	N/A
5.11		**Make it easy for users to delete user data**	
5.11-1	M	user can erase their data in a simple manner	OK
5.11-2	RF	personal data should be erased in simple manner	No personal data

5.11-3	R	clear instruction for the user how to delete personal data	Described in User Manual
5.11-4	R	user should be provided with confirmation	N/A
5.12		**Make installation and maintenance of devices easy**	
5.12-1	R	minimal decisions by the user followed security practice	OK
5.12-2	R	user manual how to setup device	OK
5.12-3	R	user manual how to check if device is securely set	OK
5.13		**Validate Input data**	
5.13-1A	M	data input at application level shall be validated	Measurements tested for serial inputs
5.13-1B	M	data input at application level via network shall be validated	It is up to the server received side
6		**Data protection provisions for consumer IoT**	
6.1	M	manufacturer should provide info about data usage	In user manual
6.2	MF	if personal data are used, consumer's consent is required	No personal data
6.3A	MF	consent can be with draw any time	N/A
6.3B	MF	storing information about this consent	N/A
6.4	RF	processing personal data should be minimized	N/A
6.5	MF	consumer shall be provided with personal data collection	N/A
6.6	MF	data in 6.1 shall be limited	N/A
6.7	RF	data should be minimized	N/A
6.8	RF	device can add protective noise	N/A

4. DECLARATION OF CONFORMITY

CE

Manufacturer: **Physicus**
Silvanska 27
841 04 Bratislava
Slovakia
Tel: +421-905-852 073
Email: physicus@physicus.eu

Description of the product: Ultralow power datalogger

Type: LogboxSE

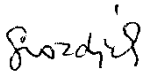
The indicated product is compliant to the following EU Directives:

Directive 2014/30/EU, Electromagnetic compatibility (EMC)
Directive 2014/35/EU, Low Voltage (LVD)
Directive 2022/30/EU, Radio Device (RED)
Directive 2011/65/EU, incl. Annex II 2015/863 (RoHS)

Applicable test standards:

EN 61326-1:2013
EN 61000-6-3
EN 61000-6-2
EN 61000-4-6
EN 61000-4-4
EN 61000-4-2
EN 18031-1:2024

Date: 30.6.2025
Issued by:



Jan Gvozdjak