Overview

The Low-Cost Ventilator was originated in response to the COVID-19 pandemic. The virus has caused a high hospitalization rate, with many patients requiring artificial ventilation. With limited medical ventilators available, this has led to triage situations where there are not enough ventilators to treat everyone who needs one. Many companies and organizations are focusing on expansion of production of certified medical ventilators. This is the ideal option, as these systems have been proven safe through the appropriate certification processes. However, this may not be enough. In case of that horrible possibility, the LCV is presented as an emergency alternative when no better options are available. The LCV is not and likely will not be properly certified. Nonetheless, this does not mean it should built without thought to its safety and security. This document analyzes possible safety and security issues with the LCV, and the design and process paths taken to counteract them.

Safety

The Hierarchy of Controls approach is a typical method for handling potentially unsafe scenarios. The best approach is to remove the hazard altogether. If that is not possible, the possibility of replacing the hazard should be evaluated. Barring that, we must isolate the people from the hazard using engineering controls. Using administrative or planning controls, we should create processes that protect the people. Finally, personal protective equipment (PPE) should be used to protect the people. This approach to evaluating the safety of the LCV helps guide the design.

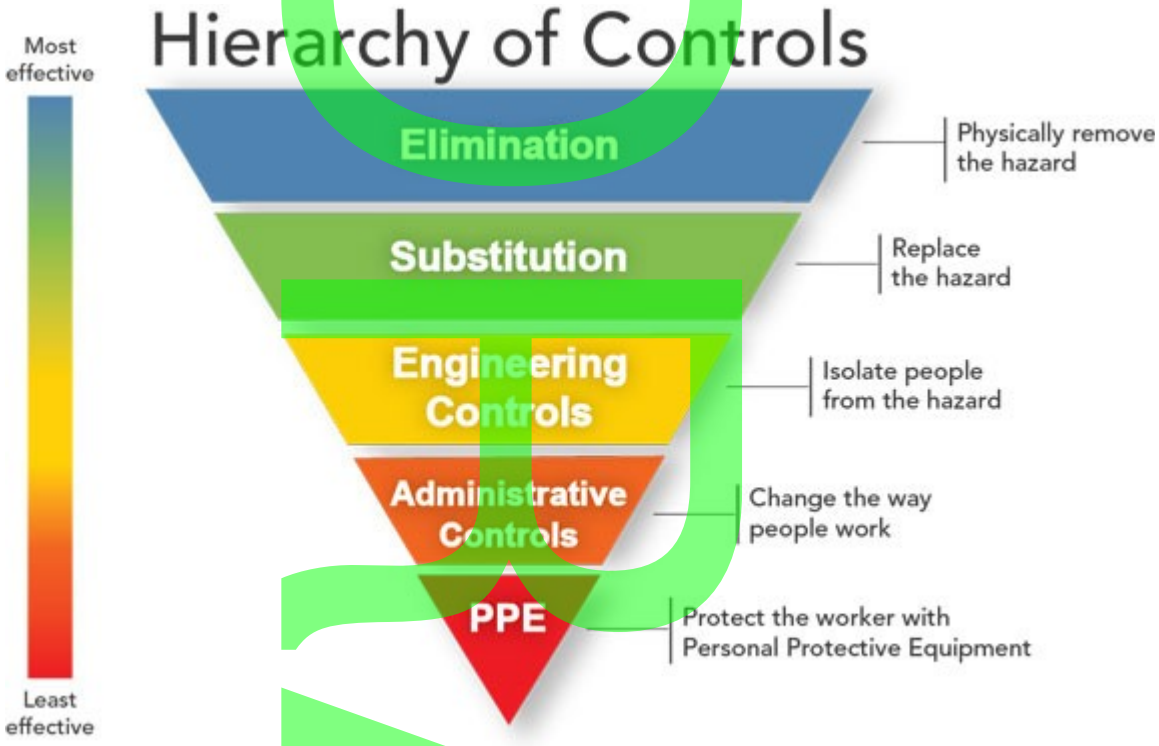

Illustration 1: Heirarchy of Controls (Source: CDC.gov)

General Safety

The first safety subsection to evaluate is general safety concerns which apply to both the patient and the medical professionals using the device.

Fire/Explosion

Medical ventilators can use compressed pure oxygen, which presents significant fire and explosion hazards.

1) Elimination

Since the presence of pure oxygen can be required for proper medical function, it cannot be completely eliminated. However, if pure oxygen is not required for a patient, it should not be used. However, certain parts can be avoided. An early design for the LCV included a solenoid which can present fire hazards unless specific and expensive explosion proof versions are used. This was eliminated from the design.

2) Substitution

Since the presence of pure oxygen can be required for proper medical function, it cannot be substituted.

3) Engineering Controls

The main fire and explosion hazard controls for the LCV are engineering controls. No parts can or will be used which can spark. This includes but is not limited to some brushed DC motors, electromechanical relays, and solenoids. The only actuator used in the LCV is a medical grade brushless blower motor specifically designed for use in medical ventilators.

The next fire and explosion hazard is overheating of parts due to improper use or voltage inversion. All connectors will be keyed so that they cannot be connected incorrectly. The power connections will be polarity protected. Fuses on the overall system and all subsystems will prevent burn-up in the case of a short. TVS diodes for ESD protection will be included at all external connections to protect the hardware.

Another possible fire and explosion hazard is the sparks generated when plugging in power to the LCV or connecting the backup battery. TODO: what to do about this? Are there slow start or arrestor circuits we could use?

4) Administrative Controls

All medical professionals using the LCV should be trained on the safe use of pure oxygen.

5) PPE

There is no PPE specifically for this hazard.

Electrical Shock

The LCV is an electrical device, and with all electrical devices care must be taken to avoid dangerous electrical shocks to people.

1) Elimination

The LCV is an electrical device, and electricity cannot be eliminated.

2) Substitution

The LCV is an electrical device, and electricity cannot be substituted.

3) Engineering Controls

Engineering controls are the main protection against electrical shock. This protection ties closely into fire and explosion hazard above, as all sparks must be prevented. However, further protections can be preformed here with respect to protecting people from electrical shock. The highest voltage used within

the LCV is 24VDC, which is typically safe to the touch. All electrical components will be enclosed in a case without holes large enough to fit fingers, so they will be physically isolated from people.

4) Administrative Controls

All users should be trained to not open the enclosure of the LCV. In case an appropriately knowledgeable person must open the device, they must unplug the device and wait some time to ensure energy stored in bulk capacitance discharges and the device is no longer energized. The amount of time is TBD based on design.

5) PPE

There is no PPE specifically for this hazard.

EMI with Other Systems

The LCV could potentially be used near other critical life support systems. It therefore must never be able to interfere with the normal operation of other systems.

1) Elimination

The LCV is an electrical device, and the possibility of it interfering with other systems can not be fully eliminated.

2) Substitution

The LCV is an electrical device, and that cannot be substituted.

3) Engineering Controls

The design of the LCV will incorporate a variety of standard approaches for avoiding EMI issues. The electronics will be enclosed within a shielded metallic case. All “high speed” signals such as SPI will have appropriate filtering for EMI control, and all traces for such signals on the PCB will be kept as short as possible. No intentional emitter will be included in the LCV design. An FCC certified power supply will be used.

4) Administrative Controls

Not applicable.

5) PPE

Not applicable.

Safety To Patient

This section covers potential safety hazards to the patient using the LCV. The LCV is intended only for emergency use when there is no other option, but it still must avoid further endangering the patient's life.

Overpressure

Certain ventilator designs, such as those with positive displacement pumps, run the risk of over-pressuring the patent's lungs, causing immense damage. This must be avoided.

1) Elimination

The LCV uses a medical-ventilator-grade blower pump for pressure control. As it is not a positive displacement pump, even uncontrolled max power cannot provide dangerous levels of pressure to the patients lungs.

2) Substitution

The potential use of a positive displacement pump was changed to a blower pump.

3) Engineering Controls

Triple redundant pressure sensors are used for feedback to the control system. Therefore, any single pressure sensor failure can be detected, and normal operation can continue. A COTS, high quality brushless motor controller module will be used to avoid design issues with this critical component. Within the firmware, protections will be made to ensure the pressure control loop has the highest priority and numerous error checks. TODO: include a mechanical pressure relief valve?

4) Administrative Controls

Trained medical professionals should be the only ones to set the control pressure levels to ensure patient safety.

5) PPE

Not applicable.

Contamination

Patients suffering from COVID-19 are vulnerable, and the LCV should not expose the patient or operator to any other biological or chemical hazards.

1) Elimination

The design of the LCV does not include any non-medical grade components within the air pathway except for the pressure sensors. The pressure sensors are isolated from the patient with a medical filter. (TODO anything more?). All components exposed to the patient are single-use and must be replaced regularly.

2) Substitution

Not applicable.

3) Engineering Controls

The user controls and enclosure of the LCV should be capable of withstanding wipedown for sanitation without damage.

4) Administrative Controls

All components exposed to the patient are single-use and must be replaced regularly. All external LCV surfaces should be regularly cleaned with appropriate cleaners.

5) PPE

Virus filters must be used between the wye and the endotracheal tube and at the exhaust port.

Incorrect Functionality

For emergency use, if the LCV does not function properly the patient could die. Medical ventilators are life support systems and therefore their correct functionality is critical. This encompasses a large variety of needs.

1) Elimination

The LCV should not be used unless all other options have been eliminated. It can only be used at the patient's own risk. Much care is taken for safety, but cannot be and is not ensured.

2) Substitution

The LCV should not be used unless all other options have been eliminated. It can only be used at the patient's own risk. Much care is taken for safety, but cannot be and is not ensured.

3) Engineering Controls

At the component level, medical ventilator grade components are used wherever possible (while maintaining general accessibility to parts), such as the blower and the mass flow sensor. Triple redundant pressure sensors are used, and a voting scheme ensures proper functionality even if a single sensor fails. The firmware will include a hardware watchdog, numerous error checks, and will abide by MISRA C standards and Doxygen-style documentation wherever possible. No dynamic memory

allocation will be allowed. The control loops will be designed with input from certified medical professionals, and tested significantly. TODO there is certainly more we can do, especially on firmware, ie. static analysis, unit testing, etc.

4) Administrative Controls

The alarm indications of the LCV should be monitored by medical professionals.

5) PPE

Not applicable.

Safety to Medical Professionals

This section covers safety concerns to the medical professionals potentially operating and monitoring the LCV.

Contamination

If the ventilator is improperly designed, it will vent contaminated air onto medical professionals in the area, worsening the situation.

1) Elimination

The LCV should not be used unless all other options have been eliminated. It can only be used at the patient's own risk. Much care is taken for safety, but cannot be and is not ensured.

2) Substitution

The LCV should not be used unless all other options have been eliminated. It can only be used at the patient's own risk. Much care is taken for safety, but cannot be and is not ensured.

3) Engineering Controls

Medical virus filters are placed in the breathing pathway to filter the air leaving the patient's lungs before venting into the nearby area. These are single-use elements and should be disposed of as biohazards. All other components in the breathing circuit should likewise be treated as single-use and biohazards. TODO how are some non-replaceable components cleaned?

4) Administrative Controls

Training documentation will be developed for precise setup of the LCV, and which parts must be replaced and treated as biohazards.

5) PPE

Appropriate PPE should be worn by medical professionals at all times, including but not limited to face masks, face shields, eye goggles, gloves, and scrubs. Virus filters must be used on the gas pathways.

Security

For many modern electronic devices, even for FDA certified medical devices, security is too often not considered at all. For the LCV, some base security concerns are analyzed.

Prevention of Function

This section is concerned with bad actors maliciously preventing the proper functionality of the LCV.

1) Elimination

Not applicable.

2) Substitution

Not applicable.

3) Engineering Controls

The electronics for the LCV are enclosed within a case, do not have a wireless radio, and all programming ports are hidden from external access. With physical access to the LCV, it is not secure against tampering, but this is not considered a major concern. In general, security against unrestricted physical access is not considered strong.

4) Administrative Controls

Not applicable.

5) PPE

Not applicable.

Personal Information

This section is concerned with bad actors maliciously extracting sensitive information from the LCV.

1) Elimination

The LCV does not have any sensitive medical information onboard. It will have no knowledge of the patient at all.

2) Substitution

Not applicable.

3) Engineering Controls

All ports are internal and no radio is included. Physical access and/or view of the input/output components would be required to extract information.

4) Administrative Controls

Ensure standard medical access control.

5) PPE

Not applicable.

Summary of Critical Design Safety Features

- Medical grade blower pump with brushless motor
- Medical grade mass flow sensor
- Triple redundant pressure sensing with voting
- Fuses on the whole system and all subsystems
- Keyed connectors to eliminate incorrect connections
- Polarity protected power connections
- ESD protection at all external connections
- 24 VDC maximum voltage for safety
- Fully enclosed electronics
- Shielded enclosure for EMI protection
- Appropriate filtering on high speed signals for EMI prevention
- No radio communications
- Piezo buzzer and error light for alarm default to on, microcontroller system keeps off. Alert is raised if microcontroller fails to do this. This is in effect a physically independent watchdog from the microcontroller.
- Hardware pulldowns on motor controller to default off
- Emergency shutoff button