Mechanical Lung Ventilator

Software Requirements Specification
for ABZ 2024 case study

Silvia Bonfanti, Angelo Gargantini

July 7, 2023

All the pdf versions of this document are available here:
`https://github.com/foselab/abz2024_casestudy_MLV`

All the questions and doubts can be discussed here:
`https://github.com/foselab/abz2024_casestudy_MLV/issues`

Authors contacts

If you have any question/comment on the case study, you can contact us:

- Silvia Bonfanti, University of Bergamo
  email: silvia.bonfanti@unibg.it

- Angelo Gargantini, University of Bergamo
  email: angelo.gargantini@unibg.it

- ABZ 2024 email: abz2024@unibg.it

Version History

Version	Date	Comment
1.0	July 3, 2023	First version

Contents

Definitions and Abbreviations

Definitions

Term	Definition
apnea backup ventilation	Switching from PSV to PCV mode in case of apnea lag
apnea lag (or apnea trigger window)	Duration of apnea that triggers a switch from PSV to PCV mode
control panel	A touchscreen display for setting parameters and operation monitoring of the ventilator
default configuration file	File which contains setting parameters with default values
drop-in (pressure)	Speed of pressure drop
internal pressure	The internal pressure in the circuit
in valve	The inspiratory control valve allows the mix of air and oxygen to enter the inspiratory limb of the patient's circuit. This valve can have • state closed when the pressure is set to 0, and • state open when the pressure is set to P_{insp}
last_inspiration_ time	Duration of the patient inspiration in the current breath cycle in PSV mode.
max_exp_pause	The maximum time duration of an Expiratory Pause
max_ins_pause	The maximum time duration of an Inspiratory Pause
max_insp_time_ psv	A timeout for the inspiration phase in PSV mode in case an expiration is not spontaneously triggered by the patient. It shall be 7 sec.
max_rm_time	The maximum time duration of a Recruitment Maneuver
min_exp_time_psv	A timeout for the expiration phase in PSV mode in case an inspiration breath is not spontaneously triggered by the patient and the apnea lag is not over.
out valve	The valve that controls the expiratory flow. The valve can be closed or open.
pressure control loop	The sw procedure that determines the output control signal to inspiratory valve to maintain the Airway Pressure (PAW) at a set target pressure
stored configuration file	File which contains setting parameters with last changes made by the user
trigger window	Time interval within which a spontaneous breathing can be detected (in PCV mode). The trigger window can start 0.7 sec after the end of the inspiration phase.
waveform	An image that represents a quantity that changes over time, e.g., inspiratory pressure. It shows the changes in amplitude over a certain amount of time. The amplitude of the signal is measured on the vertical axis while time is measured on the horizontal axis

Table 1: Definitions

Abbreviations

Term	Definition
ETS	Expiratory Trigger Sensitivity: percentage of peak flow at which the ventilator triggers expiration
FiO_2	Fraction of inspired Oxygen: the relative oxygen concentration of the air in the inspiratory limb of the circuit
$I:E_{AP}$	Ratio of Inspiratory time to Expiratory time in apnea backup mode
$I:E_{PCV}$	Ratio of Inspiratory time to Expiratory time in PCV mode
IS	Inspiratory Pressure: airway pressure during an inspiratory or inflation phase
ITS_{PCV}	Inhale Trigger Sensitivity: the drop-in pressure that triggers a new inspiration in PCV mode
ITS_{PSV}	Inhale Trigger Sensitivity: the drop-in pressure that triggers a new inspiration in PSV mode
GUI	A software component controlling a touchscreen display for the user functionalities of setting the parameters and monitoring the operation of the ventilator
PAW	Airway Pressure: the pressure measured in the entrance to the patient's airway
PCV	Pressure Controlled Ventilation: inflation type that acts to generate a constant inspiratory pressure at a set level, after a set rise time
Peak P_{insp_PCV}	Peak inspiratory Pressure: highest airway pressure reached during the previous respiratory cycle in PCV mode
Peak P_{insp_PSV}	Peak inspiratory Pressure: highest airway pressure reached during the previous respiratory cycle in PSV mode
PEEP	Positive End Expiratory Pressure: the measured respiratory pressure at the end of an expiratory phase
P_{insp_AP}	Target Inspiratory Pressure: the set pressure to supply the patient during the inspiratory phase of the breathing cycle in case of apnea backup.
P_{insp_PCV}	Target Inspiratory Pressure: the set pressure to supply the patient during the inspiratory phase of the breathing cycle in PCV mode.
P_{insp_PSV}	Target Inspiratory Pressure: the set pressure to supply the patient during the inspiratory phase of the breathing cycle in PSV modes.
PSV	Pressure Support Ventilation
PRM	Pressure for the Recruitment Maneuver
RM	Recruitment Maneuver
RR_{AP}	Respiratory Rate: the number of breaths taken by the patient per minute in apnea backup mode
RR_{PCV}	Respiratory Rate: the number of breaths taken by the patient per minute in PCV mode
V_{tidal}	Tidal Volume: the volume of air delivered by the ventilator to the lungs for each breath.
V_E	Minute Volume: (or flux) volume of gas either passing to or leaving the lung during inspiratory or inflation phases, or expiratory phase, respectively, expressed as a volume per minute. The Minute Volume is equal to the tidal volume multiplied by the respiratory rate.

Table 2: Abbreviations

1 Introduction

During the COVID-19 pandemic, a group of researchers was involved in the design, development, and certification of an electro-mechanical lung ventilator called MVM (Mechanical Ventilator Milano)[1] [3]. The project started from the idea of the physicist Cristiano Galbiati, who was soon joined by dozens of physicists, engineers, physicians, and computer scientists from 12 countries around the world[2]. The team was able to realize a ventilator that is reliable, easily reproducible on a large scale, available in a short amount of time, and at a limited cost [4]. The MVM has obtained the FDA (Food and Drug Administration) Emergency Use Authorization (EUA) followed by authorizations issued by Health Canada and the CE marking as well.

The specification of the mechanical lung ventilator is inspired by MVM, with some simplifications to make it suitable as a case study:

- we have removed one component, the supervisor which was responsible for monitoring the controller, the GUI, and the hardware. In the case of errors, it raises alarms if not already raised by the controller or the GUI, ensuring patient safety.
- we use only visual alarms, instead of audio and visual alarms.

Disclaimer

The content of this document is not the one used for the certification of MVM. We have elaborated on the original documentation, and we may have introduced some inaccuracies. So, please DO NOT use this document as software requirements specification of a real ventilator.

1.1 Mechanical lung ventilator

The mechanical lung ventilator is intended to provide ventilation support for patients that are in intensive therapy and that require mechanical ventilation. The ventilator proposed in this document works in pressure mode, i.e., the respiratory time cycle of the patient is controlled by pressure, and, therefore, this ventilator requires a source of compressed oxygen and medical air that are readily available in intensive care units. More precisely, the ventilator has two operative modes: *Pressure Controlled Ventilation* (PCV) and *Pressure Support Ventilation* (PSV). In the PCV mode, the respiratory cycle is kept constant and the pressure level changes between the target inspiratory pressure (P_{insp}) and the positive end-expiratory pressure (PEEP). New inspiration is initiated either after a breathing cycle is over, or when the patient spontaneously initiates a breath. In the former case, the breathing cycle is controlled by two parameters: the respiratory rate (RR) and the ratio between the inspiratory and expiratory times (I:E). In the latter case, a spontaneous breath is triggered when the ventilator detects a sudden pressure drop within the trigger window during expiration. The PSV mode is not suitable for patients that are not able to start breathing on their own because the respiratory cycle is controlled by the patient, and the ventilator partially takes over the work of breathing. A new respiratory cycle is initiated with the inspiratory phase, detected by the ventilator when a sudden pressure drop occurs. When the patient's inspiratory flow drops below a set fraction of the peak flow,

[1] `https://mvm.care/`

[2] At that period, many projects on mechanical ventilator started, but only a few get certified`https://github.com/PubInv/covid19-vent-list`

the ventilator stops the pressure support, thus allowing exhalation. If a new inspiratory phase is not detected within a certain amount of time (apnea lag), the ventilator will automatically switch to the PCV mode because it is assumed that the patient is not able to breathe alone.

The ventilator allows the air to enter/exit through two valves, i.e., an input valve and an output valve. When the ventilator is not running, the valves are set to safe mode: the input valve is closed and the output valve is opened. In this configuration, the ventilator does not prevent breathing thanks to some relief valves.

When the inspiration starts, the input valve is opened and the output valve is closed, while during the expiration the input valve is closed and the output valve is opened. Both in PCV and PSV mode, inspiratory pause, expiratory pause, and recruitment maneuver are allowed by user request. Inspiratory/Expiratory pause consists in closing the input and output valves of the ventilator respectively after the inspiration and expiration phases. The inspiratory pause allows measuring the pressure reached inside the alveoli at the end of the inspiratory cycle, while the expiratory pause allows measuring the residual pressure to check possible obstruction in the exhalation channel. The recruitment maneuver is an emergency procedure required after intubation, and it consists of prolonged lung inflation as necessary to reactivate the alveoli immediately; during this maneuver, the input valve is opened and the output valve is closed.

The high-level software architecture, shown in Figure 1.1, illustrates the communication among the software components: graphical user interface (GUI) and controller. The GUI is a touchscreen panel that displays the information needed to check the respiratory condition, allows parameter setting, and displays ventilation parameters and alarm settings. When the controller receives operator input from the GUI, it communicates with the valve controllers, serial interfaces, and other subcomponents and sends them commands.

Before starting the ventilation, the ventilator controller passed through three phases. The *start-up* in which the controller is initialized with default parameters, *self-test* which ensures that the hardware is fully functional, and *ventilation off* in which the controller is ready for ventilation when requested. If during ventilation and other phases the controller detects a severe condition that prevents the ventilator to sustain the ventilation, the machine is brought to fail-safe mode (in valve closed and out valve open).

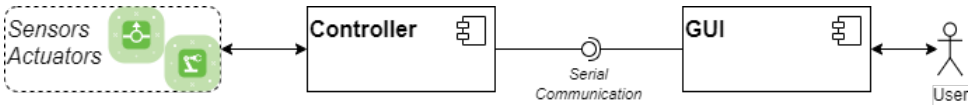


Figure 1.1: The high-level software architecture

1.2 Structure of the document

This document is structured in the following chapters:

- Chapter 2 presents the general specification of the ventilator: functional requirements, values and ranges of parameters and interfaces between components.
- Chapter 3 presents the specifications of the GUI, which is responsible for receiving information from the user and displaying information to the user.
- Chapter 4 presents the specification of the controller, which is responsible for controlling the phase of the respiratory cycle (inhalation, pause, exhalation) by operating on the valves and receiving information from sensors and commands from the GUI.
- Chapter 5 presents the specification of the alarm system which is responsible for raising alarms.

Requirement Numbering Convention

The specification is divided in requirements, and the format of each requirement ID is:
XXX.n.y
Where:
XXX = a three-letter code indicating a requirement type
n = requirement number 1-9999
y = sub-requirement number 0-9 (0 if a parent, 1 to 9 if a child)

Three-letter code	Description
AL	Alarm requirements
CONT	Controller requirements
FUN	Functional (general) requirements
GUI	GUI requirements
INT	Interfaces requirements
PER	Values and ranges requirements
SAV	Safety requirements

1.3 Suggested outcomes

During the development of the MVM software, no formal method has been applied, mainly because a lack of developers' skills with any formal method. However, we want to propose this case study in order to demonstrate the feasibility of developing the ventilator by using a formal method based approach. Mechanical lung ventilators, as well as other medical devices which incorporate software, must be certified before their use. Several standards for the validation of medical devices have been proposed – as ISO 13485, ISO 14971, IEC 60601-1, EU Directive 2007/47/EC [28] –, but they mainly consider hardware aspects of the physical components of a device, and do not mention the software component. The only reference concerning the regulation of medical software is the standard IEC (International Electrotechnical Commission) 62304. This standard provides a very general description of common life cycle activities of the software development, without giving any indication regarding process models, or methods and techniques to assure safety and reliability.

With this case study we aim to study the applicability of formal methods in software development of medical devices in order to satisfy the standards, IEC 62304 in this case.

We have envisioned several aspects of the ventilator that could be the object of research activities. In the following, we give a non-exhaustive list of possible outcomes.

- A classical approach consists in modeling the system or part of it and applying the classical V&V activities, like formal verification of the correctness or validation of scenarios. One could check that the behavior of the system is correct, like in case of some types of errors, the system goes into a fail-safe mode.
- A critical aspect of the system is its temporal behavior. Many properties and constraints have explicit temporal requirements (like after 10 seconds ...). One could model these aspects and make a temporal analysis of the system.
- After the good experience of ABZ2022, we decided to also include the GUI. Research activities could refer to modeling this critical component and analyzing the human-computer interaction.
- Generation of executable source code and implement a prototype of the ventilator on a simple electronic board like Arduino (or part of it).

Useful references

- Book on a mechanical ventilation [5]
- Papers about MVM: [1, 2, 3, 4]

Acknowledgement

We would like to thank all the people in the MVM team for the wonderful work we have done all together during the pandemic. We acknowledge the work done especially by Cristiano Galbiati, Reiner Kruecken, and Elvinia Riccobene.

2 System Requirements

This chapter contains a high-level description of the system requirements, defining the functional requirements and interface requirements. The requirements are generic and independent of any technical solution to allow greater flexibility in the ventilator development.

2.1 Functional Requirements

These requirements cover normal operating modes, e.g., start-up, PCV, PSV, and any direct responses required following abnormal operation, e.g., pressure relief, alarm conditions for control systems.

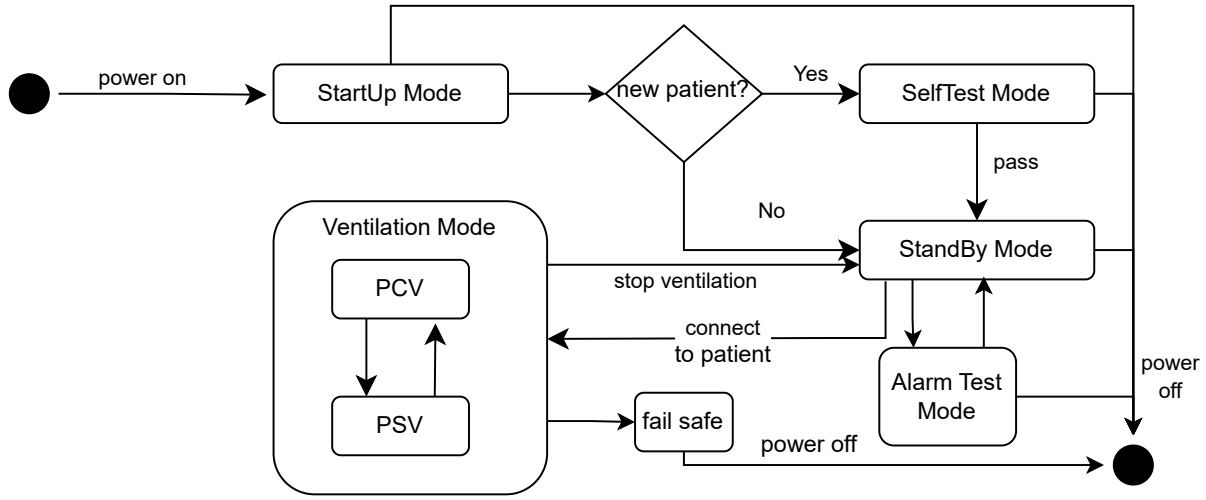


Figure 2.1: High level operation diagram

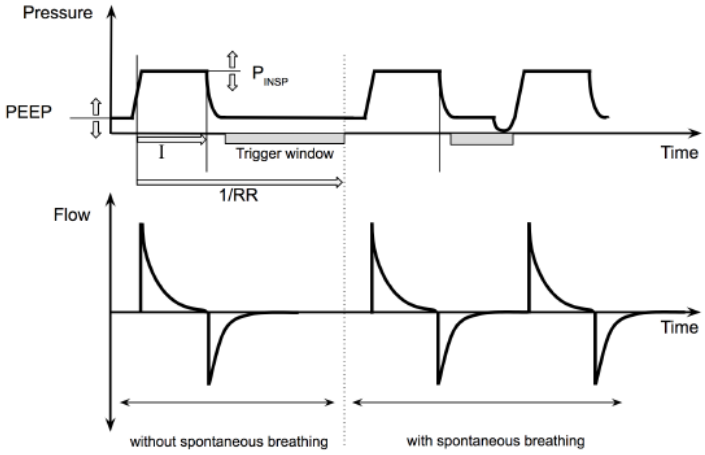
ID	Requirement / Rationale	Input Ref.
FUN.1	The system shall provide ventilation support for patients who require mechanical ventilation and weigh more than 40 kg (88 lbs). *Rationale:* ventilation of children and infants is more challenging	
FUN.2	The system shall provide pressure regulated ventilation controlling the inspiratory pressure. *Rationale:* pressure regulated ventilation is most beneficial for COVID-19 patients	
FUN.3	The system shall provide positive end expiratory pressure (PEEP) ventilation. *Rationale:* PEEP is important to keep alveoli recruited at the end of expiration	

FUN.4	The system shall implement the following operating modes: 1. Start-up Mode: The Start-up Mode initializes the system and is part of a start-up procedure to get the system ready to be used to ventilate a patient. 2. Self-test Mode: The Self-test Mode ensures that the system is fully functional and is part of the start-up procedure to get the system ready to be used to ventilate a new patient 3. Standby Mode: In the Standby Mode the ventilation is ready for ventilating a patient, ventilation is off, and ventilation parameters can be set. 4. Alarm Test Mode: The Alarm Test Mode allows the user to test the alarms. 5. Pressure Controlled Ventilation Mode (PCV): Pressure Controlled Ventilation mode is a normal operating mode that is used when patients have no spontaneous respiration. 6. Pressure Support Ventilation Mode (PSV): Pressure Support Ventilation is a normal operating mode that during which the patient initiates each breath and the ventilator supports the breath at the appropriate pressure level. 7. Fail-safe mode: the controller detects a severe condition that required an alarm to be raised and to bring the machine to a fail-safe mode (in valve closed and out valve open). *Rationale:* Pressure Controlled and Pressure Support Ventilation are the two basic modes of pressure regulated support needed for COVID-19 patients. A Start-up mode is needed to properly ensure that the system is fully functional before starting the ventilation of a patient. Pressure Controlled Ventilation is needed for patients in respiratory failure or fully sedated. Pressure Support Ventilation is needed for patients able to breathe on their own, in particular during the weaning process.
FUN.5	The Start-up Mode shall be initiated by pushing the power button of the system once the system has been connected to the breathing circuit (without connection to the patient), the air supply, and the power source. *Rationale:* need to turn on the system once all connections are attached so the sensors and valves can be properly tested.
FUN.5.1	Upon initiation of the Start-up Mode, the system shall go through an initialization process that loads default parameters and checks the system memory and the communication of the controller with the sensors and valves, as well as between the controller and the GUI. *Rationale:* Need to ensure that the system properly started.

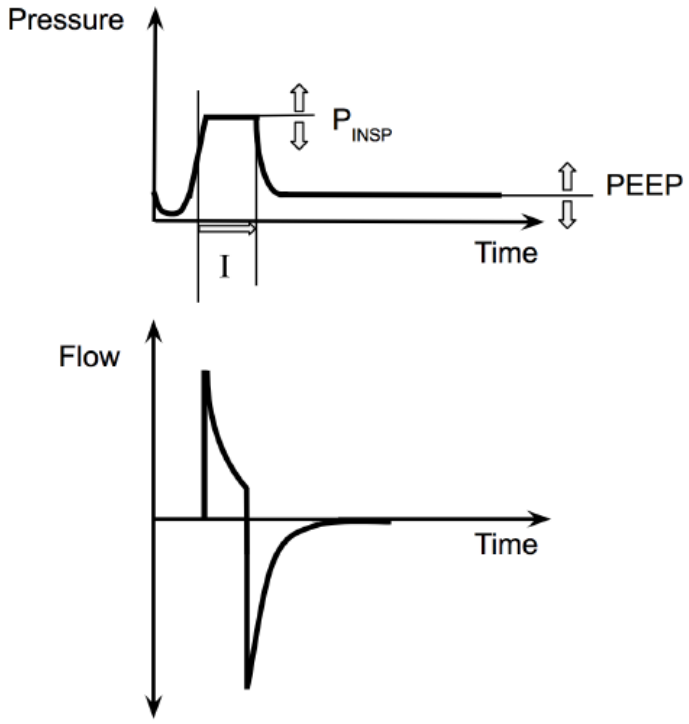
FUN.5.2	The system shall indicate to the user that the initialization process has been completed successfully or failed. In case of a failure the user shall be warned that the system is out-of-service. In addition, any other operations shall be not allowed. *Rationale:* only a fully functional unit shall be used with a patient	
FUN.5.3	The patient shall not be connected to the breathing circuit when the system is powered on and through start-up and self-test.	
FUN.6	The system shall have a self-test procedure that ensures the system and its accessories are fully functional and the alarms work.	ISO80601-2-12 201.7.9.2.8.101
FUN.6.1	The self-test procedure shall confirm the switchover from external to internal power works.	
FUN.6.2	The self-test procedure shall confirm there are no unacceptable leaks in the breathing circuit.	
FUN.6.3	The self-test procedure shall confirm the FI2 flow meter (see Figure 2.2) in the patient breathing circuit is connected in the right direction and is calibrated.	
FUN.6.4	The self-test procedure shall confirm the expiratory valve is functional.	
FUN.6.5	The self-test procedure shall confirm the oxygen sensor is calibrated.	
FUN.6.6	The self-test procedure shall confirm the local alarms are functional.	
FUN.7	If the self-test fails, the user shall be warned that the system is out-of-service. In addition, any other operations shall be not allowed.	
FUN.8	The system shall log key parameters, save them before being powered off and load them upon start-up to be made available on a log page on the GUI.	
FUN.8.1	The system shall have means to indicate visually the cumulative hours of operation of the ventilator, either 1) automatically; or 2) by operator action.	ISO 80601-2-12: 201.104
FUN.8.2	The system shall be equipped with an alarm system log with a capacity of at least 1000 events in total for: high priority alarm conditions; medium priority alarm conditions; and alarm signal inactivation states	ISO 80601-2-12: 208.6.12.101
FUN.8.3	The system shall time stamp all alarm events either via the date and time, the elapsed time since the occurrence of the alarm condition, or the elapsed time from the start of use of system	ISO 80601-2-12: 208.6.12.101
FUN.8.4	The system shall not lose the contents of the alarm system log during a loss of power for less than 7 d unless erased by authorized personnel of the hospital.	ISO 80601-2-12: 208.6.12.101
FUN.8.5	The system shall not permit the healthcare professional operator to erase the contents of the alarm system log.	ISO 80601-2-12: 208.6.12.101

FUN.8.6	The system shall provide a log to include any change of ventilator settings, including the value applied	ISO 80601-2-12: 208.6.12.101
FUN.8.7	The system shall provide a log to include any change of alarm settings, including the value applied	ISO 80601-2-12: 208.6.12.101
FUN.8.8	The system shall provide a log to include change of patient, including the patient attributes;	ISO 80601-2-12: 208.6.12.101
FUN.8.9	The system shall provide a log to include power supply source change, including the source utilized	ISO 80601-2-12: 208.6.12.101
FUN.8.10	The system shall provide a log to include results of the pre-use check.	ISO 80601-2-12: 208.6.12.101
FUN.8.11	The system shall provide a log to include the overall duration of the active use of the O2 sensor (%-hours) *Rationale:* The oxygen sensor has a limited lifetime expectancy requiring a monitoring of its use in order to track its deterioration over time	
FUN.8.12	The system shall log user-set ventilation and alarm parameters as well as the current calibration parameters. *Rationale:* user-set ventilation and alarm parameters need to be able for the resumption of ventilation in case the system has to be briefly turned off.	
FUN.9	Once the self-test has been completed successfully and configurations have been loaded properly the system shall start monitoring and reporting health parameters. *Rationale:* At this point the monitoring module is able to carry out its assigned functionality.	
FUN.10	Once the start-up has been completed successfully the user must select “New Patient” or “Resume Ventilation” before the system transitions to self-test mode *Rationale:* in order to quickly resume ventilation for the same patient in case the unit had to be powered down	
FUN.10.1	If “New Patient” is selected, the user shall have to enter patient attributes and the completion of every step of the self-test procedure (FUN.6) shall be mandatory	
FUN.10.2	If “Resume Ventilation” is selected, the system shall load the last calibration parameters, alarm thresholds, and ventilation parameters from the last active patient ventilation.	
FUN.10.3	If “Resume Ventilation” is selected, every step of the self-test procedure FUN.6 can be skipped or optionally rerun individually.	
FUN.10.4	Once all self-test steps have been completed successfully, it shall be possible to proceed to the Standby Mode.	

FUN.10.5	In Standby Mode ventilation shall be off and it shall be possible to adjust all user-controlled parameters for ventilation and alarms before connecting to the patient and starting patient ventilation.	
FUN.10.6	Once the power of the system has been off for more than 15 minutes it shall not be possible to select "Resume Ventilation"	
FUN.11	The system shall connect to pressurized gas supply of oxygen and medical air and accept pressures up to 5.2 bar. *Rationale:* this covers the range of pressures available in hospital setting	
FUN.12	The system shall provide breathing air through a standard medical supply single-limbed patient circuit with a pneumatically controlled diaphragm expiration valve. *Rationale:* this is readily available medical supply	
FUN.13	The system shall measure and display the breathing rate (number of breathes per minute). *Rationale:* observing and identifying the monitored ventilation parameters is considered a primary operating function	ISO 80601-2-12 206.101
FUN.14	The system shall measure and display the percentage of oxygen in the gas being delivered to the patient. *Rationale:* observing and identifying the monitored ventilation parameters is considered a primary operating function	ISO 80601-2-12 206.101
FUN.15	The system shall measure the ventilator pressure at/near the inlet to the patient. *Rationale:* observing and identifying the monitored ventilation parameters is considered a primary operating function	ISO 80601-2-12 201.12.4.102 (b)
FUN.16	The system shall measure and display the volume of gas delivered to the patient per breathing cycle (tidal volume). *Rationale:* observing and identifying the monitored ventilation parameters is considered a primary operating function	ISO 80601-2-12 206.101
FUN.17	The system shall measure and display the flow of gas delivered to the patient per breathing cycle. *Rationale:* observing and identifying the monitored ventilation parameters is considered a primary operating function	ISO 80601-2-12 206.101
FUN.18	The system shall have a leak compensation feature for leaks in the patient breathing circuit which shall be disabled by default. *Rationale:* regulatory requirement	
FUN.18.1	The user shall be able to disable/enable the leak compensation feature at any time.	
FUN.18.2	When enabled, the leak compensation shall be activated by the Min PEEP alarm (SAV.15)	

FUN.19	The system shall have a pressure control ventilation (PCV) mode, as characterized by the following plots of pressure and flow versus time.  *Rationale:* this is the most appropriate procedure for COVID-19 patients as it allows the immediate reopening of the alveoli and is strongly recommended by the doctors and nurses in the COVID-19 wards of Lombardy, rather than the constant flow procedure. These characteristics of the ventilator pressure transient during the inspiratory cycle are crucial to avoid barotrauma and to minimise long term fatigue of muscles and alveoli induced by forced mechanical ventilation.
FUN.20	In PCV mode the breathing cycle shall be defined by inspiratory pressure P_{insp_PCV} relative to atmosphere, respiratory rate (RR_{PCV}) and the ratio between the inspiratory and expiratory times ($I{:}E_{PCV}$). *Rationale:* standard parameters to define PCV
FUN.21	In PCV mode, a new breathing cycle shall be initiated either after a breathing cycle is over, or by patient request during expiration. *Rationale:* while the main mode of PCV is the control of the breathing cycle timing by the ventilator, the patient has to have the ability to trigger a breath on his own
FUN.21.1	A new breathing cycle shall be initiated by a sudden drop in pressure below a user-settable threshold (Inhale Trigger Sensitivity). *Rationale:* In a pressure-regulated ventilator, the speed of pressure drop initiated by the patient is the easiest way to detect the spontaneous breathing attempt
FUN.21.2	A patient breath trigger shall reset the timer for the time-cycled breathing cycle. *Rationale:* Avoid breath stacking, which would lead to hyperventilation

FUN.22	In PCV mode it shall be possible to initiate with the push of a single button a lung recruitment procedure, termed **Recruitment Maneuver (RM**). **Note:** This maneuver is not allowed in North America. *Rationale:* The RM is an emergency procedure required immediately after intubation. RM consists in the prolonged lung inflation at increased inspiratory set pressure, as necessary to reactivate the alveoli immediately after intubation.	
FUN.23	The system shall provide means to switch from PCV to PSV while PCV ventilation is active. *Rationale:* the switchover between modes should not require stopping the ventilation in order to maintain ventilation of the patient	
FUN.23.1	When a PCV-to-PSV switch is initiated by the user the system shall ask the user for confirmation/setting of PSV parameters to be used	
FUN.23.2	The switch to PSV shall occur only after the PSV parameters have been confirmed and until that has happened the PCV ventilation shall continue	
FUN.23.3	The switch to PSV shall occur at the end of a PCV inspiratory time	

FUN.24	The system shall have a pressure support ventilation (PSV) mode, as characterized by the following plots of pressure and flow versus time.  *Rationale:* In PSV mode, the ventilator supports the patient who is supposed to breathe spontaneously. PSV is needed to wean patients off the ventilation by allowing them to strengthen the muscles involved in breathing. PSV is not suitable for patients unable to initiate breaths on their own.
FUN.25	In PSV mode the breathing cycle shall be initiated by a sudden drop in pressure below a user-settable threshold (Inhale Trigger Sensitivity) *Rationale:* In a pressure-regulated ventilator, the speed of pressure drop initiated by the patient is the easiest way to detect the spontaneous breathing attempt as per ventilator experts
FUN.26	In PSV mode the expiration phase shall start when the inspiratory flow drops below a setable fraction of the peak flow (Expiratory Trigger Setting) *Rationale:* Dropping inspiratory flow indicates the end of the inspiration
FUN.27	In PSV mode the system shall check for the presence of apnea, which occurs when a patient does not take new breath within the allowable apnea lag time. *Rationale:* In case the patient stops breathing (apnea) the system needs to be able to ensure that the patient continues to be ventilated.

FUN.27.1	If apnea is detected, an apnea alarm shall be triggered. *Rationale:* Clinician needs to be made aware of the fact that patient stops breathing	
FUN.27.2	If apnea is detected, the system shall automatically switch from PSV to PCV mode with pre-determined apnea backup settings for RR_{AP} , P_{insp_AP}, $I{:}E_{AP}$. RR_{AP} and P_{insp_AP} shall be set by the user. $I{:}E_{AP}$ will be fixed at 1:2 *Rationale:* in case of apnea the ventilator needs to take over and ensure that ventilation continues to assure patient safety	
FUN.28	In PCV and PSV mode there shall be the possibility to press a single button to initiate an **Expiratory Pause** that closes both inspiratory and expiratory valve at the end of the expiration phase as long as the operator holds the button but no longer than 60 sec *Rationale:* The expiratory pause allows the determination of the residual pressure above the PEEP level, the residual value being PEEP + AutoPEEP. AutoPEEP level for the patient, providing information on the level of obstruction in the exhalation channel. AutoPEEP may be zero for most patients or significantly different from zero for patients that have obstructions in the exhalation channel, as possibly generated by secretions. In this case, the small flow during exhalation may result in an incomplete drain of the alveoli during the expiration phase.	ISO 80601-2-12 201.107.1
FUN.29	In PCV and PSV mode there shall be the possibility to press a single button to initiate an **Inspiratory Pause** (IP) that closes both inspiratory and expiratory valve at the end of the inspiratory phase as long as the operator holds the button but no longer than 40 sec *Rationale:* The Inspiratory Pause will, allowing for the measurement of the Plateau Pressure (PP), the pressure reached inside the alveoli at the end of the inspiratory cycle. PP may be lower than the target inspiratory pressure P_{insp} provided by the ventilator. The difference between PP and the PEEP is called Driving Pressure, DP (DP = PP - PEEP).	ISO 80601-2-12 201.107.2
FUN.30	The high-level operation sequence shall follow the scheme shown in Figure 2.1	

2.1.1 Safety Related Functional Requirements

This section covers the functional requirements imposed on the system based on the initiating events necessitating mitigating functions.

ID	Requirement / Rationale	Input Ref.

FUN.31	Any normal operating mode or identified failure mode of the system and its components shall always result in a state of the system that is safe for the patient. *Rationale:* patient safety is primary concern	ISO 80601-2-12
FUN.32	In a worst-case failure, the controller shall leave the system in a state that allows the patient to inhale and exhale unimpeded. *Rationale:* patient safety is primary concern	ISO 80601-2-12 201.13.2.103
FUN.33	Any power failure shall leave the system in a state that allows the patient to inhale and exhale unimpeded. *Rationale:* patient safety is primary concern	ISO 80601-2-12
FUN.34	Any failure of the gas supply shall leave the system in a state that allows the patient to inhale and exhale unimpeded. *Rationale:* patient safety is primary concern	
FUN.35	The system shall prevent airborne contaminants (particulate, viral, bacterial) being delivered from the ventilator to the patient. *Rationale:* patient safety is primary concern	
FUN.36	The system shall prevent patient expiratory viral and bacterial contaminants from entering the atmosphere. *Rationale:* need to ensure that clinicians and other patients are not exposed	
FUN.37	The system shall have an internal power source that allows operation for 120 minutes past the failure of the external power source. *Rationale:* regulatory requirement	ISO 80601-2-12
FUN.38	The system shall have clearly ranked (high/medium/low priority) visual alarms. *Rationale:* regulatory requirement	ISO 60601-1-8
FUN.38.1	The system shall raise an alarm when a parameter value goes outside the range defined for its associated alarm.	
FUN.39	The system shall prompt the user before ventilation is started to enter user-controlled alarm thresholds for SAV.3- SAV.9 *Rationale:* alarm thresholds may vary from patient to patient	
FUN.40	The system shall react to the inspiratory airway pressure at the patient being exceeded (Max P_{insp} alarm SAV.4) (e.g. by coughing) by truncating the inspiratory phase and immediately transitioning to expiration, quickly relieving the pressure. *Rationale:* need to avoid excessive pressure in the lungs	
FUN.41	A failure of the GUI (e.g. GUI freezes) or a loss of communication between the GUI and the Controller shall raise a high-priority alarm and any ongoing ventilation process shall not be interrupted. *Rationale:* in order to keep the patient safe, the ventilation needs to continue even if there is no connection between the controller and the GUI	

FUN.42	The communication between Controller and GUI shall be reliable.

2.2 Measured and displayed parameters

ID	Requirement / Rationale	Input Ref.
The system shall measure and display the following values for the patient: *Rationale:* regulatory requirement		
FUN.43	Respiratory rate (**RR**) of the patient measured by the ventilator, in units of breaths per minute (bpm).	
FUN.44	Peak inspiratory pressure (**Peak** $\mathbf{P}_{insp}$) measured for the most recent breath.	
FUN.45	Positive end expiratory pressure (**PEEP**) measured (in cmH_2O) for the most recent breath.	
FUN.46	Tidal volume ($\mathbf{V}_{tidal}$) measured for the most recent breath (in mL).	
FUN.47	Minute volume ($\mathbf{V}_E$) measured (in slpm) by the ventilator.	
FUN.48	Fraction of inspired oxygen (**FiO**$_2$).	
FUN.48.1	The user shall set the desired FiO_2 value from which the +-3% alarm limits are derived. The input FiO_2 value will have to be manually adjusted by the user until the desired FiO_2 value is displayed.	
Indication in waveform *Rationale:* regulatory requirement		
FUN.49	Instantaneous airway pressure (**PAW**), measured in cmH_2O.	
FUN.50	Instantaneous **flow**, measured in slpm.	
FUN.51	Instantaneous tidal volume ($\mathbf{V}_{tidal}$), measured in mL.	
Parameters set by the user *Rationale:* regulatory requirement		
FUN.52	Ratio of Inspiratory time to Expiratory time (**I:E**).	
FUN.53	Maximum inspiratory pressure (**Max** $\mathbf{P}_{insp}$)	
Indication of the machine status *Rationale:* regulatory requirement		
FUN.54	**Level of battery**, i.e., the percentage of battery remaining.	
FUN.55	**Power source**: if the system is receiving power from the main supply, or if it is running on backup battery power.	
FUN.56	Value of the **temperature** inside the system unit is reported.	
FUN.57	Current **status** of the system (running/stopped, PCV/PSV) is reported.	
FUN.58	The remaining time for RM is displayed.	

2.3 Values and ranges

2.3.1 Common values and ranges

ID	Requirement / Rationale	Input Ref.
PER.1	Positive End Expiratory Pressure (PEEP) The expiratory pressure valve is adjusted by hand to set the desired PEEP value. Default: - | Range: 5-20 cm H_2O | Step Size: continuous *Rationale:* This allows the alarm thresholds for the PEEP out-of-range to be set.	
PER.2	Fraction of inspired oxygen (FiO_2) The desired FiO_2 is manually set on the gas blender and reported on the GUI. Default: - | Range: 21-100 (blender dependent) | Step Size: continuous *Rationale:* This allows the alarm thresholds for the FiO_2 out-of-range to be set.	
PER.3	The user shall be able to start Recruitment Maneuver (RM). **Note: Function shall be disabled in North America**	
PER.3.1	Before the start of procedure, the user shall be able to set the Pressure for the Recruitment Maneuver (PRM) Default: 20 cmH_2O | Range: 0-50 cm H_2O | Step Size: $\pm$ 1 cm H_2O	
PER.3.2	Before the start of procedure, the user shall be able to set timer RM (Time for Recruitment Maneuver). Default: 10 sec | Range: 1-30 sec | Step Size: $\pm$ 1 sec	

2.3.2 Default values and ranges for PCV parameters

ID	Requirement / Rationale	Input Ref.
Control Settings in PCV: The following parameters take default values indicated in requirements PER.4 - PER.7 and can be changed/controlled by the user in the allowed requirements indicated in PER.4 - PER.7		
PER.4	Respiratory Rate (RR_{PCV}) Default: 12 b/min | Range: 4-50 b/min | Step Size: 1 b/min	
PER.5	I:E Ratio ($I{:}E_{PCV}$) Default: 1:2 | Range: 1:1 - 1:4 | Step Size: 0.1 in E	

PER.6 Target inspiratory pressure (P_{insp_PCV})

Default	Range	Step Size
15 cm H_2O	2-50 cm H_2O	1 cm H_2O

PER.7 ITS

Default	Range	Step Size
3 cm H_2O/sec^2	1-9 cm H_2O/sec^2	1 cm H_2O/sec^2

2.3.3 Default values and ranges for PSV parameters

ID	Requirement / Rationale	Input Ref.
Control Settings in PSV mode: The following parameters take default values indicated in requirements PER.8 - PER.14 and can be changed/controlled by the user in the allowed range indicated in requirements PER.8 - PER.14		

PER.8 Target inspiratory pressure (P_{insp_PSV})

Default	Range	Step Size
15 cm H_2O	2-50 cm H_2O	1 cm H_2O

PER.9 Inhale trigger sensitivity (ITS_{PSV})

Default	Range	Step Size
3 cm H_2O/sec^2	1-9 cm H_2O/sec^2	1 cm H_2O/sec^2

PER.10 Expiratory trigger sensitivity (ETS)

Default	Range	Step Size
30%	5-60% of peak flow	1%

PER.11 Apnea lag

Default	Range	Step Size
30 sec	10-60 sec	1 sec

Apnea backup PCV settings

PER.12 Respiratory Rate (RR_{AP})

Default	Range	Step Size
-	4-50 b/min	1 b/min

PER.13 I:E Ratio ($I{:}E_{AP}$)

Default	Range	Step Size
1:2	-	-

PER.14 Target inspiratory pressure (P_{insp_AP})

Default	Range	Step Size
0 cm H_2O	2-50 cm H_2O	1 cm H_2O

Rationale: Default value of P_{insp_AP} in the apnea backup is left unset to ensure that the user set it in PSV mode in case of apnea lag.

2.3.4 Default Alarm Thresholds Values and Ranges

ID	Requirement / Rationale	Input Ref.
Control Settings		
PER.15	Max P_{insp}	ISO 80601-2-12: 201.12.4.106

Default	Range	Step Size
40 cm H_2O	10-80 cm H_2O	1 cm H_2O

PER.16 Min P_{insp}

Default	Range	Step Size
50% of Pinsp	10-100%	10%

PER.17 Max PEEP

Default	Range	Step Size
-	3-23 cm H_2O	1 cm H_2O

PER.18 Min PEEP

Default	Range	Step Size
-	0-20 cm H_2O	1 cm H_2O

PER.19 Max V_{tidal}

Default	Range	Step Size
990 mL	50-1500 mL	50 mL

PER.20 Min V_{tidal}

Default	Range	Step Size
10 mL	10-1500 mL	10 mL

PER.21 Apnea lag

Default	Range	Step Size
30 sec	10-60 sec	1 sec

PER.22 Max V_E

Default	Range	Step Size
80 slpm	2-80 slpm	1 slpm

PER.23 Min V_E

Default	Range	Step Size
2 slpm	2-80 slpm	1 slpm

PER.24 Min RR

Default	Range	Step Size
4 b/min	4-50 b/min	1 b/min

PER.25 Max RR

Default	Range	Step Size
50 b/min	4-50 b/min	1 b/min

2.4 Sensors and interfaces

2.4.1 Sensors

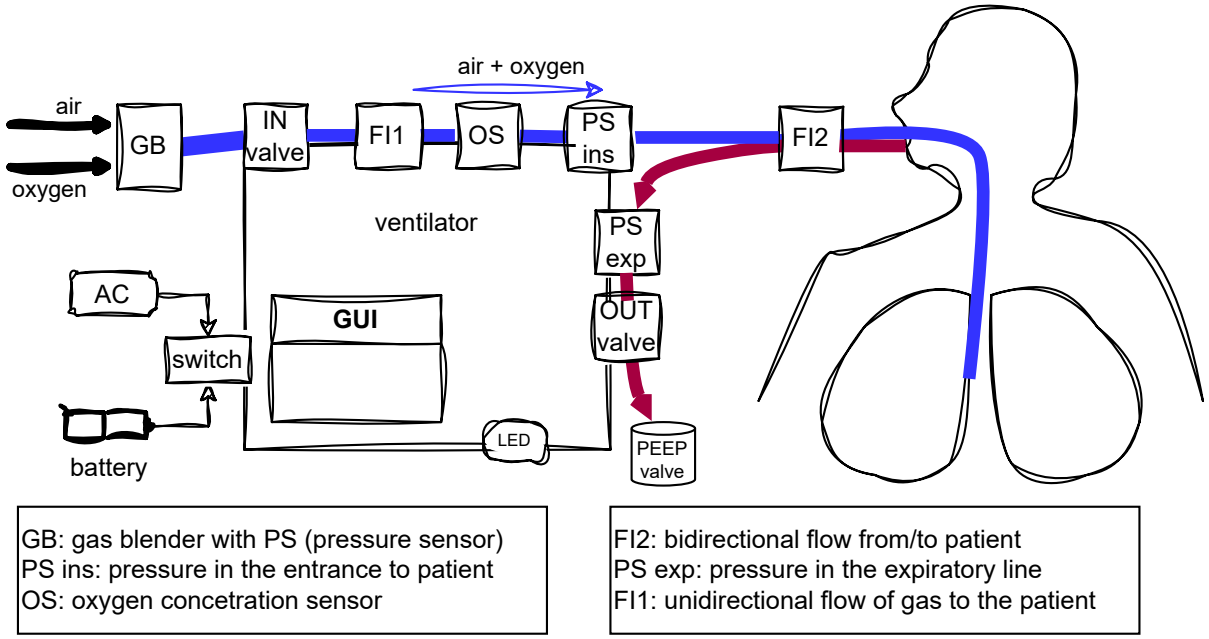


Figure 2.2: High level view of ventilator sensors

2.4.2 Interface between GUI and controller

ID	Requirement / Rationale	Input Ref.
The controller shall communicate the following parameters to the GUI when requested:		
INT.1	Airway pressure (PAW)	FUN.49
INT.2	Peak P_{insp}	FUN.44
INT.3	Measured Respiratory Rate (RR)	FUN.43
INT.4	Temperature	FUN.56
INT.5	V_E	FUN.47
INT.6	V_{tidal}	FUN.46
INT.7	Oxygen concentration (FiO_2)	FUN.48
INT.8	PEEP	FUN.45
INT.9	Battery power	FUN.55
INT.10	Battery charge level	FUN.54
INT.11	Remaining time for RM	FUN.58
INT.12	Current Status of the ventilator (running/stopped, PCV/PSV)	FUN.57
The GUI shall set the following parameters in the controller:		
INT.13	RR_{PCV}	PER.4
INT.14	$I{:}E_{PCV}$	PER.5
INT.15	P_{insp_PCV}	PER.6
INT.16	ITS_{PCV}	PER.7
INT.17	P_{insp_PSV}	PER.8
INT.18	ITS_{PSV}	PER.9

INT.19	ETS	PER.10
INT.20	Apnea lag	PER.11
INT.21	RR_{AP}	PER.12
INT.22	P_{insp_AP}	PER.14
INT.23	Max P_{insp}	PER.15
INT.24	Min P_{insp}	PER.16
INT.25	Min PEEP	PER.18
INT.26	Max PEEP	PER.17
INT.27	Max V_{tidal_exp}	PER.19
INT.28	Min V_{tidal_exp}	PER.20
INT.29	Max V_{tidal_insp}	PER.19
INT.30	Min V_{tidal_insp}	PER.20
INT.31	Max V_E	PER.21
INT.32	Min V_E	PER.22
INT.33	Min RR	PER.24
INT.34	Max RR	PER.25
INT.35	Start PCV	FUN.19
INT.36	Stop PCV/PSV	FUN.19, FUN.24
INT.37	Start PSV	FUN.24
INT.38	Expiratory Pause on	FUN.28
INT.39	Expiratory Pause off	FUN.28
INT.40	Inspiratory Pause on	FUN.29
INT.41	Inspiratory Pause off	FUN.29
INT.42	Recruitment Maneuver on	PER.3
INT.43	Recruitment Maneuver off	PER.3
INT.44	Pressure Recruitment Maneuver	PER.3.1
INT.45	Maximum RM time	PER.3.2

2.4.3 Interface between Hardware and Controller

ID	**Requirement / Rationale**	**Input Ref.**
The controller shall set the following parameters in the HW :		
INT.46	The value of the proportional solenoid valve that controls the inspiratory pressure to the patient (IN_valve). *Rationale:* the controller computes the value of the in valve to allow the patient the inspiration.	
INT.47	The value of the three-way simple solenoid valve used to control the pressure to the valve that permits patient expiratory breath (OUT_valve). *The port connected to the expiratory valve is normally open to the atmosphere. Rationale: the controller commands the out valve to allow the patient expiration.*	
INT.48	The value of the LED when an alarm is raised/reset	
The controller shall get the values from the following sensors (HW):		
INT.49	The digital spirometer flow sensor (FI1).	
INT.50	The electronic oxygen sensor (0% - 100%) (OS).	
INT.51	The differential pressure sensor to measure the flow to the patient (FI2).	

INT.52	The sensor that measures the expiratory pressure near the patient (PEEP) (PS_exp).
INT.53	The sensor that measures inspiratory pressure provided by the ventilator (PS_ins).
INT.54	The sensor that measures the supply gas pressure to the ventilator (GB).
INT.55	Temperature
INT.56	Battery charge level
INT.57	Power supply type
INT.58	Fan Tachometer

2.5 Alarm requirements

ID	Requirement / Rationale	Input Ref.
SAV.1	The system shall raise an alarm of at least low priority when the delivered oxygen concentration changes by more than 3% volume of a user-controlled target FiO_2 value. *Rationale:* a drop of oxygen concentration might indicate a failing gas supply.	ISO 80601-2-12 201.12.4.101
SAV.2	The system shall raise various alarms when the primary power source falls outside the range necessary to maintain normal operation. (related to essential performance as per Table 201.101 of the 80601-2-12) In particular: *Rationale:* regulatory requirement	ISO 80601-2-12 201.11.8.101
SAV.2.1	Upon successful switchover to backup battery (at least low priority).	ISO 80601-2-12 201.11.8.101 (d1)
SAV.2.2	When the backup battery nears depletion, and at least 10 min remain until the loss of ventilation at least a medium priority alarm shall be raised.	ISO 80601-2-12 201.11.8.101 (f1)
SAV.2.3	When the backup battery nears depletion, and at least 5 min remain until the loss of ventilation the alarm shall be escalated to high priority.	ISO 80601-2-12 201.11.8.101 (f2)
SAV.3	The system shall raise an alarm (at least low priority) when the minimum inspiratory airway pressure (Min P_{insp}) is not achieved.	
SAV.4	The system shall raise a high priority alarm when the peak inspiratory airway pressure (Max P_{insp}) is exceeded.	ISO 80601-2-12 201.12.4.106 (b1)
SAV.4.1	The high airway pressure alarm condition delay shall not exceed 200 ms and the ventilator shall: act to attempt to cause the pressure to start to decline within that duration; and act to prevent the pressure from continuing to rise.	ISO 80601-2-12 201.12.4.106 (g)

SAV.4.2	Whenever the high-pressure alarm condition occurs, the ventilator shall, within no more than two respiratory cycles or 15 s, whichever is less, reduce the airway pressure to either: the atmospheric pressure; or the set PEEP level.	ISO 80601-2-12 201.12.4.106 (h)
SAV.5	The system shall raise a PEEP alarm of at least medium priority if the expiratory airway pressure falls below the user-set low pressure alarm limit (Min PEEP).	ISO 80601-2-12 201.12.4.107 (c)
SAV.6	The system shall raise an alarm when the measured respiratory rate is below a user-controlled value (Min RR).	
SAV.7	The system shall raise an alarm when the measured respiratory rate exceeds a user-controlled value (Max RR).	
SAV.8	The system shall raise an alarm of at least medium priority when the expiratory tidal volume V_{tidal} is too low (Min V_{tidal}): patient is hypo-ventilating.	ISO 80601-2-12 201.12.4.103.1 (f,g)
SAV.9	The system shall raise an alarm of at least medium priority when the expiratory tidal volume V_{tidal} is too high (Max V_{tidal}).	ISO 80601-2-12 201.12.4.103.1 (f,g)
SAV.10	The system shall raise an alarm of at least low priority when the input gas pressure is below 3.7 bar.	ISO 80601-2-12 201.13.2.102 (C)
SAV.11	The system shall raise an alarm of at least low priority when the input gas pressure exceeds 5.2 bar.	ISO 80601-2-12 201.13.2.102 (c)
SAV.12	The system shall raise a high priority alarm when the airway pressure measured near the input valve is below a user-controlled value (Min P_{insp}).	ISO 80601-2-12 201.12.4.106 (b1)
SAV.13	The system shall raise a high priority alarm when the airway pressure measured near the input valve exceeds a user-controlled value (Max P_{insp}).	ISO 80601-2-12 201.12.4.106 (b1)
SAV.14	The system shall raise an alarm if there is significant leakage in the gas circuit (200 ml/min at 50 cmH2O) *Rationale:* ISO 80601-2-12 201.102.7.1 (a) requires that there should not be unintended leakage in the patient breathing circuit of higher than (200 ml/min at 50 cmH2O). Therefor,e such a condition should generate an alarm.	
SAV.15	The system shall raise a high priority alarm if there is an obstruction in the pneumatic circuit	ISO 80601-2-12 201.12.4.108 (b1)

SAV.15.1	The alarm condition delay shall not exceed more than two respiratory cycles or 5 s, whichever is greater.	ISO 80601-2-12 201.12.4.108 (c)
SAV.15.2	Whenever the obstruction alarm condition occurs, the ventilator shall, within no more than one respiratory cycle, reduce the airway pressure to either atmospheric pressure; or the set PEEP level.	ISO 80601-2-12 201.12.4.108 (d)
SAV.16	The system shall raise an alarm when the inspiratory flux is below a user-controlled value (Min V_E).	
SAV.17	The system shall raise an alarm when the inspiratory flux exceeds a user-controlled value (Max V_E).	
SAV.18	The system shall raise an alarm of at least medium priority when the expiratory flux is below a user-controlled value (Min V_E).	ISO 80601-2-12 201.12.4.103 (f2)
SAV.19	The system shall raise an alarm of least medium priority when the expiratory flux exceeds a user-controlled value (Max V_E).	ISO 80601-2-12 201.12.4.103 (f1)
SAV.20	The system shall raise an alarm of least medium priority if peak inspiratory pressure is 3 cmH_2O below the PEEP value.	ISO 80601-2-12 201.12.4.109
SAV.21	The system shall raise an alarm if the internal temperature of the system exceeds 75°C.	ISO 60601-1 13.1.
SAV.22	The system shall alarm for apnea (Apnea lag) in PSV mode. *Rationale:* required to ensure that patient on PSV who stops breathing is attended to	
SAV.23	The system shall alarm in case of a GUI failure (e.g. GUI freezes) or loss of communication between Controller and GUI.	
SAV.24	The system shall raise PEEP alarm of at least medium priority if the expiratory airway pressure exceeds the user-set desired pressure PEEP alarm limit (Max PEEP). (related to essential performance as per Table 201.101 of the 80601-2-12)	ISO 80601-2-12 201.12.4.107
SAV.24.1	The alarm condition delay for high PEEP alarm condition shall not exceed the duration of three inflations.	ISO 80601-2-12 201.12.4.107 (d)
SAV.25	The ventilator shall be equipped with an alarm system that detects a technical alarm condition to indicate when conditions in the patient breathing circuit reach the alarm limit (Min PEEP) for disconnection. (related to essential performance as per Table 201.101 of the 80601-2-12)	ISO 80601-2-12 201.12.4.109
SAV.26	The system shall alarm in case the communication of the controller with any of the sensors is lost	

3 GUI Requirements

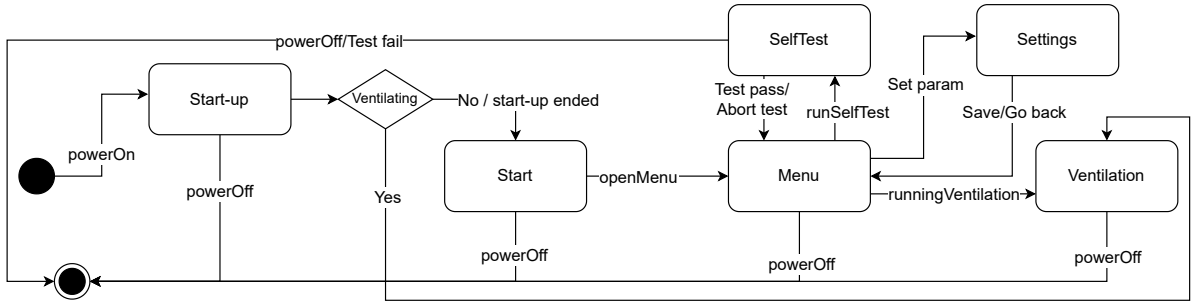


Figure 3.1: GUI state machine

ID	Requirement / Rationale	Input Ref.
GUI.1	GUI shall implement the following modes (see Figure 3.1):	FUN.4
GUI.1.1	Start-up Mode: In start-up mode the GUI initializes itself with default configuration parameters. Start-up mode is completed once start-up parameter validation and initialization have been completed.	
GUI.1.2	Start Mode: allows the user to resume ventilation.	
GUI.1.3	Menu Mode: allows the user to select different activities.	
GUI.1.4	Self Test Mode: allows the user to perform a sequence of tests.	
GUI.1.5	Ventilation Mode: the GUI is monitoring and controlling the ventilation of the patient.	
Start-up Mode: In start-up mode the GUI initializes itself with default configuration parameters.		
GUI.2	The transition from Start-up Mode to Ventilation occurs if the GUI finds that the controller is already running in ventilation mode. In this case when exiting the start-up mode, it resumes the ventilation *Rationale:* the GUI may have crashed while the controller keeps ventilating. When the GUI is restarted, it resumes its operation reading the settings from the controller.	FUN.10
GUI.3	The transition from Start-up Mode to Start shall occur once the configurations have been loaded and the controller is not running in ventilation.	FUN.10
Start Mode: In start mode the user can resume ventilation		
GUI.4	The transition from Start to Menu shall occur if the user wants to test the machine and set the proper parameters for a new patient. *Rationale:* the clinician decides to check the status of the machine sensors before starting ventilation.	FUN.4

GUI.5	The transition from Start to Menu shall occur if the doctor decides to resume ventilation and the system has not been powered off for more than 15 minutes. Self-test mode is optional. *Rationale:* the clinician wants to resume the ventilation of the connected patient, without performing the self test procedures.	FUN.10
Menu Mode: Menu mode allows the user to select different activities		
GUI.6	The transition from Menu to Self Test shall occur if the user wants to check the behavior of the machine. *Rationale:* the clinician tests the machine.	FUN.4
GUI.7	The transition from Menu to Ventilation shall occur when the Self test is passed, if required, and the clinician wants to proceed with the ventilation.	FUN.4
GUI.8	The transition from Menu to Settings shall occur when the Self test is passed if required, and the clinician wants to change the settings for the ventilation.	FUN.4
Self Test Mode: Self test mode allows the user to perform a sequence of tests		
GUI.9	The transition from Self Test to Menu shall occur if the test passes or the user decides to abort the test.	FUN.6
GUI.10	If the Self Test fails, the GUI exits, and the user shall obtain a replacement of the unit and tag the problematic unit for a maintenance inspection.	FUN.6

3.1 Start-up Mode

ID	Requirement / Rationale	Input Ref.
GUI.11	The GUI shall be able to test the communication with the Controller.	FUN.5.1
GUI.12	If the Controller is not ventilating, when start-up is finished, the GUI shall be able to move to Start Mode.	FUN.4
GUI.13	If Controller is ventilating: *Rationale:* if the GUI starts and the Controller is already ventilating the GUI shall be able to display the information of the ventilation. This can happen e.g. if the GUI crashes while running ventilation and then it is restarted.	
GUI.13.1	The GUI shall be able to update parameter settings with values read from the Controller.	
GUI.13.2	The GUI shall be able to immediately move to the main ventilation screen (Ventilation Mode) after having loaded parameters from the Controller.	
GUI.13.3	The ventilation is assumed to be running (the GUI is showing that ventilation is in progress).	
GUI.14	The GUI shall be able to check system memory.	FUN.5.1
GUI.15	The patient shall not be connected to the breathing circuit when the system is powered on and through start-up and self-test, a warning message shall be displayed at system startup.	FUN.5.3

3.1.1 Start-up Configuration Parameters

A set of default values for all parameters shall be provided and loaded from a configuration file on the machine when it is turned on. The default values are in Chapter 2.

ID	Requirement / Rationale	Input Ref.
PCV mode		
GUI.16	Respiratory Rate (RR_{PCV})	PER.4
GUI.17	I:E Ratio ($I:E_{PCV}$)	PER.5
GUI.18	Target inspiratory pressure (P_{insp_PCV})	PER.6
GUI.19	Inhale trigger sensitivity (ITS_{PCV})	PER.7
PSV mode		
GUI.20	Target inspiratory pressure (P_{insp_PSV})	PER.8
GUI.21	Inhale trigger sensitivity (ITS_{PSV})	PER.9
GUI.22	Expiratory trigger sensitivity (ETS)	PER.10
GUI.23	Apnea lag	PER.11
Apnea backup		
GUI.24	Respiratory Rate (RR_{AP})	PER.12
GUI.25	I:E Ratio ($I:E_{AP}$)	PER.13
GUI.26	Target inspiratory pressure (P_{insp_AP})	PER.14
Alarm thresholds		
GUI.27	Max P_{insp} *Rationale:* Max P_{insp} is the maximum value for PAW before the alarm is generated	PER.15
GUI.28	Min P_{insp} *Rationale:* Min P_{insp} is the minimum value for PAW before the alarm is generated	PER.16
GUI.29	Max V_{tidal_exp}	PER.19
GUI.30	Min V_{tidal_exp}	PER.20
GUI.31	Max V_{tidal_insp}	PER.19
GUI.32	Min V_{tidal_insp}	PER.20
GUI.33	Min V_E	PER.23
GUI.34	Max V_E	PER.22
GUI.35	Min RR	PER.24
GUI.36	Max RR	PER.25
GUI.37	Min PEEP	PER.18
GUI.38	Max PEEP	PER.17
RM parameters		
GUI.39	Pressure for the Recruitment Maneuver (PRM)	PER.3.1
GUI.40	Time for Recruitment Maneuver (timer RM)	PER.3.2
Constant parameters		
GUI.41	Maximum duration of Inspiratory Pause	FUN.29
GUI.42	Maximum duration of Expiratory Pause	FUN.28
GUI.43	The time between the end of the inspiratory phase and the start of the trigger window (triggerWindowDelay) = 0.7 sec *Rationale:* This time window is required to allow the pressure going from P_{insp} to PEEP at the end of inspiration phase.	

GUI.44	Maximum inspiratory time in PSV mode (max_insp_time_psv) = 7 sec *Rationale:* it is required to avoid the patient staying infinitely in inspiration phase if flow drop is not detected (see CONT.33)	

3.2 Start Mode

ID	Requirement / Rationale	Input Ref.
GUI.45	The user shall be able to resume the ventilation:	FUN.10
GUI.45.1	The GUI shall be able to move to "Ventilation Mode".	FUN.10
GUI.45.2	The GUI shall be able to load setting parameters from the last known configuration saved by the system and stored in the system. This configuration is protected by a md5 file to guarantee that the settings are not corrupted. Before loading, the GUI checks the integrity of the file.	FUN.10
GUI.45.3	The GUI shall be able to start the ventilation as needed	FUN.10
GUI.45.4	The user shall be able to select a new patient. The GUI shall move to "Menu Mode".	FUN.10
GUI.45.5	The GUI shall be able to load parameters from the default configuration file.	FUN.10
GUI.45.6	The user shall be able to enter user controlled parameters for ventilation and alarm at the beginning of the normal ventilation mode that is chosen.	FUN.10
GUI.46	The GUI requires a configuration file. Upon detecting that a configuration file does not exist, the application shall report the failure condition and terminate. *Rationale:* the ventilator requires a configuration file for initialization.	

3.3 Menu Mode

ID	Requirement / Rationale	Input Ref.
GUI.47	The user shall be able to start a self test procedure from the self test mode menu.	FUN.6
GUI.48	The user shall be able to set the parameters for ventilation. If the user selects to change the settings, the GUI shall be able to move to the settings state in the ventilation mode only if self test has been passed if it is required ("new patient" was selected)	FUN.6
GUI.49	The user shall be able to proceed to ventilation only if the self test has been passed if it is required ("new patient" was selected).	FUN.6

3.4 Self-Test Mode

In self-test mode the user performs some checks (see FUN.6 and its sub-requirements), if they pass the ventilator can continue to the next state.

ID	Requirement / Rationale	Input Ref.
GUI.50	The user shall be able to start the self-test procedure from the self-test mode menu.	FUN.6
GUI.50.1	The user shall be able to interrupt the self-test procedure and return to the main menu of self-test mode.	FUN.6.2
GUI.50.2	If the self-test fails, the self-test procedure is interrupted and the GUI stops.	FUN.6.2
GUI.50.3	Only after the self-test procedure is successfully completed, the user shall be able to proceed to return to the main menu.	FUN.6.2

3.5 Ventilation Mode

ID	Requirement / Rationale	Input Ref.
GUI.51	When the GUI enters the Ventilation mode, it shall be able to show the real time data coming from the controller *Rationale:* this is the main screen containing all the data coming from the controller	
GUI.52	The Ventilation mode shall implement the following modes (see Figure 3.1): 1. Show Real Time Data Mode: display health parameters 2. Settings Mode: update and display setting parameters 3. Frozen view Mode: allow the user to freeze the screen and analyse waveforms in detailed 4. Alarm Settings Mode: allow the user to perform a sequence of tests	
GUI.53	The GUI shall be able to show the alarms when they are raised.	FUN.38
GUI.54	The user shall be able to snooze an alarms when they have been raised. *Rationale:* the user is able to snooze alarms when they are raised by the system	
GUI.55	The user shall be able to lock the GUI; it will never lock itself automatically. *Rationale:* the user must lock the GUI to avoid mistakes when he has to clean the ventilator	
GUI.56	The user shall be able to unlock the GUI, it will never unlock itself automatically. *Rationale:* the user must unlock the GUI when he has finished ventilator cleaning procedure	
GUI.57	The user shall be able to enter the PIN to unlock the GUI. *Rationale:* a pin is necessary to unlock the GUI to be sure that the user wants to unlock it. Only holding a button is not enough because it can be done accidentally.	

GUI.58	The user shall be able to start the inspiratory pause by pushing and holding a GUI button. The inspiratory pause shall end when the button is released or no later than 40 sec after initiation.	FUN.29
GUI.59	The user shall be able to start the expiratory pause by pushing and holding a GUI button. The expiratory pause shall end when the button is released or no later than 60 sec after initiation	FUN.28
GUI.60	Expiratory and inspiratory pause buttons shall both be disabled for 1 minute after the end of a pause.	FUN.28

3.6 Show Real Time Data Mode

ID	Requirement / Rationale	Input Ref.
GUI.61	The user shall be able to start ventilation in PCV or PSV by pressing a start button. *Rationale:* the user can choose the ventilation mode.	
GUI.61.1	The user shall be able to change ventilation mode (PCV or PSV) even if the machine is already ventilating.	FUN.23
GUI.61.2	If ventilation is on, the system shall ask the user for confirmation/setting of PSV parameters (P_{insp_PSV}, ITS_{PSV}, ETS) and apnea parameters (apnea lag, P_{insp_AP} and RR_{AP}) when a PCV to PSV switch is initiated by the user. Until that has happened the PCV ventilation shall continue.	FUN.23
GUI.61.3	Before running the PSV mode for the first time for a given patient, the user shall set the Apnea backup settings.	FUN.27.2
GUI.61.4	The GUI shall ask for a confirmation when start mode is requested.	FUN.23.1
GUI.62	The user shall be able to stop ventilation by pressing a stop button if running. *Rationale:* if the user wants to stop the ventilation in PCV or PSV mode he can do it under his responsibility.	
GUI.62.1	The GUI shall ask for a confirmation when a stop is requested.	
GUI.63	The user shall be able to freeze the monitored waveforms for further inspection while ventilation continues. The GUI will move to the Frozen mode. *Rationale:* this functionality is required to analyse in detail the waveforms values.	
GUI.64	The user shall be able to change the alarm settings.	FUN.39
GUI.65	The user shall be able to change the settings of the user-controlled ventilation parameters.	FUN.10

The GUI shall be able to display the following information.

ID	Requirement / Rationale	Input Ref.
GUI.66	The GUI shall be able to always show current active alarms	

Values measured and displayed by the ventilator for the patient		
GUI.67	Respiratory rate (**RR**) of the patient measured by the ventilator, in units of breaths per minute (bpm).	FUN.43
GUI.68	Peak inspiratory pressure (**Peak $\mathbf{P}_{insp}$**) measured for the most recent breath.	FUN.44
GUI.69	Positive end expiratory pressure (**PEEP**) measured (in cmH_2O) for the most recent breath.	FUN.45
GUI.70	Tidal volume ($\mathbf{V}_{tidal}$) measured for the most recent breath (in mL).	FUN.46
GUI.71	Minute volume (V_E) measured (in lpm) by the ventilator.	FUN.47
GUI.72	Fraction of inspired oxygen (**FiO_2**).	FUN.48
Indication in waveform		
GUI.73	Instantaneous airway pressure (**PAW**), measured in cmH_2O.	FUN.49
GUI.74	Instantaneous flow (V_E), measured in lpm.	FUN.50
GUI.75	Instantaneous tidal volume ($\mathbf{V}_{tidal}$), measured in mL.	FUN.51
Parameters shown to the user if in PCV mode		
GUI.76	Ratio of Inspiratory time to Expiratory time (**I:E**) set by the user	FUN.52
GUI.77	Maximum Inspiratory pressure (**Max $\mathbf{P}_{insp\_PCV}$**)	FUN.53
Parameters shown to the user if in PSV mode		
GUI.78	Maximum Inspiratory pressure (**Max $\mathbf{P}_{insp\_PSV}$**)	FUN.53
Parameters shown in RM mode		
GUI.79	Remaining time for RM	FUN.58
Indication of the machine status		
GUI.80	*Level of battery*, i.e., the percentage of battery remaining.	FUN.54
GUI.81	*Power source*: if the ventilator is receiving power from the main supply, or if it is running on backup battery power.	FUN.55
GUI.82	Value of the *temperature* inside the ventilator unit is reported in °C.	FUN.56
GUI.83	Current *status* of the ventilator (running/stopped, PCV/PSV).	FUN.57

3.7 Settings Mode

ID	Requirement / Rationale	Input Ref.
GUI.84	The GUI shall display the current value of the parameters *Rationale:* the user can see current value of ventilator parameters	
GUI.85	The user shall be able to load parameters default value. *Rationale:* the user must always be able to load parameters default value.	

GUI.86	The GUI shall store the last setting values in a file to be read in case the ventilation is resumed (see resume operation in Start Mode). *Rationale:* In case of "Resume ventilation" the user wants to start ventilation with previous parameters.	

The following parameters take values indicated in Section 2.3.

ID	Requirement / Rationale	Input Ref.
GUI.87	The GUI shall provide a menu page to insert and send the settings to the Controller.	SAV.50
GUI.87.1	Before sending the settings to the Controller, the GUI shall ask for confirmation to the user. After the confirmation the GUI shall transmit the parameters to the Controller and check that the controller accepts the values. The GUI shall read back the parameters from the Controller and check that they are equal to the values set by the user. *Rationale:* Asking confirmation to the user before sending the values will mitigate the risks of setting wrong values due to human errors. Checking the values with the get commands will confirm that the controller has the parameters set required by the user.	SAV.50
GUI.88	The GUI shall send the settings to the Controller using an ENTER / CONFIRM paradigm.	SAV.50
Common Control Settings		
GUI.89	Desired FiO_2	PER.2
Control Settings in PCV		
GUI.90	Respiratory Rate (RR_{PCV})	PER.4
GUI.91	I:E Ratio ($I{:}E_{PCV}$)	PER.5
GUI.92	Target inspiratory pressure (P_{insp_PCV})	PER.6
GUI.93	Inhale trigger sensitivity (ITS_{PCV})	PER.7
Control Settings in PSV		
GUI.94	Target inspiratory pressure (P_{insp_PSV})	PER.8
GUI.95	Inhale trigger sensitivity (ITS_{PSV})	PER.9
GUI.96	Expiratory trigger sensitivity (ETS)	PER.10
GUI.97	Apnea lag	PER.11
Apnea backup settings		
GUI.98	Respiratory Rate (RR_{AP})	PER.12
GUI.99	I:E Ratio ($I{:}E_{AP}$) *Rationale:* The value of the I:E Ratio when recovering from apnea lag is fixed.	PER.13
GUI.100	Target inspiratory pressure (P_{insp_AP})	PER.14
Control Settings in RM		
GUI.101	Pressure for the Recruitment Maneuver (PRM)	PER.3.1
GUI.102	Timer RM (Time for Recruitment Maneuver).	PER.3.2

3.8 Frozen Mode

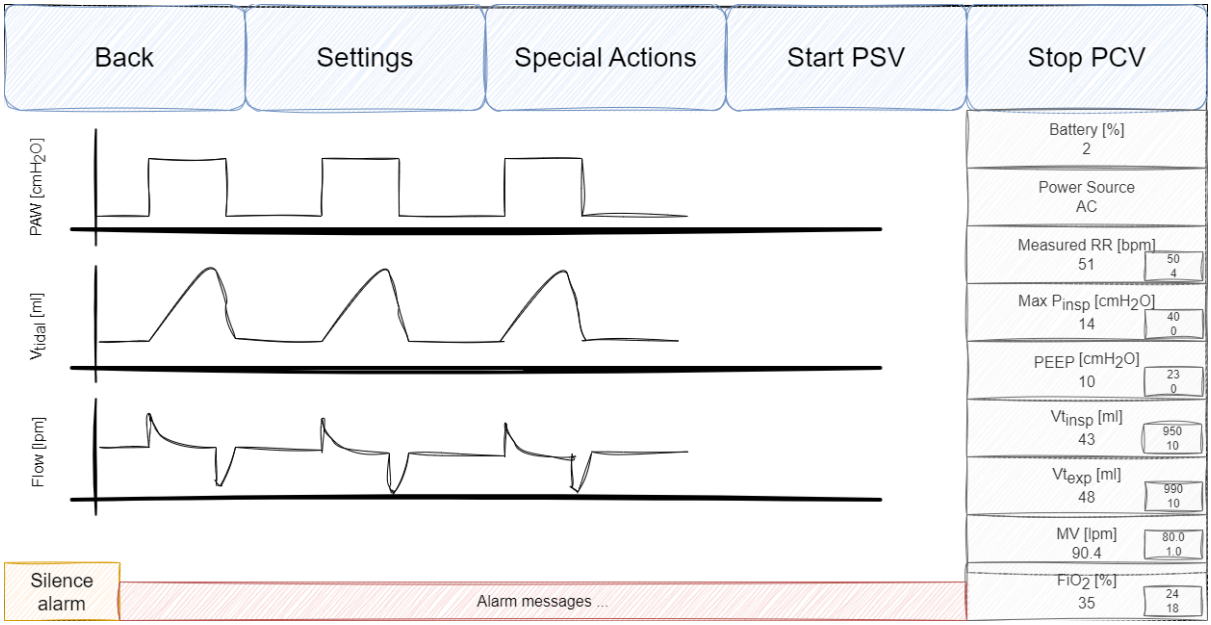


Figure 3.2: Draft of GUI

ID	Requirement / Rationale	Input Ref.
GUI.103	Frozen waveforms shall be shifted and re-scaled along both the vertical and the horizontal axes.	
GUI.104	The user shall be able to quit the frozen mode.	
GUI.105	The ventilation shall continue uninterrupted when Frozen Mode is enabled.	

3.9 Alarm settings Mode

ID	Requirement / Rationale	Input Ref.
GUI.106	During Alarm setting mode, the user shall be able to change the boundaries for raising alarms (the ranges are listed in Section 2.3).	PER.15 PER.16 PER.18 PER.19 PER.20 PER.21 PER.22 PER.23 PER.24 PER.25 PER.17
GUI.107	The user shall be able to select the parameters they want to display in Show RealTime Data Mode and their order.	

4 Controller Requirements

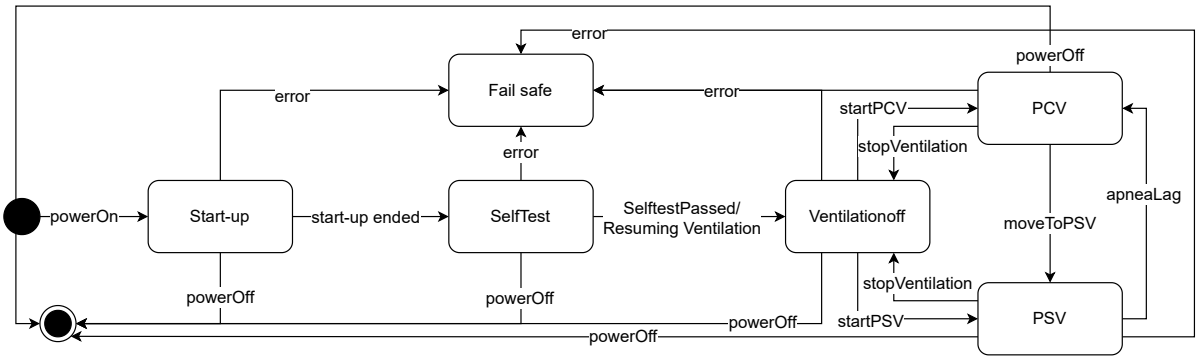


Figure 4.1: Controller state machine

ID	Requirement / Rationale	Input Ref.
CONT.1	The controller shall implement the following modes (see Figure 4.1):	FUN.4
CONT.1.1	Start-up Mode: In start-up mode the controller initializes itself with default configuration parameters (if any), checks the system memory and the communication of the controller with the sensors and valves, as well as between the controller and the GUI. Start-up mode is completed once the required activities have been completed.	FUN.5
CONT.1.2	Self-Test Mode: in the Self Test mode the controller allows the GUI to do all the operations necessary to perform the self-test.	FUN.6
CONT.1.3	VentilationOff: In ventilation off, the machine does not ventilate, the in valve is closed and the out valve is opened.	
CONT.1.4	Pressure Controlled Ventilation Mode: Pressure Controlled Ventilation mode is used when patients have no spontaneous respiration.	FUN.19
CONT.1.5	Pressure Support Ventilation Mode: Pressure Support Ventilation mode is used when the patients are able to initiate every breath and the machine supports them.	FUN.24
CONT.1.6 CONT.1.7	Fail-safe: the controller forces input and output valves to their de-energized states (in valve close and out valve open)	
Start-up Mode: In start-up mode the controller initializes itself with default configuration parameters.		
CONT.2	The transition to Start-up Mode shall be allowed by pushing the power button located on the back side of the ventilator unit to turn it on.	FUN.5

CONT.3	The transition from Start-up Mode to Self test Mode shall occur once the configurations have been loaded and the internal checking is terminated. *Rationale:* At this point, the monitoring module is able to carry out the assigned functionality.	FUN.5
Self-test Mode: In the Self Test mode, the controller allows the GUI to do all the operations necessary to perform the self-test.		
CONT.4	The transition from Self-Test Mode to VentilationOff Mode shall occur:	FUN.6
CONT.4.1	When the self-test procedure has successfully been completed	FUN.6
CONT.4.2	When the GUI asks for resuming ventilation	FUN.6
Ventilation Off: In ventilation off, the machine does not ventilate, the in valve is closed and the out valve is opened.		
CONT.5	The transition from VentilationOff to PSV shall occur if the change mode command is received from the GUI. *Rationale:* the ventilation starts in PCV mode when the user selects the start command from the GUI.	
CONT.6	The transition from VentilationOff to PCV mode shall occur if the change mode command is received from the GUI. *Rationale:* the ventilation starts in PSV mode when the user selects the start command from the GUI.	
PCV Mode: In PCV mode patients have no spontaneous respiration.		
CONT.7	The transition from PCV to PSV shall occur if ventilation is on, the transition from PCV to PSV shall occur at the end of a PCV inspiratory time if the change mode command has been received from the GUI. *Rationale:* the doctor decides when the patient has some ability to breathe spontaneously.	FUN.23
CONT.8	The transition from PCV to VentilationOff shall occur if the user stops the ventilation in PCV mode. *Rationale:* the ventilation stops when the user selects the stop command from the GUI.	
PSV Mode: In PSV mode patients are able to initiate every breath, and the machine supports them.		
CONT.9	The transition from PSV to PCV shall occur if the patient does not trigger a breath within the time of the apnea trigger window. The switch shall occur with respiratory rate, target inspiratory pressure and I:E defined for the apnea backup mode. *Rationale:* the patient is not able to breathe	FUN.27
CONT.10	The transition from PSV to VentilationOff shall occur if the user stops the ventilation in PSV mode. *Rationale:* the ventilation stops when the user selects the stop command from the GUI.	
Final State (Stop Mode): In Final State the machine is turned off.		

CONT.11	Final State shall be reached by pushing the power button located on the back side of the ventilator unit to turn it off. *Rationale:* the ventilator is turned off when the user pushes the power button on the ventilator unit.	
CONT.11.1	During Final state, all parameters (if any) are to be safely stored before the final state is complete and the unit is de-energized.	

4.1 Start-up Mode

ID	Requirement / Rationale	Input Ref.
CONT.12	A set of default values for all parameters shall be provided and loaded from a configuration file on the machine when it is turned on. The parameters are listed in Section 3.1.1.	FUN.5
CONT.13	The controller shall check the communication of the controller with the sensors and valves.	FUN.5.1
CONT.14	The controller shall check the communication of the controller with GUI.	FUN.5.1
CONT.15	If the pressure sensor fails to connect or reports an error condition after a fixed number of retries (maximum 5), the controller shall transition to the fail-safe mode.	
CONT.16	If the external ADC fails to initialize or reports an error condition after a fixed number of retries (maximum 5), the controller shall transition to the fail-safe mode.	

4.2 Self-test Mode

ID	Requirement / Rationale	Input Ref.
CONT.17	During the self test mode the controller shall allow the GUI to perform all the self-test specified in the FUN.6.	FUN.6
CONT.18	During the self test mode the controller shall perform the self-test specified in the FUN.6.	FUN.6
CONT.19	If the Self-test fails, the controller shall not be able to proceed to ventilation.	FUN.6

4.3 PCV Mode

ID	Requirement / Rationale	Input Ref.

CONT.20	In PCV mode the breathing cycle shall be defined by inspiratory pressure P_{insp_PCV} relative to atmosphere, respiratory rate (RR_{PCV}) and the ratio between the inspiratory and expiratory times ($I{:}E_{PCV}$). Rationale: this is the most appropriate procedure for COVID-19 patients as it allows the immediate reopening of the alveoli and is strongly recommended by the doctors and nurses in the COVID-19 wards, rather than the constant flow procedure. These characteristics of the ventilator pressure transient during the inspiratory cycle are crucial to avoid barotrauma and to minimise long term fatigue of muscles and alveoli induced by forced mechanical ventilation.	FUN.19	
CONT.21	The breath cycle shall start with the inspiration phase.	FUN.19	
CONT.22	The cycle starts with the inspiration phase that lasts an *Inspiratory time* $I = 60$ x $I{:}E_{PCV}/(RR_{PCV}$ x $(1 + I{:}E_{PCV}))$ seconds. After that the expiration phase begins.	FUN.20	
CONT.23	At the end of an inspiration phase, if the Inspiratory Pause is set by the GUI, an Inspiratory Pause shall start (see CONT.41).	FUN.29	
CONT.24	At the end of an inspiration phase, if inspiratory pause is not required and the Recruitment Maneuver (RM) is set by the GUI, a Recruitment Maneuver shall start (see CONT.43).	FUN.22 PER.3	+
CONT.25	When in the expiration phase, a new inspiration shall be initiated either after a breathing cycle is over, or when a spontaneous breath is detected. The maximum duration of the expiration phase (i.e., the *Expiratory time*) yields $E = 60$ / $(RR_{PCV}$ x $(1 + I{:}E_{PCV}))$ Rationale: While the main mode of PCV is mandatory breathing control with constant rate, clinical advice is that the patient also needs to be able to trigger a breath spontaneously.	FUN.21	
CONT.26	Within the trigger window during the expiratory phase, in the case of spontaneous breathing, the ventilator shall trigger a new breathing cycle (i.e., it goes in inspiration phase) when it detects a sudden drop in pressure below the inhale trigger sensitivity (i.e., it yields the condition $drop\text{-}in(PAW) < ITS_{PCV}$). Rationale: In a pressure-regulated ventilator, the speed of pressure drops initiated by the patient is the easiest way to detect the spontaneous breathing attempt as per ventilator experts.	FUN.21	
CONT.27	If the controller is in the expiration phase, and it does not detect a spontaneous breath (i.e., the condition $drop\text{-}in(PAW) > ITS_{PCV}$ is false), within the expiration time, if the Expiratory Pause start is set by the GUI, an Expiratory Pause shall start (see CONT.42).	FUN.28	

CONT.28	The target inspiratory pressure level shall be controlled by the Inspiratory Pressure parameter (P_{insp_PCV}) and it is kept constant.	FUN.20

4.4 PSV Mode

ID	Requirement / Rationale	Input Ref.
CONT.29	The Pressure Support Ventilation (PSV) mode shall support the breathing of the patient with positive pressure up to a peak value of P_{insp_PSV} while the patient triggers every breath and maintains control of the respiratory rate. *Rationale:* PSV is not suitable for patients unable to initiate breaths on their own.	FUN.24
CONT.30	The breath cycle shall start with the inspiration phase.	FUN.24
CONT.31	The target inspiratory pressure level shall be controlled by the Inspiratory Pressure parameter (P_{insp_PSV}).	FUN.24
CONT.32	The inspiration phase lasts until the inspiration peak is reached but no later than the *max_insp_time_psv* is over. After that the expiration phase begins. *Rationale:* In PSV mode, the ventilator supports the patient who is supposed to breathe spontaneously. In case a spontaneous expiration is not triggered, the ventilator forces the expiration phase after a suitable timeout (around 7 sec) to wait for a spontaneous breath.	FUN.40
CONT.33	When the inspiratory flow (V_E) drops below a fraction of the peak flow (Expiratory Trigger Setting (ETS)) of a given breath (i.e., it yields the condition V_E<*ETS*Peak* V_E), the ventilator shall stop providing pressure allowing exhalation.	FUN.26
CONT.34	At the end of an inspiration phase, if the Inspiratory Pause is set by the GUI, an Inspiratory Pause shall start (see CONT.41).	FUN.29
CONT.35	At the end of an inspiration phase if no inspiration pause is required and the Recruitment Maneuver (RM) is set by the GUI, a Recruitment Maneuver shall start (see CONT.43).	PER.3
CONT.36	If the patient is in expiration phase:	
CONT.36.1	A new inspiration shall be initiated by a sudden drop in pressure below the inhale trigger sensitivity (ITS_{PSV}), which shall be set by the user (i.e., it yields the condition *drop-in(PAW)* > ITS_{PSV}). *Rationale:* In a pressure-regulated ventilator, the speed of pressure drop initiated by the patient is the easiest way to detect the spontaneous breathing attempt as per ventilator experts.	FUN.25

CONT.36.2	If the controller is in expiration phase and a spontaneous breath is not detected (i.e., the condition *drop-in(PAW) > ITS_{PSV})* is false), within the interval [*min_exp_time_psv* : *apnea lag*], if the Expiratory Pause is set by the GUI, an Expiratory Pause shall start (see CONT.42).	FUN.28
CONT.36.3	min_exp_time_psv shall be the half of the last_inspiration_time. min_exp_time_psv shall be in the interval [0.4 : 2] sec. *Rationale:* The min_exp_time_psv prevents moving immediately to inspiration allowing the patient to expirate.	
CONT.37	If the patient does not trigger a breath within the time of the apnea trigger window (apnea lag) the ventilator shall switch to PCV mode (apnea backup ventilation) with respiratory rate RR_{AP}, inspiratory pressure P_{insp_AP}, and the ratio between inspiratory time and Expiratory time $I{:}E_{AP}$. *Rationale:* Need to ensure patients continue to receive breaths. The operator needs to set the apnea backup PCV setting before starting the ventilation in PSV mode, otherwise the ventilator will not start operating.	FUN.27

4.5 Requirements Common to all Modes

ID	Requirement / Rationale	Input Ref.
CONT.38	When the ventilator is in Start-up or VentilationOff mode, the in valve pressure shall be set to close and the out valve shall be open. *Rationale:* if the machine is not ventilating the valves are in a secure configuration state, in valve is closed and out valve is opened.	
CONT.39	When the ventilator is in an Inspiration state, the out valve shall be closed and the in valve pressure shall be set to target inspiratory pressure (P_{insp} of the corresponding mode).	
CONT.39.1	P_{insp_PCV} if current mode is PCV.	FUN.20
CONT.39.2	P_{insp_PSV} if current mode is PSV.	FUN.24
CONT.39.3	P_{insp_AP} if current model is PCV from apnea backup.	FUN.27.2
CONT.40	When the ventilator is in an expiration state the in valve shall be closed (pressure 0) and the out valve shall be open. *Rationale:* The ventilator opens the out valve to allow the patient to expirate, while the in valve is closed to avoid air in.	

CONT.41	In PCV and PSV modes there shall be the possibility to initiate an Inspiratory Pause if it is set by the GUI. *Rationale:* The Inspiratory Pause will initiate a forced hold at the end of inspiration, allowing for the measurement of the Plateau Pressure (PP), the pressure reached inside the alveoli at the end of the inspiratory cycle. PP may be lower than the Set Inspiratory Pressure (SIP) provided by the ventilator. The difference between PP and the PEEP is called Driving Pressure, DP (DP = PP - PEEP).	FUN.29
CONT.41.1	When the Inspiratory Pause is set by the GUI, the ventilator shall wait for the end of the next inspiration phase, and if the Inspiratory Pause still required, both the inspiratory and expiratory valves will close until the inspiratory pause is stopped by the GUI.	FUN.29
CONT.41.2	When inspiratory pause timeout (max_ins_pause) is over, the cycle shall proceed immediately to expiration. *Rationale:* The timeout prevents stopping the patient breath cycle in case of human error.	
CONT.42	In PCV and PSV modes there shall be the possibility to initiate an Expiratory Pause if it is set by the GUI. *Rationale:* The Expiratory Pause will initiate a forced hold at the end of expiration, allowing the measurement of the AutoPEEP level for the patient, providing information on the level of obstruction in the exhalation channel. AutoPEEP may be zero for most patients or significantly different from zero for patients that have obstructions in the exhalation channel, as possibly generated by secretions. In this case, the small flow during exhalation may result in an incomplete drain of the alveoli during the expiration phase.	FUN.28
CONT.42.1	When the Expiratory Pause is set by the GUI, the ventilator shall wait for the end of the next expiration phase, and if the Expiratory Pause is still required, both the inspiratory and expiratory valves will close until the expiratory pause is stopped by the GUI.	FUN.28
CONT.42.2	When expiratory pause timeout (max_exp_pause) is over, the cycle shall proceed immediately to inspiration. *Rationale:* the timeout prevents stopping the patient breath cycle in case of human error.	
CONT.43	In PCV and PSV mode, at the end of an inspiration and if inspiratory pause is not required, it shall be possible to initiate a lung recruitment procedure, termed Recruitment Maneuver (RM), if it is required by the GUI. Not available in North America. *Rationale:* The RM is an emergency procedure required immediately after the end of the intubation. RM consists in the prolonged lung inflation at increased inspiratory set pressure, as necessary to reactivate the alveoli immediately after intubation.	FUN.22

CONT.43.1	The controller shall stop RM if it is required from the GUI. *Rationale:* The GUI stops the RM if required by the user.	
CONT.43.2	The Recruitment Maneuver, if not actively stopped by the GUI, has a timeout (*max_rm_time*). After the Recruitment Maneuver phase expiration phase begins. *Rationale:* It is not reasonable to keep the patient in this emergency state without letting him breathe.	
CONT.43.3	In RM the out valve shall be closed and the in valve shall be opened to allow lung inflation at PRM.	FUN.22
CONT.44	If PAW exceeds Max P_{insp} during inspiration, the cycle shall proceed immediately to expiration.	FUN.40
CONT.45	Before monitoring a sudden drop in pressure below the inhale trigger sensitivity ITS, the controller shall wait for the trigger window (0.7 sec).	

5 Alarms

ID	Requirement / Rationale	Input Ref.
AL.1	The user shall be able to set alarm thresholds when the ventilator is either ventilating or not.	FUN.39
AL.1.1	If ventilator is ventilating, the alarm threshold used while user changes are the last saved.	FUN.39
AL.2	The visual alarms shall follow the requirements listed in Section 5.2.	
AL.3	The system shall have clearly ranked (high/medium/low priority) visual alarms. *Rationale:* regulatory requirement	ISO 60601-1-8 + FUN.38
AL.4	ALARM SYSTEMS Shall generate visual ALARM SIGNALS to indicate the presence of ALARM CONDITIONS, their priority and each specific ALARM CONDITION.	IEC 60601-1-8 6.3.2.1
AL.5	Additional requirements for 1 m (operator's position) visual alarm signals and information signals High priority alarm signals should be accompanied by information describing possible causes of the alarm condition and appropriate actions to take in response. Operator action may be required to display this information.	ISO 80601-2-12 208.6.3.2.2.2.101
AL.6	If MULTIPLE ALARM CONDITIONS occur at the same time, each individual ALARM CONDITION shall be visually indicated	IEC 60601-1-8 6.3.2.2.2
AL.7	Visual information signals, if provided, shall be correctly perceived as different from HIGH PRIORITY or MEDIUM PRIORITY visual alarm signals. *Rationale:* the user must be able to identify the priority of the alarms by using different colors for instance.	IEC 60601-1-8 6.3.2.2.2
AL.8	An alarm system shall be provided with at least one manufacturer configured alarm preset.	IEC 60601-1-8 6.5.2
AL.9	The system shall prevent the operator from saving changes to the alarm preset	IEC 60601-1-8 6.5.2
AL.10	If an operator-adjustable alarm limit is provided the alarm limit shall be displayed when required by the operator	IEC 60601-1-8 6.6.2.1
AL.11	During adjustment of any alarm limit, the alarm system shall continue to operate normally	IEC 60601-1-8 6.6.2.3
AL.12	(**Acknowledgment**) The machine shall allow the operator to cease the alarm signal for which no associated alarm condition currently exists (ALARM RESET).	IEC 60601-1-8 6.8

5.1 Alarm list

All the alarms shall be displayed on the GUI (except those referred to GUI failure), and each alarm belongs to one of the three priority classes; each of these classes requires to display the alarm on the GUI.

ID	Requirement / Rationale	Input Ref.
AL.13	*Power disconnection* The system has successfully switched over to backup battery. Alarm condition: PowerType(t1) = power and PowerType(t2) = battery where t1<t2 Priority: MEDIUM Raised by: Controller	SAV.2.1
AL.14	*Battery Failure*	SAV.2
AL.14.1	*Battery fail* A battery failure when the system is powered from AC shall be detected and signalled. Alarm condition: Battery failure Priority: HIGH Raised by: Controller	SAV.2
AL.14.2	When the ventilator is connected to the battery and 10 minutes of backup battery power remain. Alarm condition: Remaining battery time < 10 min Priority: HIGH Raised by: Controller	SAV.2.2
AL.14.3	When the ventilator is connected to the battery and 5 minutes of backup battery power remain. Alarm condition: Remaining battery time < 5 min Priority: HIGH Raised by: Controller	SAV.2.3
AL.15	*Internal power voltages*	SAV.2
AL.15.1	*System Internal power under-over voltage* The system shall raise an alarm if the internal power voltages are out of safe ranges. Alarm condition: SystemVoltage < 10.5 V or SystemVoltage > 14.1 V Priority: HIGH Raised by: Controller	SAV.2

AL.15.2 — *Power supply under-over voltage* — SAV.2

The system shall raise an alarm if the power supply voltages are out of safe ranges.

Alarm condition	PowerSupply < 11 V or PowerSupply > 14.5 V
Priority	HIGH
Raised by	Controller

AL.15.3 — *Battery supply under-over voltage* — SAV.2

The system shall raise an alarm if the battery supply voltages are out of safe ranges.

Alarm condition	BatteryVoltage < 4.5 V or BatteryVoltage > 5.2 V
Priority	HIGH
Raised by	Controller

AL.15.4 — *GUI under-over voltage* — SAV.2

The system shall raise an alarm if the GUI power voltages are out of safe ranges.

Alarm condition	GUIVoltage < 4.7 V GUIVoltage > 5.5 V
Priority	HIGH
Raised by	Controller

AL.16 — *ADC failure* — FUN.33

The system shall raise an alarm if ADC devices do not respond after a fixed number of retries (maximum 5) or report an error.

Alarm condition	ADC is not responding
Priority	HIGH
Raised by	Controller

AL.16.1 — Whenever the ADC alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.

AL.17 — *Leakage in gas circuit* — SAV.14

The system shall raise an alarm if there is significant leakage in the gas circuit.

Alarm condition	Unintended leakage from the ventilator should not exceed: 200 ml/min at 50 cmH_20
Priority	MEDIUM
Raised by	Controller

AL.18	*Complete Obstruction in pneumatic circuit* The system shall raise an obstruction in pneumatic circuit alarm when the alarm limit for obstruction is reached. Alarm condition: Internal pressure exceeds 5bar and PAW is below 1.5bar in two consecutive observations Priority: HIGH Raised by: Controller	SAV.15
AL.18.1	The controller shall drive input and output valves to their safe state.	
AL.19	*Partial Obstruction in pneumatic circuit* The system shall raise an partial obstruction in pneumatic circuit alarm when alarm limit for partial obstruction is reached. Alarm condition: Internal pressure exceeds double of PAW in two consecutive observations Priority: HIGH Raised by: Controller	SAV.15
AL.20	*Obstruction in inhale branch - Inspiratory airway pressure too low.* Obstruction in the inhale branch shall be raised if the PAW is out of range. Alarm condition: PAW $<$ Min P_{insp} Priority: HIGH Raised by: Controller	SAV.3 SAV.12
AL.20.1	The alarm condition delay shall not exceed more than two respiratory cycles or 5 s, whichever is greater.	
AL.21	*Obstruction in exhale branch - PEEP too high* Obstruction in the exhale branch shall be raised if the PEEP is out of range. Alarm condition: PEEP $>$ Max PEEP Priority: HIGH Raised by: Controller	SAV.24
AL.21.1	The alarm condition delay shall not exceed more than two respiratory cycles or 5 s, whichever is greater.	SAV.24.1
AL.21.2	Whenever the obstruction alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.	

AL.22	*Obstruction in patient branch - Inspiratory flux too low* The obstruction in the patient branch shall be raised when the flow is out of range.	SAV.15 SAV.16 SAV.18

Alarm condition	V_E< Min V_E
Priority	HIGH
Raised by	Controller

AL.23	*Oxygen level too high* The system shall raise an alarm when the delivered oxygen concentration value (%) exceeds the set FiO_2 + 3%, i.e., due to failing gas supply.	SAV.1

Alarm condition	OS > desired FiO_2+ 3%
Priority	MEDIUM
Raised by	Controller

AL.24	*Oxygen level too low* The system shall raise an alarm when the delivered oxygen concentration value (%) is below the set FiO_2 - 3%, i.e., due to failing gas supply.	SAV.1

Alarm condition	OS < desired FiO_2- 3%
Priority	MEDIUM
Raised by	Controller

AL.25	*Inspiratory flux too high* *The* system shall raise an alarm when inspiratory flux (V_E) exceeds Max V_E.	SAV.17 SAV.19

Alarm condition	V_E > Max V_E
Priority	MEDIUM
Raised by	Controller

AL.26	*Inspiratory airway pressure too high* Inspiratory PAW exceeds the user-set high-pressure alarm limit.	SAV.4 SAV.13

Alarm condition	PAW > Max P_{insp}
Priority	HIGH
Raised by	Controller

AL.26.1	The high airway pressure alarm condition delay shall not exceed 200 ms.	SAV.4.1
AL.26.2	Whenever the high-pressure alarm condition occurs, the controller shall raise the alarm, within no more than two respiratory cycles or 15 s.	SAV.4.2
AL.26.3	The controller shall drive input and output valves to their safe state reducing the airway pressure to either: the atmospheric pressure; or the set PEEP level.	SAV.4.2

AL.27 — *Disconnection alarm condition - PEEP too low* — SAV.5, SAV.25

The ventilator shall be equipped with an alarm system that detects a technical alarm condition to indicate when conditions in the ventilator reach the alarm limit for disconnection.

Alarm condition	PEEP < Min PEEP
Priority	HIGH
Raised by	Controller

AL.28 — *Gas pressure input too low* — SAV.10

The system shall raise an alarm when the pressure at the entrance of the circuit is too low.

Alarm condition	When the input valve is open and the pressure out of the gas blender is too low: $P_{in\_GB} < MIN\_P_{in\_GB}$, $MIN\_P_{in\_GB}$ =3800 cmH_2O
Priority	MEDIUM
Raised by	Controller

AL.29 — *Gas pressure input too high* — SAV.11

The system shall raise an alarm when the pressure at the entrance of the circuit is too high.

Alarm condition	When the input valve is open and the pressure out of the gas blender is too high: $P_{in\_GB} > MAX\_P_{in\_GB}$, $MAX\_P_{in\_GB}$=5300 cmH_2O
Priority	MEDIUM
Raised by	Controller

AL.30 — *Over Temperature alarm* — SAV.21

The system shall raise an alarm if the internal temperature of the system exceeds 75°C. The controller shall transition to the fail-safe mode.

Alarm condition	BoardTemperature > 75°C
Priority	HIGH
Raised by	Controller

AL.31 — Expiratory V_{tidal_exp} *too low* — SAV.8

The system shall raise an alarm when the patient is hypo-ventilating, i.e., expiratory tidal volume is below the V_{tidal_exp} min limit.

Alarm condition	V_{tidal_exp} < Min V_{tidal_exp}
Priority	MEDIUM
Raised by	Controller

AL.32 — Expiratory V_{tidal_exp} *too high* — SAV.9

The system shall raise an alarm when the patient is hyperventilating, i.e. expiratory tidal volume exceeds V_{tidal_exp} max limit.

Alarm condition	V_{tidal_exp} > Max V_{tidal_exp}
Priority	MEDIUM
Raised by	Controller

AL.33 — Inspiratory V_{tidal_insp} too low — SAV.8

The system shall raise an alarm when the patient inspiratory tidal volume is below the V_{tidal_insp} min limit.

Alarm condition	V_{tidal_insp} < Min V_{tidal_insp}
Priority	MEDIUM
Raised by	Controller

AL.34 — Inspiratory V_{tidal_insp} too high — SAV.9

The system shall raise an alarm when the inspiratory tidal volume exceeds V_{tidal_insp} max limit.

Alarm condition	V_{tidal_insp} > Max V_{tidal_insp}
Priority	MEDIUM
Raised by	Controller

AL.35 — *Respiratory rate too low* — SAV.6

The system shall raise an alarm when the measured respiratory rate is below Min RR.

Alarm condition	RR < Min RR
Priority	HIGH
Raised by	Controller

AL.36 — *Respiratory rate too high* — SAV.7

The system shall raise an alarm when the measured respiratory rate exceeds Max RR.

Alarm condition	RR > Max RR
Priority	HIGH
Raised by	Controller

AL.37	*Apnea alarm* The system shall raise an alarm when the time since last inspiration greater than apnea lag.	SAV.22

Alarm condition	When the expiratory duration in PSV mode is greater than the apnea lag.
Priority	HIGH
Raised by	Controller

AL.38	*GUI failure* The system shall raise an alarm if the communication between controller and GUI is lost, or in case of a GUI failure.	201.13.2.104 + SAV.26

Alarm condition	No communication between controller and GUI
Priority	HIGH
Raised by	Controller

AL.39	*Unable to read sensor pressure* The system shall raise an alarm if the communication between controller and sensor pressure is lost.	201.13.2.104 + SAV.26

Alarm condition	No communication between controller and sensor prssure
Priority	HIGH
Raised by	Controller

AL.40	*Unable to read oxygen sensor* The system shall raise an alarm if the communication between controller and oxygen sensor (OS) is lost.	201.13.2.104 + SAV.26

Alarm condition	No communication between controller and oxygen sensor
Priority	HIGH
Raised by	Controller

AL.41	*Unable to read sensor flux* The system shall raise an alarm if the communication between controller and sensor flux (FI2) is lost.	201.13.2.104 + SAV.26

Alarm condition	No communication between controller and sensor flux
Priority	HIGH
Raised by	Controller

FUN.59	*Unable to read gas flow to patient* The system shall raise an alarm if the communication between controller and gas flow sensor (FI1) is lost.	201.13.2.104 + SAV.26

Alarm condition	No communication between Controller and sens FI2
Priority	MEDIUM
Raised by	Controller

AL.42	*Fan tachometer* The controller shall raise an alarm if fan tachometer input indicates fan is not rotating.	FUN.32

Alarm condition	Fan is not rotating
Priority	HIGH
Raised by	Controller

AL.42.1	Whenever the FAN alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.

AL.43	*I:E ratio* The I:E ratio is less than 0.01 for more than 4 consecutive cycles.	FUN.32

Alarm condition	I:E < 0.01
Priority	HIGH
Raised by	Controller

AL.43.1	Whenever the I:E ratio alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.

AL.44	*Input valve failure* The controller shall raise an alarm if the input valve (IN valve) does not change value.	FUN.32

Alarm condition	Input valve does not change value when the phase swaps from inspiratory to expiratory and vice versa
Priority	HIGH
Raised by	Controller

AL.44.1	Whenever the input valve alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.

AL.45 — *Out valve failure* — FUN.51

The controller shall raise an alarm if out valve (OUT valve) does not change its state.

Alarm condition	Out valve does not change state when the phase swaps from expiratory to inspiratory and vice versa.
Priority	HIGH
Raised by	Controller

AL.45.1 — Whenever the output valve alarm condition occurs, the controller shall drive input and output valves to their safe state, within no more than one respiratory cycle.

AL.46 — *SD GUI failure*

The system shall raise an alarm in case the GUI is not able to update the log file.

Alarm condition	The GUI is not able to update the log file
Priority	MEDIUM
Raised by	GUI

5.2 Visual alarm signals

The IEC 60601-1-8 indicates the following characteristics of visual alarms:

Category	**Color**	**Flashing frequency**	**Duty cycle**
High	Red	2,0Hz	50%
Medium	Yellow	0,6Hz	50%
Low	Yellow	Constant	100%

The alarm is visualized using an RGB LED mounted on the ventilator.

Bibliography

[1] Andrea Bombarda, Silvia Bonfanti, Angelo Gargantini, and Elvinia Riccobene. Developing a prototype of a mechanical ventilator controller from requirements to code with ASMETA. *Electronic Proceedings in Theoretical Computer Science*, 349:13–29, November 2021.

[2] Walter Bonivento, Angelo Gargantini, Reiner Krücken, and Alessandro Razeto. The mechanical ventilator milano. *Nuclear Physics News*, 31(3):30–33, July 2021.

[3] A. Abba et al. The novel mechanical ventilator milano for the COVID-19 pandemic. *Physics of Fluids*, 33(3):037122, mar 2021.

[4] Maria Chiara Di Guardo, Elona Marku, Walter Marcello Bonivento, Manuel Castriotta, Fernando Ferroni, Cristiano Galbiati, Giuseppe Gorini, and Michela Loi. When nothing is certain, anything is possible: open innovation and lean approach at MVM. *R&D Management*, jan 2021.

[5] Yuan Lei. *Medical Ventilator System Basics: A clinical guide*. Oxford University Press, July 2017.