To whom it may concern

Our reference
-

Phone number
+49 451 882-0

Fax
+49 451 882-76166

E-mail
product-security@draeger.com

Vulnerability and Incident Reporting
product-security@draeger.com

Cyber Security Whitepaper

Evita V800 / V600, Babylog VN800 / VN600 Intensive care Ventilators, Software 2.n

2024-01-29

Dear customers, dear health care Professionals,

at Dräger we develop technology for life. Our customers, regardless of what sector they're in, depend on this technology and expect that Dräger products will be secured against vulnerabilities that could affect the functioning of the products and the security, integrity and privacy of the electronic information and data used by the products. The security, integrity and privacy of the sensitive data of our customers, patients, and operators of our systems are deeply embedded in our development processes.
Security is not a feature or a property of a single device, nor is it the sole responsibility of the device manufacturer or the operating organization. It is a collaborative effort that is needed to ensure a device to be securely integrated in its target environment.

This document describes the security characteristics of the Evita V800 / V600, Babylog VN800 / VN600 Intensive care Ventilators, Software 2.n.

Contents

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

1 Target Environment Overview

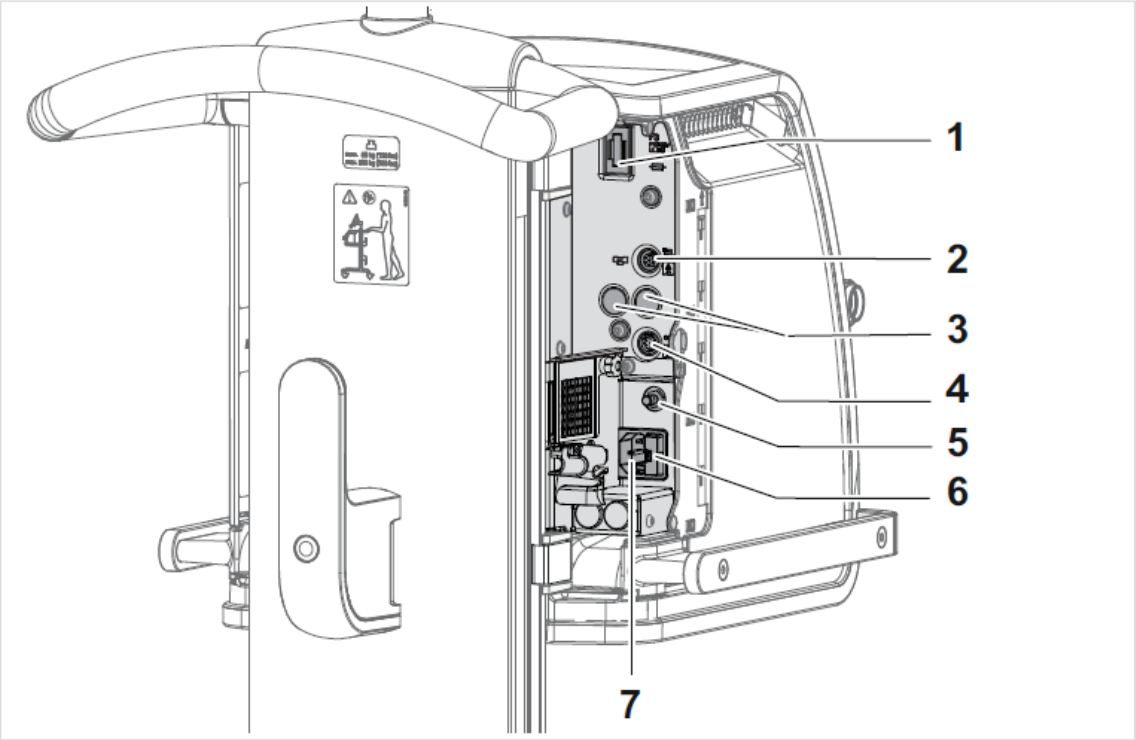
The device is suitable for stationary use in hospitals or hospital like facilities or for intra hospital patient transport. It can be operated in a Patient Area Network with serial (RS-232) point-to-point connections.

Local Area Network over Ethernet (RJ45) is only designed for connection with the Dräger ServiceConnect Gateway (SCG) or a Dräger service computer.

2 External Interfaces

This section gives an overview of all external interfaces of the device.
To reduce the attack surface of the device, and thereby the risk of patient harm or data privacy issues, the intended use of the ports must be complied with. The following will describe each port in detail in order to be able to assess the risk of potential device malfunctions due to an attack, intended or unintended misuse.

2.1 Rear of Ventilation unit



ID	Interface description
1	Fuse for the internal battery
2	Neo Flow Port for the neonatal flow sensor
3	Ports for future extensions
4	CO_2 Port for the CO_2 sensor
5	Potential equalization pin
6	Fuse for the mains power supply
7	Port for the mains power supply

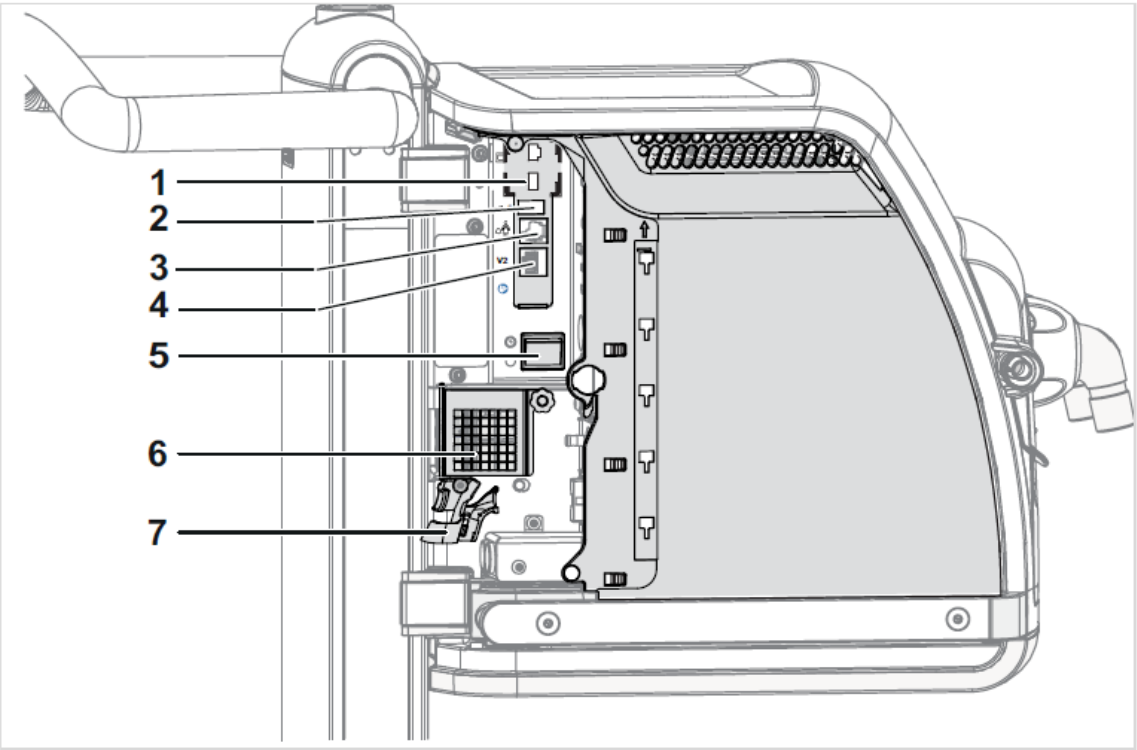
Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

2.2 Left of Ventilation unit



ID	Interface description
1	Port for the System cable which leads to the display unit
2	USB ports
3	Port for nurse call
4	Port for future extensions
5	Main switch
6	Room air filter with cover
7	Strain relief for cable

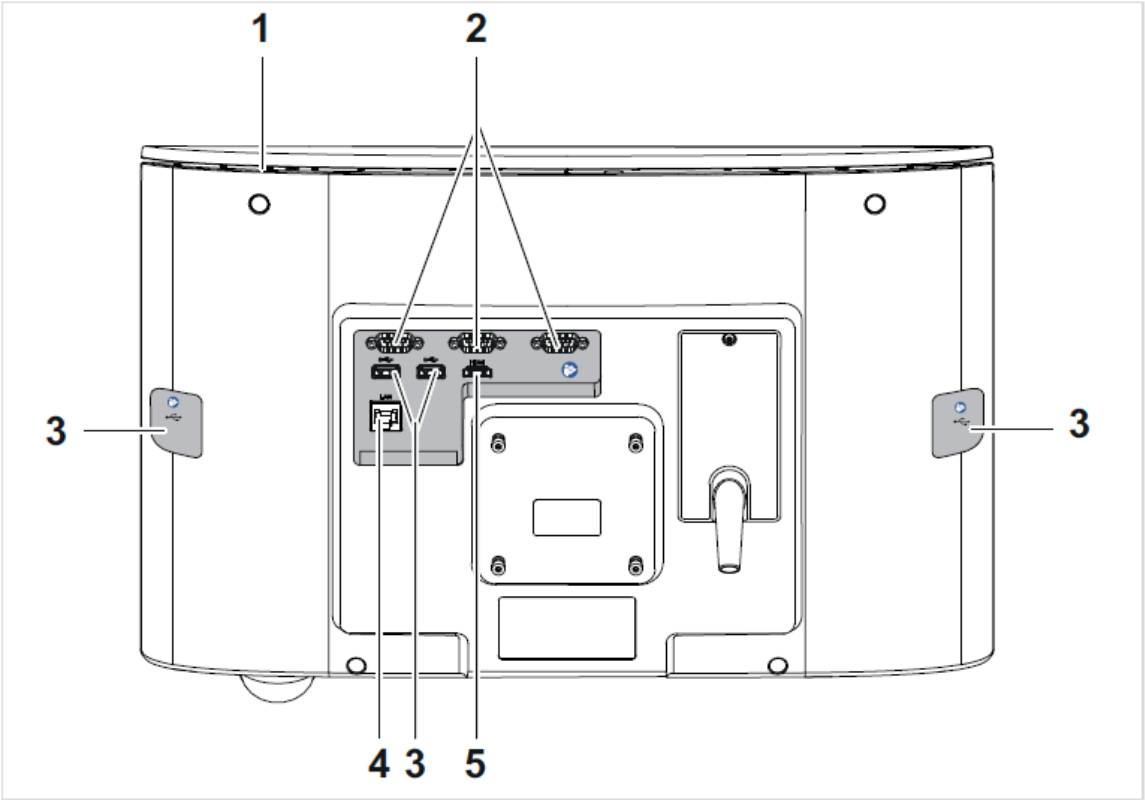
Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner

2.3 Rear of display unit



ID	Interface description
1	Alarm bar
2	COM Serial ports (RS-232)
3	USB ports
4	LAN Port for Service purposes
5	HDMI Port for external device (e.g., projector)

2.4 NeoFlow Port for the neonatal flow sensor

Analog data interface. It is not possible to impair the device functionality over this interface.

2.5 C02 Port for the C02 sensor

Interface for communication with the Drager MCable Mainstream CO_2 Sensor.

2.6 Port for the System cable which leads to the display unit

The System cable connects the Ventilation unit with the display unit of the Ventilator. As the display unit can be separated from the ventilation unit to mount it at a suitable place in the ICU installation, it is designed pluggable for an easier handling and cabling.

2.7 USB ports

The Ventilator provides five USB ports, whereas four ports are located on the display unit and one is located on the ventilation unit. They are intended for

- Data export (e.g. user log) to USB storage media (i.e. USB stick)
- Exchange of configuration data to and from USB storage media
- Activation of optional ventilator functions.

To prevent gaining any kind of control over the ventilator only device class mass storage device and device class hub are accepted by USB configuration, i.e. human interface devices such as keyboard or mouse are not supported. In addition, any USB human interface device drivers are removed from the operating System.

Of course, auto play is not needed and not supported. This further prevents infecting the ventilator with any kind of malware.

Thereby it is not likely to impair the device functionality over this interface.

2.8 Port for nurse call

Port is dedicated for the nurse call and electrically decoupled. Please refer to the instructions for use (reference in chapter “Technical Data”) for a detailed description of the features. It is not possible to impair the device functionality over this interface as it is a data output only.

2.9 Port for future extensions

Currently not intended for end user usage. Hence, the port is disabled and must not be connected.

2.10 COM Serial ports (RS-232)

The device provides three RS-232 serial communication interfaces. These interfaces can be used for transferring data between the device and an external medical or non-medical device (e.g., patient monitors or computers for data management Systems) via the Drager-proprietary MEDIBUS / MEDIBUS.X serial protocol (see chapter “Technical References”).

The data that can be transferred comprises measured values, therapy settings, and further status information. The data transferred does **not** include any personally identifiable information, such as the name of the patient. The only personal data transmitted is therapy data with information on the patient’s weight and height. For a complete overview of the transferrable values please refer to the Medibus.X profile definition (chapter “Technical References”).

The MEDIBUS library is developed at Drager following our high-quality standards for safety and security incorporated in our development processes. The following design considerations lead to an acceptable risk level for permanent connections:

The MEDIBUS library of the device is a **read only interface.** It is not possible to set or modify any values in the ventilator. Data can only be queried by the connected device.

Incorrect data packages or packages with unknown target codes are **discarded without causing a noticeable load** on the device, preventing denial of Service. This is guaranteed by executing fuzz and load tests as part of the release process of the device.

The RS-232 connection is designed to be a **non-distributed point-to-point connection.** A device identification mechanism is implemented to prevent accidental connections and to prevent non-MEDIBUS devices to communicate with the device. Due to the nature of the intended use of the interface, no further authentication mechanisms are necessary. Hence, man in the middle attacks would require physical access to the point-to-point connection.

The MEDIBUS protocol has **predefined field lengths and checksums for data corruption that are verified on incoming messages** prior to the actual message content processing preventing misusing buffer overflow for remote code execution. No memory operations use input of uncontrolled lengths, thereby buffer overflow errors are prevented by design. This, among others, is furthermore checked by automated scans like static code analysis. The MEDIBUS Service runs as **a separate process,** independent from the therapy functions of the device.

Note on RS-232 to ethernet converters: The MEDIBUS serial interfaces were designed for connections in proximity to the device. Off the shelf serial to ethernet converters could impose additional risks on data privacy and device security by increasing the exposure of the serial ports. The operating organization must ensure that adequate authentication and authorization mechanisms exists in the converter solution to ensure that only trusted devices may communicate with the medical device. Please note that such set-ups need a thorough risk management and are solely within the responsibility of the operating organization.

2.11 LAN Port for Service purposes

As mentioned above, LAN (Local Area Network) over ethernet (RJ45 connector) is only designed for connection with the Drager Service Connect Gateway (SCG) or a Drager service computer. The Drager service computer is used only with a crossed point-to-point connection (“cross-cable”) between the device and the Service laptop. Restricted to these applications, all unused network ports are closed. When a very high network load like provoked by a denial-of-service attack is detected, the network adapter is disabled to ensure that system performance is cannot be affected.

To prevent accidental or malicious connections it is possible to use RJ45 jack locks or jack seals.

2.12 HDMI Port for external device

Provides a High-Definition Multimedia Interface (HDMI) to an external video monitor that shows contents of the display unit screen on an external monitor for presentation or training purposes. Not intended to show patient data during therapy. Consumer Electronics Control (CEC) is not implemented, i.e. no control of the ventilator via HDMI functionalities is possible.

3 Operating System

3.1 Type

The ventilators use the embedded operating System WindRiver VxWorks 7 which is an industrial standard for embedded devices and for embedded medical devices.

3.2 Considering Malware Protection

The software of the embedded device is a closed system. All executables of the system are known before manufacturing of the device and the system is locked down to prevent execution of all further executables. In addition, the executables are verified on boot and frequently also during normal operation.

Antivirus solutions are meant for general purpose IT system where not all executables are known in advance. Hence, systems like antivirus, next generation endpoint protection, advanced threat protection or application whitelisting solutions are not applicable to closed embedded operating Systems.

3.3 Considering Firewalls

As mentioned above, the LAN is used for Service purposes only. Hence, the needed network ports are also known when manufacturing the device and all unnecessary ports are closed and unnecessary services are disabled. Hence, an additional software firewall on the device is not needed.

4 System Verification

4.1 Automated Vulnerability Scanning and Code Analysis

The system is checked with automated vulnerability Scanners, such as Nessus, and static code analysis software, such as Coverity, continuously and as part of the release process.

4.2 Penetration Test

A penetration test of the system has been performed by an external Company specialized on cyber security and all findings have been addressed appropriately.

5 Security Architecture

The device design further includes the following security measures to minimize the influence on therapy.

- The device has a redundant architecture in hardware and software.
- The ventilation software runs on a separated real time process (VxWorks), thereby the ventilation is separated from other parts of like human interface or service.
- In case of any problem with the human interface process or the display unit, the monitoring of the minute volume and FiU2 is always active and visible on separated display on the ventilation unit. In addition, a bar display indicates the inspiratory and expiratory phases.
- The System prevents any modification via communication interfaces (e.g., software installation) during therapy mode.
- All electrical connector ports are short-circuiting protected

Caution: Only equipment complying with IEC60950 shall be connected to data interfaces (see device instructions for use for details, chapter technical data")

Caution: Equipment not listed in the instructions for use shall only be connected with approval by each respective manufacturer (see device Instructions for use for details, chapter "Technical Data").

6 Patch Management

Patches for the device are rolled out by service technicians as a Software update via the LAN interface. They cannot be applied by the operating organization.

7 Vulnerability Monitoring

At Dräger we understand that importance of monitoring public information for vulnerabilities. Our product security team monitors a variety of information sources for published security vulnerabilities in third party components and maps these to the possibly affected Dräger products. These sources include the National Vulnerability Database (NVD), MITRE's CVE List, VulnDB, and several vendor specific RSS feeds, mailing lists, and websites. Furthermore Dräger is member of the German Alliance for Cybersecurity ("Allianz für Cybersicherheit"), which provides timely information on current threats and vulnerabilities.

8 Reporting Security Vulnerabilities and Security Advisories

At Dräger we put a lot of effort and dedication into the safety and security of our devices. However, we are aware that every device can contain unknown security vulnerabilities. To assist us with our development efforts, Dräger encourages and supports security researchers and customers to responsibly report to us any potential security and privacy vulnerabilities identified in our products. Therefore, Dräger maintains a product security page at http://static.draeger.com/security/ in order to provide contact details and information concerning the procedures to follow to test and report vulnerabilities.

We also publish security advisories on this product security page, containing information about threats and mitigations concerning our products.

If you encounter any issues with our products which do not implicate security or privacy vulnerabilities, or if you encounter any other issue which might affect patient, user, or operator safety, please contact your local Sales & Service representative.

9 Technical References

9.1 Common

- Protocol Definition, Dräger RS-232 MEDIBUS 9028258
- Profile Definition for Data and Communication, MEDIBUS.X 9052608
- Rules and Standards for Implementation, MEDIBUS.X 9052607

9.2 Specific Evita V800, Evita V600, Babylog VN800, Babylog VN600

- Communication protocol for Evita V800/V600 and Babylog VN800/VN600
  SW 1 .n, 9056567 en, Edition: 1 - 2019-01
- Instructions for use Babylog VN800 / VN600
  9511645- GA 6500.640 / 6500.660 en, Edition: 1 – 2021-12
- Instructions for use Evita V800 / Evita V600
  9511608 - GA 6500.600 / 6500.620 en, Edition: 1 – 2021-12

Steve Dallas

Steve Dallas
Chief Product Security Officer

Drägerwerk AG & Co. KGaA
Moislinger Allee 53-55
23558 Lübeck, Germany
Postal address:
23542 Lübeck, Germany
Tel +49 451 882-0
Fax +49 451 882-2080
info@draeger.com
www.draeger.com
VAT no. DE135082211

Bank details:
Commerzbank AG, Lübeck
IBAN: DE95 2304 0022 0014 6795 00
Swift-Code: COBA DE FF 230
Sparkasse zu Lübeck
IBAN: DE15 2305 0101 0001 0711 17
Swift-Code: NOLADE21SPL

Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7903 HL
General partner: Drägerwerk Verwaltungs AG
Registered office: Lübeck
Commercial register:
Local court Lübeck HRB 7395 HL

Chairman of the Supervisory Board
for Drägerwerk AG & Co. KGaA
and Drägerwerk Verwaltungs AG:
Prof. Dr. Nikolaus Schweickart
Executive Board:
Stefan Dräger (chairman)
Rainer Klug
Gert-Hartwig Lescow
Dr. Reiner Piske
Anton Schrofner