**Emergency Ventilator**

Risk Evaluation

Issue/change record

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Date | Author | Reason of issue/summary |
| 0.A | 05/04/2020 |  | DRAFT, released for ongoing development |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Device 4](#_Toc37010249)

[1.1 Intended use 4](#_Toc37010250)

[2 Risk management plan 5](#_Toc37010251)

[2.1 Responsibility and authority 5](#_Toc37010252)

[2.2 Requirements for review 5](#_Toc37010253)

[2.3 Methodology for obtaining information for reviews 6](#_Toc37010254)

[2.4 Methodology for risk analysis 6](#_Toc37010255)

[2.5 Criteria for risk acceptability 7](#_Toc37010256)

[3 Risk analysis 10](#_Toc37010257)

[3.1 Hazards analysis 10](#_Toc37010258)

[3.1.1 Top level 10](#_Toc37010259)

[3.1.2 Patient pressure too high 10](#_Toc37010260)

[3.1.3 Pressure too low 11](#_Toc37010261)

[3.1.4 CO2 not eliminated from blood 12](#_Toc37010262)

[3.1.5 O2 does not saturate blood 12](#_Toc37010263)

[3.1.6 Cross-contamination 12](#_Toc37010264)

[3.1.7 Electrical 13](#_Toc37010265)

[3.1.8 Mechanical 13](#_Toc37010266)

[3.1.9 Biological 13](#_Toc37010267)

[3.1.10 Environmental disturbance 13](#_Toc37010268)

[3.1.11 Use error 14](#_Toc37010269)

[3.1.12 Microprocessor 15](#_Toc37010270)

[3.1.13 Electronics 15](#_Toc37010271)

[3.1.14 Calibration 15](#_Toc37010272)

[3.2 Initial risk evaluation 15](#_Toc37010273)

[3.2.1 Hazard: Patient Pressure is too high 15](#_Toc37010274)

[3.2.2 Hazard: Pressure too low 16](#_Toc37010275)

[3.2.3 Hazard: CO2 not eliminated from blood 16](#_Toc37010276)

[3.2.4 Hazard: O2 does not saturate blood 16](#_Toc37010277)

[3.2.5 Hazard: Cross-contamination 16](#_Toc37010278)

[3.2.6 Hazard: Electrical 16](#_Toc37010279)

[3.2.7 Hazard: Mechanical 16](#_Toc37010280)

[3.2.8 Hazard: Biological 17](#_Toc37010281)

[3.2.9 Hazard: Environmental disturbance 17](#_Toc37010282)

[3.2.10 Hazard: Use error 17](#_Toc37010283)

[3.2.11 Hazard: Microprocessor 17](#_Toc37010284)

[3.2.12 Hazard: Electronics 17](#_Toc37010285)

[3.3 Risks reduction and final evaluation 18](#_Toc37010286)

[4 Conclusion 24](#_Toc37010287)

# Device

The device is a ventilator intended for providing mass intensive respiratory care, in facilities that might be lacking in full hospital infrastructure, abundant oxygen supplies and clinical experiences – such as under pandemic emergency conditions.

The ventilator is designed for a simplified clinical protocol that demands minimal training and re-training. It is further designed to be mass-producible and requiring minimal maintenance. The gas cycling operation is designed to minimise oxygen consumption.

The ventilator uses conventional Pressure Controlled SIMV (Synchronised Intermittent Mandatory Ventilation) mode of ventilation only. It interfaces with intubated, unconscious and semi-conscious, patients; and it interfaces with pressure ventilation masks on conscious patients. There is no need to select and switch between alternative modes or interfaces.

SIMV behaves as PSV (Pressure Support Ventilation) when the patient makes full efforts, and it behaves as CMV (Continuous Mandatory Ventilation) if the patient does not make any efforts. When used with a mask on a conscious, spontaneously breathing patient, the SIMV behaves as nPSV or Synchronised BiPAP (by setting IP low). Switching the IP cycle off (or setting it equal to PEEP) makes SIMV behaves as CPAP (whether the patient is intubated or has a mask interface).

For purpose of simplicity, the I:E ratio (Inspiratory-Expiratory) is fixed 1:2. Inspiration flow rate fixed 60L/min, which produces an IP rise time of about 0.45s into a 600mL lung.

The device is not intended to be marketed as a commercial medical device. The device conforms to medical device requirements for basic safety and essential performance. There is not, yet, any basis for proving the clinical efficacy of the device.

The ventilator is designed to operate in combination with an external power supply, a breathing circuit and a respiratory gas humidifier (HME or water chamber).

## Intended use

The ventilator is intended for use with adult and young adult patients from 50kg and upwards. It interfaces with intubated, unconscious and semi-conscious, patients; and it interfaces with pressure ventilation masks on conscious patients.

The device is intended to be operated and maintained by rapidly trained, lesser confident intensive care personnel – oversee by expert respiratory therapists.

The general operating environment are hospitals and temporary healthcare facilities. Although the device is suitable for intra-hospital transport (moving patient between hospital departments, while being ventilated), it is not classed as a transport device. It is not designed for road or air transport.

The risk management plan considers environmental exposures that can occur during normal conditions of use, shipping and storage. It covers the complete life-cycle of the device and assumes that a mandatory level of maintenance is performed.

# Risk management plan

The plan and risk management activities are performed in conformance to the current revision of ISO14971 on the application of risk management to medical devices, including the information guidance published with this standard. Specific documented company processes for risk management, providing more details on inputs and outputs for particular activities, are integrated into the company quality management system. This plan requires adherence to the ISO14971 standard and the documented company processes.

## Responsibility and authority

The overall responsibility for safety and performance of company products rests with the board of directors of the manufacturer whose brand name appears on the ventilator. The responsibility and authority for device risk management is delegated to the organisations Quality and Regulatory Affairs Manager, who will ensure this plan and its associated activities are effectively implemented and maintained.

The organisation’s senior management team is delegated responsibility for receiving and reviewing summary reports on device risk management activities, to verify their completeness, effectiveness and to take corrective action on any shortfall. The senior management team will ensure that risk management activities are sufficiently and competently resourced. The quality management system incorporates documented process for management review, including the recording of decisions and actions.

The product development process incorporates parts of the risk management process (e.g. the process for this document). Individual design engineers are responsible for ensuring that this process is appropriately implemented during the development project, which will include requirements for conformance with recognised (harmonized) safety and performance standards; and that devices are not released into the market prior to have undergone a risk evaluation and review in accordance with requirements set out in this plan.

## Requirements for review

The risk acceptance criteria, analysis, evaluation and controls for the device are reviewed in accordance with the documented organisational process for product risk management, which is at least annually or following any event that draws the current controls into question. A review triggered by the latter reason, may be limited in scope to the systems potentially affected.

Risk management review will consider information available in records and determine whether any:

1. Previously unrecognised hazards are present;
2. Previous conclusion concerning acceptability of risks remains valid;
3. Previous conclusion concerning acceptability of residual risks remains valid.

Results of the evaluation process are recorded in the risk management file, including:

1. Degree of effectiveness of the risk analysis and controls for the device;
2. New controls and/or actions required to reduce risk or to assure that risk is maintain at a specified acceptable level;
3. New user information required concerning residual risks.

The organisation’s senior management team will periodically receive and review summary reports as follows:

1. Monthly on any open adverse incidents, including actions and progress;
2. Quarterly summary of device risks situation, compared to objectives set out in this plan;
3. Outcomes of risk management reviews, at the earliest opportunity after their occurrence.

## Methodology for obtaining information for reviews

The quality management system incorporates documented processes for dealing with device safety issues in a systematic manner, including:

1. Incorporating basic safety requirement from harmonized international standards – i.e. the IEC 60601 (ISO 80601) series of standards on medical electrical equipment.
2. Maintaining production traceability of safety critical parts; and recording outcomes of inspection and testing, including software validation (PEMS). Every individual device is subjected to 100% final inspection and testing. Any deviance from intended performance is recorded.
3. Receive, record and handle adverse incidents, including processes for Corrective and Preventive Action, Advisory Notices and Recall.
4. Receive, record and monitor general market feedback concerning performance in the field.
5. Post-introduction market surveillance for input into the ongoing products planning and specification process, including appraisals of strengths, weaknesses and trends in state-of-art in similar devices in the market. Areas of search include relationships with market drivers (medical practitioners), user visit reports, trade fairs, and competitor products reviews.

Information relating to new or revised standards is obtained through:

1. Notified Body surveillance and advanced updates
2. Government publications.

## Methodology for risk analysis

Available information and sources of information will be systematically used to identify and estimate the risk of the anticipated sources of harm associated with the device. Information includes testing and validation data, including from the Programmable Electrical Medical Systems (PEMS) validation.

The analysis considers internal (self) sources and environmental (external) sources and causes. The scope of analysis includes intended use and any likely and reasonably foreseeable misuse.

The identification will consider:

1. Is there a source of harm?
2. Who is most vulnerable to the harm?
3. How could the hazard occur?

The information is used to estimate the reasonably foreseeable sequence of events that could result in a hazardous situation. Where certain aspects are unknown, the analysis will involve seeking out missing information, in order to be able to qualify/quantify the risk. All identified risks are recorded.

Where established knowledge confirms that it would be impossible for a certain hazard being realised, then the particular aspect is, by definition, not a risk and it should not necessitate any further evaluation.

## Criteria for risk acceptability

Risk acceptability is based on a rating of the probability of occurrence of harm and severity of the consequence of that harm. The rating may be weighed or influenced by recognized standards and/or perception factors – in the context of the particular markets.

The context is that candidate patients for life-supporting ventilation are either deeply unconscious or have compromised lung function or strength, or both, and would be unable to sustain own breathing over time. Patient monitoring provides clear indication of effectiveness of treatment and whether patient is in immediate danger of respiratory failure.

The alternatives to the simplified approach to ventilation provided by this device, is to move the patient to a more advanced intensive care unit, where more advanced respiratory care resources exist. However, such resources can be insufficient in times of a widespread pandemic. The device subject to this assessment fill an essential gap in the needs to treat patients. The alternative is unviable.

Ventilation is an output-based therapy and involves a large degree of variability in clinical application, skills and judgement. The important aspects for the device are that it performs reliably and accurately, with relevant and timely information feedback to the user.

Table 1: Definition of probability of occurrence of harm

|  |  |
| --- | --- |
| Frequent | 1 occurrence in every 5 device operating days, or every 1 patient treatment sessions |
| Probable | 1 occurrence in every 50 device operating days, or every 12 patient treatment sessions |
| Occasional | 1 occurrence in every 500 device operating days, or every 125 patient treatment sessions |
| Remote | 1 occurrence in every 5,000 device operating days, or every 1,250 patient treatment sessions |
| Improbable | 1 occurrence in every 50,000 device operating days, or every 12,500 patient treatment sessions |
| Almost impossible | 1 occurrence in every 500,000 device operating days, or every 125,000 patient treatment sessions |
| Assumptions and context:   * Average patient treatment session is 5 days * Average number of sessions per year per device is 60 patients * Number of ventilator operating days per year per device is 160 days * Estimated market life of device design is 15 year, of which 14 years is in non-use storage. * Total number of devices in the market is 10,000 units * Total number of patients exposed to all devices over the market life of the device design is 600,000 patients, during emergency situations over the 15 years device life (used 1 year). * Total number of device operating days over the market life of the device design is 3 million days, over 10 years when the device is only used intermittently for a combined 1 year. * Ventilation therapy involves significant variability in clinical application, skills and judgement, which has a bearing on the quality of patient outcomes with any given device. | |

Table 2: Definitions of consequences of harm

|  |  |
| --- | --- |
| Catastrophic | Potential for resulting in death or multiple deaths |
| Critical | Potential for resulting in permanent non-trivial impairment or life-threatening injury |
| Serious | Potential for injury or impairment requiring additional professional medical intervention. |
| Minor | Potential for temporary injury or impairment not requiring additional professional medical intervention. |
| Negligible | Results in inconvenience or temporary discomfort |
| Persons to be considered as possibly affected are patients, clinical personnel (users of the device), hospital technical and cleaning personnel, device manufacturer’s service personnel, relatives and any other visitors who could potentially come into contact with the device. | |

Table 3: Risk rating, by classifying probability and consequence of harm

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Probability of occurrence of harm | Consequence of harm | | | | |
| Negligible | Minor | Serious | Critical | Catastrophic |
| Frequent | 15 | 10 | 6 | 3 | 1 |
| Probable | 19 | 14 | 9 | 5 | 2 |
| Occasional | 24 | 18 | 13 | 8 | 4 |
| Remote | 27 | 23 | 17 | 12 | 7 |
| Improbable | 29 | 26 | 22 | 16 | 11 |
| Almost impossible | 30 | 28 | 25 | 21 | 20 |
| Where review and sound reasoned judgement establishes that it would be practically impossible for a harm being realized (i.e. it figures below the range of probability), then the particular aspect is, by definition, not a risk and it should not necessitate any further consideration | | | | | |

Table 4: General interpretation of risk acceptability

|  |  |  |
| --- | --- | --- |
| Risk rating | Risk acceptability | Action, in general |
| 1 – 6 | Intolerable | Devices should not be placed in the market, until risk is reduced to a tolerable level. Any existing users in the field must be notified urgently. Establish fastest possible time period for any field corrective action. Generally, any field device should be withdrawn from use. |
| 7 – 15 | Moderate | Devices should not be placed in the market, until risk is reduced to a tolerable level. Any existing users in the field must be notified at the earliest practical time. Establish fastest practical time period for any field corrective action. Urgent user information and action required, if associated with a potentially ‘catastrophic’ consequence. |
| 16 – 24 | Tolerable | Efforts should be made to reduce the risk, where benefits of the solution outweigh the disruption and cost of implementation – in respect of the influencing factors described below. A time period should be defined for implementation. Monitoring is required to ensure that any established controls are maintained. |
| 25 – 30 | Negligible | Additional controls are generally not required. Monitoring is required to ensure that any established controls are maintained. |

The interpretation of risk acceptability in table 4 is a general one. The final acceptance and action for a particular risk may be influenced by the following factors:

1. Accepted 'state-of-art' solutions. For example, account for precedence in similar devices where similar type of risks has been reduced further. Even a negligible risk must be reduced, if it is the conventional and technically easy to do so.
2. Risk perception, as per ISO14971. For example, what is the patients (legal guardian for infants), medical practitioners and general public level of tolerance, based the state of health of the patient population, socio-economics, political and cultural conditioning.
3. Undesirable side effects weighed against anticipated benefits, as per ISO14971 and MDR requirements. The anticipated benefit may vary with the individual user; for example, depending on the degree of alternative capacity or the immediate emergency of their situation. Some of these judgements can only be made by a qualified medical practitioner, with understanding of the patients’ situations. Consider also the degree of effectiveness of disclosure of residual risks and the practitioners training in managing these (ability to effectively/timely recognise and respond the side-effects).

Where a factor influences the final acceptability, compared to the rating outcome from table 1, the reasoning must be described in the test and reviews conducted.

# Risk analysis

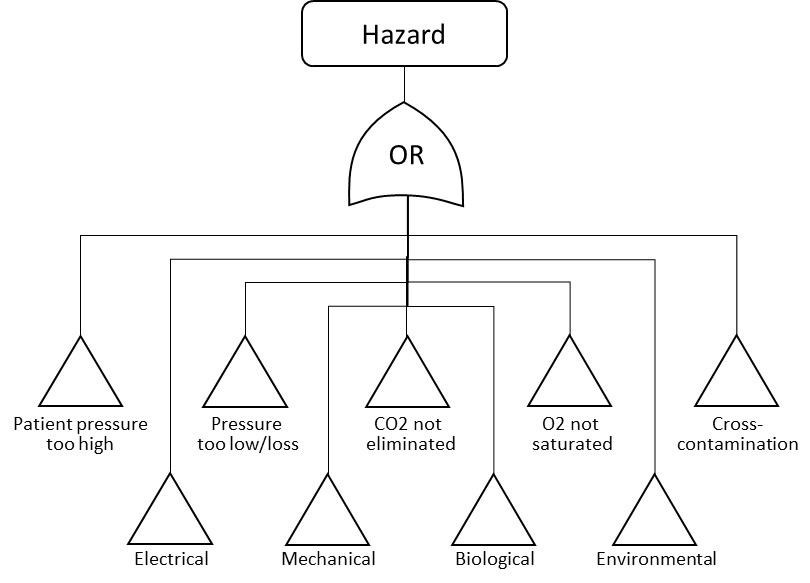
## Hazards analysis

IEC60601-1 and IEC 60601-2-12defines the basic safety requirements. A single fault condition shall not cause a monitoring or alarm system and the corresponding control function to fail in such a way that the monitoring function becomes simultaneously ineffective, and therefore fails to detect the loss of the monitored function. Any fault that can lead to a hazard and that is not detected by intrinsic means or by periodic inspection (e.g. an oxidant leak, software defect) shall be regarded as a normal condition and not a single fault condition.

For each identified hazard (or top event) a fault tree is generated to help determine their initiating causes. Only the ‘single fault condition’ consideration needs to be applied. This greatly simplifies the analysis of the fault tree since only OR (no AND) conditions are considered. Causes that are common to more than one hazard and can be further analysed are designated separate fault trees. These sub trees are referenced by a triangle shape. The initiating causes are indicated by the rounded boxes (shaded grey) in the fault trees that follow.

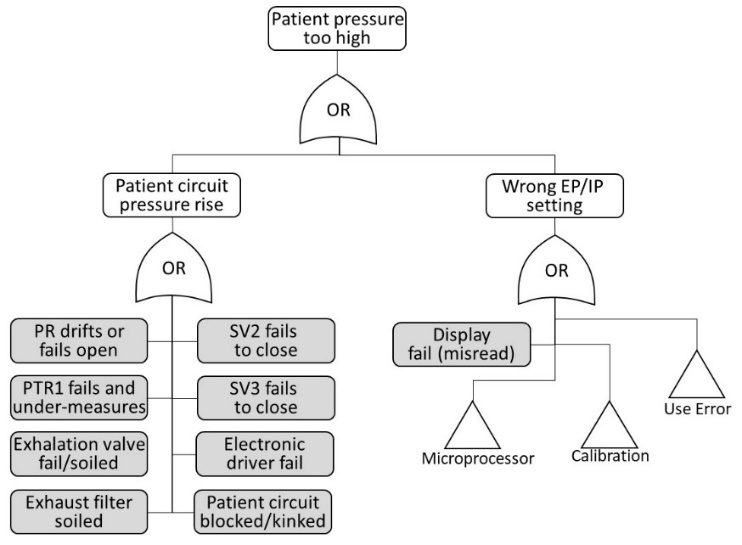
### Top level

The identified ‘top event’ hazards are as follows. The triangles refer to sub-trees, which are detailed in the sections that follow.

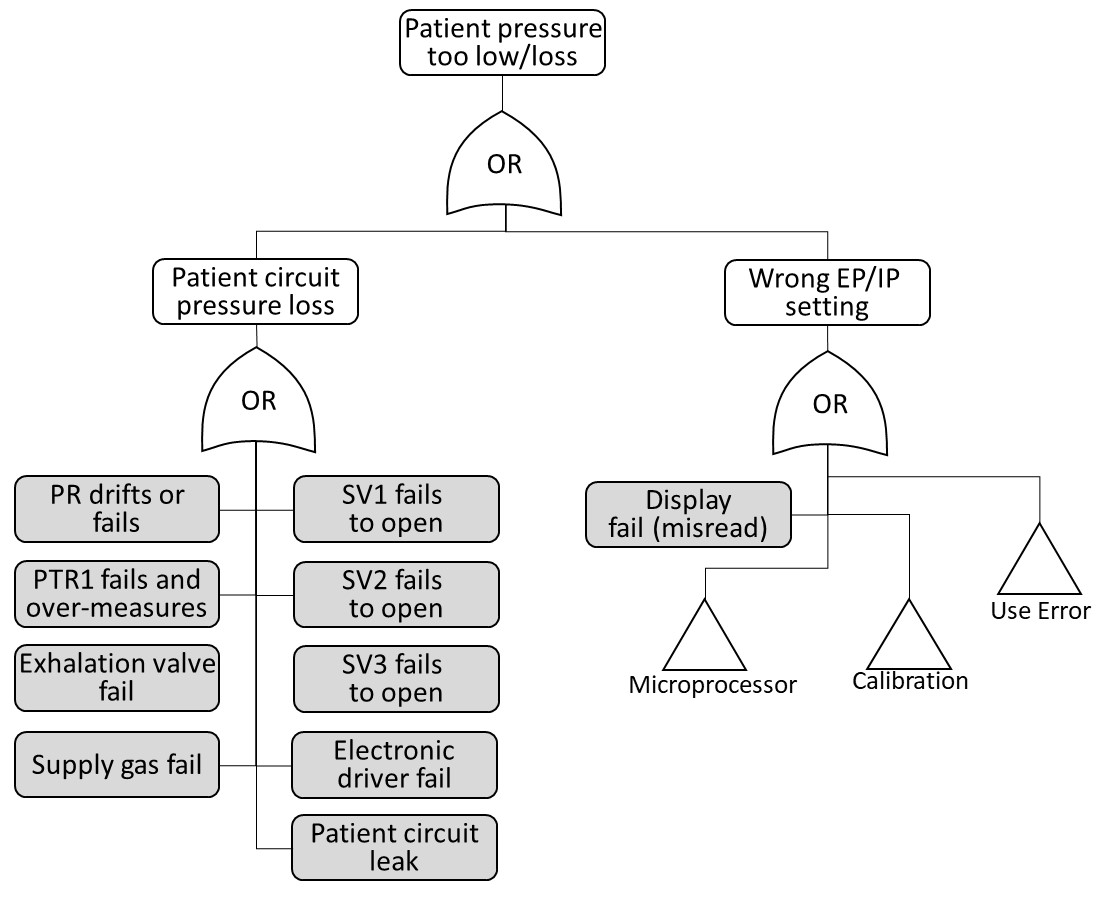


### Patient pressure too high

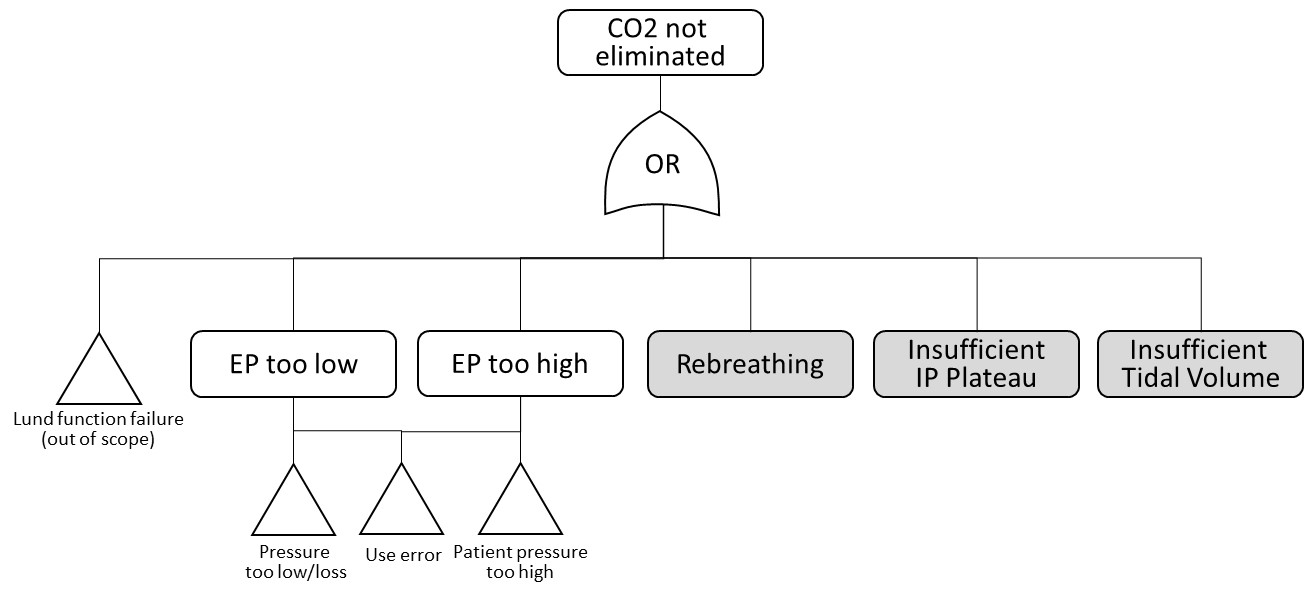
Too high a patient pressure can result in worst case result in acute lung damage, or a slower developing volu- and baro-trauma. It can also result in ventilatory insufficiency, by not permitting the lung to wash out CO2.



### Pressure too low

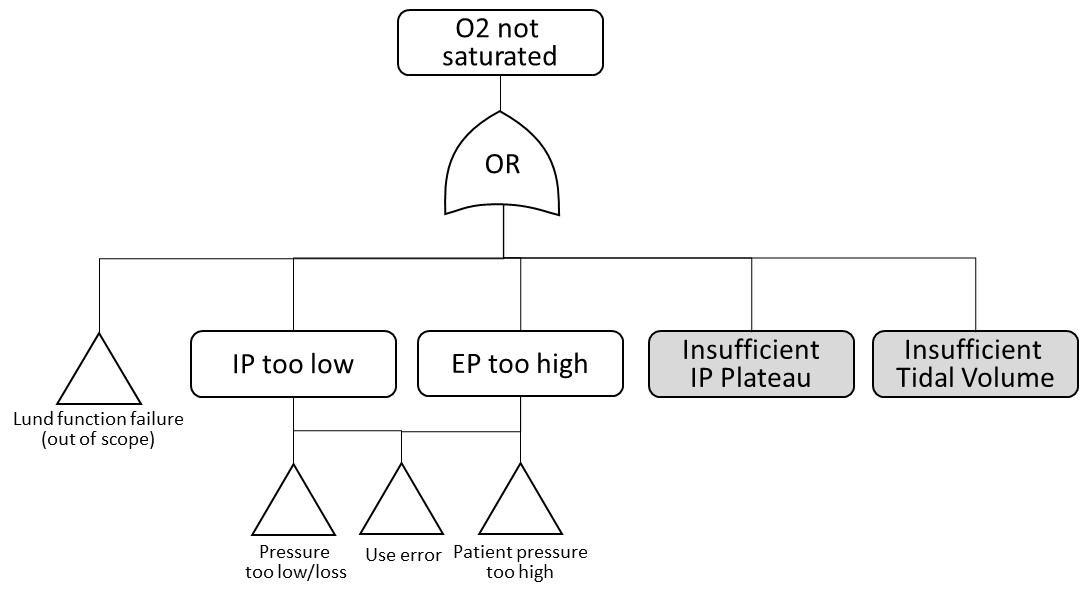


### CO2 not eliminated from blood

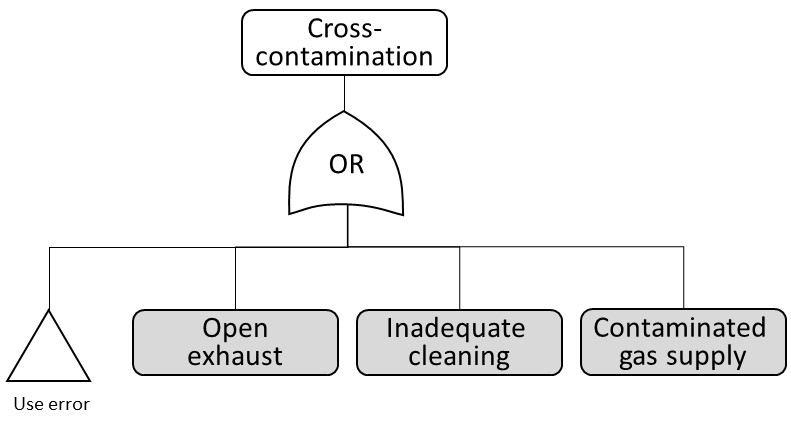


Note: The patient’s underlying illness is not a condition of the ventilator. The EP is a determinant of optimised CO2 elimination. The optimal EP varies and the lung condition varies. It is natural that EP needs monitoring an occasionally adjusted.

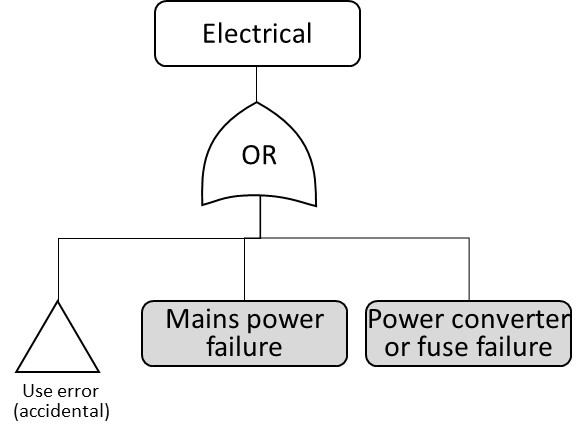
### O2 does not saturate blood



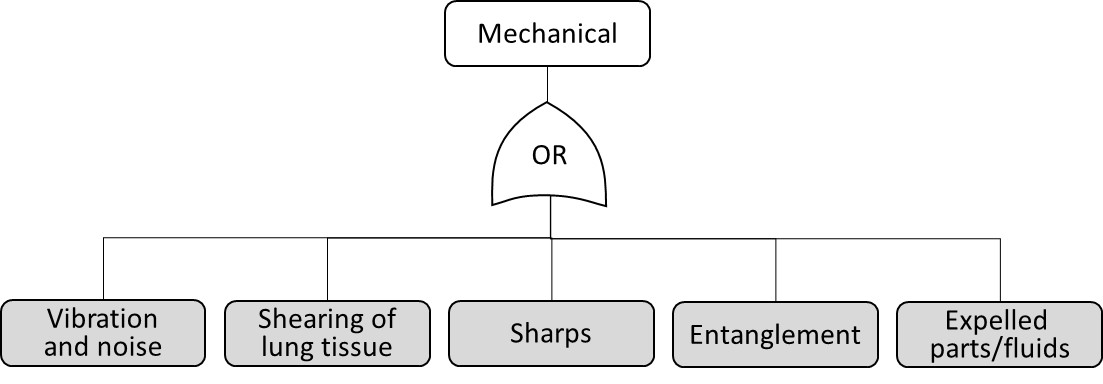
### Cross-contamination



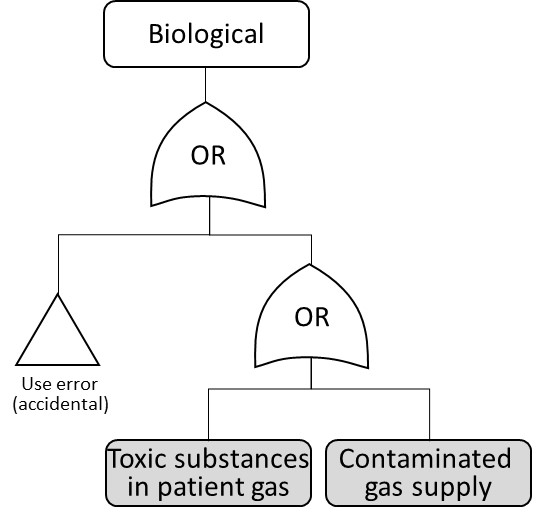
### Electrical



### Mechanical



### Biological

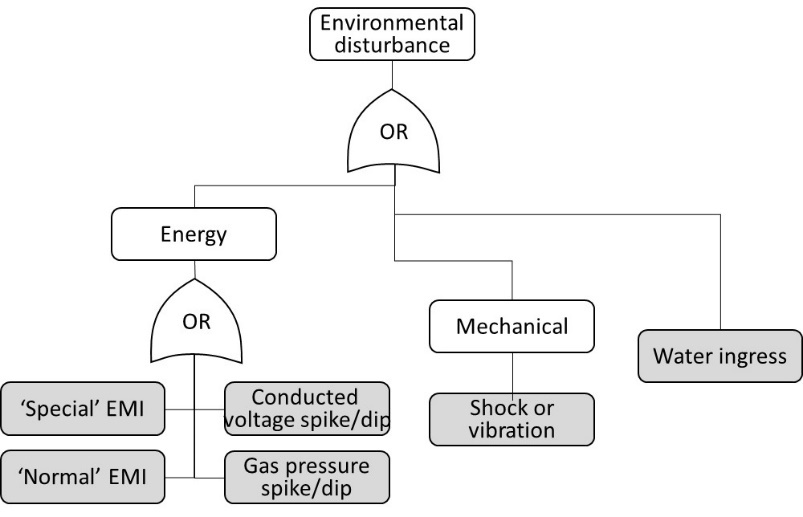


Note: The patient circuit and patient interface are separate combination parts that are subjected to their own risk management and conformity assessment.

Toxcity and leaching. No phalates. PU stable. Clean valves.

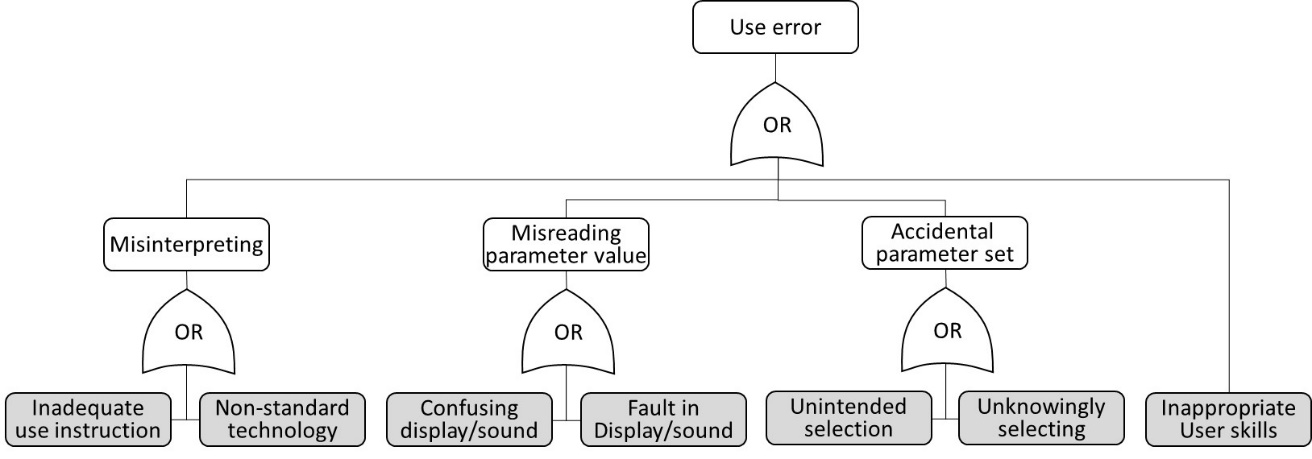
### Environmental disturbance

The term ‘environmental’ means aspects external to the system subjected to the hazard. This may be external to the device as a whole, or between two or more internal sub-systems. ‘Normal’ EMI means immunity levels presumed in international standards for EMC. ‘Special’ level means in excess of ‘normal’ levels – e.g. in proximity to MRI scanner or other radiation equipment. Normal hazards are usually covered by compliance with 60601-1-2 on EMC, for normal EMI levels. The hazards introduced by special levels are addressed by warnings in the user manual and/or on the device as appropriate.

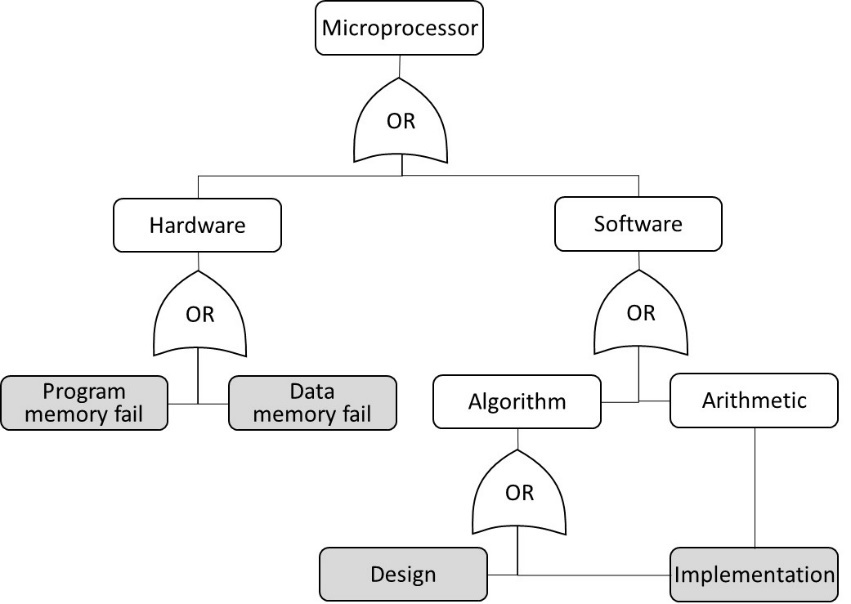


### Use error

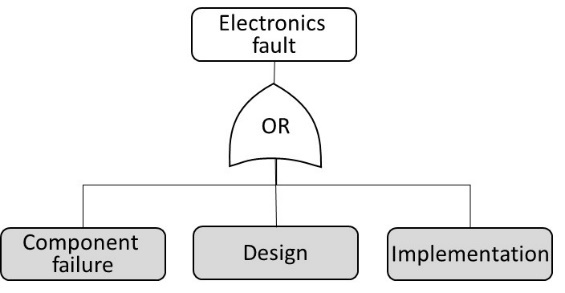
The term ‘use’ extends to any person interacting with the device during clinical application and servicing/calibration. This is foremost clinical and technical servicing personnel, but also other people, incidentally, entering the device environment – such as hospital cleaning personnel, patient parent, siblings and other hospital visitors.



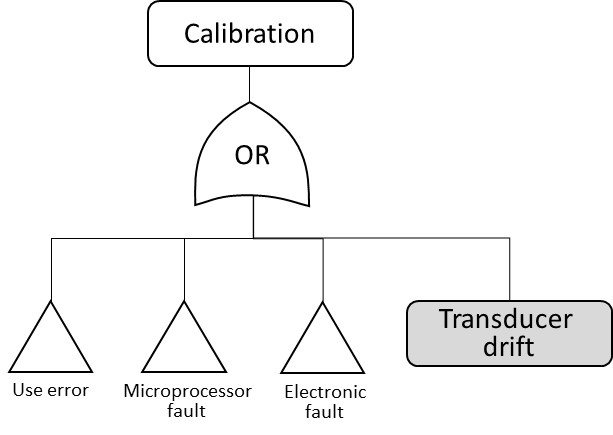
### Microprocessor



### Electronics



### Calibration



## Initial risk evaluation

Summarise the initiating causes for each hazard (each greyed box above) and estimates a risk level for each one, assuming no design controls. The evaluation assumed the situation without risk controls or design mitigation.

### Hazard: Patient Pressure is too high

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| PR drifts or fails open | Remote | Catastrophic | 7 | Moderate |
| PTR1 fails and under-measures | Remote | Catastrophic | 7 | Moderate |
| Exhalation valve fails/soiled | Remote | Catastrophic | 7 | Moderate |
| Solenoid valve SV2 fails open | Remote | Catastrophic | 7 | Moderate |
| Solenoid valve SV3 fails open | Remote | Catastrophic | 7 | Moderate |
| Electronic valve driver fails | Remote | Catastrophic | 7 | Moderate |
| Patient circuit blocked/kinked | Remote | Critical | 12 | Moderate |
| Display failure | Almost imp. | Critical | 21 | Tolerable |

### Hazard: Pressure too low

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| PR drifts or fails | Remote | Catastrophic | 7 | Moderate |
| PTR1 fails and over-measures | Remote | Catastrophic | 7 | Moderate |
| Exhalation valve fails | Remote | Catastrophic | 7 | Moderate |
| Solenoid valve SV1 fails closed | Improbable | Catastrophic | 11 | Moderate |
| Solenoid valve SV2 fails closed | Improbable | Catastrophic | 11 | Moderate |
| Solenoid valve SV3 fails closed | Improbable | Catastrophic | 11 | Moderate |
| Electronic valve driver fails | Remote | Catastrophic | 7 | Moderate |
| Supply gas fail | Occasional | Catastrophic | 4 | Intolerable |
| Display failure | Almost imp. | Critical | 21 | Tolerable |

### Hazard: CO2 not eliminated from blood

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Rebreathing | Improbable | Critical | 16 | Tolerable |
| Insufficient EP plateau | Probable | Critical | 5 | Moderate |
| Insufficient Tidal Volume | Probable | Critical | 5 | Intolerable |

### Hazard: O2 does not saturate blood

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Insufficient IP plateau | Remote | Critical | 12 | Moderate |
| Insufficient Tidal Volume | Probable | Critical | 5 | Intolerable |

### Hazard: Cross-contamination

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Open exhaust | Frequent | Serious | 6 | Intolerable |
| Inadequate cleaning | Probable | Serious | 9 | Moderate |
| Contaminated gas supply | Improbably | Serious | 22 | Tolerable |

### Hazard: Electrical

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Mains power failure | Probable | Catastrophic | 2 | Intolerable |
| Power converter or fuse failure | Occasional | Catastrophic | 4 | Intolerable |

Note: The operating context can include temporary makeshift care facilities.

### Hazard: Mechanical

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Vibration and noise | Frequent | Negligible | 15 | Moderate |
| Shearing of lung tissue | Occasional | Serious | 13 | Moderate |
| Sharps | Occasional | Minor | 18 | Tolerable |
| Entanglement | Probable | Minor | 14 | Moderate |
| Expelled parts/fluids | Remote | Minor | 23 | Tolerable |

### Hazard: Biological

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Toxic substance is fresh gas | Remote | Serious | 17 | Tolerable |
| Contaminated supply gas | Remote | Serious | 17 | Tolerable |

### Hazard: Environmental disturbance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| ‘Special’ EMI | Remote | Critical | 12 | Moderate |
| ‘Normal’ EMI | Frequent | Critical | 3 | Intolerable |
| Conducted voltage spike/dip | Occasional | Serious | 13 | Moderate |
| Gas pressure spike/dip | Probable | Serious | 9 | Moderate |
| Shock or vibration (environmental) | Occasional | Minor | 18 | Tolerable |
| Water ingress | Occasional | Critical | 8 | Moderate |

### Hazard: Use error

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Inadequate use instructions | Probable | Critical | 5 | Intolerable |
| Unconventional technology/methods | Occasional | Serious | 13 | Moderate |
| Confusing interface/display/sound | Occasional | Serious | 13 | Moderate |
| Faulty display/sounder | Almost imp. | Critical | 21 | Tolerable |
| Unintended selection | Probable | Critical | 5 | Intolerable |
| Unknowingly making selection | Occasional | Critical | 8 | Moderate |
| Inappropriate user skills | Probable | Critical | 5 | Intolerable |

### Hazard: Microprocessor

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Program memory fail | Improbable | Catastrophic | 11 | Moderate |
| Data memory fail | Improbable | Catastrophic | 11 | Moderate |
| Inadequacy in software design | Remote | Critical | 12 | Moderate |
| Inadequacy in software implementation | Remote | Critical | 12 | Moderate |

### Hazard: Electronics

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Initiating cause | Occurrence | Consequence | Rating | Risk Level |
| Component failure | Improbable | Critical | 16 | Tolerable |
| Inadequacy in electronic design | Remote | Critical | 12 | Moderate |
| Inadequacy in electronic implementation | Remote | Critical | 12 | Moderate |

## Risks reduction and final evaluation

This section lists all the identified initiating root hazards and their initial risk evaluation. The risk is identified and evaluated in the previous sections, in accordance with the device risk management plan (ref i), as a risk rating (R) derived from probability (P) and consequence (C).

It then describes the risk reduction methods employed in the design. The residual risk is ascertained, taking into account the risk reduction methods and an indication of the effectiveness of the risk control is given.

| **Hazard / Initiating Cause** | **Initial rating** | **Risk reduction technique** | **Residual risk rating** | **Final risk level** |
| --- | --- | --- | --- | --- |
| Mains power failure | 2 | Design incorporates a power loss alarm and 45 minutes backup battery. See Functional Specification. | 19 | Tolerable |
| ‘Normal’ EMI | 3 | The equipment electrical and electronic circuit is designed in accordance with best EMC practices, by qualified electronics engineers with extensive experiences in high-speed data communications. The data and actuator lines are copied form a design (of a third party manufacturer) that has obtained testing certificate of conformity to IEC 60601-1-2. Risk analysis demonstrates the associated EMC risks are tolerated, under the emergency circumstances. See conformity assessment to ISO 60601 series of standards. | 19 | Tolerable |
| Power converter or fuse failure | 4 | Design incorporates a power loss alarm and 45 minutes backup battery. See Functional Specification. | 19 | Tolerable |
| Supply gas fail | 4 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. | 18 | Tolerable |
| Inadequate use instructions | 5 | User instructions are validated by usability evaluation. The ventilator operating concept is simplified for basic respiratory care skills. See Pre-clinical Evaluation. | 16 | Tolerable |
| Inappropriate user skills | 5 | The ventilator operating concept is simplified for basic respiratory care skills. User instructions defines the user responsibility and skills level, in accordance with IEC 60601-2-12. See conformity assessment to ISO 60601 series of standards. | 17 | Tolerable |
| Insufficient EP plateau | 5 | Ventilator will alarm if EP deviates by +/-2mbar or if expiration decay time exceeds 0.7s, which in worse case would limit the IP plateau. | 17 | Tolerable |
| Insufficient Tidal Volume | 5 | User instructions states that any changes in the trends should be reviewed or investigated by a suitably qualified clinician, with view to prescribe adjustments to the ventilator settings or associated therapy. It specifically states that “a decreasing Tdi could indicate declining lung compliance and onset of ARDS (Acute Respiratory Distress Syndrome). The clinician might want to review (with blood gas measures) and consider whether to increase IP to achieve sufficient Tidal Volume, or increase BPM to achieve sufficient Minute Volume”. | 17 | Tolerable |
| Unintended selection | 5 | Parameter changes requires interaction with a least 3 pushes on 2 different buttons, that are spaced more than 2 ginger widths. See conformity assessment to ISO 60601 series of standards. | 25 | Tolerable |
| Open exhaust | 6 | User instructions recommends using a bacteria filter and consider hospital infection controls. | 18 | Tolerable |
| Electronic valve driver fails | 7 | Functional specification lists critical parts and their ratings, confirming they operate within. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 23 | Tolerable |
| Exhalation valve fails/soiled | 7 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. User instructions recommends using a bacteria filter and consider hospital infection controls. | 23 | Tolerable |
| PR drifts or fails | 7 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. | 17 | Tolerable |
| PTR1 fails and over-/under measures | 7 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. | 17 | Tolerable |
| Solenoid valve SV2 fails open | 7 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. Separate monitor can perform a safe shutdown by SV1 on overpressure. | 17 | Tolerable |
| Solenoid valve SV3 fails open | 7 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. See Functional Specification. Separate monitor can perform a safe shutdown by SV1 on overpressure. | 17 | Tolerable |
| Unknowingly making selection | 8 | Parameter changes requires interaction with a least 3 pushes on 2 different buttons, that are spaced more than 2 ginger widths. See conformity assessment to ISO 60601 series of standards. | 21 | Tolerable |
| Water ingress | 8 | Enclosure is designed to IEC 60601-1 and IEC 60601-2-12. See conformity assessment to ISO 60601 series of standards. IEC 60601-1 water test documented in Pre-clinical Evaluation. | 24 | Tolerable |
| Gas pressure spike/dip | 9 | Both monitor and controller have independent pressure sensors and shutdown valves, the closes supply if breathing circuit pressure exceeds 40mbar. Dual fail safe. See Functional Specification. See conformity assessment to ISO 60601 series of standards. | 19 | Tolerable |
| Inadequate cleaning | 9 | Design affords easy cleaning surfaces. User instructions describes the method of cleaning. See conformity assessment to ISO 60601 series of standards. | 18 | Tolerable |
| Data memory fail | 11 | EEPROM uses best 3 of 5 routine, to correct from data corruption. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 26 | Tolerable |
| Program memory fail | 11 | Power-up self-test with checksum. | 22 | Tolerable |
| Solenoid valve SV1 fails closed | 11 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 22 | Tolerable |
| Solenoid valve SV2 fails closed | 11 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 22 | Tolerable |
| Solenoid valve SV3 fails closed | 11 | Design will detect a pressure cycle fail and alarm. Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 22 | Tolerable |
| ‘Special’ EMI | 12 | User instructions warns that the ventilator IS NOT compatible with MRI scanner control zones and other equipment radiating high electro-magnetic power. | 16 | Tolerable |
| Inadequacy in electronic design | 12 | The equipment electrical and electronic circuit is designed and implemented in accordance with best practices, by qualified electronics engineers with extensive experiences medical devices and in high-speed data communications. The reference design is copied form a design (of a third party manufacturer) that has obtained testing certificate of conformity to IEC 60601-1-2. Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 16 | Tolerable |
| Inadequacy in electronic implementation | 12 | The equipment electrical and electronic circuit is designed and implemented in accordance with best practices, by qualified electronics engineers with extensive experiences medical devices and in high-speed data communications. The reference design is copied form a design (of a third party manufacturer) that has obtained testing certificate of conformity to IEC 60601-1-2. Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 16 | Tolerable |
| Inadequacy in software design | 12 | The equipment software is designed and implemented in accordance with best practices, by qualified electronics engineers with extensive experiences medical devices and in high-speed data communications. Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 16 | Tolerable |
| Inadequacy in software implementation | 12 | The equipment software is designed and implemented in accordance with best practices, by qualified electronics engineers with extensive experiences medical devices and in high-speed data communications. Specification. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 16 | Tolerable |
| Insufficient IP plateau | 12 | Ventilator will alarm if IP is not reached or if the IP rise time exceeds 0.7s, which in worse case would limit the IP plateau. | 17 | Tolerable |
| Patient circuit blocked/kinked | 12 | Ventilator will alarm if IP rise time or EP decay time exceeds 0.7s, which in would indicate a restrictive circuit. | 23 | Tolerable |
| Conducted voltage spike/dip | 13 | The equipment electrical and electronic circuit is designed in accordance with best EMC practices, by qualified electronics engineers with extensive experiences in high-speed data communications. The data and actuator lines are copied form a design (of a third party manufacturer) that has obtained testing certificate of conformity to IEC 60601-1-2. Risk analysis demonstrates the associated EMC risks are tolerated, under the emergency circumstances. See conformity assessment to ISO 60601 series of standards. | 19 | Tolerable |
| Confusing interface/display/sound | 13 | The ventilator operating concept is simplified for basic respiratory care skills. Both ventilator and user instructions are validated by usability evaluation. See Pre-clinical Evaluation. | 26 | Tolerable |
| Shearing of lung tissue | 13 | Pressure rise time is calibrated to produce maximum 60L/min in rush flow. Safety shut down if pressure reached 40mbar, which reduces the risk of barotrauma.  User instructions states that any changes in the trends should be reviewed or investigated by a suitably qualified clinician, with view to prescribe adjustments to the ventilator settings or associated therapy. It recommends using a combination blood CO2 measurement device, which eliminates the risk of operating the EP too low (atelectasis). It further specifically states that “an increasing Tdi could indicate improving lung compliance. The clinician might want to review (with blood gas measures) and consider if IP can be reduced, to maintain a steady Tidal Volume and prevent over-distending the lung”. | 23 | Tolerable |
| Unconventional technology/methods | 13 | User instructions are validated by usability evaluation. See Pre-clinical Evaluation.  User instructions defines the user responsibility and skills level, in accordance with IEC 60601-2-12. See conformity assessment to ISO 60601 series of standards. | 17 | Tolerable |
| Entanglement | 14 | The power cord it attached to the ventilator with a P-clip, to reduce the risk of accidental disconnection. See conformity assessment to ISO 60601 series of standards. | 23 | Tolerable |
| Vibration and noise (from device) | 15 | Solenoid valves are mounted on dampener grommets. Complies with conventional 42dB noise threshold, applied to equipment in the intensive care unit. See conformity assessment to ISO 60601 series of standards. | 27 | Tolerable |
| Component failure (electronic) | 16 | Functional specification lists critical parts and their ratings, confirming they operate within. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. See conformity assessment to ISO 60601 series of standards. | 22 | Tolerable |
| Rebreathing | 16 | Incorporates a pair of low resistance directional valves to enable spontaneous breathing, without rebreathing. See Functional Specification. | 21 | Tolerable |
| Contaminated supply gas | 17 | User instructions includes a warning that “In case of low confidence in the contamination status of the supply gas, then use a particle and appropriate filer on the ‘Gas Output’ port”. | 22 | Tolerable |
| Toxic substance is fresh gas | 17 | Functional Specification lists critical parts and their ratings, including specifying ‘clean’ pneumatic components in the fresh gas flow path. This is convention in ventilator design. See conformity assessment to ISO 60601 series of standards. | 22 | Tolerable |
| Sharps | 18 | Design is assessed to IEC 60601 section on mechanical risks. See conformity assessment to ISO 60601 series of standards. | 23 | Tolerable |
| Shock or vibration (environmental) | 18 | Ventilator is mounted on rubber feet. See conformity assessment to ISO 60601 series of standards. | 23 | Tolerable |
| Display failure | 21 | Powerup self-test momentarily displays ‘8888888888888888’ to enable user to observe any faulty display element. | 25 | Tolerable |
| Faulty sounder | 21 | Main alarming module, the Monitor, has a microphone verifying that alarm sounds are produced. Controller and monitor implemented separately, to prevent any single fault from preventing the alarming function. If Monitor stops responding, the Controller will sound a backup alarm sounder. Duality. |  | Tolerable |
| Expelled parts/fluids | 23 | Any expelled gasses are mechanically harmless. The exhaled air exhaust could contain contaminants. User instructions recommends using a bacteria filter and consider hospital infection controls. |  | Tolerable |

# Conclusion

Based on the above analysis and evaluation, which has identified and estimated all known hazards, and conditional upon the successful validation of the system test results, the risks associated with the using the ventilator in clinic are reduced to acceptable levels. This conclusion relates to essential requirements for device safety, in respect of all current medical device standards.