Demonstration Safety Case Argument for the Gravity Ventilator (gVent)

Critical Systems Labs Inc., Vancouver, BC, Canada

WWW.CRITICALSYSTEMSLABS.COM

Demonstration Safety Case Argument for the Gravity Ventilator (gVent)

A Representative Example

DISCLAIMER: *This safety case argument was produced by Critical Systems Labs Inc. (CSL) based on publicly available information provided by COSMIC Medical*[1] *about their Gravity Ventilator (gVent) prototype project*[2]*. This document contains representative example of a safety assurance case for a novel system for use in education or research settings. Since this safety case argument is an example, it is not suitable for use as part of regulatory process or safety assurance activities for a medical device intended for use in a healthcare or medical setting. To CSL's knowledge gVent has not received approval for use as a medical device with humans.*

Background and Context

COSMIC Medical began in early 2020 in Vancouver as a volunteer-driven, open-source initiative to tackle critical equipment shortages triggered by the global COVID-19 pandemic. As hospitals worldwide braced for surges in respiratory failure and ventilator demand, the founders — a mix of physicians, engineers and students — launched multiple rapid-response projects aiming to provide low-cost, easily manufactured respiratory support devices.

Within this effort, gVent emerged as a novel alternative to traditional ventilators and bag-valve-mask (BVM) systems. Rather than relying on complex, specialized medical-grade parts, which became scarce during the pandemic, gVent was designed entirely with readily available materials and simple mechanical principles, making it potentially deployable in resource-limited settings or under emergency circumstances.

Project Objectives and Overview

gVent is a gravity- and water-based positive-pressure ventilator that uses two cylindrical vessels and a water seal to generate pressurized gases for patient ventilation. As hospital-supplied medical air/oxygen enters the system, the rising pressure pushes an inner cylinder upward; when a valve is opened, this pressurized mixture is delivered to the patient. Through control of the valve (via electronics), the system can regulate key respiratory parameters, such as inspiratory pressure, tidal volume, respiratory rate, and I:E ratio, offering both mandatory ventilation (for sedated patients) and patient-triggered support (for spontaneously breathing patients).

Because of the water-seal mechanism, gVent delivers ventilation with constant plateau pressures, reducing risk of barotrauma compared with many other low-cost ventilator designs. Prototype testing (including at a hospital simulation lab) demonstrated proof-of-concept functionality over multi-hour cycles, with pressure, flow, tidal volume, and alarm systems performing as intended.

Following the development of the technology, Critical Systems Labs Inc. developed a safety case argument for gVent as a demonstration of the Eliminative Argumentation (EA) methodology applied to a prototype medical device. This safety case was developed using CSL's *Socrates – Assurance Case Editor* product[3].

[1] https://www.cosmicmedical.ca/

[2] https://github.com/COSMIC-medical/gVent

[3] https://criticalsystemslabs.com/socrates-assurance/

The following system overview is intended to orient the reader gVent device as presented on COSMIC Medical’s website (https://www.cosmicmedical.ca/gvent).

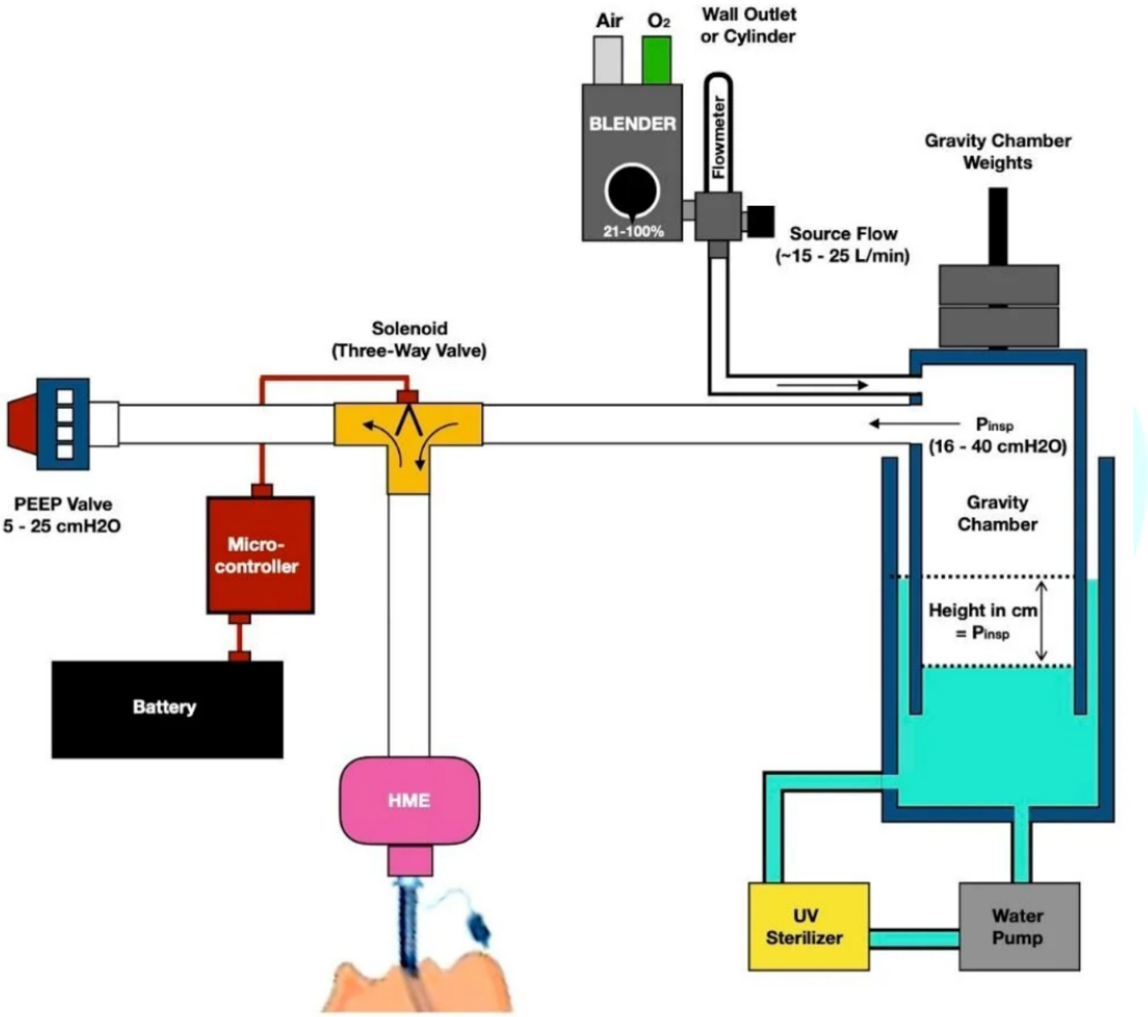


Figure 1 - System design (from https://www.cosmicmedical.ca/gvent)

Argument Visualization and Supporting Artifacts

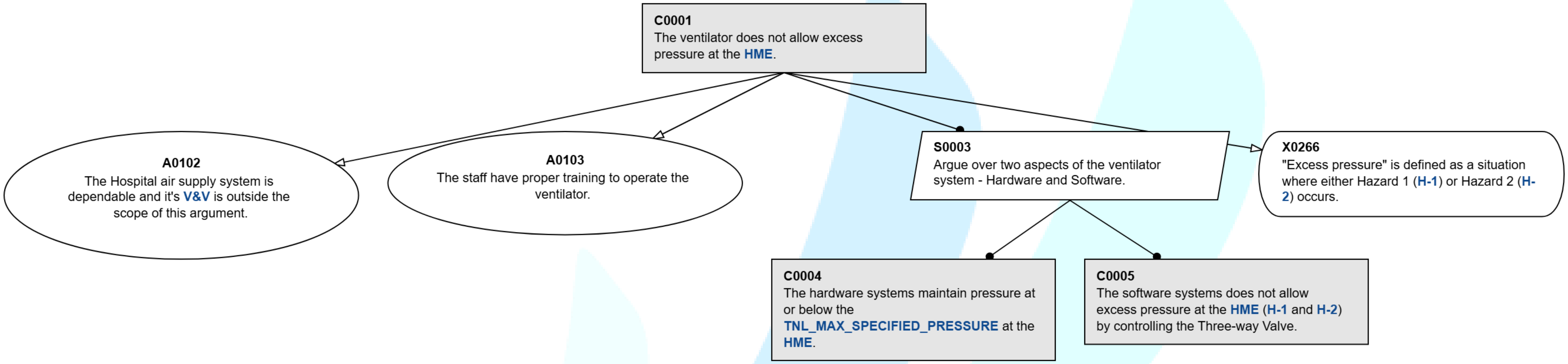
The safety case argument is presented in the remainder of this document. Each diagram corresponds to a “sub-argument” fragment. When composed together, the sub-arguments collectively make the safety case argument.

A version of this argument is available in an archival JSON format on CSL’s website:

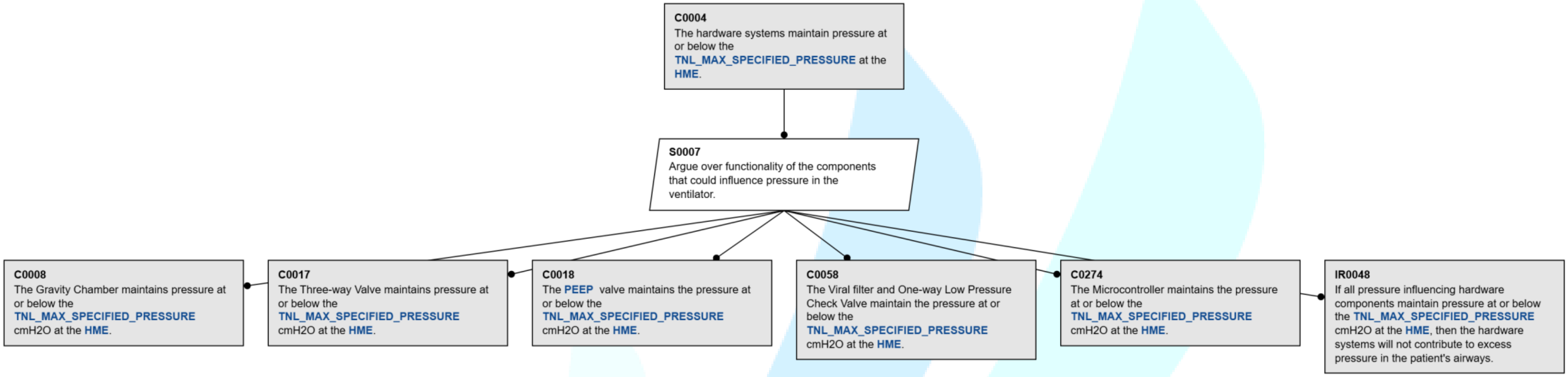
- https://criticalsystemslabs.com/resources-hub/2025GVent/gvent-argument.json

Argument

C0001 - The ventilator does not allow excess pressure at the HME.			
Parent subtree(s)	None	**Descendant subtree(s)**	C0004, C0005
Glossary Terms	HME, TNL_MAX_SPECIFIED_PRESSURE, H-1, H-2, V&V		


C0001
The ventilator does not allow excess pressure at the HME.
A0102
The Hospital air supply system is dependable and it's V&V is outside the scope of this argument.
A0103
The staff have proper training to operate the ventilator.
S0003
Argue over two aspects of the ventilator system - Hardware and Software.
X0266
"Excess pressure" is defined as a situation where either Hazard 1 (H-1) or Hazard 2 (H-2) occurs.
C0004
The hardware systems maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE at the HME.
C0005
The software systems does not allow excess pressure at the HME (H-1 and H-2) by controlling the Three-way Valve.

C0004 - The hardware systems maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE at the HME.			
Parent subtree(s)	C0001	**Descendant subtree(s)**	C0008, C0017, C0018, IR0048, C0058, C0274
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, PEEP		



C0004
The hardware systems maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE at the HME.

S0007
Argue over functionality of the components that could influence pressure in the ventilator.

C0008
The Gravity Chamber maintains pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0017
The Three-way Valve maintains pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

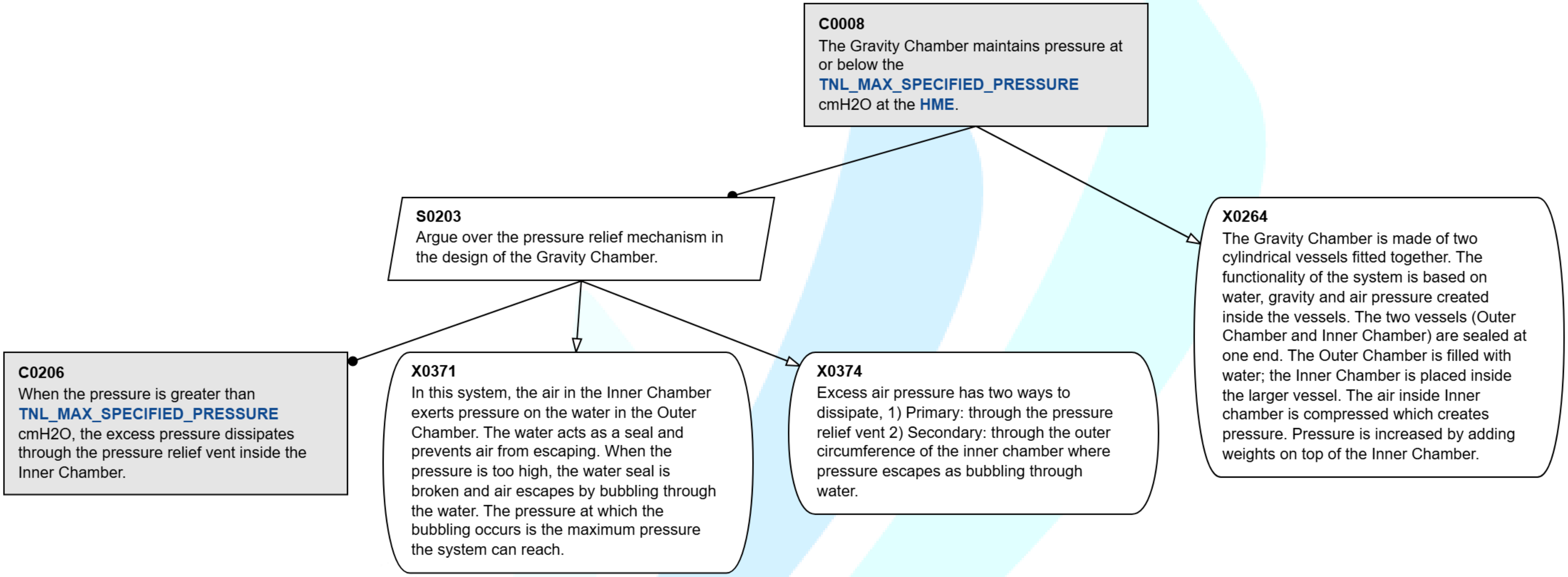
C0018
The PEEP valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0058
The Viral filter and One-way Low Pressure Check Valve maintain the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0274
The Microcontroller maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

IR0048
If all pressure influencing hardware components maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME, then the hardware systems will not contribute to excess pressure in the patient's airways.

C0008 - The Gravity Chamber maintains pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0004	**Descendant subtree(s)**	C0206
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



C0008
The Gravity Chamber maintains pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

S0203
Argue over the pressure relief mechanism in the design of the Gravity Chamber.

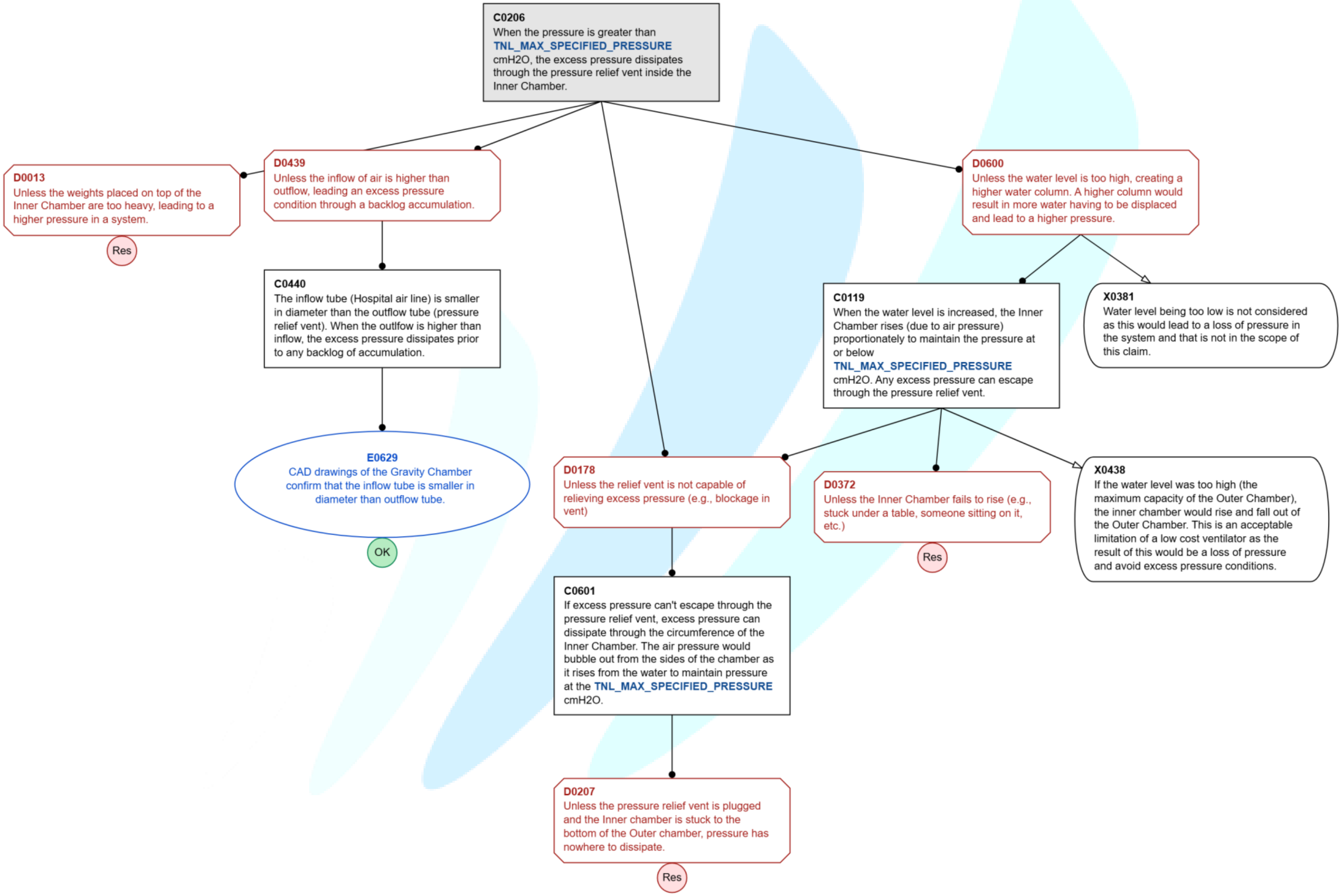
X0264
The Gravity Chamber is made of two cylindrical vessels fitted together. The functionality of the system is based on water, gravity and air pressure created inside the vessels. The two vessels (Outer Chamber and Inner Chamber) are sealed at one end. The Outer Chamber is filled with water; the Inner Chamber is placed inside the larger vessel. The air inside Inner chamber is compressed which creates pressure. Pressure is increased by adding weights on top of the Inner Chamber.

C0206
When the pressure is greater than **TNL_MAX_SPECIFIED_PRESSURE** cmH2O, the excess pressure dissipates through the pressure relief vent inside the Inner Chamber.

X0371
In this system, the air in the Inner Chamber exerts pressure on the water in the Outer Chamber. The water acts as a seal and prevents air from escaping. When the pressure is too high, the water seal is broken and air escapes by bubbling through the water. The pressure at which the bubbling occurs is the maximum pressure the system can reach.

X0374
Excess air pressure has two ways to dissipate, 1) Primary: through the pressure relief vent 2) Secondary: through the outer circumference of the inner chamber where pressure escapes as bubbling through water.

C0206 - When the pressure is greater than TNL_MAX_SPECIFIED_PRESSURE cmH2O, the excess pressure dissipates through the pressure relief vent inside t...			
Parent subtree(s)	C0008	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE		



C0206
When the pressure is greater than **TNL_MAX_SPECIFIED_PRESSURE** cmH2O, the excess pressure dissipates through the pressure relief vent inside the Inner Chamber.

D0013
Unless the weights placed on top of the Inner Chamber are too heavy, leading to a higher pressure in a system.

D0439
Unless the inflow of air is higher than outflow, leading an excess pressure condition through a backlog accumulation.

D0600
Unless the water level is too high, creating a higher water column. A higher column would result in more water having to be displaced and lead to a higher pressure.

C0440
The inflow tube (Hospital air line) is smaller in diameter than the outflow tube (pressure relief vent). When the outflow is higher than inflow, the excess pressure dissipates prior to any backlog of accumulation.

C0119
When the water level is increased, the Inner Chamber rises (due to air pressure) proportionately to maintain the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O. Any excess pressure can escape through the pressure relief vent.

X0381
Water level being too low is not considered as this would lead to a loss of pressure in the system and that is not in the scope of this claim.

E0629
CAD drawings of the Gravity Chamber confirm that the inflow tube is smaller in diameter than outflow tube.

D0178
Unless the relief vent is not capable of relieving excess pressure (e.g., blockage in vent)

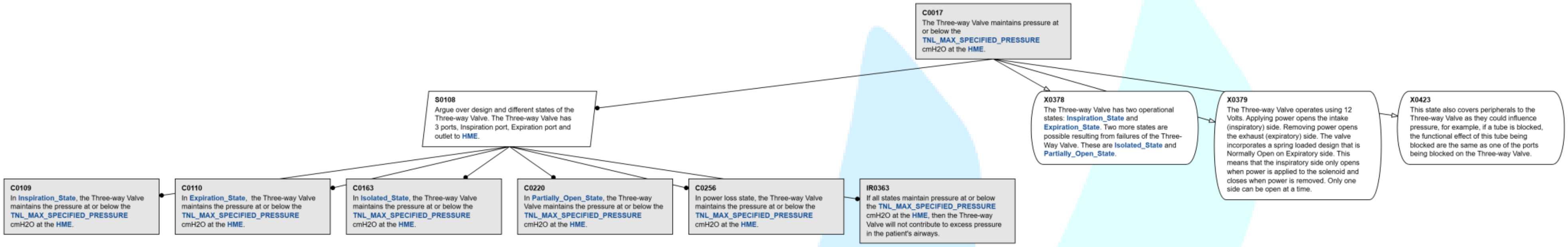
D0372
Unless the Inner Chamber fails to rise (e.g., stuck under a table, someone sitting on it, etc.)

X0438
If the water level was too high (the maximum capacity of the Outer Chamber), the inner chamber would rise and fall out of the Outer Chamber. This is an acceptable limitation of a low cost ventilator as the result of this would be a loss of pressure and avoid excess pressure conditions.

C0601
If excess pressure can't escape through the pressure relief vent, excess pressure can dissipate through the circumference of the Inner Chamber. The air pressure would bubble out from the sides of the chamber as it rises from the water to maintain pressure at the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O.

D0207
Unless the pressure relief vent is plugged and the Inner chamber is stuck to the bottom of the Outer chamber, pressure has nowhere to dissipate.

C0017 - The Three-way Valve maintains pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0004, D0580	**Descendant subtree(s)**	C0109, C0110, C0163, C0220, C0256, IR0363
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, PEEP, Inspiration_State, Expiration_State, Isolated_State, Partially_Open_State		



C0017
The Three-way Valve maintains pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

S0108
Argue over design and different states of the Three-way Valve. The Three-way Valve has 3 ports, Inspiration port, Expiration port and outlet to HME.

X0378
The Three-way Valve has two operational states: Inspiration_State and Expiration_State. Two more states are possible resulting from failures of the Three-Way Valve. These are Isolated_State and Partially_Open_State.

X0379
The Three-way Valve operates using 12 Volts. Applying power opens the intake (inspiratory) side. Removing power opens the exhaust (expiratory) side. The valve incorporates a spring loaded design that is Normally Open on Expiratory side. This means that the inspiratory side only opens when power is applied to the solenoid and closes when power is removed. Only one side can be open at a time.

X0423
This state also covers peripherals to the Three-way Valve as they could influence pressure, for example, if a tube is blocked, the functional effect of this tube being blocked are the same as one of the ports being blocked on the Three-way Valve.

C0109
In Inspiration_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0110
In Expiration_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

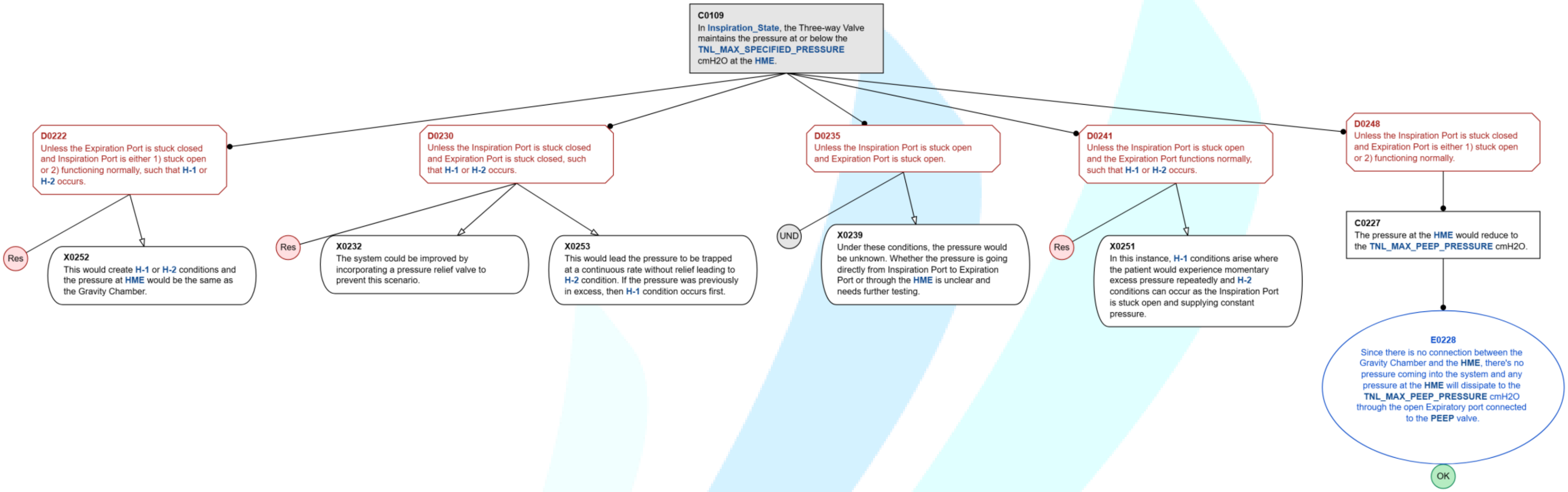
C0163
In Isolated_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0220
In Partially_Open_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0256
In power loss state, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

IR0363
If all states maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME, then the Three-way Valve will not contribute to excess pressure in the patient's airways.

C0109 - In Inspiration_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	Inspiration_State, TNL_MAX_SPECIFIED_PRESSURE, HME, H-1, H-2, TNL_MAX_PEEP_PRESSURE, PEEP		



C0109
In Inspiration_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

D0222
Unless the Expiration Port is stuck closed and Inspiration Port is either 1) stuck open or 2) functioning normally, such that H-1 or H-2 occurs.

X0252
This would create H-1 or H-2 conditions and the pressure at HME would be the same as the Gravity Chamber.

D0230
Unless the Inspiration Port is stuck closed and Expiration Port is stuck closed, such that H-1 or H-2 occurs.

X0232
The system could be improved by incorporating a pressure relief valve to prevent this scenario.

X0253
This would lead the pressure to be trapped at a continuous rate without relief leading to H-2 condition. If the pressure was previously in excess, then H-1 condition occurs first.

D0235
Unless the Inspiration Port is stuck open and Expiration Port is stuck open.

X0239
Under these conditions, the pressure would be unknown. Whether the pressure is going directly from Inspiration Port to Expiration Port or through the HME is unclear and needs further testing.

D0241
Unless the Inspiration Port is stuck open and the Expiration Port functions normally, such that H-1 or H-2 occurs.

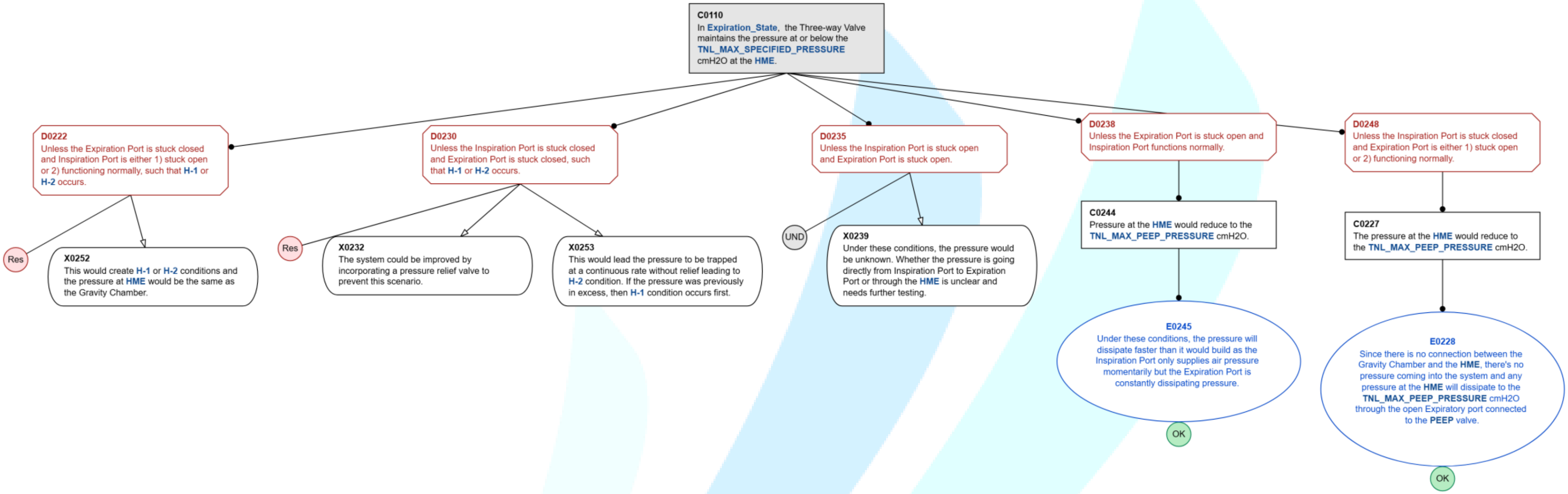
X0251
In this instance, H-1 conditions arise where the patient would experience momentary excess pressure repeatedly and H-2 conditions can occur as the Inspiration Port is stuck open and supplying constant pressure.

D0248
Unless the Inspiration Port is stuck closed and Expiration Port is either 1) stuck open or 2) functioning normally.

C0227
The pressure at the HME would reduce to the TNL_MAX_PEEP_PRESSURE cmH2O.

E0228
Since there is no connection between the Gravity Chamber and the HME, there's no pressure coming into the system and any pressure at the HME will dissipate to the TNL_MAX_PEEP_PRESSURE cmH2O through the open Expiratory port connected to the PEEP valve.

C0110 - In Expiration_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	Expiration_State, TNL_MAX_SPECIFIED_PRESSURE, HME, H-1, H-2, TNL_MAX_PEEP_PRESSURE, PEEP		



C0110
In **Expiration_State**, the Three-way Valve maintains the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

D0222
Unless the Expiration Port is stuck closed and Inspiration Port is either 1) stuck open or 2) functioning normally, such that **H-1** or **H-2** occurs.

X0252
This would create **H-1** or **H-2** conditions and the pressure at **HME** would be the same as the Gravity Chamber.

D0230
Unless the Inspiration Port is stuck closed and Expiration Port is stuck closed, such that **H-1** or **H-2** occurs.

X0232
The system could be improved by incorporating a pressure relief valve to prevent this scenario.

X0253
This would lead the pressure to be trapped at a continuous rate without relief leading to **H-2** condition. If the pressure was previously in excess, then **H-1** condition occurs first.

D0235
Unless the Inspiration Port is stuck open and Expiration Port is stuck open.

X0239
Under these conditions, the pressure would be unknown. Whether the pressure is going directly from Inspiration Port to Expiration Port or through the **HME** is unclear and needs further testing.

D0238
Unless the Expiration Port is stuck open and Inspiration Port functions normally.

C0244
Pressure at the **HME** would reduce to the **TNL_MAX_PEEP_PRESSURE** cmH2O.

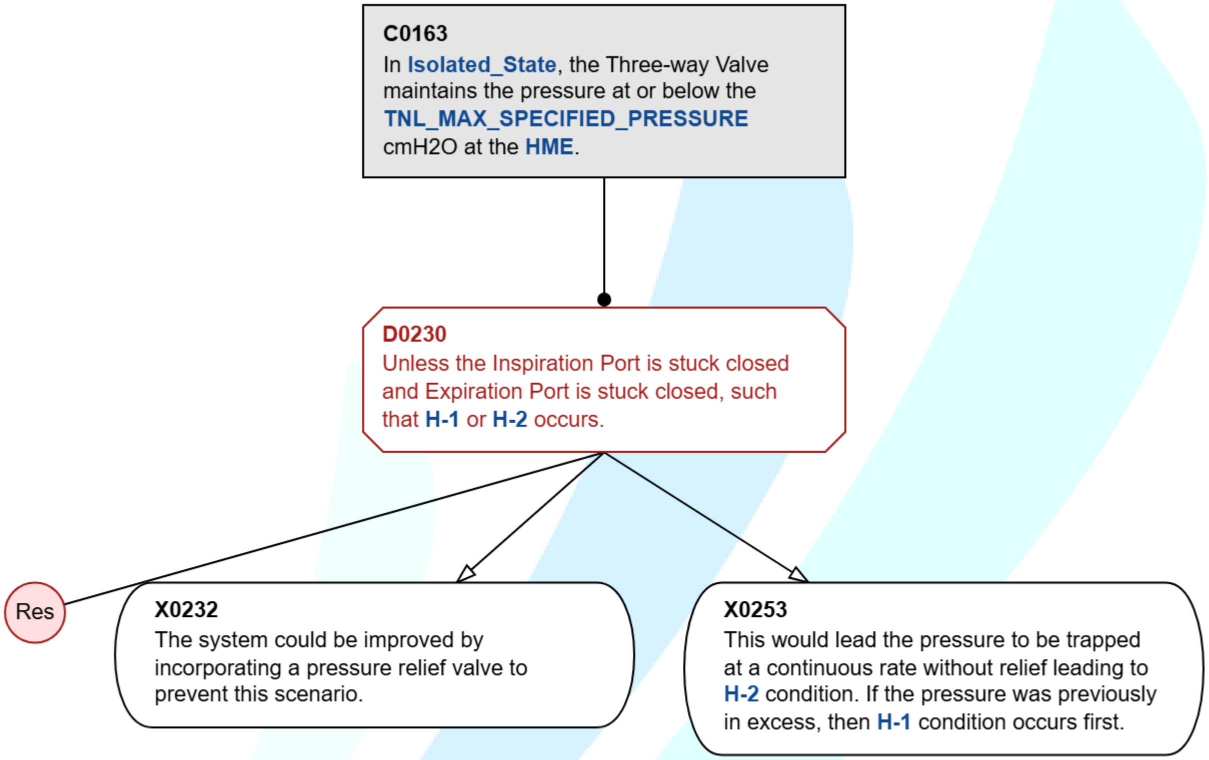
E0245
Under these conditions, the pressure will dissipate faster than it would build as the Inspiration Port only supplies air pressure momentarily but the Expiration Port is constantly dissipating pressure.

D0248
Unless the Inspiration Port is stuck closed and Expiration Port is either 1) stuck open or 2) functioning normally.

C0227
The pressure at the **HME** would reduce to the **TNL_MAX_PEEP_PRESSURE** cmH2O.

E0228
Since there is no connection between the Gravity Chamber and the **HME**, there's no pressure coming into the system and any pressure at the **HME** will dissipate to the **TNL_MAX_PEEP_PRESSURE** cmH2O through the open Expiratory port connected to the **PEEP** valve.

C0163 - In Isolated_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	Isolated_State, TNL_MAX_SPECIFIED_PRESSURE, HME, H-1, H-2		



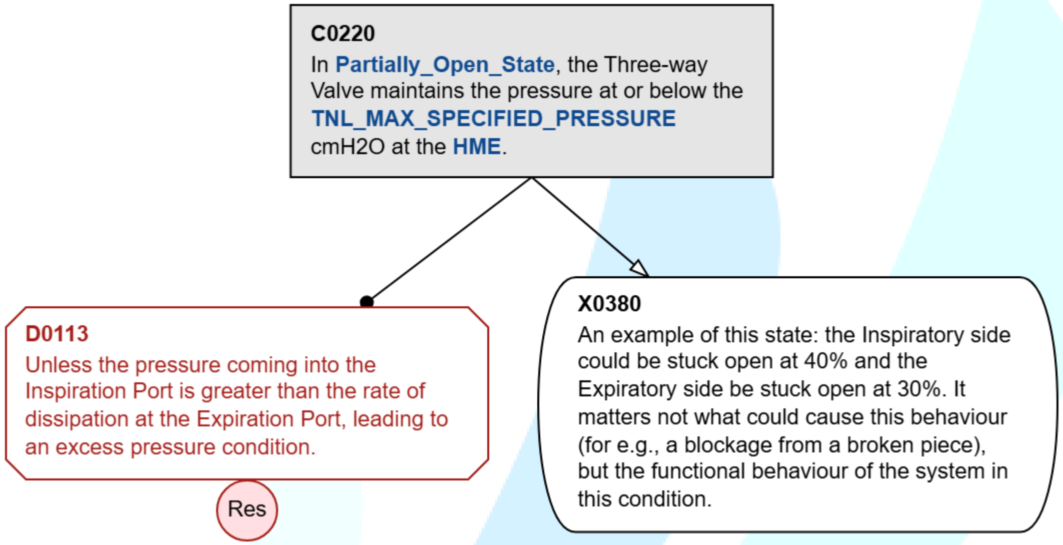
C0163
In **Isolated_State**, the Three-way Valve maintains the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

D0230
Unless the Inspiration Port is stuck closed and Expiration Port is stuck closed, such that **H-1** or **H-2** occurs.

X0232
The system could be improved by incorporating a pressure relief valve to prevent this scenario.

X0253
This would lead the pressure to be trapped at a continuous rate without relief leading to **H-2** condition. If the pressure was previously in excess, then **H-1** condition occurs first.

C0220 - In Partially_Open_State, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	Partially_Open_State, TNL_MAX_SPECIFIED_PRESSURE, HME		

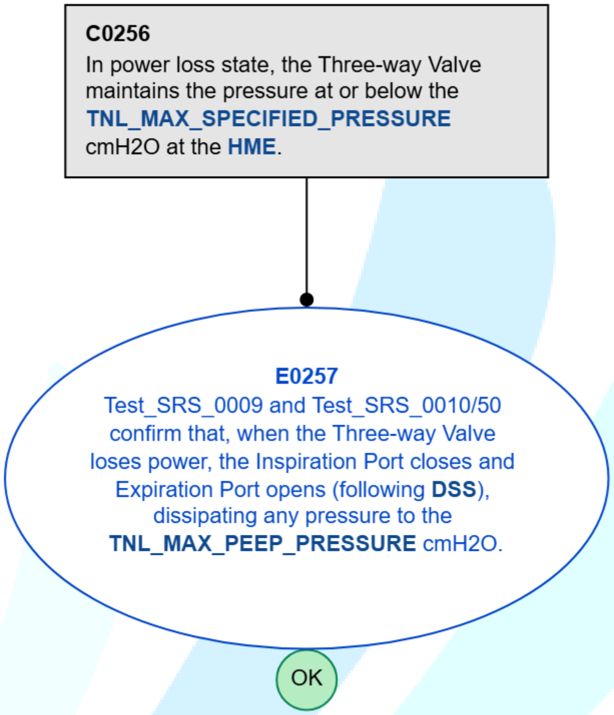


C0220
In **Partially_Open_State**, the Three-way Valve maintains the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

D0113
Unless the pressure coming into the Inspiration Port is greater than the rate of dissipation at the Expiration Port, leading to an excess pressure condition.

X0380
An example of this state: the Inspiratory side could be stuck open at 40% and the Expiratory side be stuck open at 30%. It matters not what could cause this behaviour (for e.g., a blockage from a broken piece), but the functional behaviour of the system in this condition.

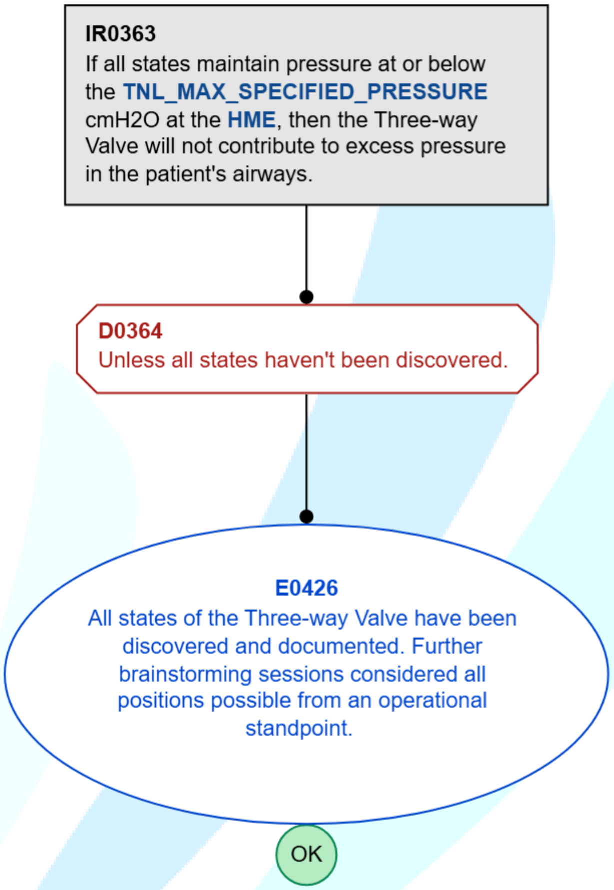
C0256 - In power loss state, the Three-way Valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, DSS, TNL_MAX_PEEP_PRESSURE		



C0256
In power loss state, the Three-way Valve maintains the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

E0257
Test_SRS_0009 and Test_SRS_0010/50 confirm that, when the Three-way Valve loses power, the Inspiration Port closes and Expiration Port opens (following **DSS**), dissipating any pressure to the **TNL_MAX_PEEP_PRESSURE** cmH2O.

IR0363 - If all states maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME, then the Three-way Valve will not contribute to...			
Parent subtree(s)	C0017	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		

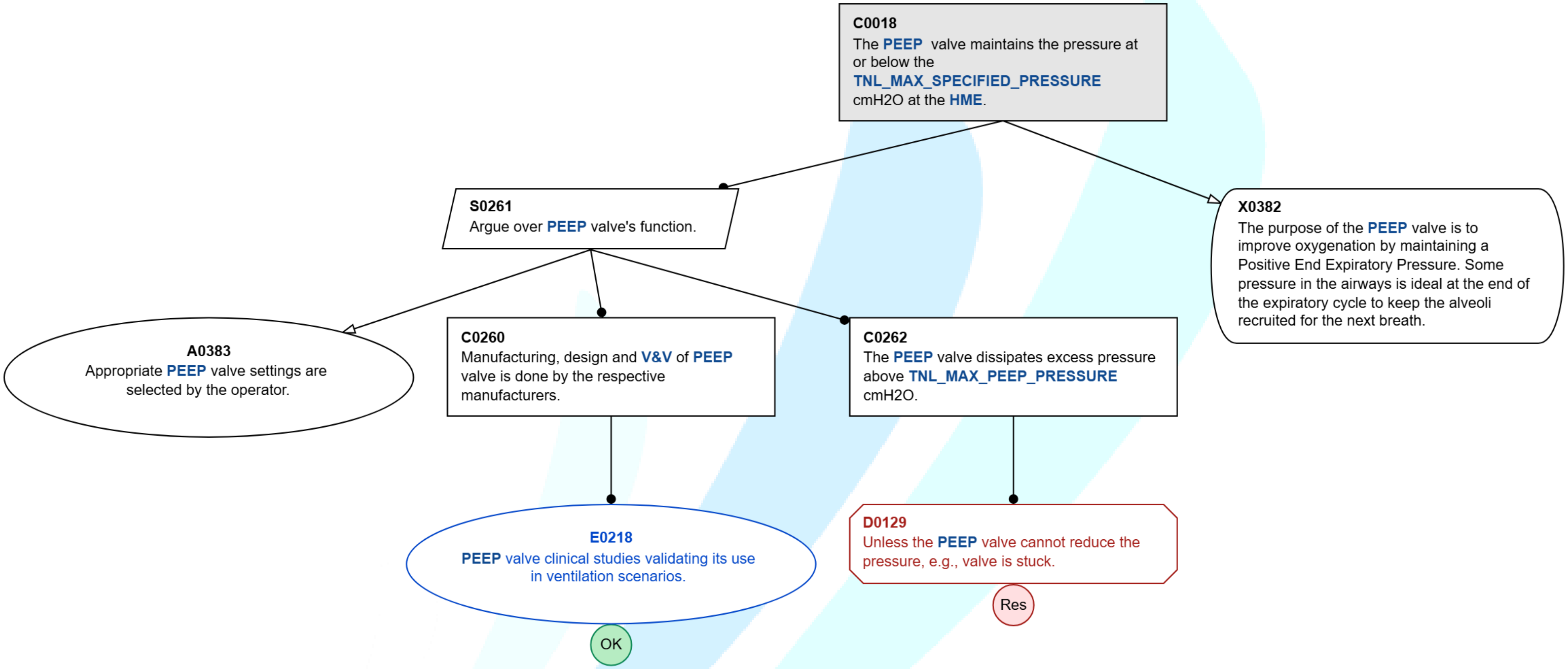


IR0363
If all states maintain pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**, then the Three-way Valve will not contribute to excess pressure in the patient's airways.

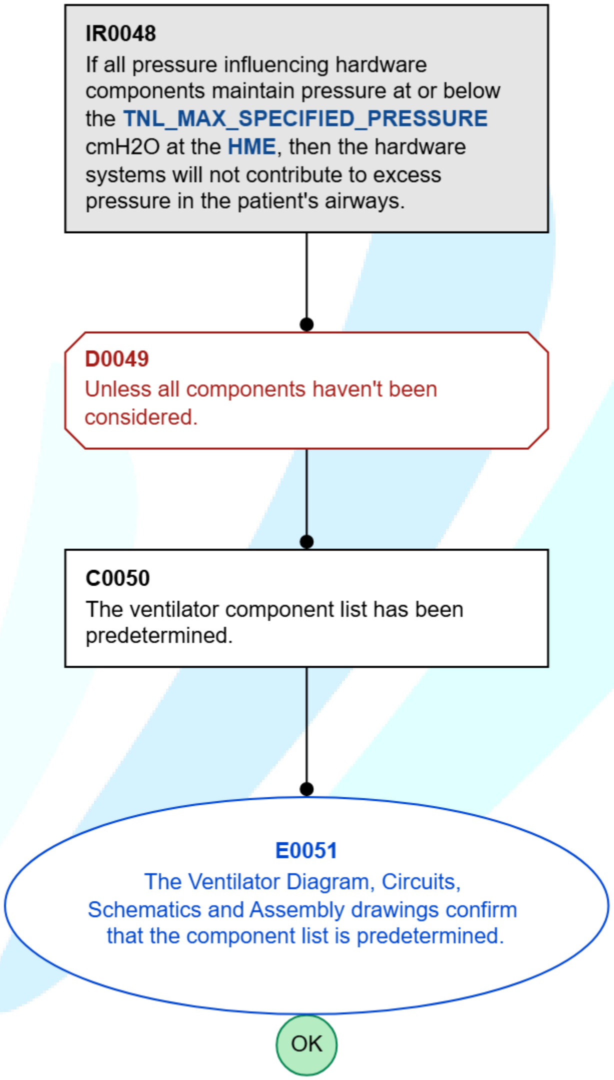
D0364
Unless all states haven't been discovered.

E0426
All states of the Three-way Valve have been discovered and documented. Further brainstorming sessions considered all positions possible from an operational standpoint.

C0018 - The PEEP valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0004	**Descendant subtree(s)**	None
Glossary Terms	PEEP, TNL_MAX_SPECIFIED_PRESSURE, HME, V&V, TNL_MAX_PEEP_PRESSURE		


C0018
The PEEP valve maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.
S0261
Argue over PEEP valve's function.
X0382
The purpose of the PEEP valve is to improve oxygenation by maintaining a Positive End Expiratory Pressure. Some pressure in the airways is ideal at the end of the expiratory cycle to keep the alveoli recruited for the next breath.
A0383
Appropriate PEEP valve settings are selected by the operator.
C0260
Manufacturing, design and V&V of PEEP valve is done by the respective manufacturers.
C0262
The PEEP valve dissipates excess pressure above TNL_MAX_PEEP_PRESSURE cmH2O.
E0218
PEEP valve clinical studies validating its use in ventilation scenarios.
OK
D0129
Unless the PEEP valve cannot reduce the pressure, e.g., valve is stuck.
Res

IR0048 - If all pressure influencing hardware components maintain pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME, then the hard...			
Parent subtree(s)	C0004	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



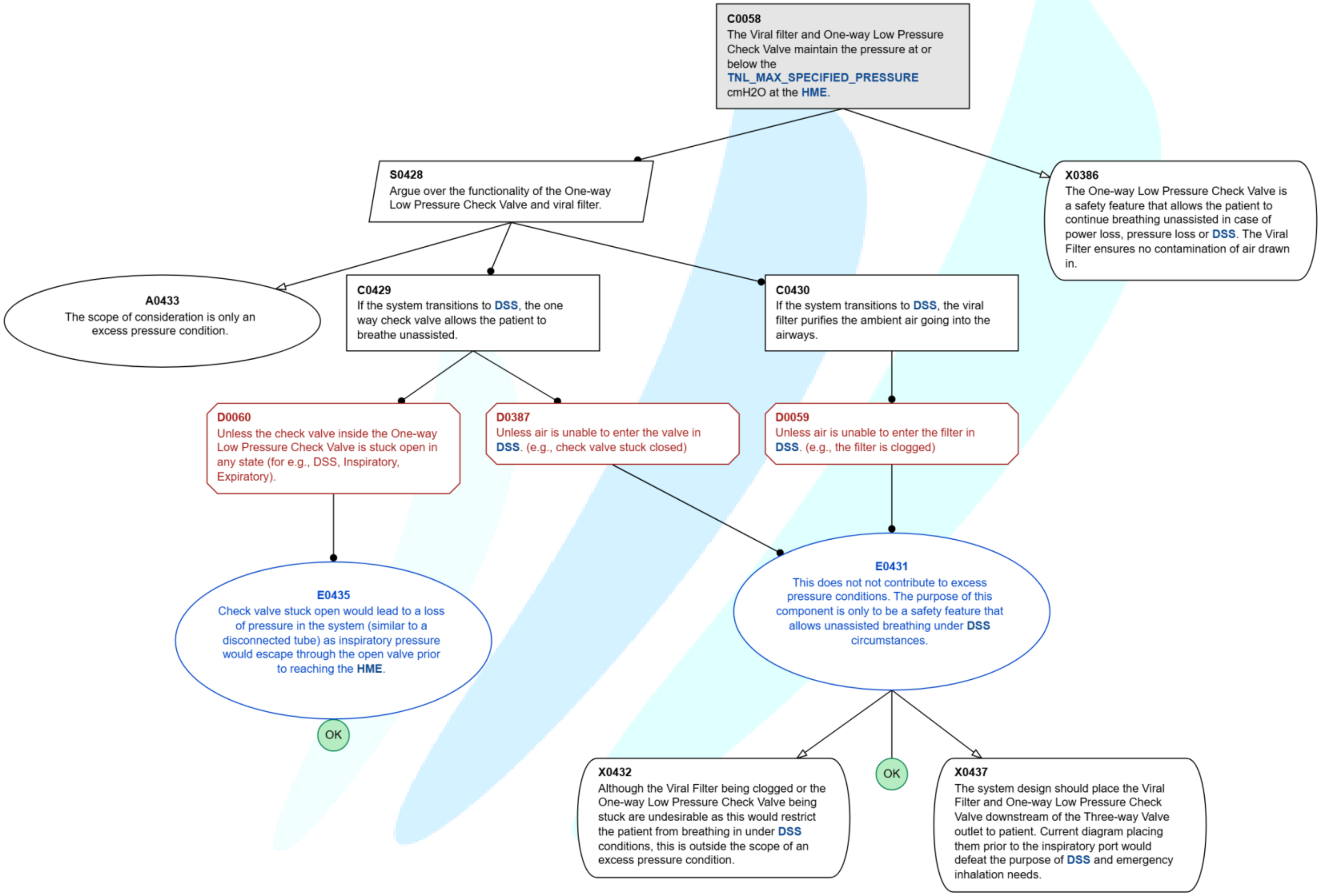
IR0048
If all pressure influencing hardware components maintain pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**, then the hardware systems will not contribute to excess pressure in the patient's airways.

D0049
Unless all components haven't been considered.

C0050
The ventilator component list has been predetermined.

E0051
The Ventilator Diagram, Circuits, Schematics and Assembly drawings confirm that the component list is predetermined.

C0058 - The Viral filter and One-way Low Pressure Check Valve maintain the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0004	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, DSS		



C0058
The Viral filter and One-way Low Pressure Check Valve maintain the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

S0428
Argue over the functionality of the One-way Low Pressure Check Valve and viral filter.

X0386
The One-way Low Pressure Check Valve is a safety feature that allows the patient to continue breathing unassisted in case of power loss, pressure loss or **DSS**. The Viral Filter ensures no contamination of air drawn in.

A0433
The scope of consideration is only an excess pressure condition.

C0429
If the system transitions to **DSS**, the one way check valve allows the patient to breathe unassisted.

C0430
If the system transitions to **DSS**, the viral filter purifies the ambient air going into the airways.

D0060
Unless the check valve inside the One-way Low Pressure Check Valve is stuck open in any state (for e.g., DSS, Inspiratory, Expiratory).

D0387
Unless air is unable to enter the valve in **DSS**. (e.g., check valve stuck closed)

D0059
Unless air is unable to enter the filter in **DSS**. (e.g., the filter is clogged)

E0435
Check valve stuck open would lead to a loss of pressure in the system (similar to a disconnected tube) as inspiratory pressure would escape through the open valve prior to reaching the **HME**.

OK

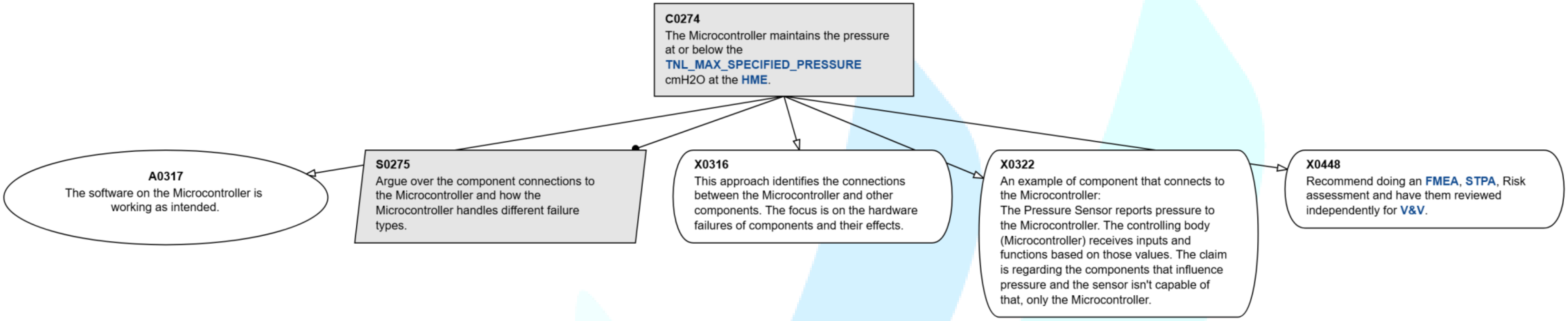
E0431
This does not not contribute to excess pressure conditions. The purpose of this component is only to be a safety feature that allows unassisted breathing under **DSS** circumstances.

OK

X0432
Although the Viral Filter being clogged or the One-way Low Pressure Check Valve being stuck are undesirable as this would restrict the patient from breathing in under **DSS** conditions, this is outside the scope of an excess pressure condition.

X0437
The system design should place the Viral Filter and One-way Low Pressure Check Valve downstream of the Three-way Valve outlet to patient. Current diagram placing them prior to the inspiratory port would defeat the purpose of **DSS** and emergency inhalation needs.

C0274 - The Microcontroller maintains the pressure at or below the TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0004	**Descendant subtree(s)**	S0275
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, PEEP, FMEA, STPA, V&V		



C0274
The Microcontroller maintains the pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

A0317
The software on the Microcontroller is working as intended.

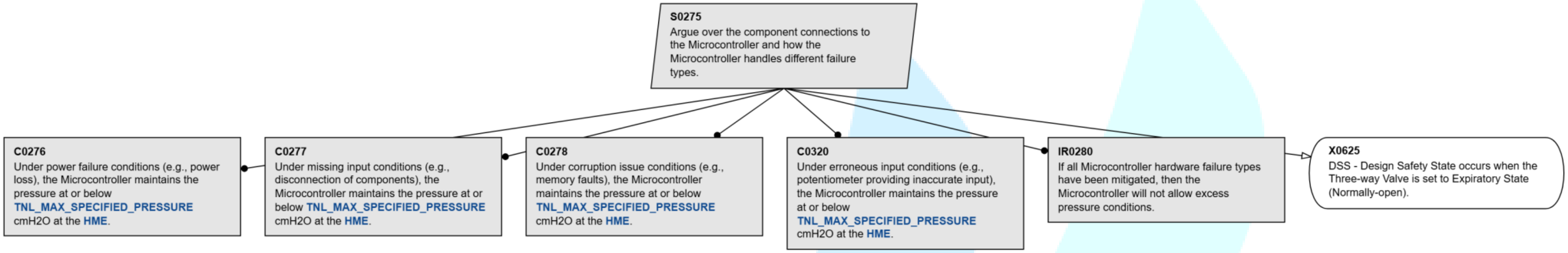
S0275
Argue over the component connections to the Microcontroller and how the Microcontroller handles different failure types.

X0316
This approach identifies the connections between the Microcontroller and other components. The focus is on the hardware failures of components and their effects.

X0322
An example of component that connects to the Microcontroller:
The Pressure Sensor reports pressure to the Microcontroller. The controlling body (Microcontroller) receives inputs and functions based on those values. The claim is regarding the components that influence pressure and the sensor isn't capable of that, only the Microcontroller.

X0448
Recommend doing an **FMEA**, **STPA**, Risk assessment and have them reviewed independently for **V&V**.

S0275 - Argue over the component connections to the Microcontroller and how the Microcontroller handles different failure types.			
Parent subtree(s)	C0274	**Descendant subtree(s)**	C0276, C0277, C0278, IR0280, C0320
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



S0275
Argue over the component connections to the Microcontroller and how the Microcontroller handles different failure types.

C0276
Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0277
Under missing input conditions (e.g., disconnection of components), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

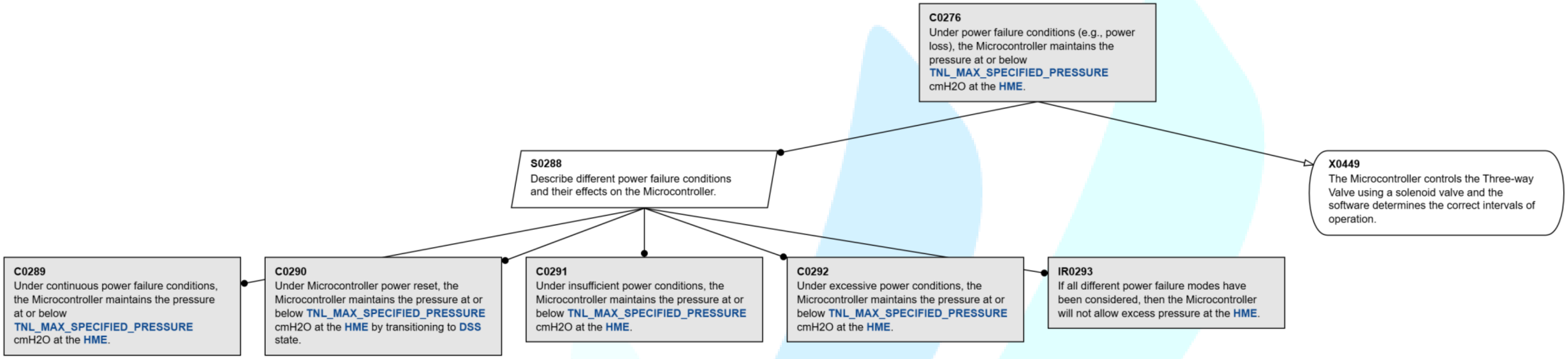
C0278
Under corruption issue conditions (e.g., memory faults), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0320
Under erroneous input conditions (e.g., potentiometer providing inaccurate input), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

IR0280
If all Microcontroller hardware failure types have been mitigated, then the Microcontroller will not allow excess pressure conditions.

X0625
DSS - Design Safety State occurs when the Three-way Valve is set to Expiratory State (Normally-open).

C0276 - Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O a...			
Parent subtree(s)	S0275, C0084	**Descendant subtree(s)**	C0289, C0290, C0291, C0292, IR0293
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, DSS		



C0276
Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

S0288
Describe different power failure conditions and their effects on the Microcontroller.

X0449
The Microcontroller controls the Three-way Valve using a solenoid valve and the software determines the correct intervals of operation.

C0289
Under continuous power failure conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

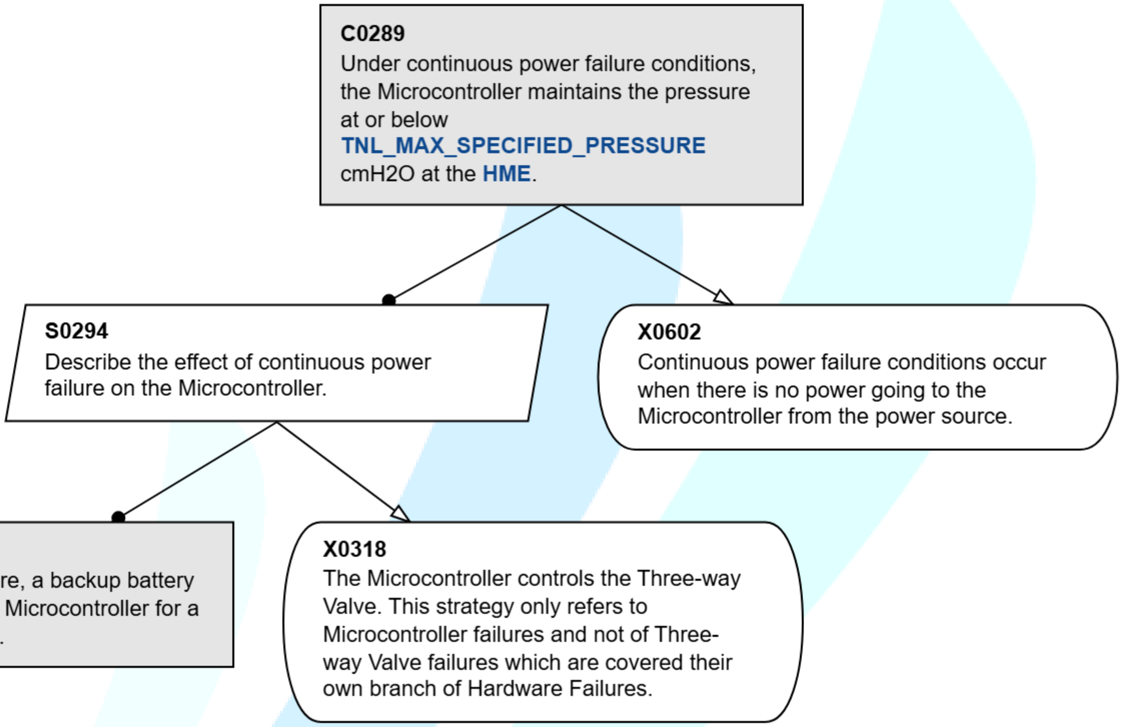
C0290
Under Microcontroller power reset, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME by transitioning to DSS state.

C0291
Under insufficient power conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0292
Under excessive power conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

IR0293
If all different power failure modes have been considered, then the Microcontroller will not allow excess pressure at the HME.

C0289 - Under continuous power failure conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HM...			
Parent subtree(s)	C0276	**Descendant subtree(s)**	C0297
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



C0289
Under continuous power failure conditions, the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

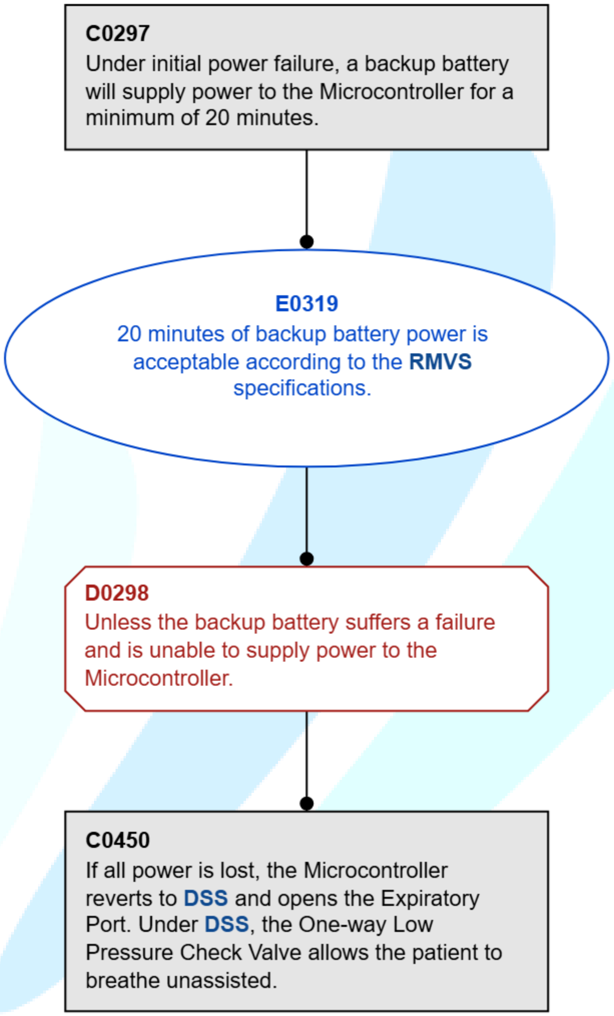
S0294
Describe the effect of continuous power failure on the Microcontroller.

X0602
Continuous power failure conditions occur when there is no power going to the Microcontroller from the power source.

C0297
Under initial power failure, a backup battery will supply power to the Microcontroller for a minimum of 20 minutes.

X0318
The Microcontroller controls the Three-way Valve. This strategy only refers to Microcontroller failures and not of Three-way Valve failures which are covered their own branch of Hardware Failures.

C0297 - Under initial power failure, a backup battery will supply power to the Microcontroller for a minimum of 20 minutes.			
Parent subtree(s)	C0289	**Descendant subtree(s)**	C0450
Glossary Terms	RMVS, DSS		



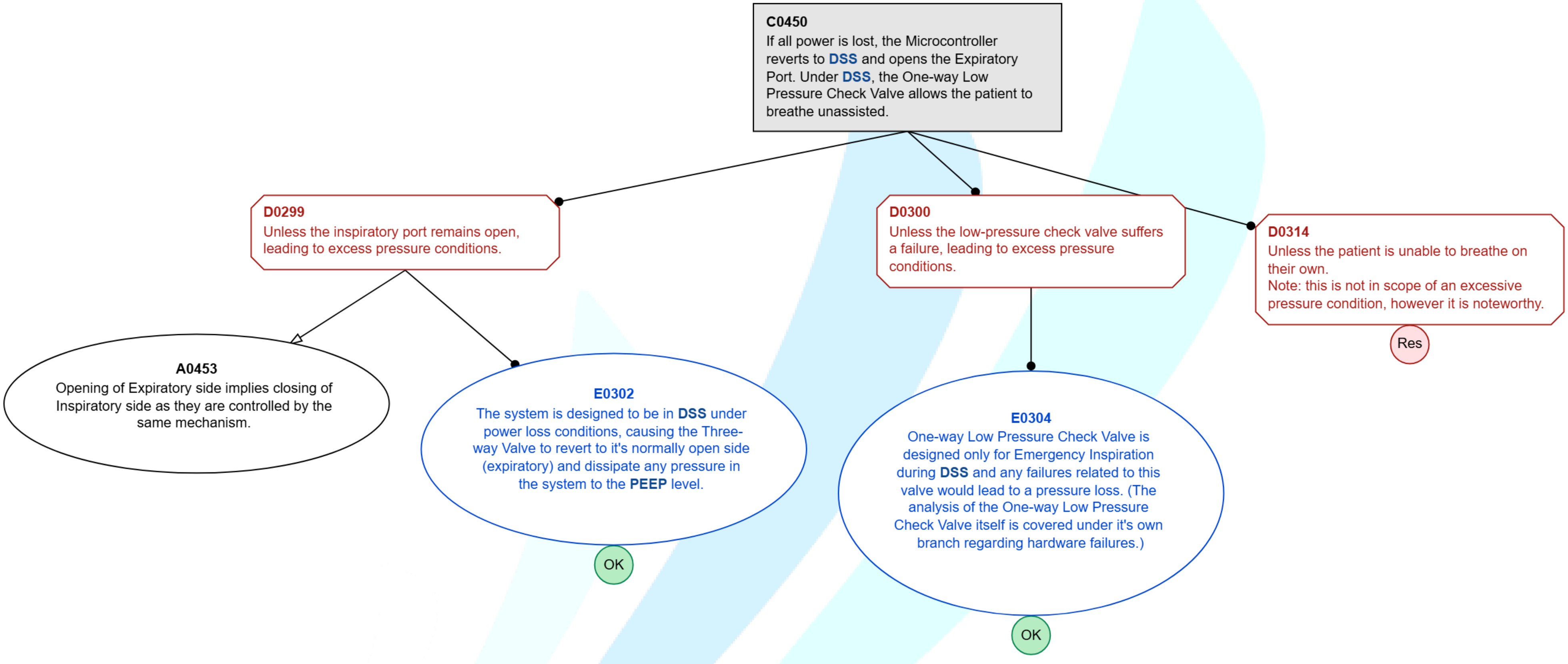
C0297
Under initial power failure, a backup battery will supply power to the Microcontroller for a minimum of 20 minutes.

E0319
20 minutes of backup battery power is acceptable according to the **RMVS** specifications.

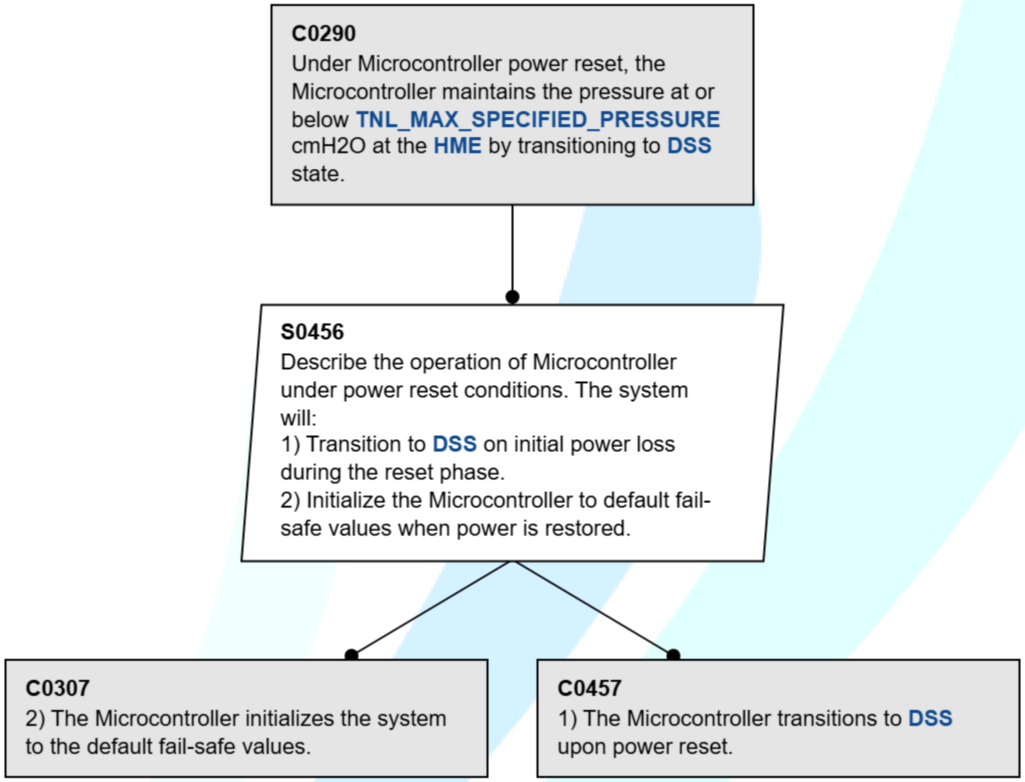
D0298
Unless the backup battery suffers a failure and is unable to supply power to the Microcontroller.

C0450
If all power is lost, the Microcontroller reverts to **DSS** and opens the Expiratory Port. Under **DSS**, the One-way Low Pressure Check Valve allows the patient to breathe unassisted.

C0450 - If all power is lost, the Microcontroller reverts to DSS and opens the Expiratory Port. Under DSS, the One-way Low Pressure Check Valve allo...			
Parent subtree(s)	C0297	**Descendant subtree(s)**	None
Glossary Terms	DSS, PEEP		


C0450
If all power is lost, the Microcontroller reverts to DSS and opens the Expiratory Port. Under DSS, the One-way Low Pressure Check Valve allows the patient to breathe unassisted.
D0299
Unless the inspiratory port remains open, leading to excess pressure conditions.
D0300
Unless the low-pressure check valve suffers a failure, leading to excess pressure conditions.
D0314
Unless the patient is unable to breathe on their own.
Note: this is not in scope of an excessive pressure condition, however it is noteworthy.
Res
A0453
Opening of Expiratory side implies closing of Inspiratory side as they are controlled by the same mechanism.
E0302
The system is designed to be in DSS under power loss conditions, causing the Three-way Valve to revert to it's normally open side (expiratory) and dissipate any pressure in the system to the PEEP level.
OK
E0304
One-way Low Pressure Check Valve is designed only for Emergency Inspiration during DSS and any failures related to this valve would lead to a pressure loss. (The analysis of the One-way Low Pressure Check Valve itself is covered under it's own branch regarding hardware failures.)
OK

C0290 - Under Microcontroller power reset, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME by tra...			
Parent subtree(s)	C0276	**Descendant subtree(s)**	C0307, C0457
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, DSS		



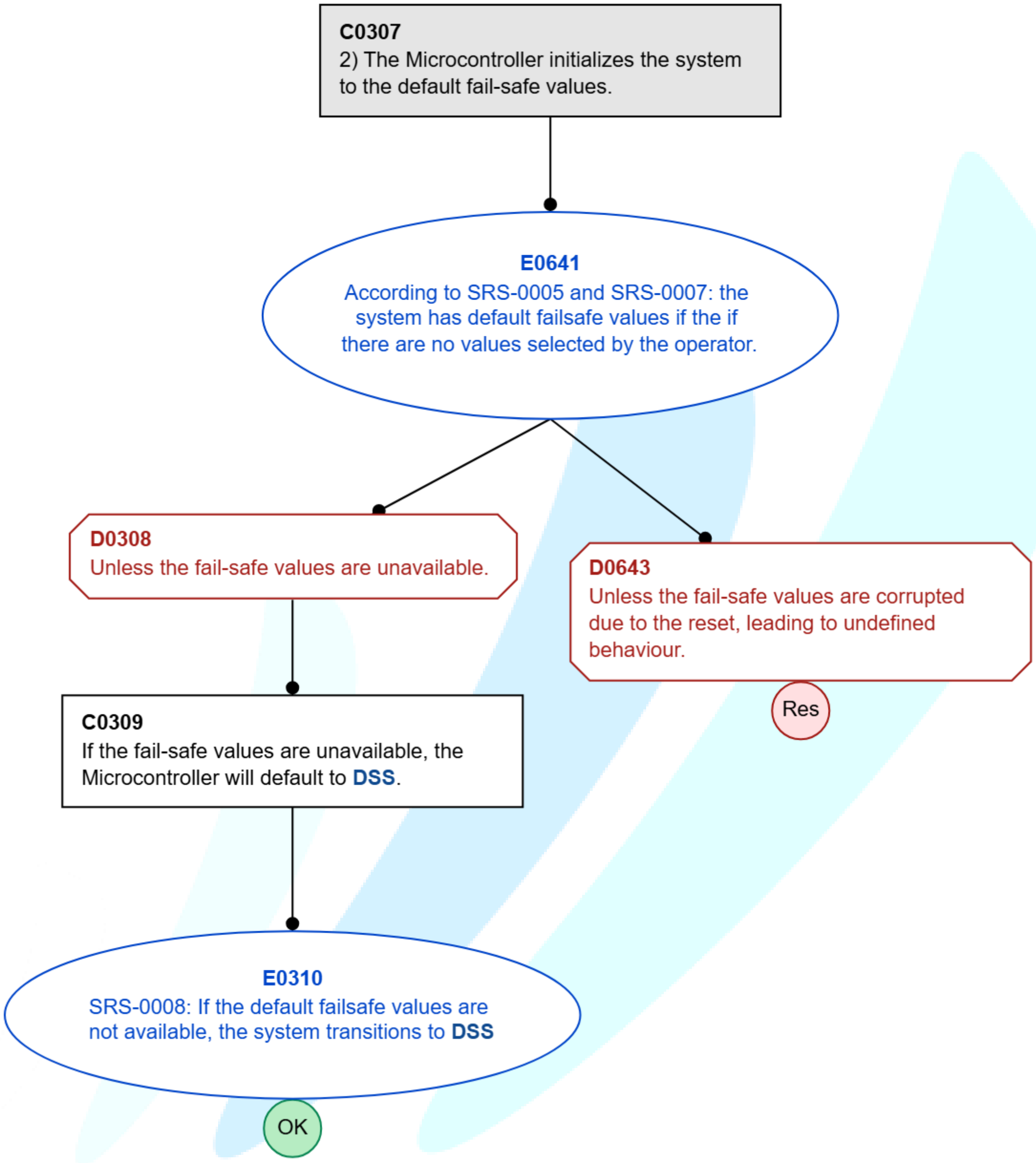
C0290
Under Microcontroller power reset, the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME** by transitioning to **DSS** state.

S0456
Describe the operation of Microcontroller under power reset conditions. The system will:
1) Transition to **DSS** on initial power loss during the reset phase.
2) Initialize the Microcontroller to default fail-safe values when power is restored.

C0307
2) The Microcontroller initializes the system to the default fail-safe values.

C0457
1) The Microcontroller transitions to **DSS** upon power reset.

C0307 - 2) The Microcontroller initializes the system to the default fail-safe values.			
Parent subtree(s)	C0290	**Descendant subtree(s)**	None
Glossary Terms	DSS		



C0307
2) The Microcontroller initializes the system to the default fail-safe values.

E0641
According to SRS-0005 and SRS-0007: the system has default failsafe values if the if there are no values selected by the operator.

D0308
Unless the fail-safe values are unavailable.

D0643
Unless the fail-safe values are corrupted due to the reset, leading to undefined behaviour.

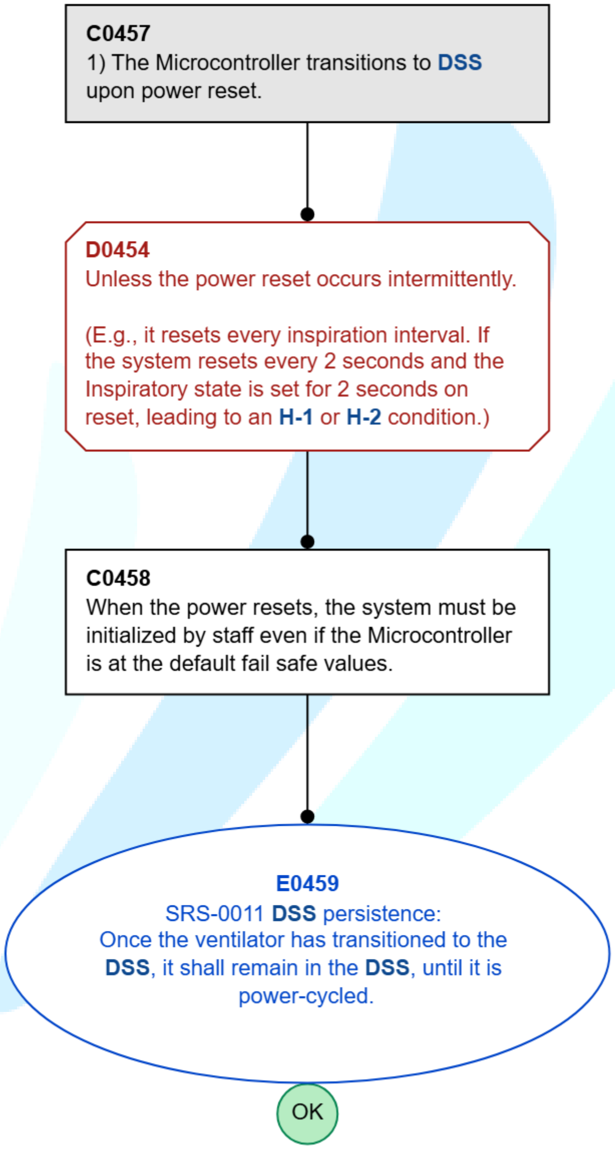
Res

C0309
If the fail-safe values are unavailable, the Microcontroller will default to **DSS**.

E0310
SRS-0008: If the default failsafe values are not available, the system transitions to **DSS**

OK

C0457 - 1) The Microcontroller transitions to DSS upon power reset.			
Parent subtree(s)	C0290	**Descendant subtree(s)**	None
Glossary Terms	H-1, H-2, DSS		



C0457
1) The Microcontroller transitions to **DSS** upon power reset.

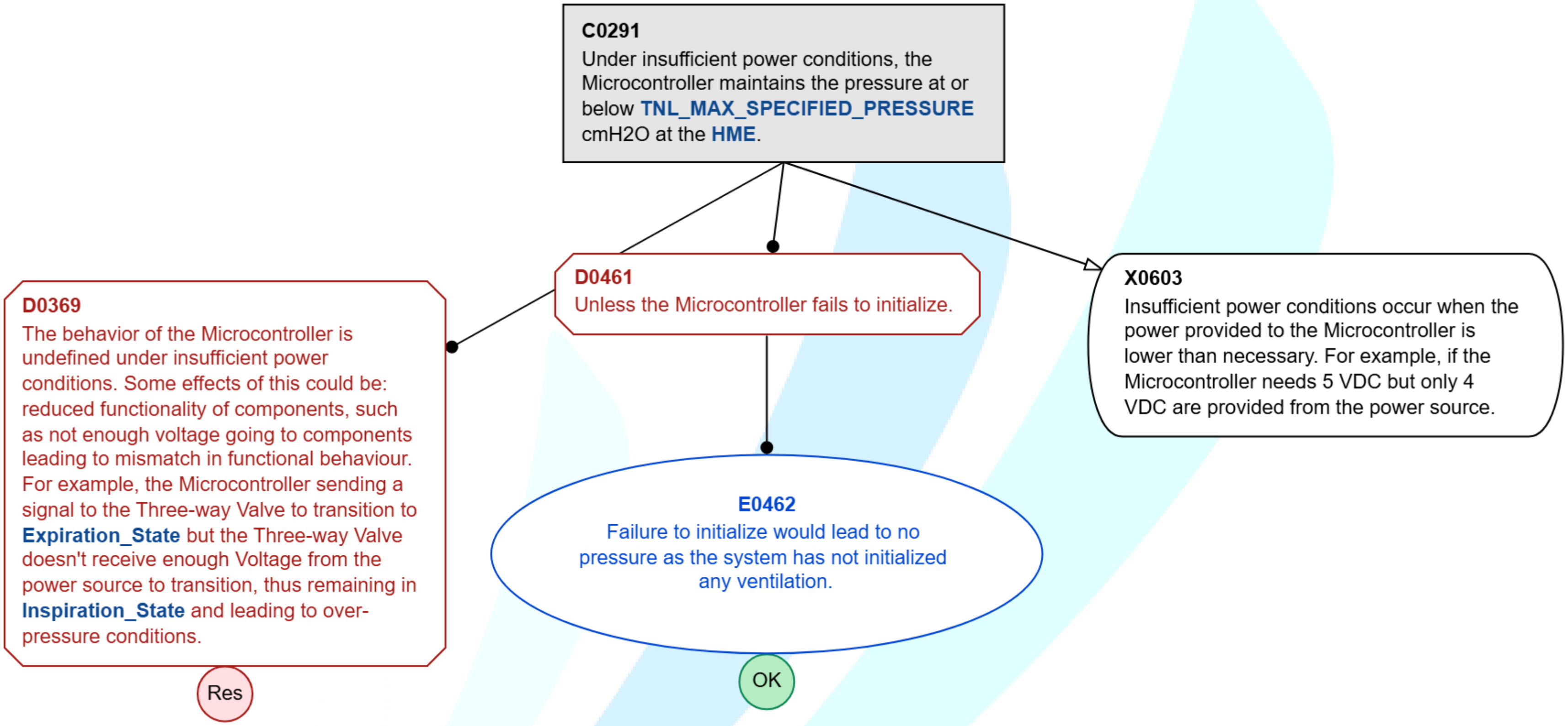
D0454
Unless the power reset occurs intermittently.

(E.g., it resets every inspiration interval. If the system resets every 2 seconds and the Inspiratory state is set for 2 seconds on reset, leading to an **H-1** or **H-2** condition.)

C0458
When the power resets, the system must be initialized by staff even if the Microcontroller is at the default fail safe values.

E0459
SRS-0011 **DSS** persistence:
Once the ventilator has transitioned to the **DSS**, it shall remain in the **DSS**, until it is power-cycled.

C0291 - Under insufficient power conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0276	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, Expiration_State, Inspiration_State		



C0291
Under insufficient power conditions, the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

D0369
The behavior of the Microcontroller is undefined under insufficient power conditions. Some effects of this could be: reduced functionality of components, such as not enough voltage going to components leading to mismatch in functional behaviour. For example, the Microcontroller sending a signal to the Three-way Valve to transition to **Expiration_State** but the Three-way Valve doesn't receive enough Voltage from the power source to transition, thus remaining in **Inspiration_State** and leading to over-pressure conditions.

Res

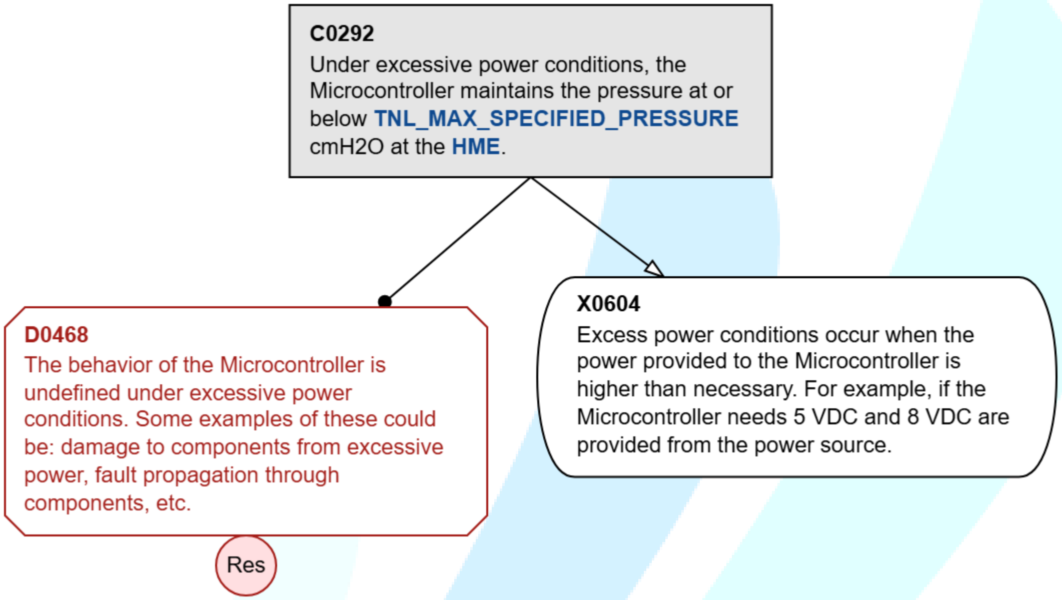
D0461
Unless the Microcontroller fails to initialize.

E0462
Failure to initialize would lead to no pressure as the system has not initialized any ventilation.

OK

X0603
Insufficient power conditions occur when the power provided to the Microcontroller is lower than necessary. For example, if the Microcontroller needs 5 VDC but only 4 VDC are provided from the power source.

C0292 - Under excessive power conditions, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0276	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		

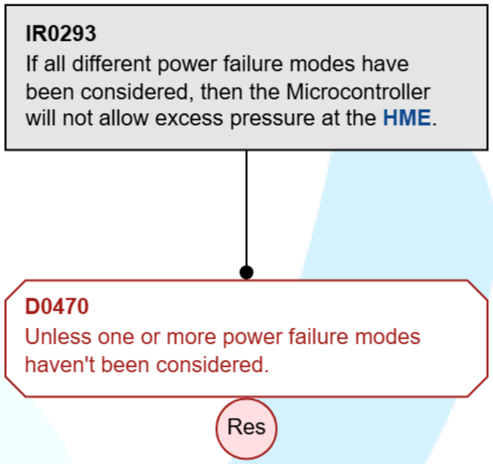


C0292
Under excessive power conditions, the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

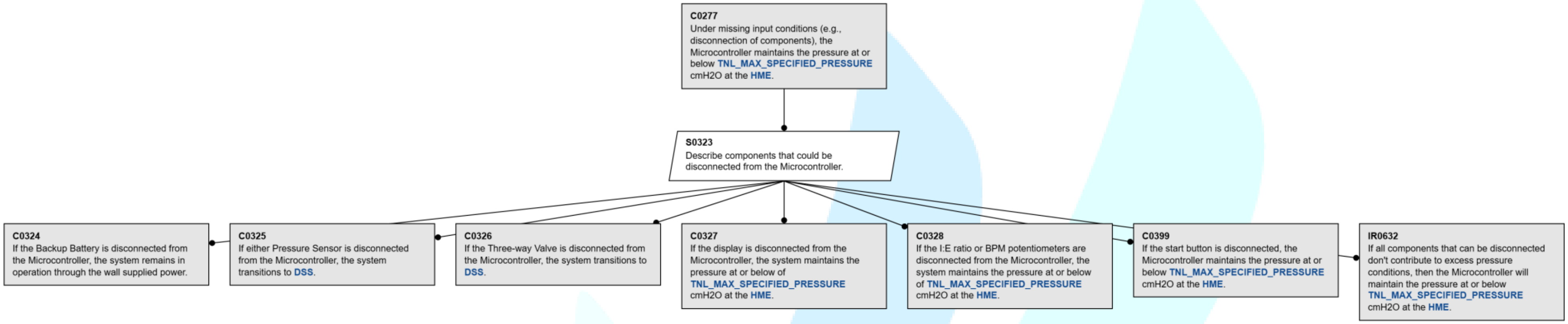
D0468
The behavior of the Microcontroller is undefined under excessive power conditions. Some examples of these could be: damage to components from excessive power, fault propagation through components, etc.

X0604
Excess power conditions occur when the power provided to the Microcontroller is higher than necessary. For example, if the Microcontroller needs 5 VDC and 8 VDC are provided from the power source.

IR0293 - If all different power failure modes have been considered, then the Microcontroller will not allow excess pressure at the HME.			
Parent subtree(s)	C0276	**Descendant subtree(s)**	None
Glossary Terms	HME		


IR0293
If all different power failure modes have been considered, then the Microcontroller will not allow excess pressure at the HME.
D0470
Unless one or more power failure modes haven't been considered.
Res

C0277 - Under missing input conditions (e.g., disconnection of components), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED...			
Parent subtree(s)	S0275	**Descendant subtree(s)**	C0324, C0325, C0326, C0327, C0328, C0399, IR0632
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, DSS		



C0277
Under missing input conditions (e.g., disconnection of components), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

S0323
Describe components that could be disconnected from the Microcontroller.

C0324
If the Backup Battery is disconnected from the Microcontroller, the system remains in operation through the wall supplied power.

C0325
If either Pressure Sensor is disconnected from the Microcontroller, the system transitions to DSS.

C0326
If the Three-way Valve is disconnected from the Microcontroller, the system transitions to DSS.

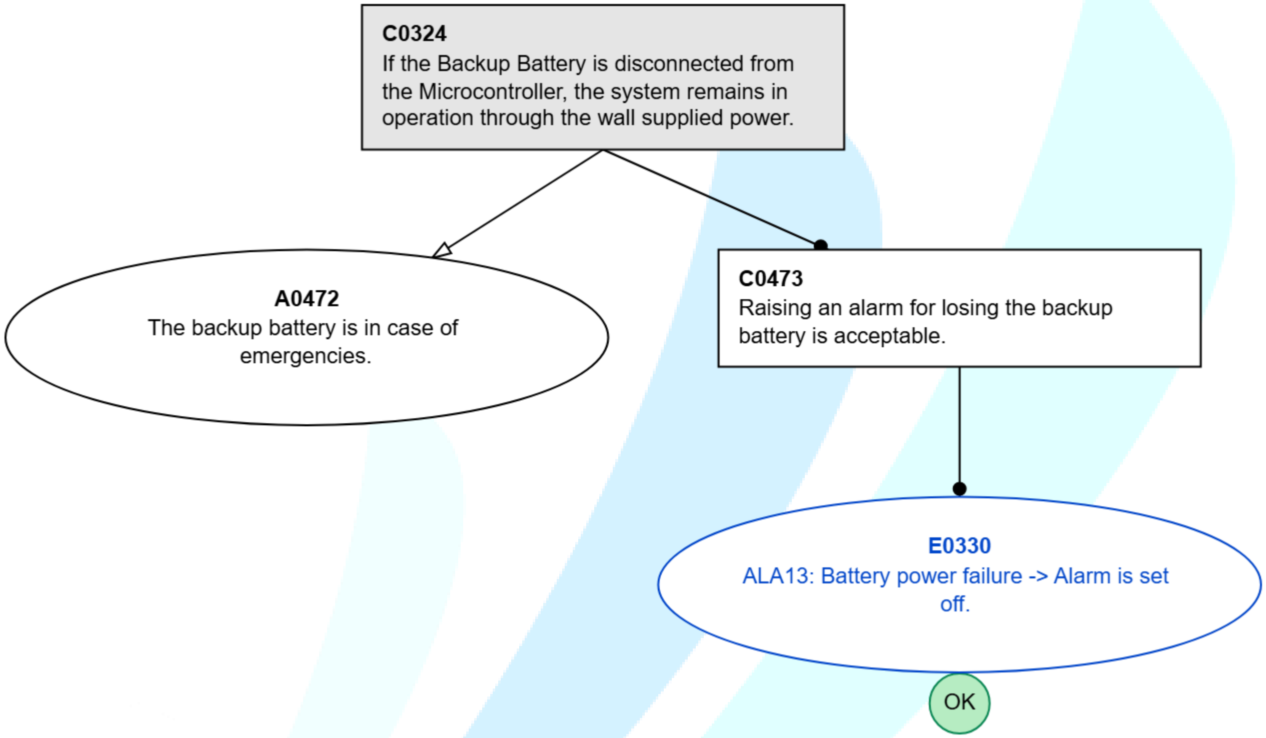
C0327
If the display is disconnected from the Microcontroller, the system maintains the pressure at or below of TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

C0328
If the I:E ratio or BPM potentiometers are disconnected from the Microcontroller, the system maintains the pressure at or below of TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

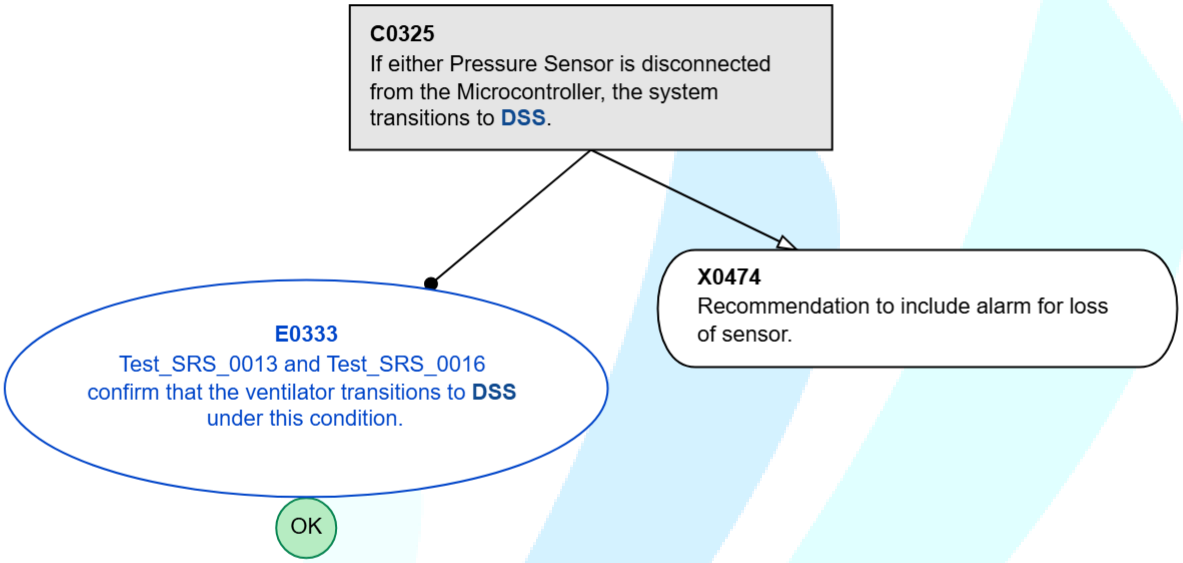
C0399
If the start button is disconnected, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

IR0632
If all components that can be disconnected don't contribute to excess pressure conditions, then the Microcontroller will maintain the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

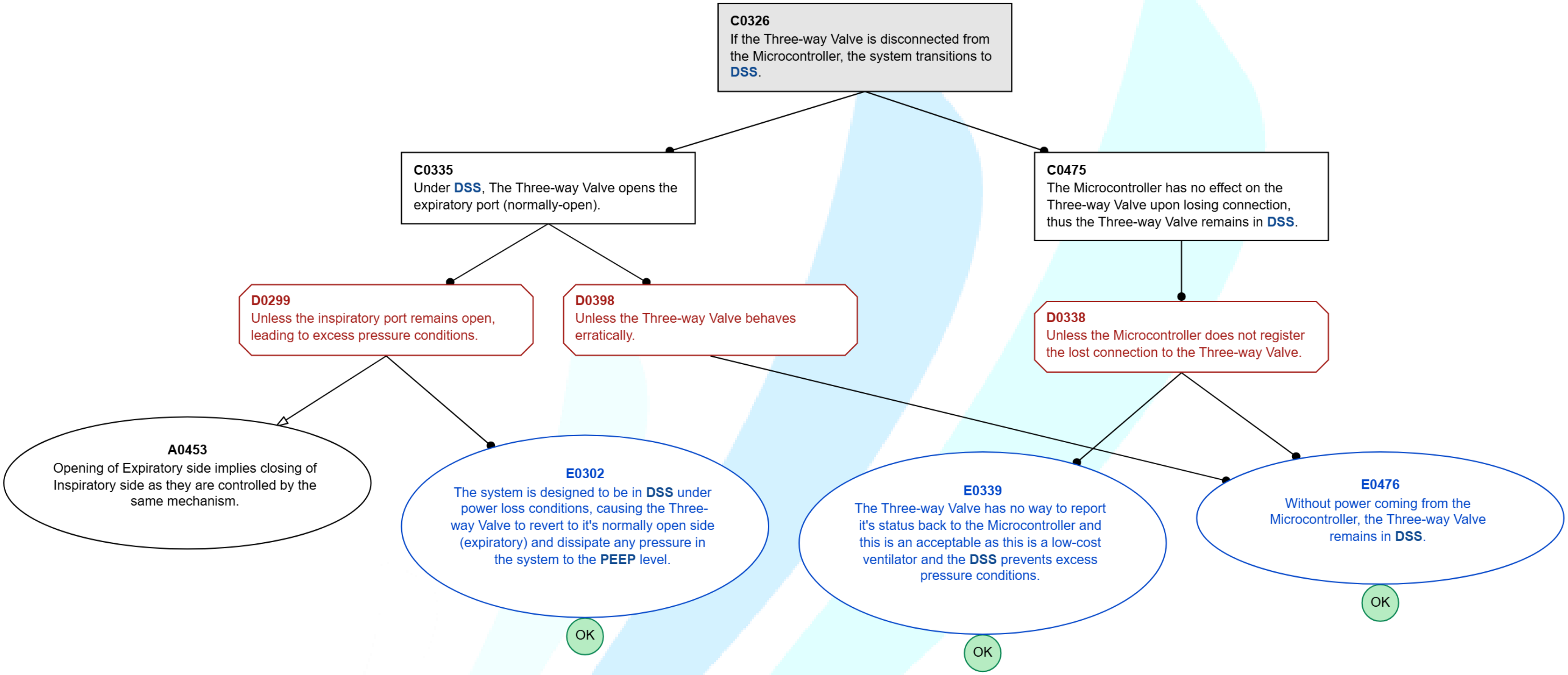
C0324 - If the Backup Battery is disconnected from the Microcontroller, the system remains in operation through the wall supplied power.			
Parent subtree(s)	C0277	**Descendant subtree(s)**	None
Glossary Terms	None		


C0324
If the Backup Battery is disconnected from the Microcontroller, the system remains in operation through the wall supplied power.
A0472
The backup battery is in case of emergencies.
C0473
Raising an alarm for losing the backup battery is acceptable.
E0330
ALA13: Battery power failure -> Alarm is set off.
OK

C0325 - If either Pressure Sensor is disconnected from the Microcontroller, the system transitions to DSS.			
Parent subtree(s)	C0277	**Descendant subtree(s)**	None
Glossary Terms	DSS		


C0325
If either Pressure Sensor is disconnected from the Microcontroller, the system transitions to DSS.
E0333
Test_SRS_0013 and Test_SRS_0016 confirm that the ventilator transitions to DSS under this condition.
OK
X0474
Recommendation to include alarm for loss of sensor.

C0326 - If the Three-way Valve is disconnected from the Microcontroller, the system transitions to DSS.			
Parent subtree(s)	C0277	**Descendant subtree(s)**	None
Glossary Terms	DSS, PEEP		



C0326
If the Three-way Valve is disconnected from the Microcontroller, the system transitions to **DSS**.

C0335
Under **DSS**, The Three-way Valve opens the expiratory port (normally-open).

C0475
The Microcontroller has no effect on the Three-way Valve upon losing connection, thus the Three-way Valve remains in **DSS**.

D0299
Unless the inspiratory port remains open, leading to excess pressure conditions.

D0398
Unless the Three-way Valve behaves erratically.

D0338
Unless the Microcontroller does not register the lost connection to the Three-way Valve.

A0453
Opening of Expiratory side implies closing of Inspiratory side as they are controlled by the same mechanism.

E0302
The system is designed to be in **DSS** under power loss conditions, causing the Three-way Valve to revert to it's normally open side (expiratory) and dissipate any pressure in the system to the **PEEP** level.

OK

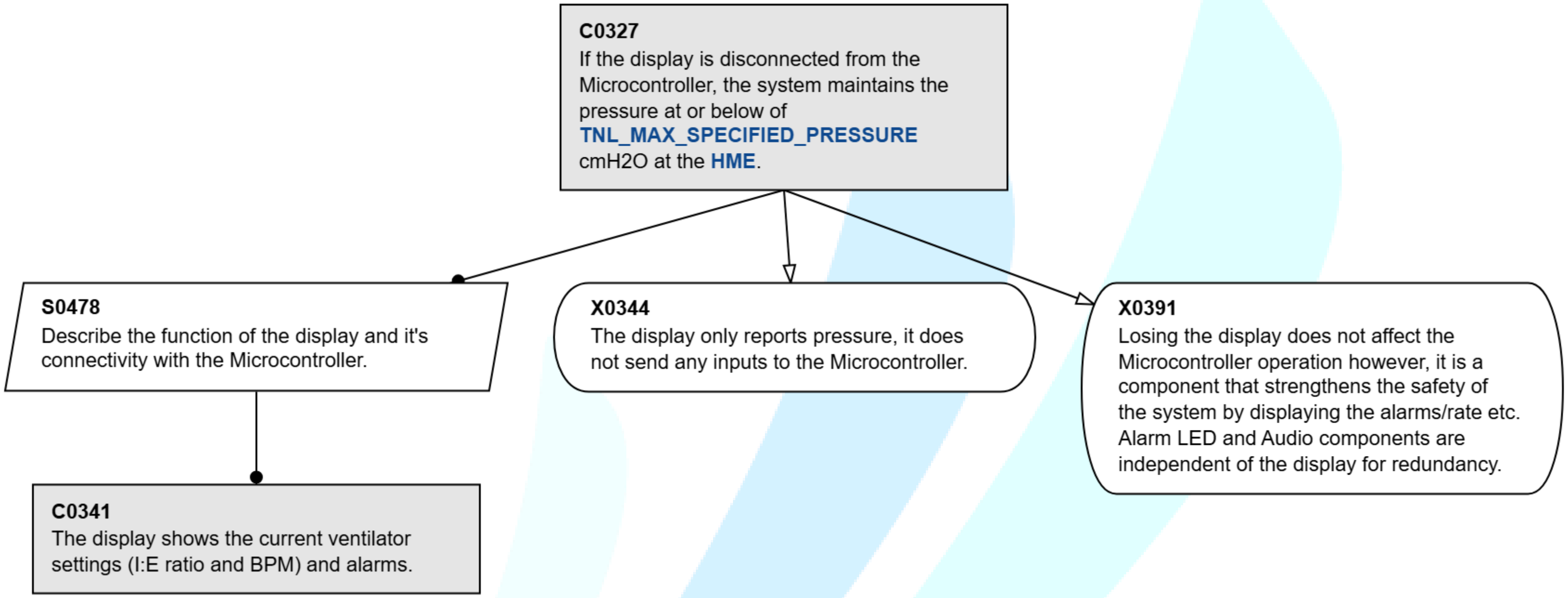
E0339
The Three-way Valve has no way to report it's status back to the Microcontroller and this is an acceptable as this is a low-cost ventilator and the **DSS** prevents excess pressure conditions.

OK

E0476
Without power coming from the Microcontroller, the Three-way Valve remains in **DSS**.

OK

C0327 - If the display is disconnected from the Microcontroller, the system maintains the pressure at or below of TNL_MAX_SPECIFIED_PRESSURE cmH2O a...			
Parent subtree(s)	C0277	**Descendant subtree(s)**	C0341
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		


C0327
If the display is disconnected from the Microcontroller, the system maintains the pressure at or below of **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

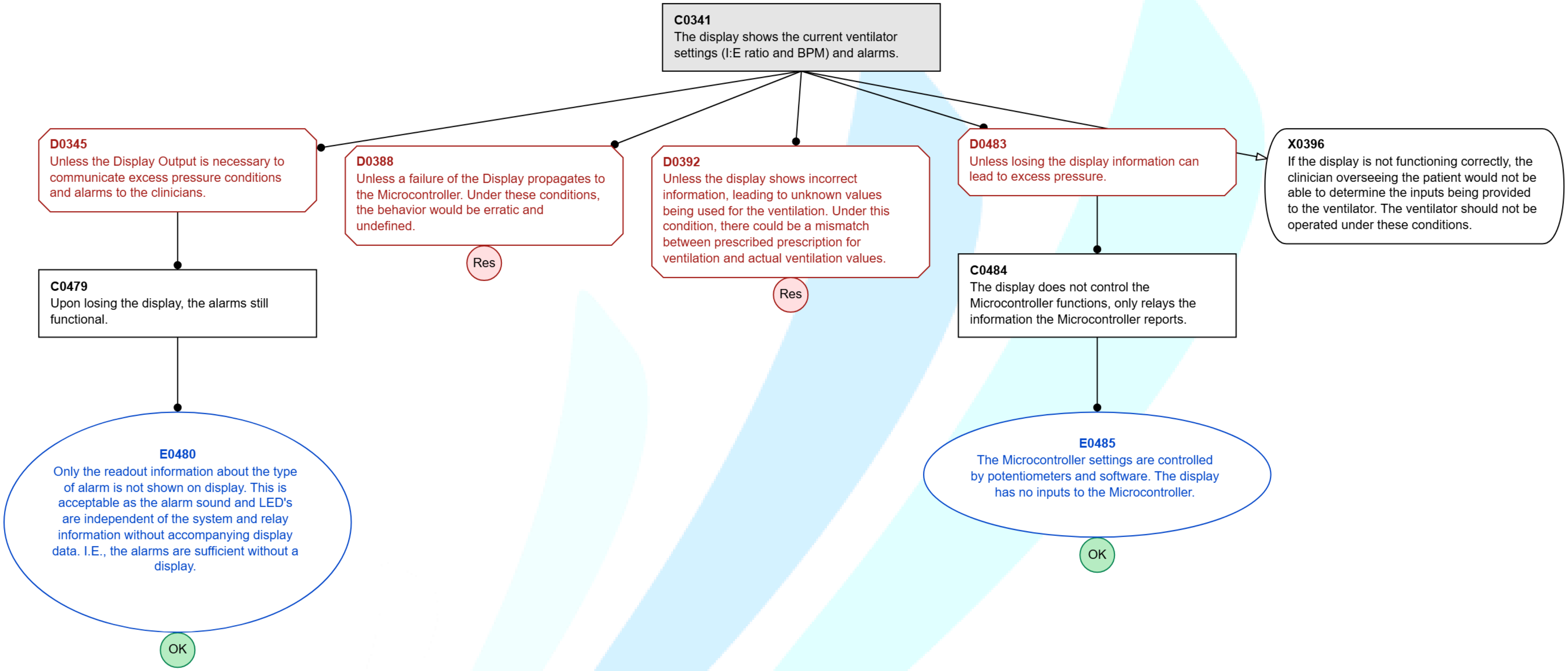
S0478
Describe the function of the display and it's connectivity with the Microcontroller.

X0344
The display only reports pressure, it does not send any inputs to the Microcontroller.

X0391
Losing the display does not affect the Microcontroller operation however, it is a component that strengthens the safety of the system by displaying the alarms/rate etc. Alarm LED and Audio components are independent of the display for redundancy.

C0341
The display shows the current ventilator settings (I:E ratio and BPM) and alarms.

C0341 - The display shows the current ventilator settings (I:E ratio and BPM) and alarms.			
Parent subtree(s)	C0327	**Descendant subtree(s)**	None
Glossary Terms	None		



C0341
The display shows the current ventilator settings (I:E ratio and BPM) and alarms.

D0345
Unless the Display Output is necessary to communicate excess pressure conditions and alarms to the clinicians.

C0479
Upon losing the display, the alarms still functional.

E0480
Only the readout information about the type of alarm is not shown on display. This is acceptable as the alarm sound and LED's are independent of the system and relay information without accompanying display data. I.E., the alarms are sufficient without a display.

OK

D0388
Unless a failure of the Display propagates to the Microcontroller. Under these conditions, the behavior would be erratic and undefined.

Res

D0392
Unless the display shows incorrect information, leading to unknown values being used for the ventilation. Under this condition, there could be a mismatch between prescribed prescription for ventilation and actual ventilation values.

Res

D0483
Unless losing the display information can lead to excess pressure.

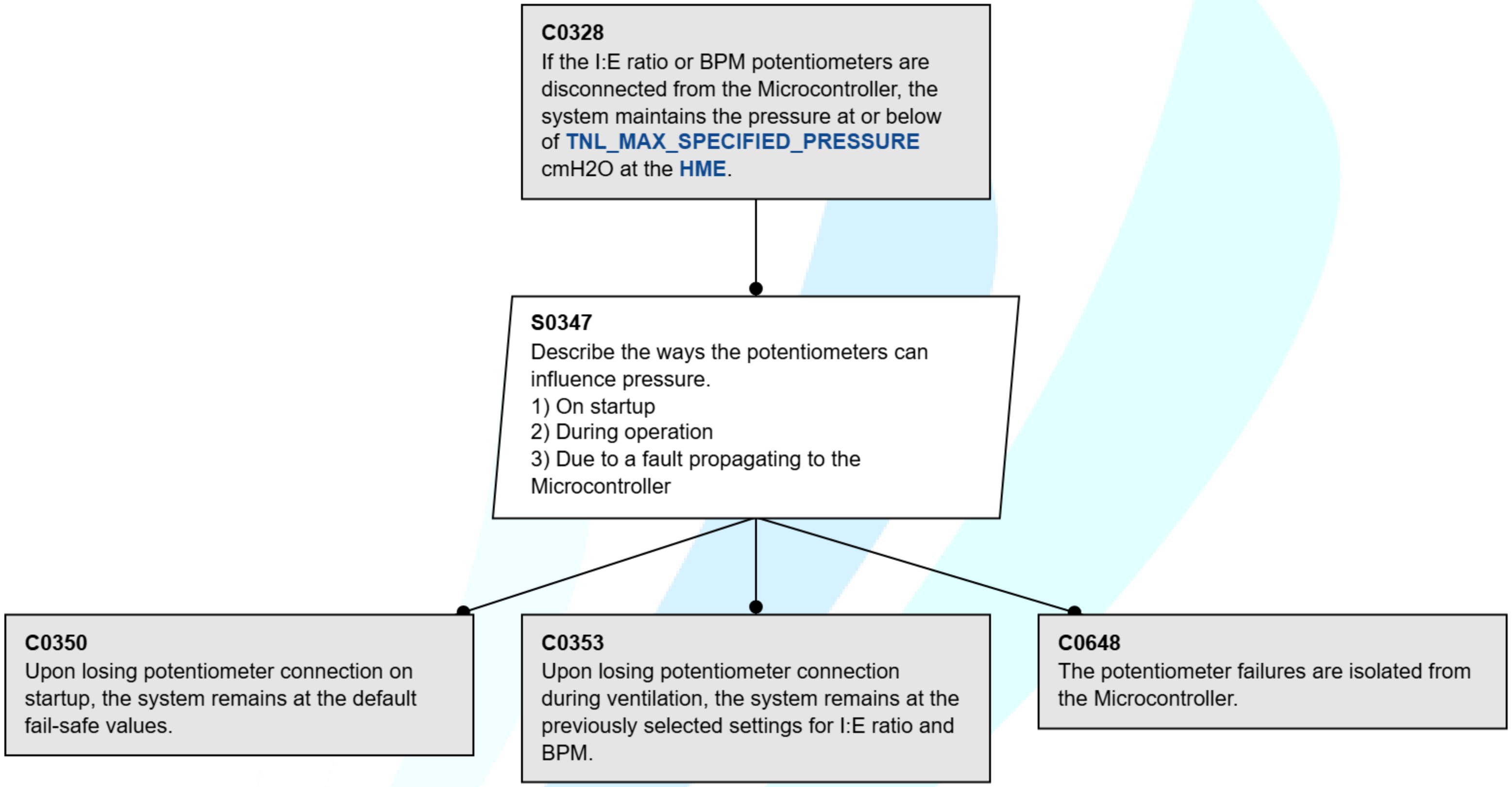
C0484
The display does not control the Microcontroller functions, only relays the information the Microcontroller reports.

E0485
The Microcontroller settings are controlled by potentiometers and software. The display has no inputs to the Microcontroller.

OK

X0396
If the display is not functioning correctly, the clinician overseeing the patient would not be able to determine the inputs being provided to the ventilator. The ventilator should not be operated under these conditions.

C0328 - If the I:E ratio or BPM potentiometers are disconnected from the Microcontroller, the system maintains the pressure at or below of TNL_MAX_S...			
Parent subtree(s)	C0277	**Descendant subtree(s)**	C0350, C0353, C0648
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



C0328
If the I:E ratio or BPM potentiometers are disconnected from the Microcontroller, the system maintains the pressure at or below of **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

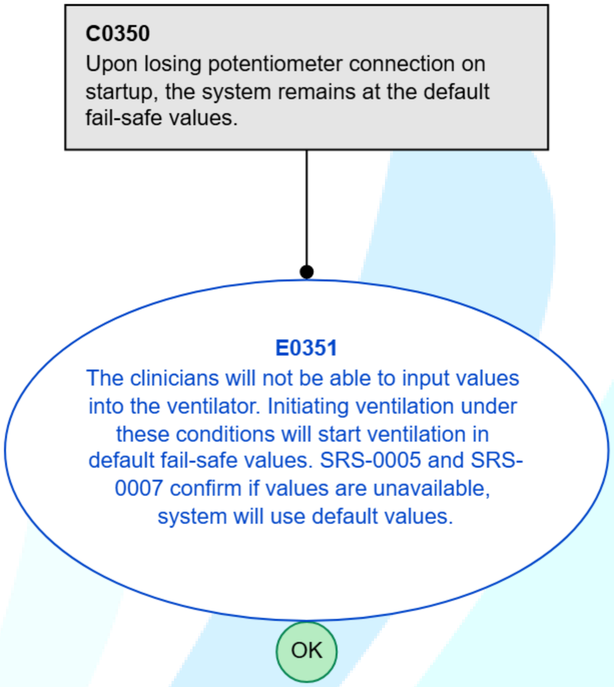
S0347
Describe the ways the potentiometers can influence pressure.
1) On startup
2) During operation
3) Due to a fault propagating to the Microcontroller

C0350
Upon losing potentiometer connection on startup, the system remains at the default fail-safe values.

C0353
Upon losing potentiometer connection during ventilation, the system remains at the previously selected settings for I:E ratio and BPM.

C0648
The potentiometer failures are isolated from the Microcontroller.

C0350 - Upon losing potentiometer connection on startup, the system remains at the default fail-safe values.			
Parent subtree(s)	C0328	**Descendant subtree(s)**	None
Glossary Terms	None		

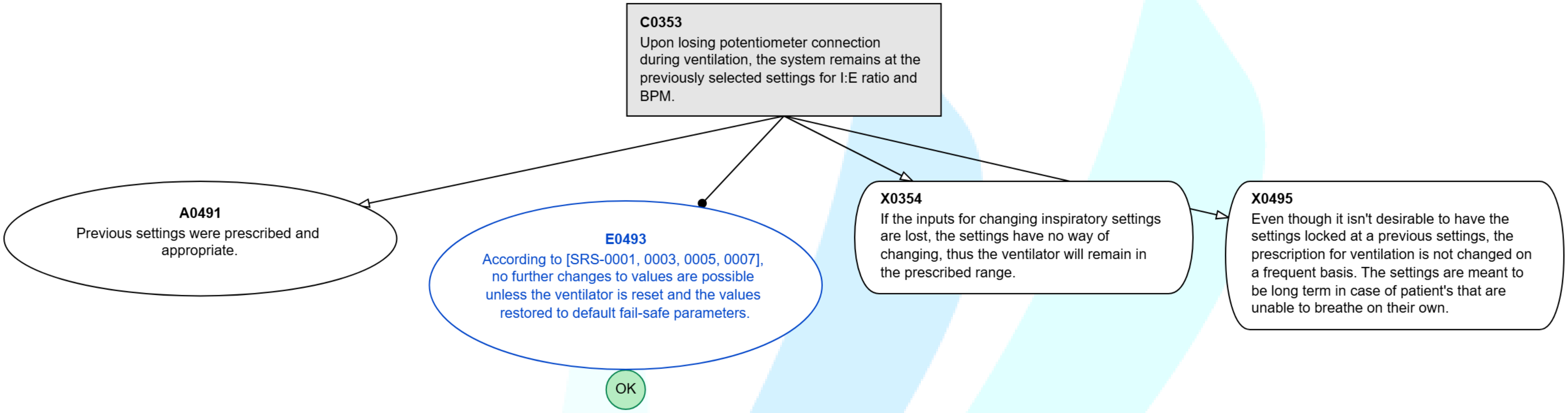


C0350
Upon losing potentiometer connection on startup, the system remains at the default fail-safe values.

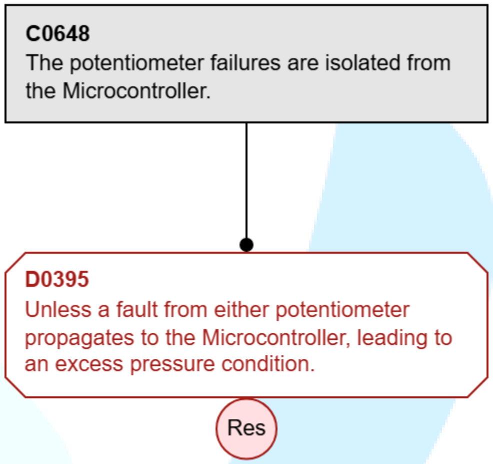
E0351
The clinicians will not be able to input values into the ventilator. Initiating ventilation under these conditions will start ventilation in default fail-safe values. SRS-0005 and SRS-0007 confirm if values are unavailable, system will use default values.

OK

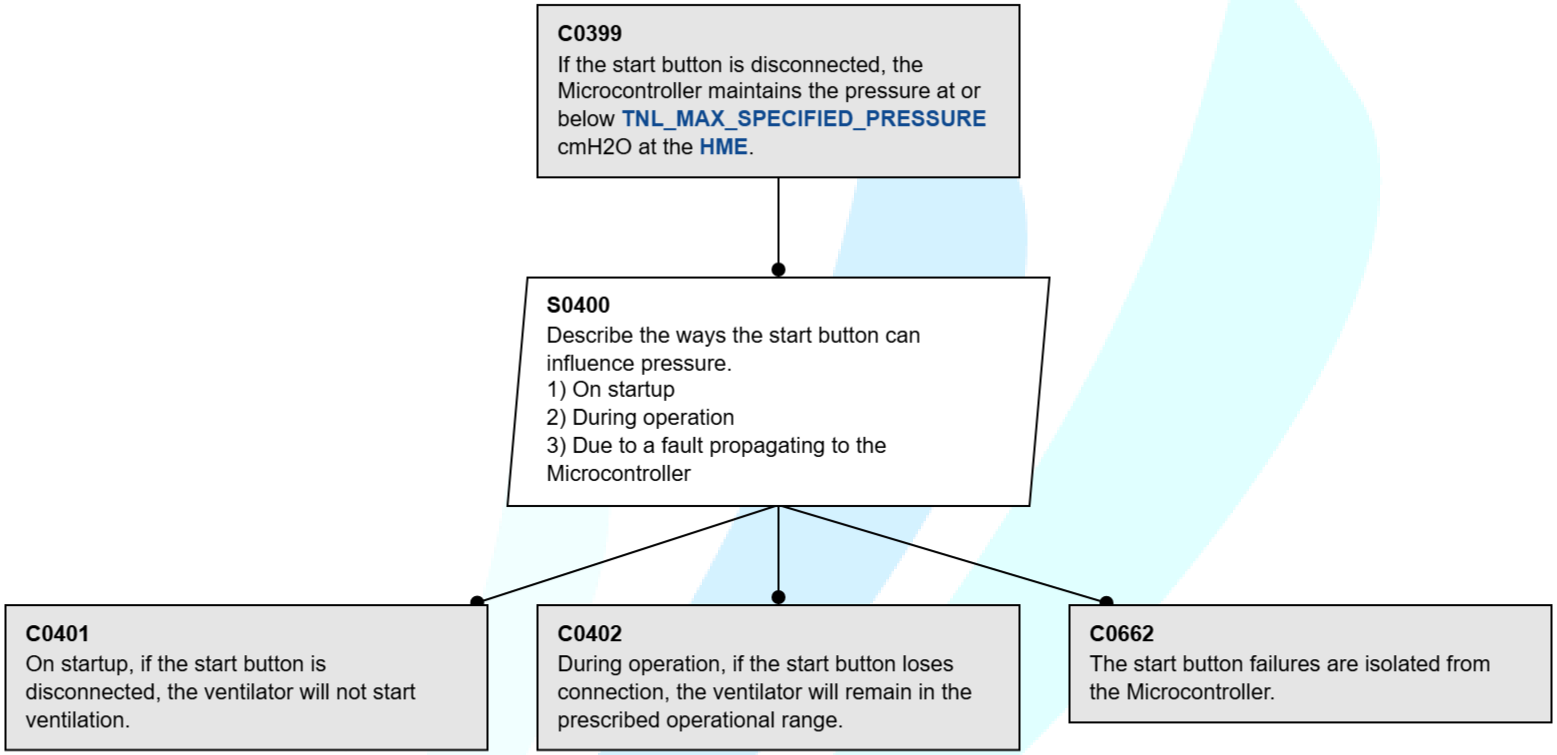
C0353 - Upon losing potentiometer connection during ventilation, the system remains at the previously selected settings for I:E ratio and BPM.			
Parent subtree(s)	C0328, C0419	**Descendant subtree(s)**	None
Glossary Terms	None		


C0353
Upon losing potentiometer connection during ventilation, the system remains at the previously selected settings for I:E ratio and BPM.
A0491
Previous settings were prescribed and appropriate.
E0493
According to [SRS-0001, 0003, 0005, 0007], no further changes to values are possible unless the ventilator is reset and the values restored to default fail-safe parameters.
OK
X0354
If the inputs for changing inspiratory settings are lost, the settings have no way of changing, thus the ventilator will remain in the prescribed range.
X0495
Even though it isn't desirable to have the settings locked at a previous settings, the prescription for ventilation is not changed on a frequent basis. The settings are meant to be long term in case of patient's that are unable to breathe on their own.

C0648 - The potentiometer failures are isolated from the Microcontroller.			
Parent subtree(s)	C0328	**Descendant subtree(s)**	None
Glossary Terms	None		


C0648
The potentiometer failures are isolated from the Microcontroller.
D0395
Unless a fault from either potentiometer propagates to the Microcontroller, leading to an excess pressure condition.
Res

C0399 - If the start button is disconnected, the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.			
Parent subtree(s)	C0277	**Descendant subtree(s)**	C0401, C0402, C0662
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



C0399
If the start button is disconnected, the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

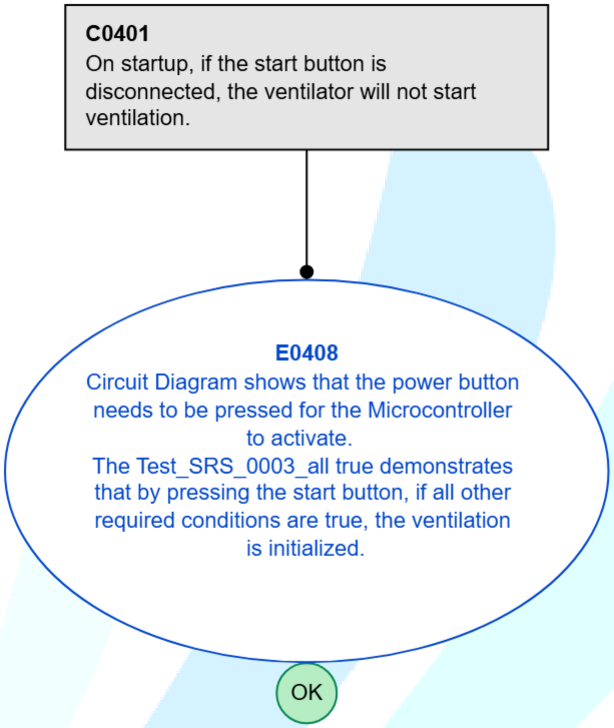
S0400
Describe the ways the start button can influence pressure.
1) On startup
2) During operation
3) Due to a fault propagating to the Microcontroller

C0401
On startup, if the start button is disconnected, the ventilator will not start ventilation.

C0402
During operation, if the start button loses connection, the ventilator will remain in the prescribed operational range.

C0662
The start button failures are isolated from the Microcontroller.

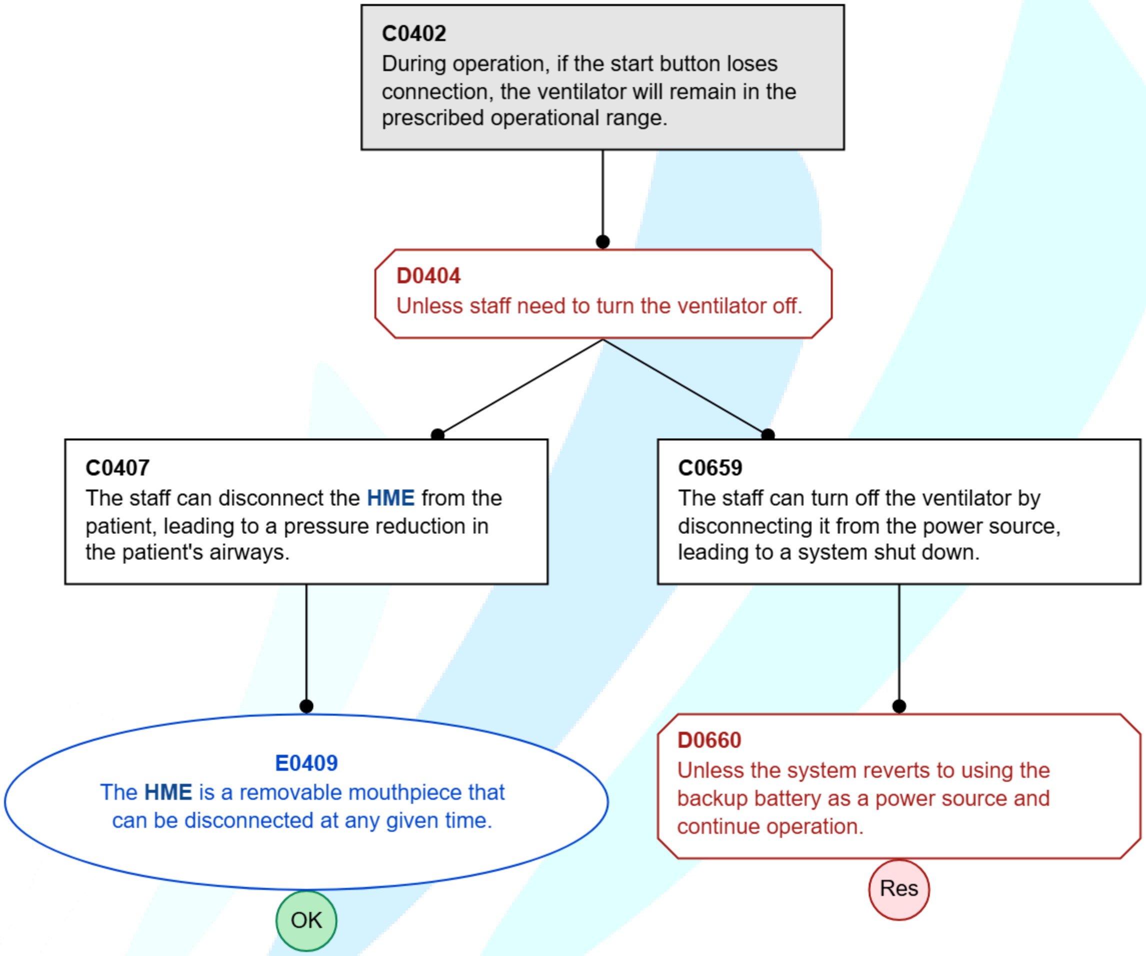
C0401 - On startup, if the start button is disconnected, the ventilator will not start ventilation.			
Parent subtree(s)	C0399	**Descendant subtree(s)**	None
Glossary Terms	None		



C0401
On startup, if the start button is disconnected, the ventilator will not start ventilation.

E0408
Circuit Diagram shows that the power button needs to be pressed for the Microcontroller to activate.
The Test_SRS_0003_all true demonstrates that by pressing the start button, if all other required conditions are true, the ventilation is initialized.

C0402 - During operation, if the start button loses connection, the ventilator will remain in the prescribed operational range.			
Parent subtree(s)	C0399	**Descendant subtree(s)**	None
Glossary Terms	HME		



C0402
During operation, if the start button loses connection, the ventilator will remain in the prescribed operational range.

D0404
Unless staff need to turn the ventilator off.

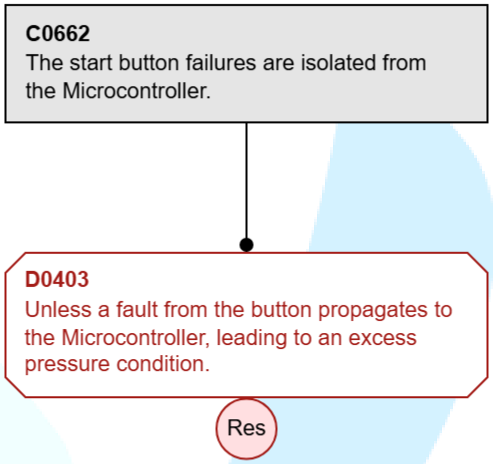
C0407
The staff can disconnect the **HME** from the patient, leading to a pressure reduction in the patient's airways.

C0659
The staff can turn off the ventilator by disconnecting it from the power source, leading to a system shut down.

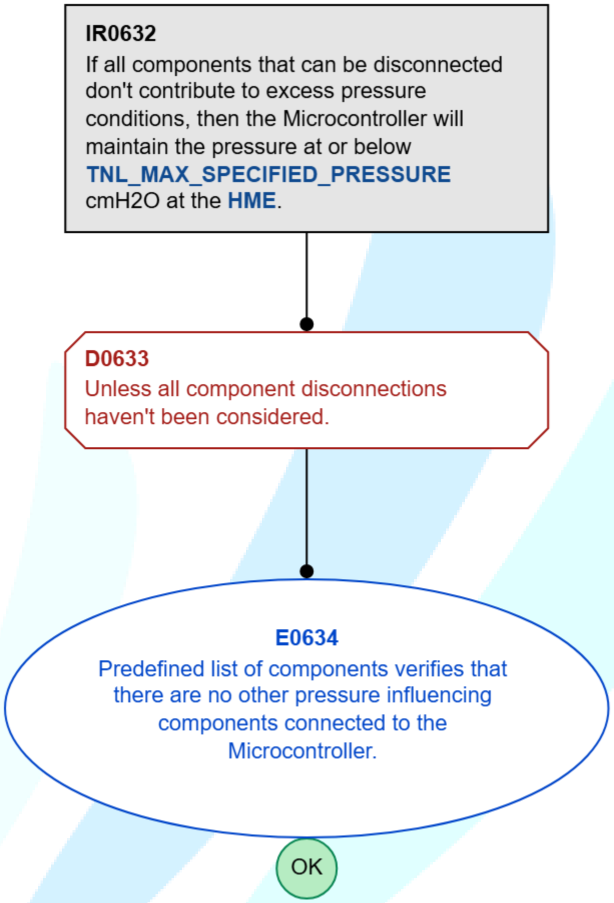
E0409
The **HME** is a removable mouthpiece that can be disconnected at any given time.

D0660
Unless the system reverts to using the backup battery as a power source and continue operation.

C0662 - The start button failures are isolated from the Microcontroller.			
Parent subtree(s)	C0399	**Descendant subtree(s)**	None
Glossary Terms	None		


C0662
The start button failures are isolated from the Microcontroller.
D0403
Unless a fault from the button propagates to the Microcontroller, leading to an excess pressure condition.
Res

IR0632 - If all components that can be disconnected don't contribute to excess pressure conditions, then the Microcontroller will maintain the pressu...			
Parent subtree(s)	C0277	**Descendant subtree(s)**	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		

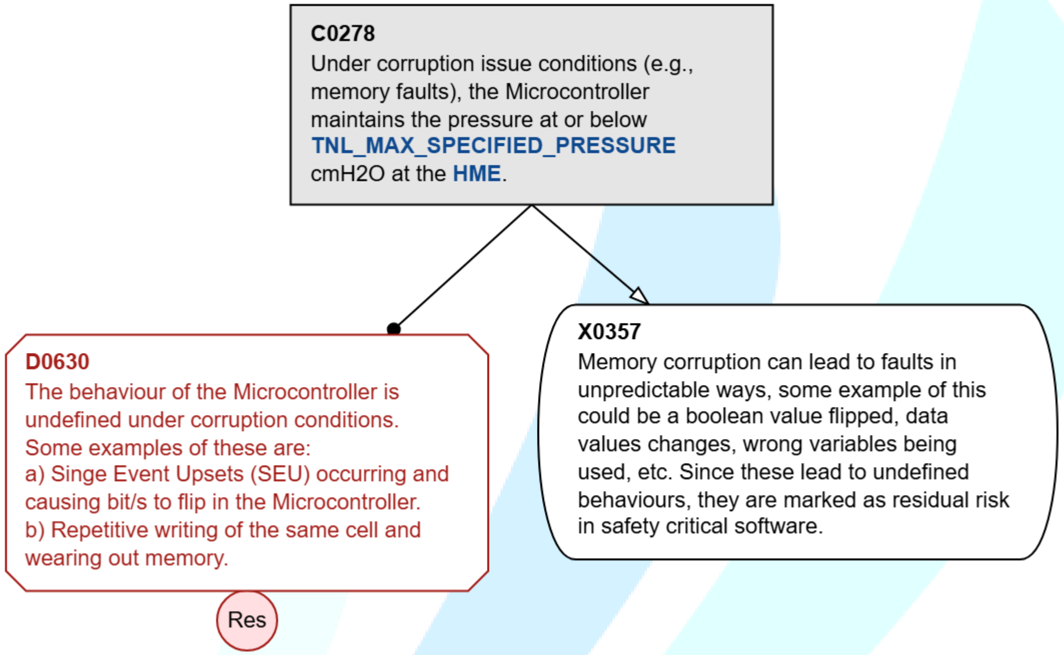


IR0632
If all components that can be disconnected don't contribute to excess pressure conditions, then the Microcontroller will maintain the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

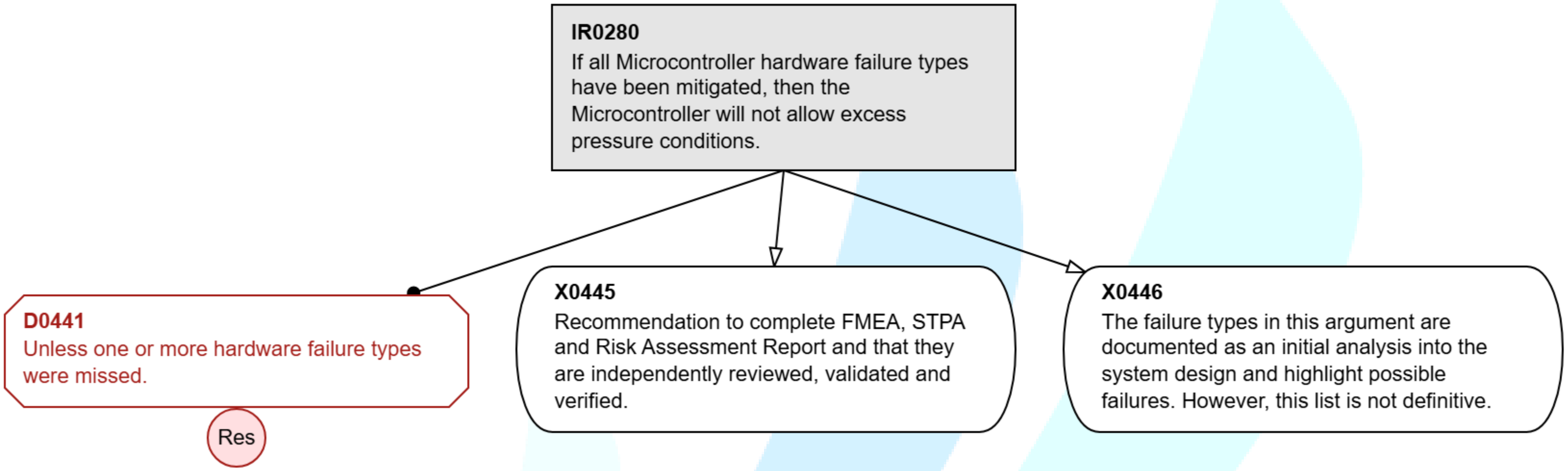
D0633
Unless all component disconnections haven't been considered.

E0634
Predefined list of components verifies that there are no other pressure influencing components connected to the Microcontroller.

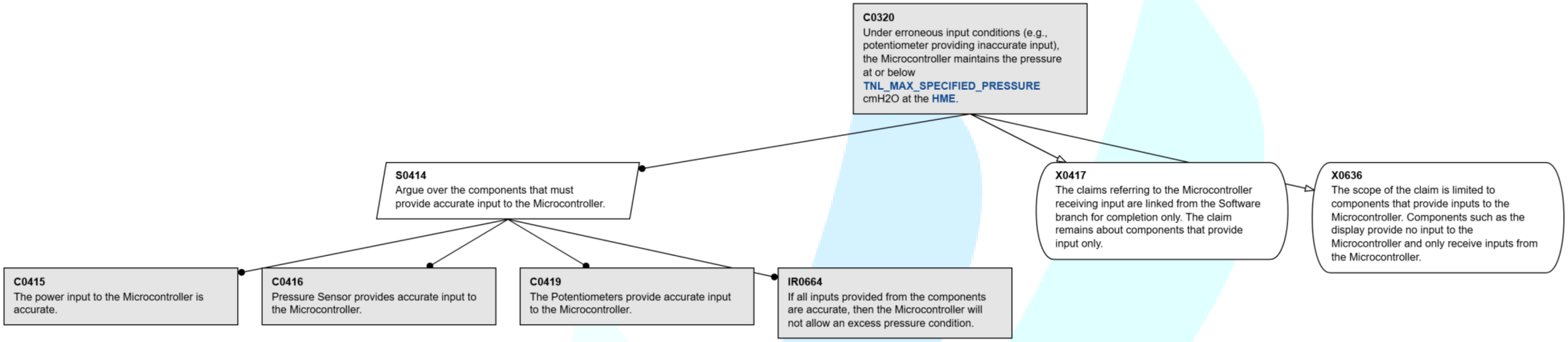
C0278 - Under corruption issue conditions (e.g., memory faults), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE c...			
Parent subtree(s)	S0275	Descendant subtree(s)	None
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		


C0278
Under corruption issue conditions (e.g., memory faults), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.
D0630
The behaviour of the Microcontroller is undefined under corruption conditions. Some examples of these are:
a) Singe Event Upsets (SEU) occurring and causing bit/s to flip in the Microcontroller.
b) Repetitive writing of the same cell and wearing out memory.
Res
X0357
Memory corruption can lead to faults in unpredictable ways, some example of this could be a boolean value flipped, data values changes, wrong variables being used, etc. Since these lead to undefined behaviours, they are marked as residual risk in safety critical software.

IR0280 - If all Microcontroller hardware failure types have been mitigated, then the Microcontroller will not allow excess pressure conditions.			
Parent subtree(s)	S0275	**Descendant subtree(s)**	None
Glossary Terms	None		


IR0280
If all Microcontroller hardware failure types have been mitigated, then the Microcontroller will not allow excess pressure conditions.
D0441
Unless one or more hardware failure types were missed.
Res
X0445
Recommendation to complete FMEA, STPA and Risk Assessment Report and that they are independently reviewed, validated and verified.
X0446
The failure types in this argument are documented as an initial analysis into the system design and highlight possible failures. However, this list is not definitive.

C0320 - Under erroneous input conditions (e.g., potentiometer providing inaccurate input), the Microcontroller maintains the pressure at or below TN...			
Parent subtree(s)	S0275	**Descendant subtree(s)**	C0415, C0416, C0419, IR0664
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME		



C0320
Under erroneous input conditions (e.g., potentiometer providing inaccurate input), the Microcontroller maintains the pressure at or below TNL_MAX_SPECIFIED_PRESSURE cmH2O at the HME.

S0414
Argue over the components that must provide accurate input to the Microcontroller.

X0417
The claims referring to the Microcontroller receiving input are linked from the Software branch for completion only. The claim remains about components that provide input only.

X0636
The scope of the claim is limited to components that provide inputs to the Microcontroller. Components such as the display provide no input to the Microcontroller and only receive inputs from the Microcontroller.

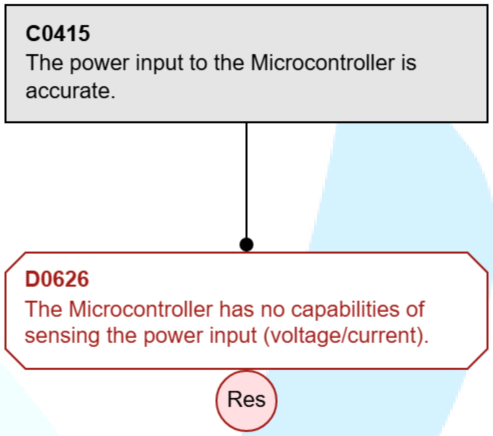
C0415
The power input to the Microcontroller is accurate.

C0416
Pressure Sensor provides accurate input to the Microcontroller.

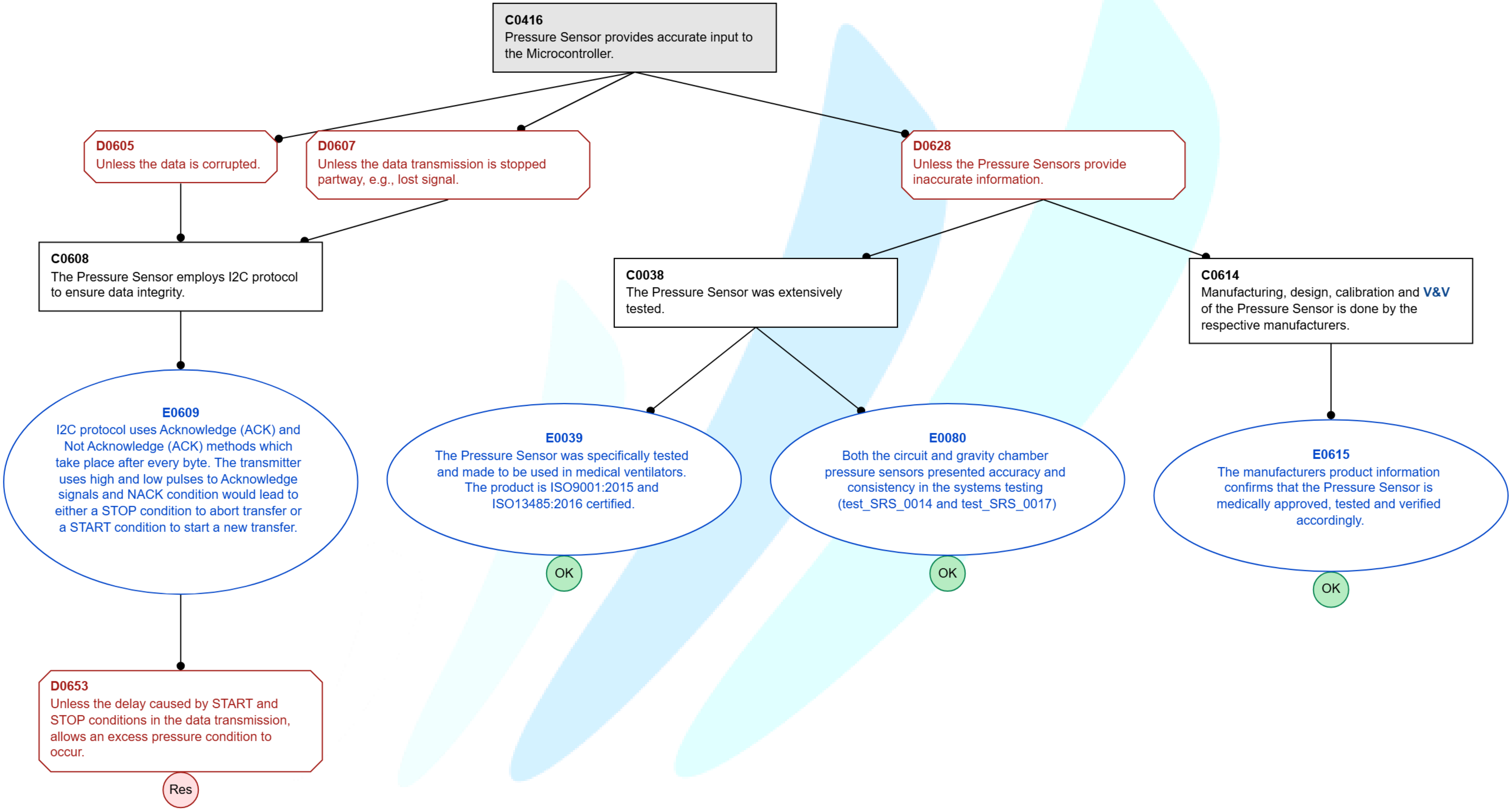
C0419
The Potentiometers provide accurate input to the Microcontroller.

IR0664
If all inputs provided from the components are accurate, then the Microcontroller will not allow an excess pressure condition.

C0415 - The power input to the Microcontroller is accurate.			
Parent subtree(s)	C0320	**Descendant subtree(s)**	None
Glossary Terms	None		


C0415
The power input to the Microcontroller is accurate.
D0626
The Microcontroller has no capabilities of sensing the power input (voltage/current).
Res

C0416 - Pressure Sensor provides accurate input to the Microcontroller.			
Parent subtree(s)	C0320, S0029	**Descendant subtree(s)**	None
Glossary Terms	V&V		



C0416
Pressure Sensor provides accurate input to the Microcontroller.

D0605
Unless the data is corrupted.

D0607
Unless the data transmission is stopped partway, e.g., lost signal.

D0628
Unless the Pressure Sensors provide inaccurate information.

C0608
The Pressure Sensor employs I2C protocol to ensure data integrity.

C0038
The Pressure Sensor was extensively tested.

C0614
Manufacturing, design, calibration and **V&V** of the Pressure Sensor is done by the respective manufacturers.

E0609
I2C protocol uses Acknowledge (ACK) and Not Acknowledge (ACK) methods which take place after every byte. The transmitter uses high and low pulses to Acknowledge signals and NACK condition would lead to either a STOP condition to abort transfer or a START condition to start a new transfer.

E0039
The Pressure Sensor was specifically tested and made to be used in medical ventilators. The product is ISO9001:2015 and ISO13485:2016 certified.

OK

E0080
Both the circuit and gravity chamber pressure sensors presented accuracy and consistency in the systems testing (test_SRS_0014 and test_SRS_0017)

OK

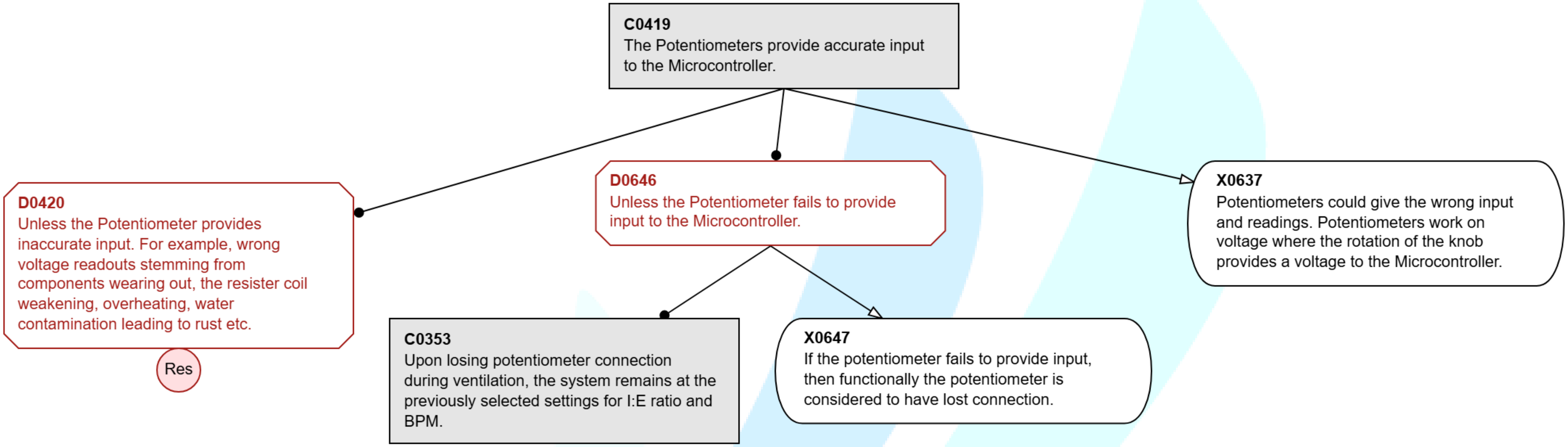
E0615
The manufacturers product information confirms that the Pressure Sensor is medically approved, tested and verified accordingly.

OK

D0653
Unless the delay caused by START and STOP conditions in the data transmission, allows an excess pressure condition to occur.

Res

C0419 - The Potentiometers provide accurate input to the Microcontroller.			
Parent subtree(s)	C0320, D0114	**Descendant subtree(s)**	C0353
Glossary Terms	None		



C0419
The Potentiometers provide accurate input to the Microcontroller.

D0420
Unless the Potentiometer provides inaccurate input. For example, wrong voltage readouts stemming from components wearing out, the resister coil weakening, overheating, water contamination leading to rust etc.

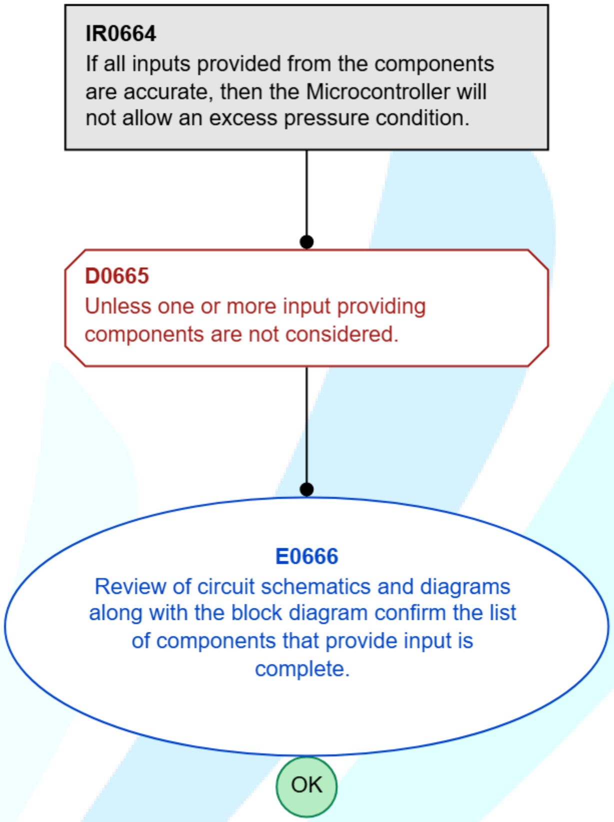
D0646
Unless the Potentiometer fails to provide input to the Microcontroller.

X0637
Potentiometers could give the wrong input and readings. Potentiometers work on voltage where the rotation of the knob provides a voltage to the Microcontroller.

C0353
Upon losing potentiometer connection during ventilation, the system remains at the previously selected settings for I:E ratio and BPM.

X0647
If the potentiometer fails to provide input, then functionally the potentiometer is considered to have lost connection.

IR0664 - If all inputs provided from the components are accurate, then the Microcontroller will not allow an excess pressure condition.			
Parent subtree(s)	C0320	**Descendant subtree(s)**	None
Glossary Terms	None		

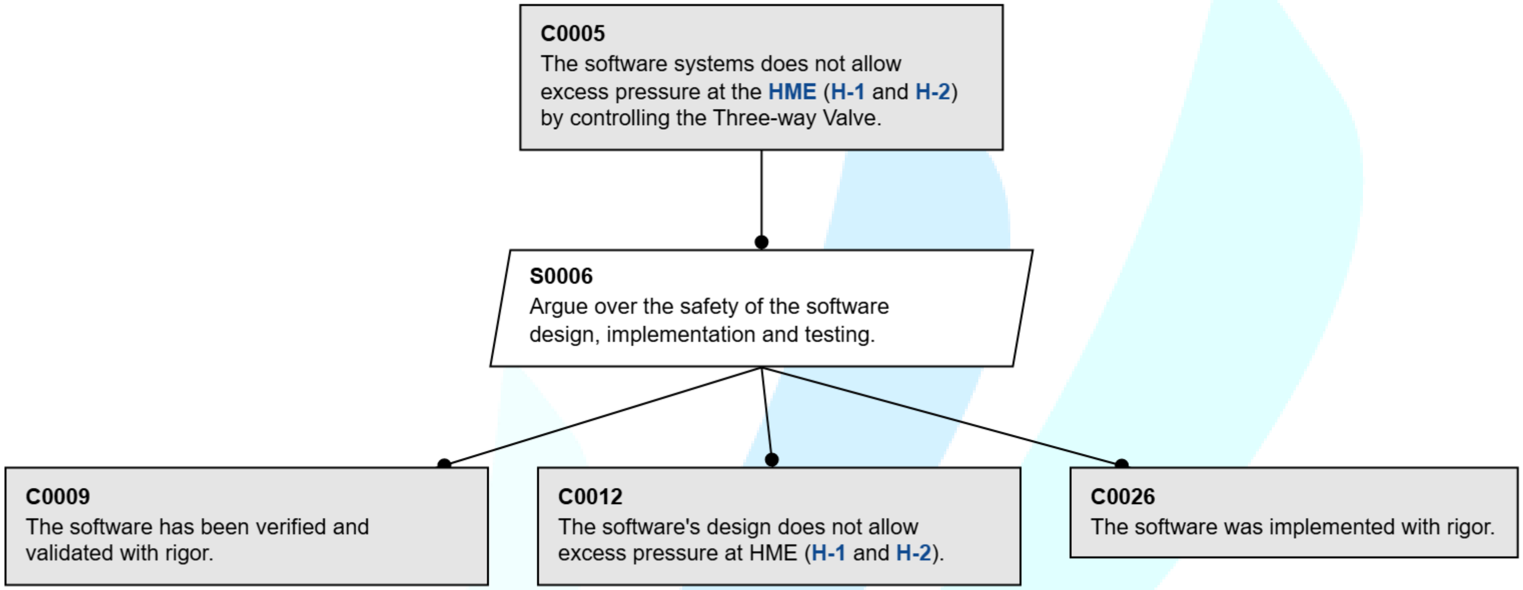


IR0664
If all inputs provided from the components are accurate, then the Microcontroller will not allow an excess pressure condition.

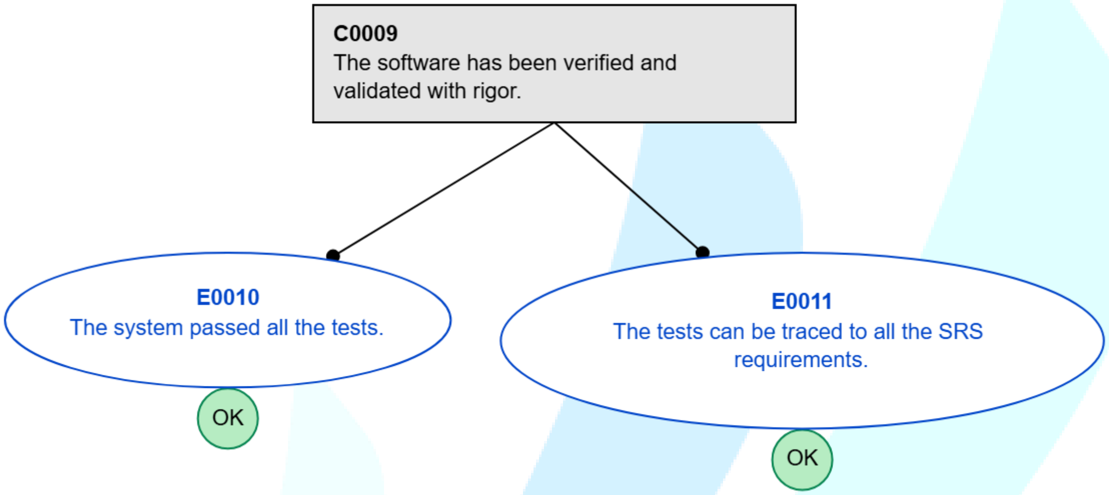
D0665
Unless one or more input providing components are not considered.

E0666
Review of circuit schematics and diagrams along with the block diagram confirm the list of components that provide input is complete.

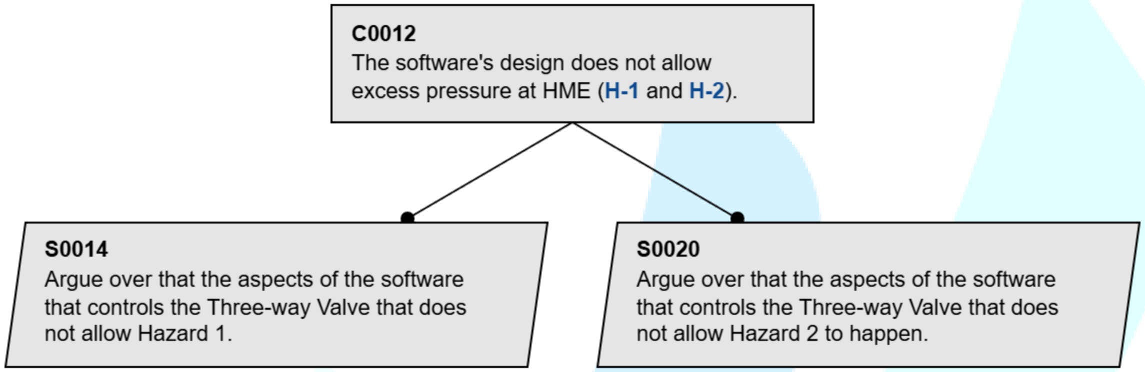
C0005 - The software systems does not allow excess pressure at the HME (H-1 and H-2) by controlling the Three-way Valve.			
Parent subtree(s)	C0001	**Descendant subtree(s)**	C0009, C0012, C0026
Glossary Terms	HME, H-1, H-2		


C0005
The software systems does not allow excess pressure at the HME (H-1 and H-2) by controlling the Three-way Valve.
S0006
Argue over the safety of the software design, implementation and testing.
C0009
The software has been verified and validated with rigor.
C0012
The software's design does not allow excess pressure at HME (H-1 and H-2).
C0026
The software was implemented with rigor.

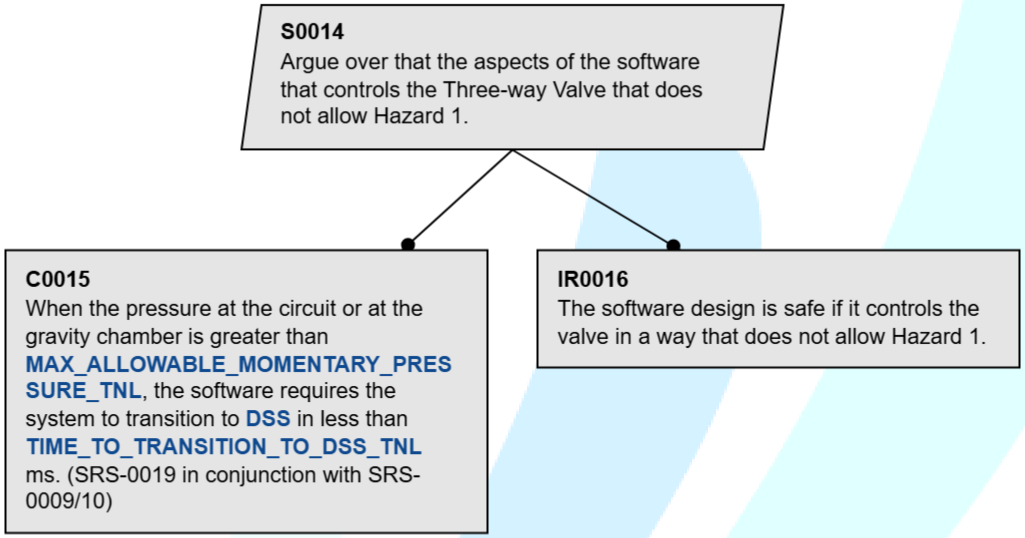
C0009 - The software has been verified and validated with rigor.			
Parent subtree(s)	C0005	**Descendant subtree(s)**	None
Glossary Terms	None		


C0009
The software has been verified and validated with rigor.
E0010
The system passed all the tests.
OK
E0011
The tests can be traced to all the SRS requirements.
OK

C0012 - The software's design does not allow excess pressure at HME (H-1 and H-2).			
Parent subtree(s)	C0005	**Descendant subtree(s)**	S0014, S0020
Glossary Terms	H-1, H-2		


C0012
The software's design does not allow excess pressure at HME (H-1 and H-2).
S0014
Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 1.
S0020
Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 2 to happen.

S0014 - Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 1.			
Parent subtree(s)	C0012	**Descendant subtree(s)**	C0015, IR0016
Glossary Terms	MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL, DSS, TIME_TO_TRANSITION_TO_DSS_TNL		

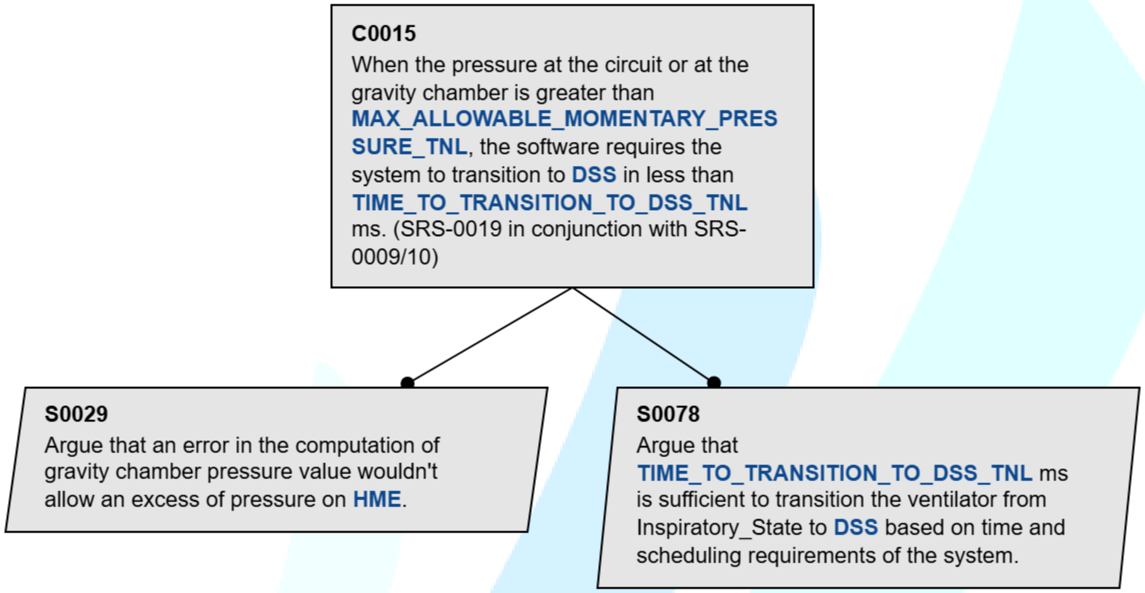


S0014
Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 1.

C0015
When the pressure at the circuit or at the gravity chamber is greater than **MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL**, the software requires the system to transition to **DSS** in less than **TIME_TO_TRANSITION_TO_DSS_TNL** ms. (SRS-0019 in conjunction with SRS-0009/10)

IR0016
The software design is safe if it controls the valve in a way that does not allow Hazard 1.

C0015 - When the pressure at the circuit or at the gravity chamber is greater than MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL, the software requires the s...			
Parent subtree(s)	S0014	Descendant subtree(s)	S0029, S0078
Glossary Terms	MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL, DSS, TIME_TO_TRANSITION_TO_DSS_TNL, HME		

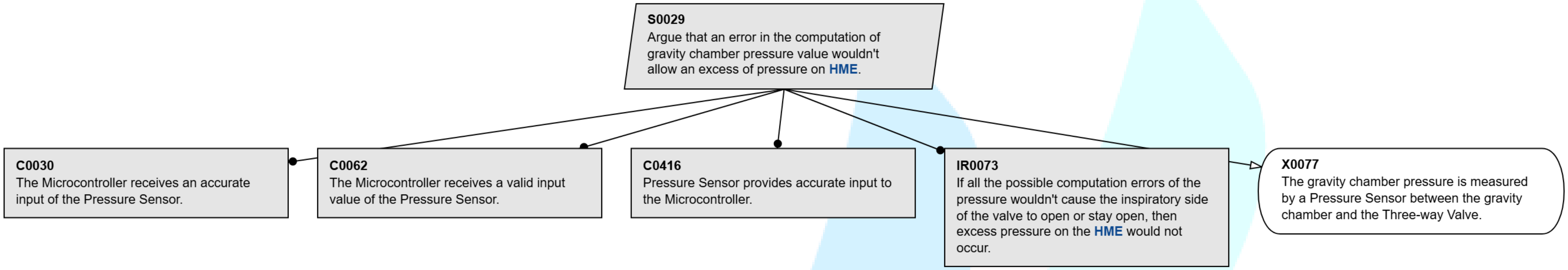


C0015
When the pressure at the circuit or at the gravity chamber is greater than **MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL**, the software requires the system to transition to **DSS** in less than **TIME_TO_TRANSITION_TO_DSS_TNL** ms. (SRS-0019 in conjunction with SRS-0009/10)

S0029
Argue that an error in the computation of gravity chamber pressure value wouldn't allow an excess of pressure on **HME**.

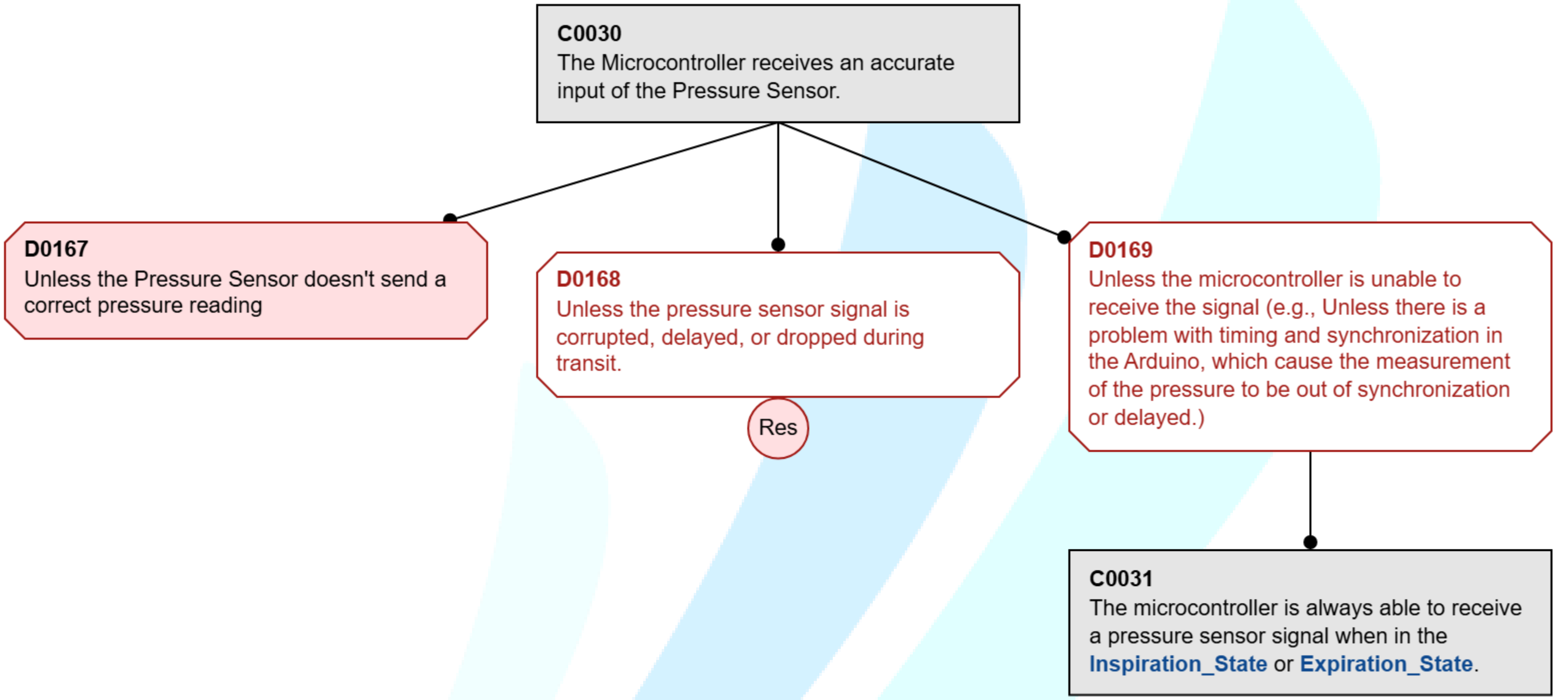
S0078
Argue that **TIME_TO_TRANSITION_TO_DSS_TNL** ms is sufficient to transition the ventilator from Inspiratory_State to **DSS** based on time and scheduling requirements of the system.

S0029 - Argue that an error in the computation of gravity chamber pressure value wouldn't allow an excess of pressure on HME.			
Parent subtree(s)	C0015	**Descendant subtree(s)**	C0030, C0062, IR0073, C0416
Glossary Terms	HME		



S0029
Argue that an error in the computation of gravity chamber pressure value wouldn't allow an excess of pressure on HME.
C0030
The Microcontroller receives an accurate input of the Pressure Sensor.
C0062
The Microcontroller receives a valid input value of the Pressure Sensor.
C0416
Pressure Sensor provides accurate input to the Microcontroller.
IR0073
If all the possible computation errors of the pressure wouldn't cause the inspiratory side of the valve to open or stay open, then excess pressure on the HME would not occur.
X0077
The gravity chamber pressure is measured by a Pressure Sensor between the gravity chamber and the Three-way Valve.

C0030 - The Microcontroller receives an accurate input of the Pressure Sensor.			
Parent subtree(s)	S0029, C0099	**Descendant subtree(s)**	C0031, D0167
Glossary Terms	Inspiration_State, Expiration_State		



C0030
The Microcontroller receives an accurate input of the Pressure Sensor.

D0167
Unless the Pressure Sensor doesn't send a correct pressure reading

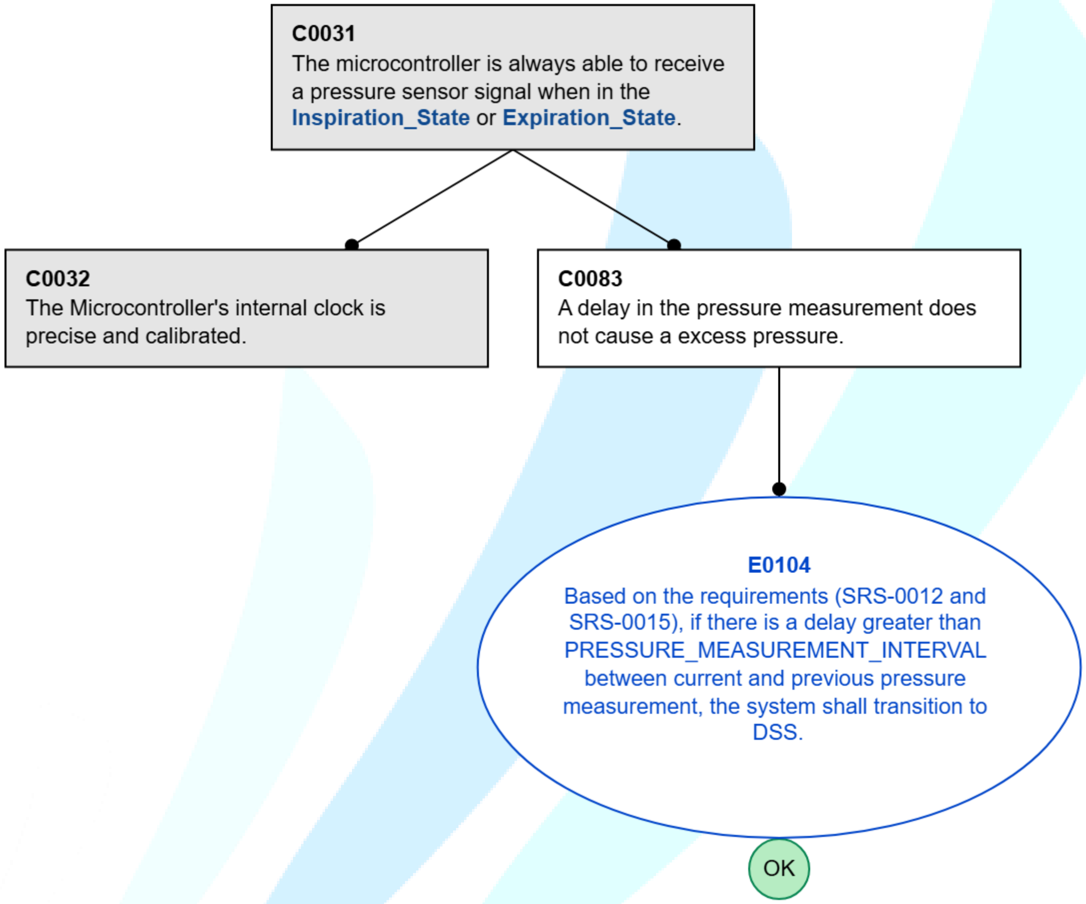
D0168
Unless the pressure sensor signal is corrupted, delayed, or dropped during transit.

Res

D0169
Unless the microcontroller is unable to receive the signal (e.g., Unless there is a problem with timing and synchronization in the Arduino, which cause the measurement of the pressure to be out of synchronization or delayed.)

C0031
The microcontroller is always able to receive a pressure sensor signal when in the **Inspiration_State** or **Expiration_State**.

C0031 - The microcontroller is always able to receive a pressure sensor signal when in the Inspiration_State or Expiration_State.			
Parent subtree(s)	C0030	**Descendant subtree(s)**	C0032
Glossary Terms	Inspiration_State, Expiration_State		



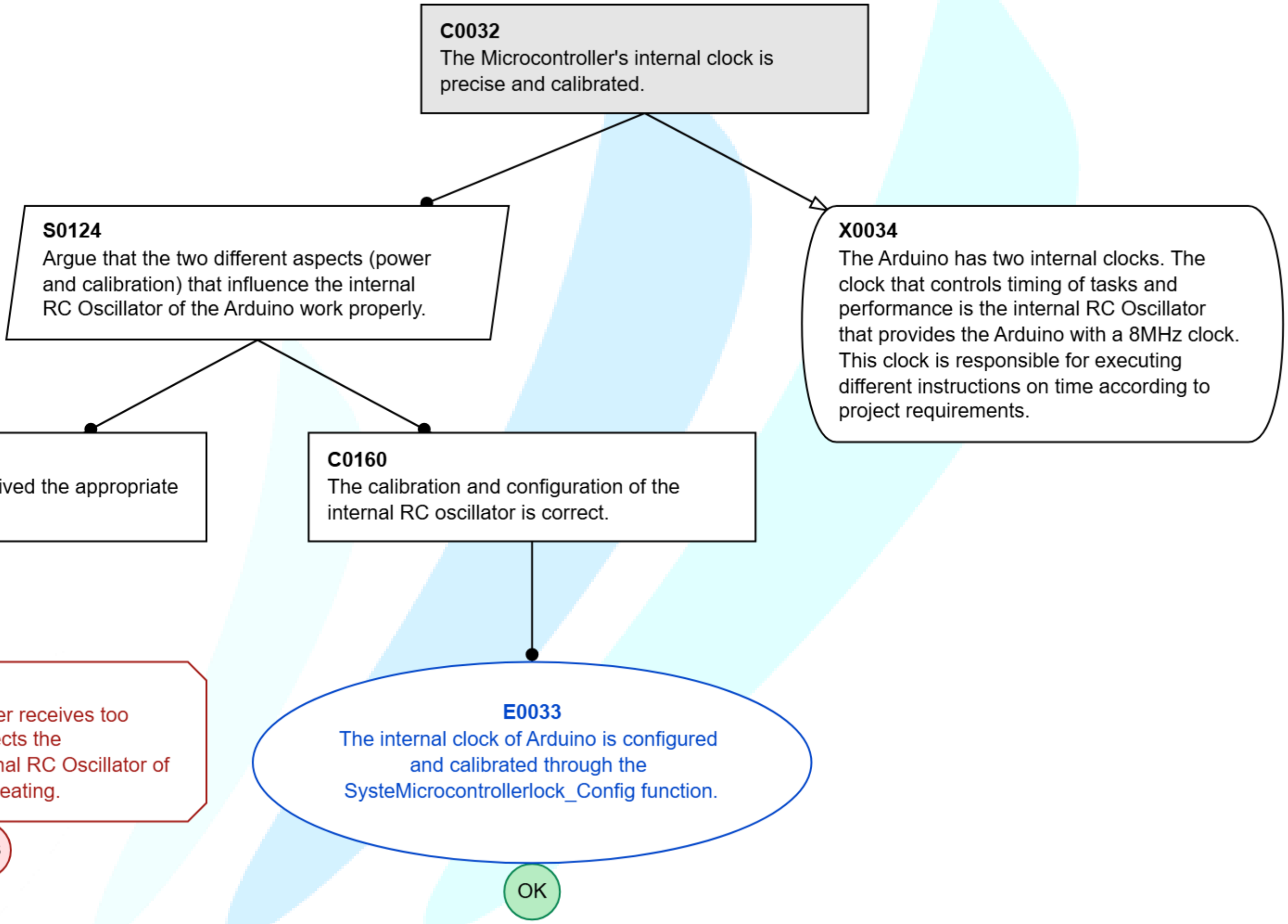
C0031
The microcontroller is always able to receive a pressure sensor signal when in the **Inspiration_State** or **Expiration_State**.

C0032
The Microcontroller's internal clock is precise and calibrated.

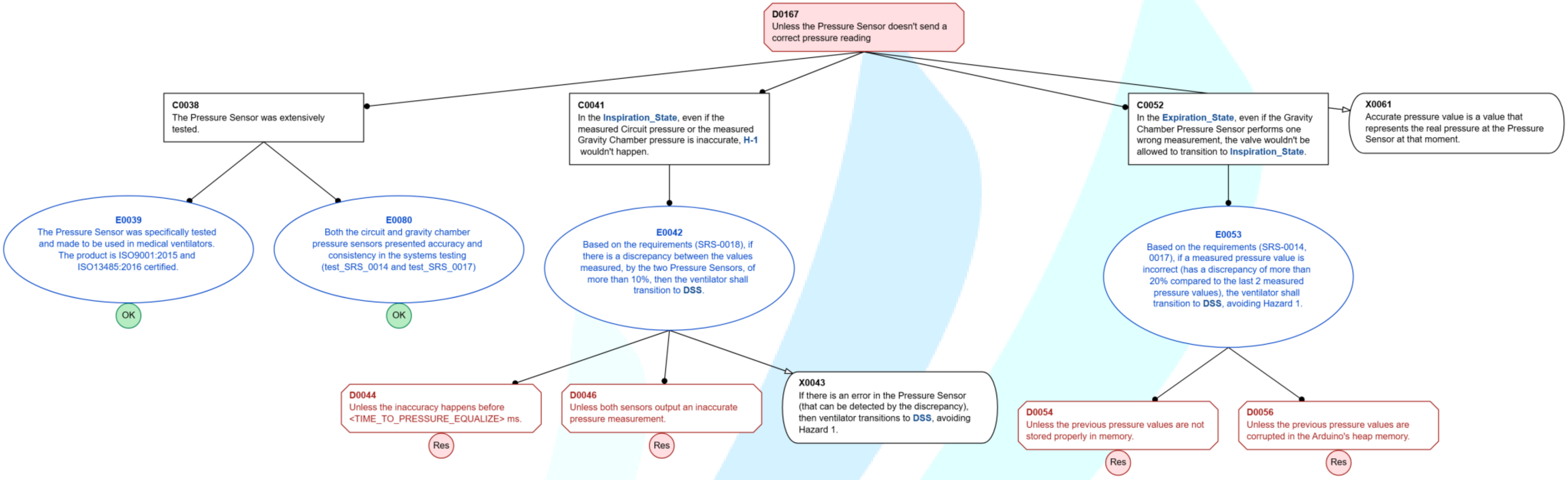
C0083
A delay in the pressure measurement does not cause a excess pressure.

E0104
Based on the requirements (SRS-0012 and SRS-0015), if there is a delay greater than PRESSURE_MEASUREMENT_INTERVAL between current and previous pressure measurement, the system shall transition to DSS.

C0032 - The Microcontroller's internal clock is precise and calibrated.			
Parent subtree(s)	C0031, S0078, S0101, C0022, C0466	**Descendant subtree(s)**	None
Glossary Terms	None		


C0032
The Microcontroller's internal clock is precise and calibrated.
S0124
Argue that the two different aspects (power and calibration) that influence the internal RC Oscillator of the Arduino work properly.
X0034
The Arduino has two internal clocks. The clock that controls timing of tasks and performance is the internal RC Oscillator that provides the Arduino with a 8MHz clock. This clock is responsible for executing different instructions on time according to project requirements.
C0159
The microcontroller received the appropriate amount of power.
C0160
The calibration and configuration of the internal RC oscillator is correct.
D0035
Unless the Microcontroller receives too much voltage, which affects the performance of the internal RC Oscillator of the Arduino due to overheating.
Res
E0033
The internal clock of Arduino is configured and calibrated through the SysteMicrocontrollerlock_Config function.
OK

D0167 - Unless the Pressure Sensor doesn't send a correct pressure reading			
Parent subtree(s)	C0030, C0023	**Descendant subtree(s)**	None
Glossary Terms	Inspiration_State, H-1, DSS, Expiration_State		



D0167
Unless the Pressure Sensor doesn't send a correct pressure reading

C0038
The Pressure Sensor was extensively tested.

C0041
In the **Inspiration_State**, even if the measured Circuit pressure or the measured Gravity Chamber pressure is inaccurate, **H-1** wouldn't happen.

C0052
In the **Expiration_State**, even if the Gravity Chamber Pressure Sensor performs one wrong measurement, the valve wouldn't be allowed to transition to **Inspiration_State**.

X0061
Accurate pressure value is a value that represents the real pressure at the Pressure Sensor at that moment.

E0039
The Pressure Sensor was specifically tested and made to be used in medical ventilators. The product is ISO9001:2015 and ISO13485:2016 certified.

OK

E0080
Both the circuit and gravity chamber pressure sensors presented accuracy and consistency in the systems testing (test_SRS_0014 and test_SRS_0017)

OK

E0042
Based on the requirements (SRS-0018), if there is a discrepancy between the values measured, by the two Pressure Sensors, of more than 10%, then the ventilator shall transition to **DSS**.

E0053
Based on the requirements (SRS-0014, 0017), if a measured pressure value is incorrect (has a discrepancy of more than 20% compared to the last 2 measured pressure values), the ventilator shall transition to **DSS**, avoiding Hazard 1.

D0044
Unless the inaccuracy happens before <TIME_TO_PRESSURE_EQUALIZE> ms.

Res

D0046
Unless both sensors output an inaccurate pressure measurement.

Res

X0043
If there is an error in the Pressure Sensor (that can be detected by the discrepancy), then ventilator transitions to **DSS**, avoiding Hazard 1.

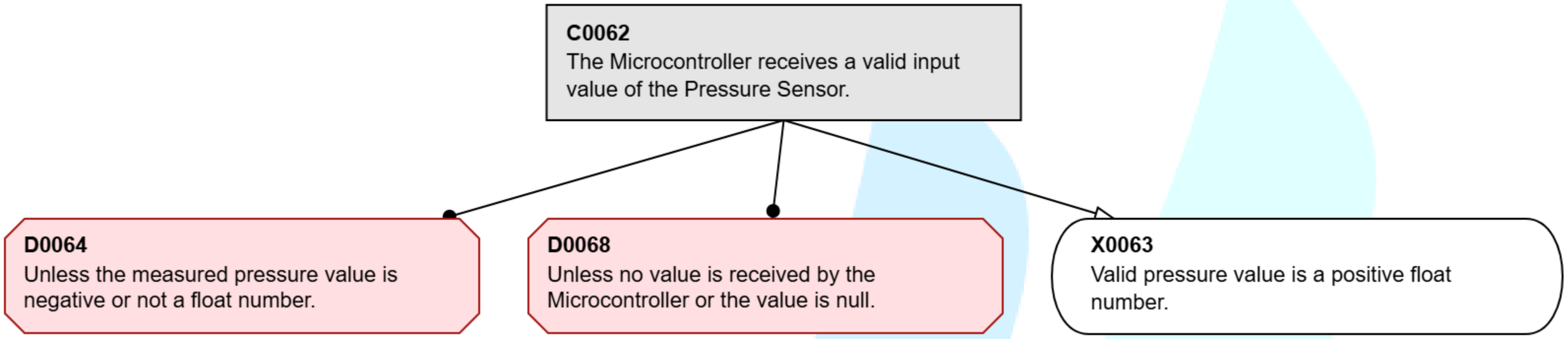
D0054
Unless the previous pressure values are not stored properly in memory.

Res

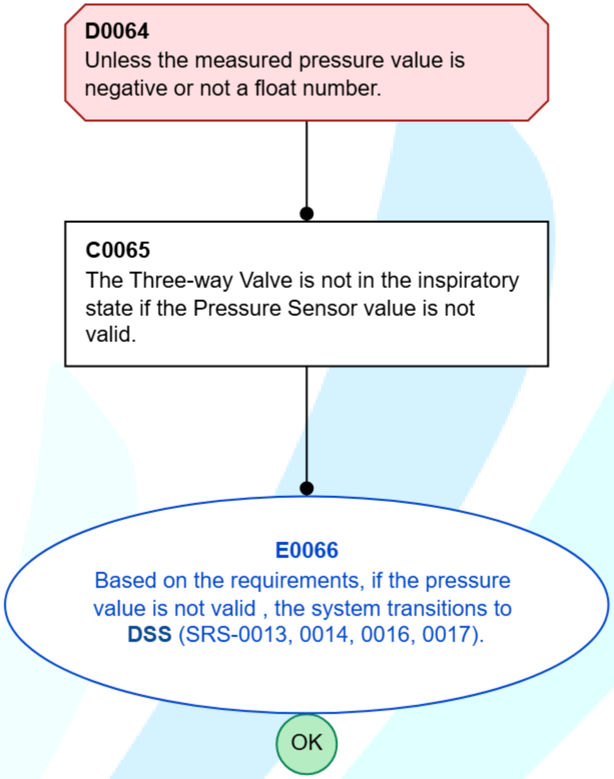
D0056
Unless the previous pressure values are corrupted in the Arduino's heap memory.

Res

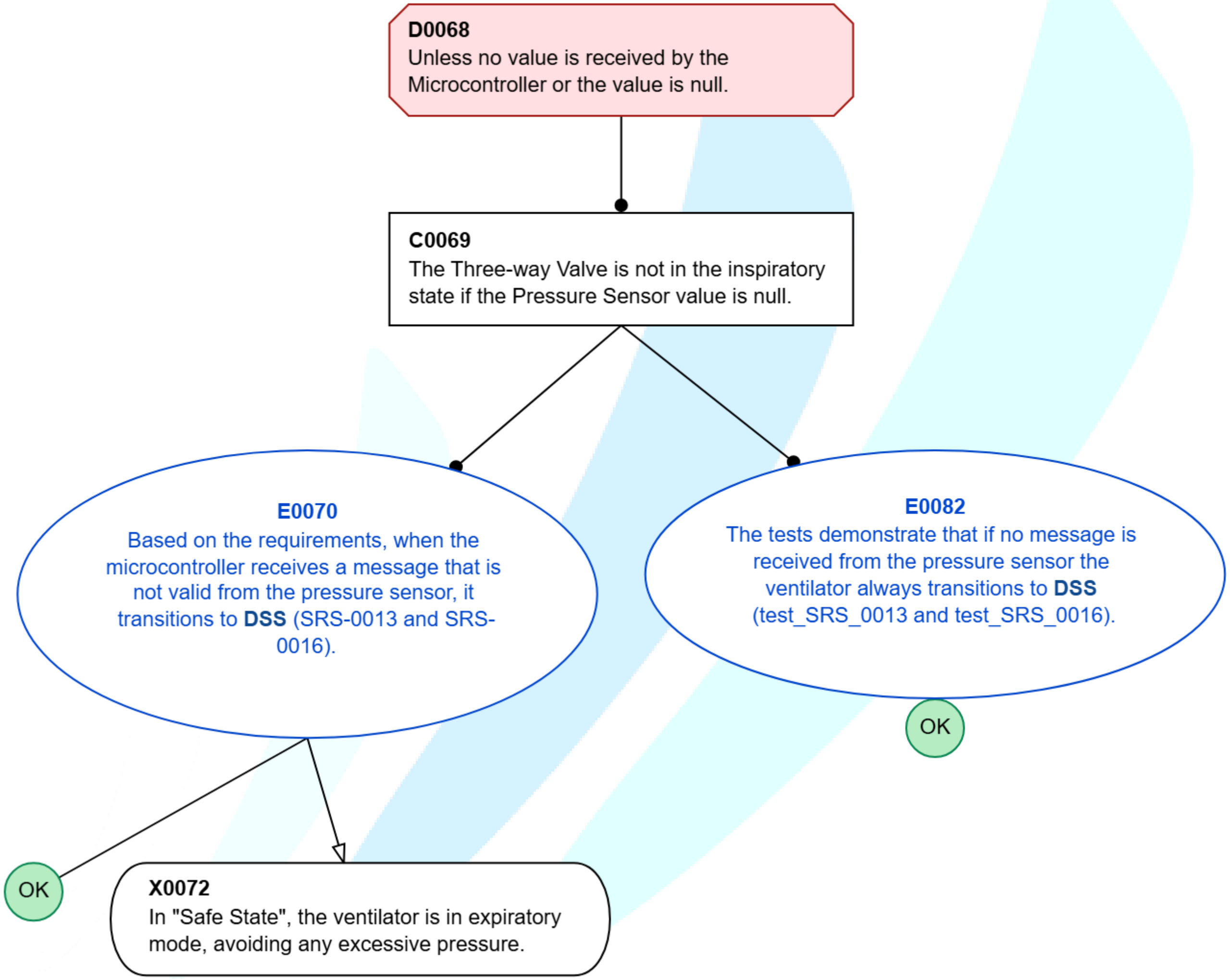
C0062 - The Microcontroller receives a valid input value of the Pressure Sensor.			
Parent subtree(s)	S0029, C0099	**Descendant subtree(s)**	D0064, D0068
Glossary Terms	None		


C0062
The Microcontroller receives a valid input value of the Pressure Sensor.
D0064
Unless the measured pressure value is negative or not a float number.
D0068
Unless no value is received by the Microcontroller or the value is null.
X0063
Valid pressure value is a positive float number.

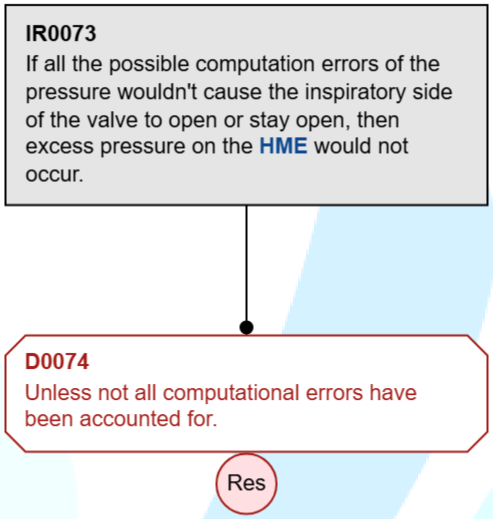
D0064 - Unless the measured pressure value is negative or not a float number.			
Parent subtree(s)	C0062, C0023	**Descendant subtree(s)**	None
Glossary Terms	DSS		


D0064
Unless the measured pressure value is negative or not a float number.
C0065
The Three-way Valve is not in the inspiratory state if the Pressure Sensor value is not valid.
E0066
Based on the requirements, if the pressure value is not valid , the system transitions to DSS (SRS-0013, 0014, 0016, 0017).
OK

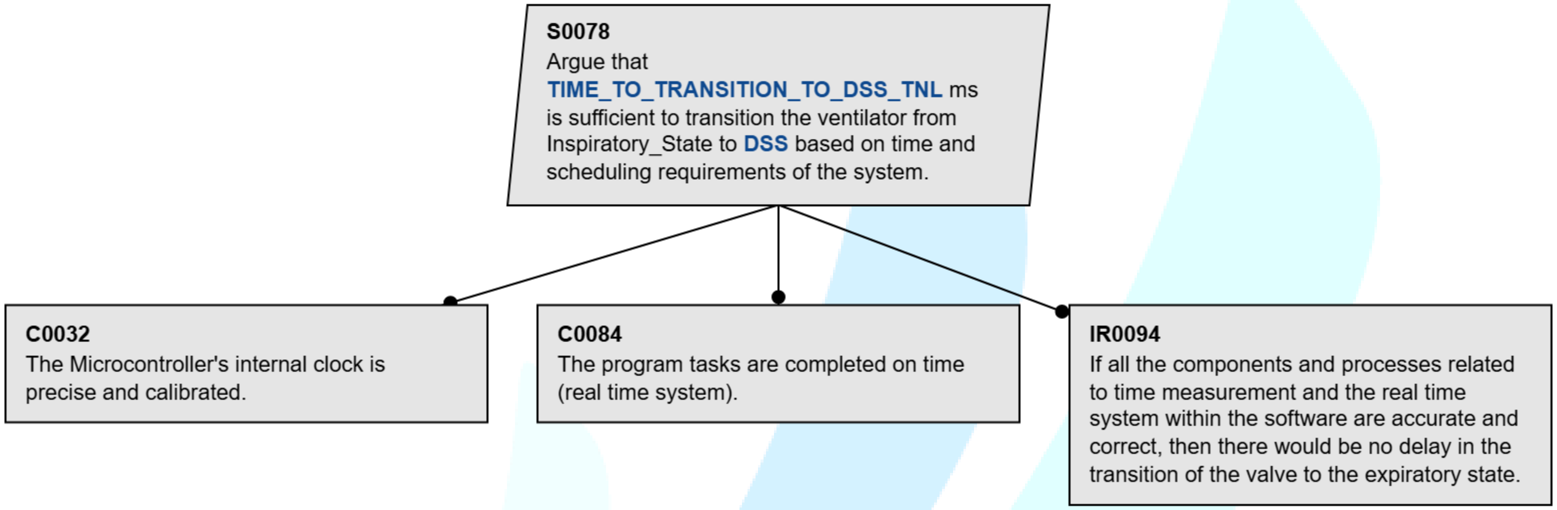
D0068 - Unless no value is received by the Microcontroller or the value is null.			
Parent subtree(s)	C0062, C0023	**Descendant subtree(s)**	None
Glossary Terms	DSS		


D0068
Unless no value is received by the Microcontroller or the value is null.
C0069
The Three-way Valve is not in the inspiratory state if the Pressure Sensor value is null.
E0070
Based on the requirements, when the microcontroller receives a message that is not valid from the pressure sensor, it transitions to DSS (SRS-0013 and SRS-0016).
E0082
The tests demonstrate that if no message is received from the pressure sensor the ventilator always transitions to DSS (test_SRS_0013 and test_SRS_0016).
OK
OK
X0072
In "Safe State", the ventilator is in expiratory mode, avoiding any excessive pressure.

IR0073 - If all the possible computation errors of the pressure wouldn't cause the inspiratory side of the valve to open or stay open, then excess pr...			
Parent subtree(s)	S0029	**Descendant subtree(s)**	None
Glossary Terms	HME		


IR0073
If all the possible computation errors of the pressure wouldn't cause the inspiratory side of the valve to open or stay open, then excess pressure on the HME would not occur.
D0074
Unless not all computational errors have been accounted for.
Res

S0078 - Argue that TIME_TO_TRANSITION_TO_DSS_TNL ms is sufficient to transition the ventilator from Inspiratory_State to DSS based on time and sched...			
Parent subtree(s)	C0015	**Descendant subtree(s)**	C0032, C0084, IR0094
Glossary Terms	TIME_TO_TRANSITION_TO_DSS_TNL, DSS		



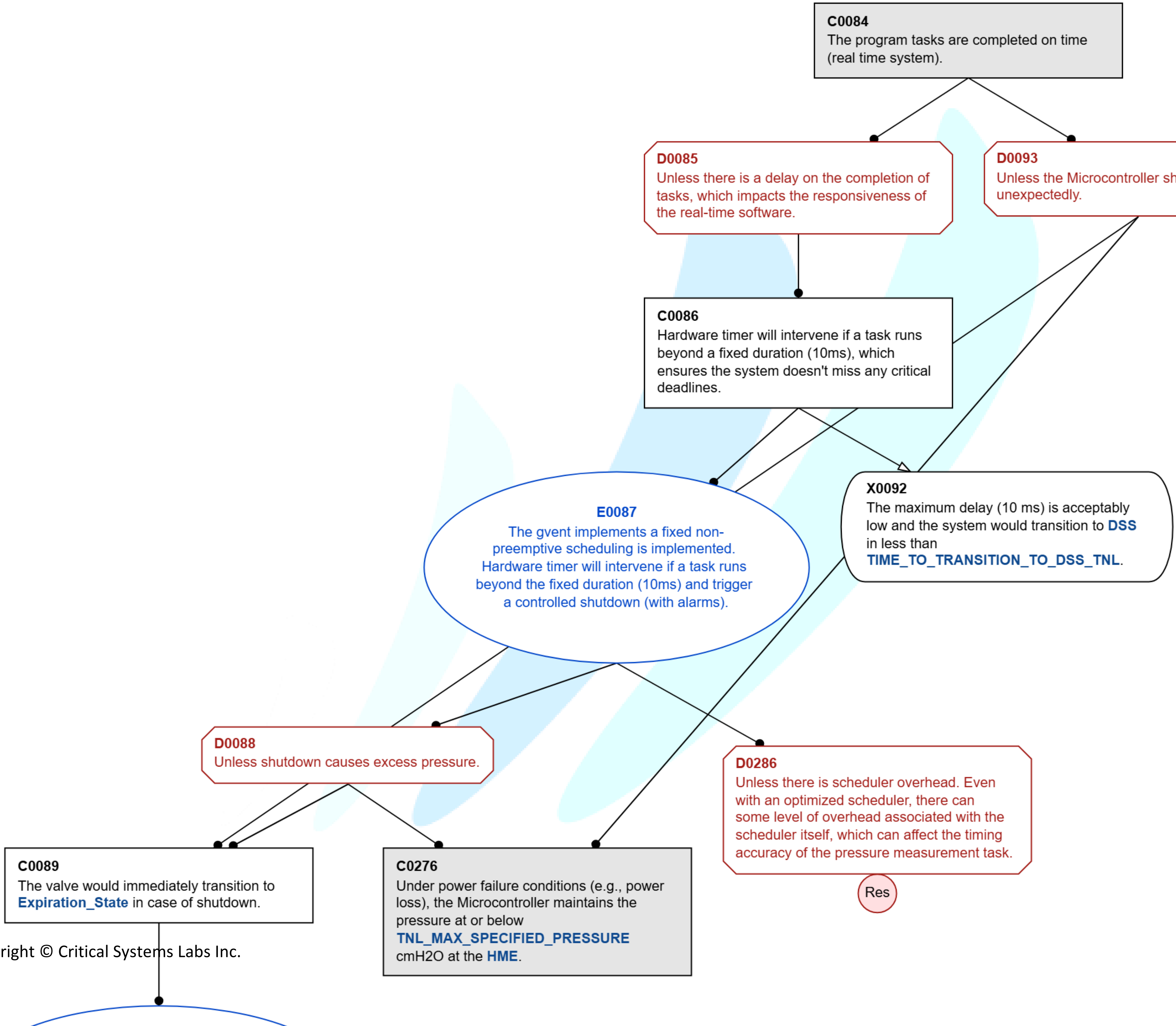
S0078
Argue that **TIME_TO_TRANSITION_TO_DSS_TNL** ms is sufficient to transition the ventilator from Inspiratory_State to **DSS** based on time and scheduling requirements of the system.

C0032
The Microcontroller's internal clock is precise and calibrated.

C0084
The program tasks are completed on time (real time system).

IR0094
If all the components and processes related to time measurement and the real time system within the software are accurate and correct, then there would be no delay in the transition of the valve to the expiratory state.

C0084 - The program tasks are completed on time (real time system).			
Parent subtree(s)	S0078, S0101	**Descendant subtree(s)**	C0276
Glossary Terms	Expiration_State, DSS, TIME_TO_TRANSITION_TO_DSS_TNL, TNL_MAX_SPECIFIED_PRESSURE, HME		



C0084
The program tasks are completed on time (real time system).

D0085
Unless there is a delay on the completion of tasks, which impacts the responsiveness of the real-time software.

D0093
Unless the Microcontroller shutdown unexpectedly.

C0086
Hardware timer will intervene if a task runs beyond a fixed duration (10ms), which ensures the system doesn't miss any critical deadlines.

E0087
The gvent implements a fixed non-preemptive scheduling is implemented. Hardware timer will intervene if a task runs beyond the fixed duration (10ms) and trigger a controlled shutdown (with alarms).

X0092
The maximum delay (10 ms) is acceptably low and the system would transition to **DSS** in less than **TIME_TO_TRANSITION_TO_DSS_TNL**.

D0088
Unless shutdown causes excess pressure.

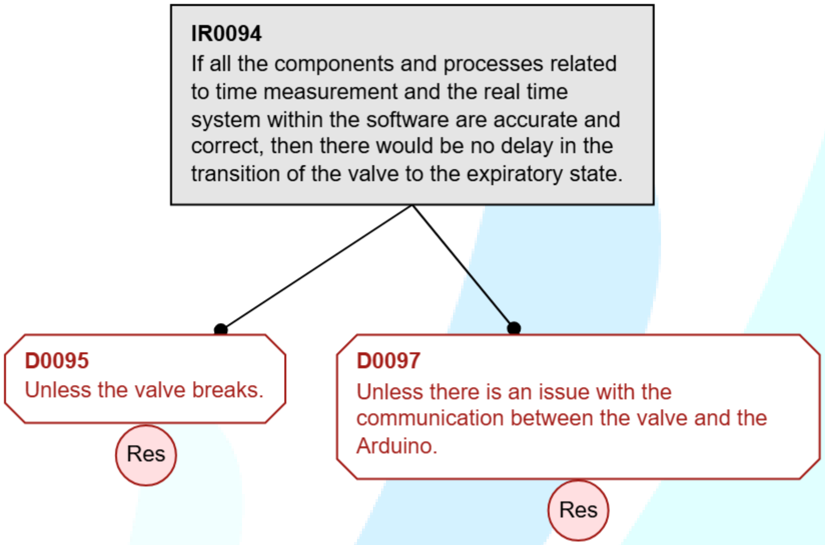
D0286
Unless there is scheduler overhead. Even with an optimized scheduler, there can some level of overhead associated with the scheduler itself, which can affect the timing accuracy of the pressure measurement task.

Res

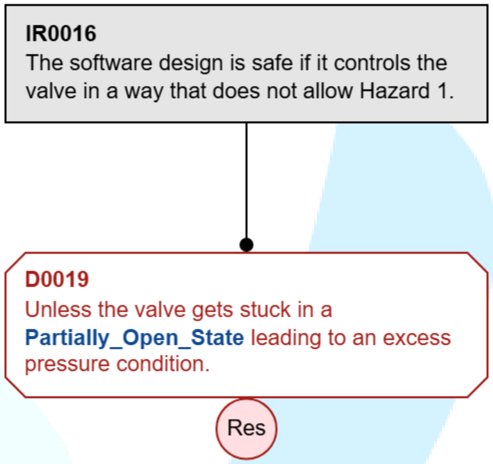
C0089
The valve would immediately transition to **Expiration_State** in case of shutdown.

C0276
Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

IR0094 - If all the components and processes related to time measurement and the real time system within the software are accurate and correct, then ...			
Parent subtree(s)	S0078	**Descendant subtree(s)**	None
Glossary Terms	None		


IR0094
If all the components and processes related to time measurement and the real time system within the software are accurate and correct, then there would be no delay in the transition of the valve to the expiratory state.
D0095
Unless the valve breaks.
Res
D0097
Unless there is an issue with the communication between the valve and the Arduino.
Res

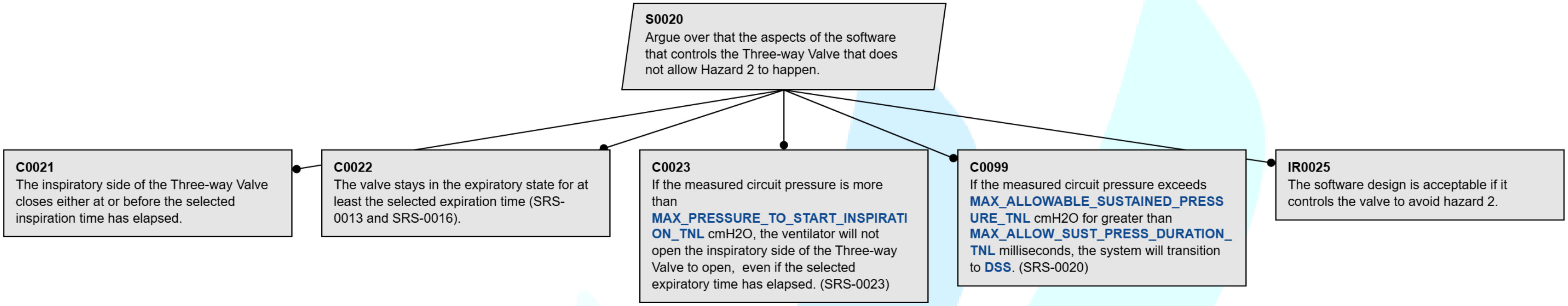
IR0016 - The software design is safe if it controls the valve in a way that does not allow Hazard 1.			
Parent subtree(s)	S0014	**Descendant subtree(s)**	None
Glossary Terms	Partially_Open_State		



IR0016
The software design is safe if it controls the valve in a way that does not allow Hazard 1.

D0019
Unless the valve gets stuck in a **Partially_Open_State** leading to an excess pressure condition.

S0020 - Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 2 to happen.			
Parent subtree(s)	C0012	**Descendant subtree(s)**	C0021, C0022, C0023, IR0025, C0099
Glossary Terms	MAX_PRESSURE_TO_START_INSPIRATION_TNL, MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL, MAX_ALLOW_SUST_PRESS_DURATION_TNL, DSS		



S0020
Argue over that the aspects of the software that controls the Three-way Valve that does not allow Hazard 2 to happen.

C0021
The inspiratory side of the Three-way Valve closes either at or before the selected inspiration time has elapsed.

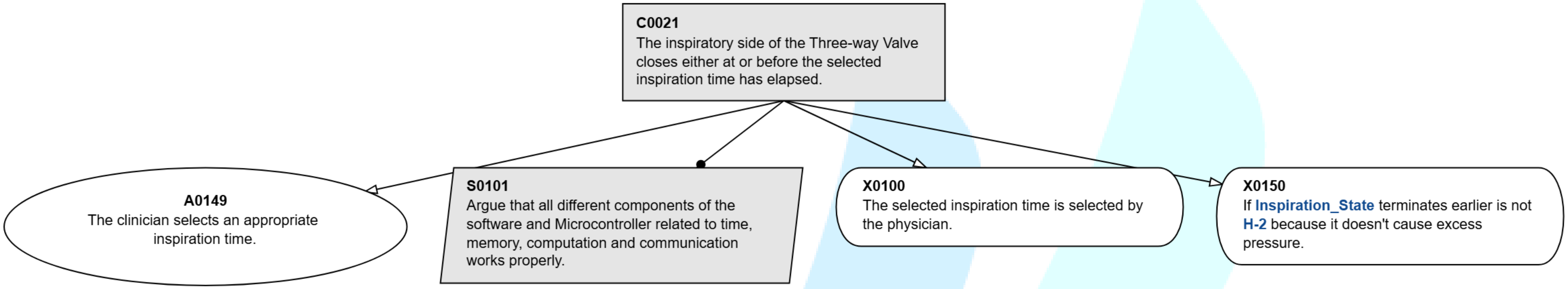
C0022
The valve stays in the expiratory state for at least the selected expiration time (SRS-0013 and SRS-0016).

C0023
If the measured circuit pressure is more than **MAX_PRESSURE_TO_START_INSPIRATION_TNL** cmH2O, the ventilator will not open the inspiratory side of the Three-way Valve to open, even if the selected expiratory time has elapsed. (SRS-0023)

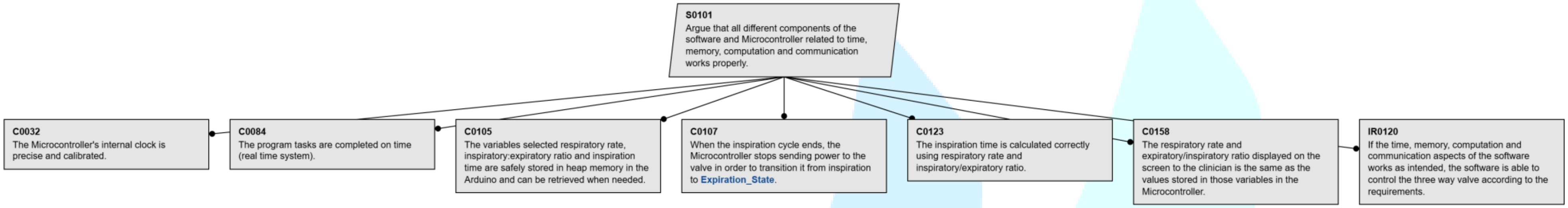
C0099
If the measured circuit pressure exceeds **MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL** cmH2O for greater than **MAX_ALLOW_SUST_PRESS_DURATION_TNL** milliseconds, the system will transition to **DSS**. (SRS-0020)

IR0025
The software design is acceptable if it controls the valve to avoid hazard 2.

C0021 - The inspiratory side of the Three-way Valve closes either at or before the selected inspiration time has elapsed.			
Parent subtree(s)	S0020	**Descendant subtree(s)**	S0101
Glossary Terms	Inspiration_State, H-2		


C0021
The inspiratory side of the Three-way Valve closes either at or before the selected inspiration time has elapsed.
A0149
The clinician selects an appropriate inspiration time.
S0101
Argue that all different components of the software and Microcontroller related to time, memory, computation and communication works properly.
X0100
The selected inspiration time is selected by the physician.
X0150
If Inspiration_State terminates earlier is not H-2 because it doesn't cause excess pressure.

S0101 - Argue that all different components of the software and Microcontroller related to time, memory, computation and communicatio n works properl...			
Parent subtree(s)	C0021	**Descendant subtree(s)**	C0032, C0084, C0105, C0107, IR0120, C0123, C0158
Glossary Terms	Expiration_State		



S0101
Argue that all different components of the software and Microcontroller related to time, memory, computation and communication works properly.

C0032
The Microcontroller's internal clock is precise and calibrated.

C0084
The program tasks are completed on time (real time system).

C0105
The variables selected respiratory rate, inspiratory:expiratory ratio and inspiration time are safely stored in heap memory in the Arduino and can be retrieved when needed.

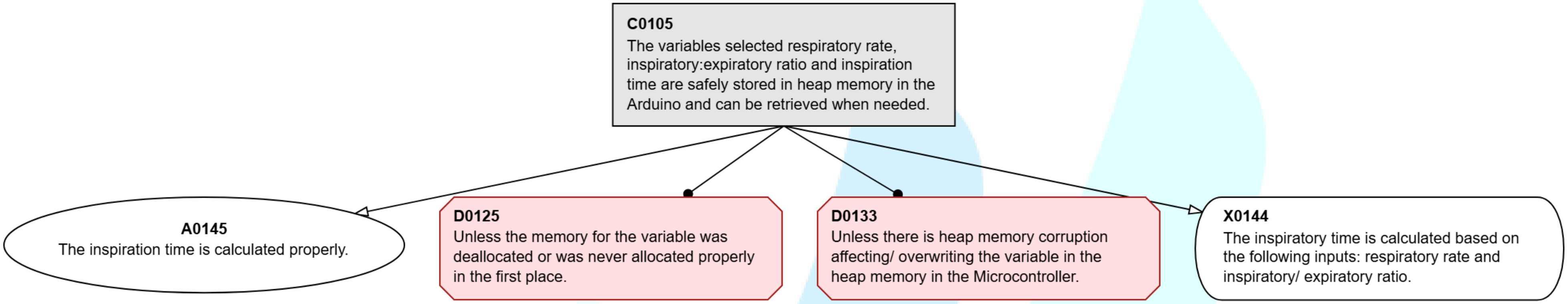
C0107
When the inspiration cycle ends, the Microcontroller stops sending power to the valve in order to transition it from inspiration to **Expiration_State**.

C0123
The inspiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.

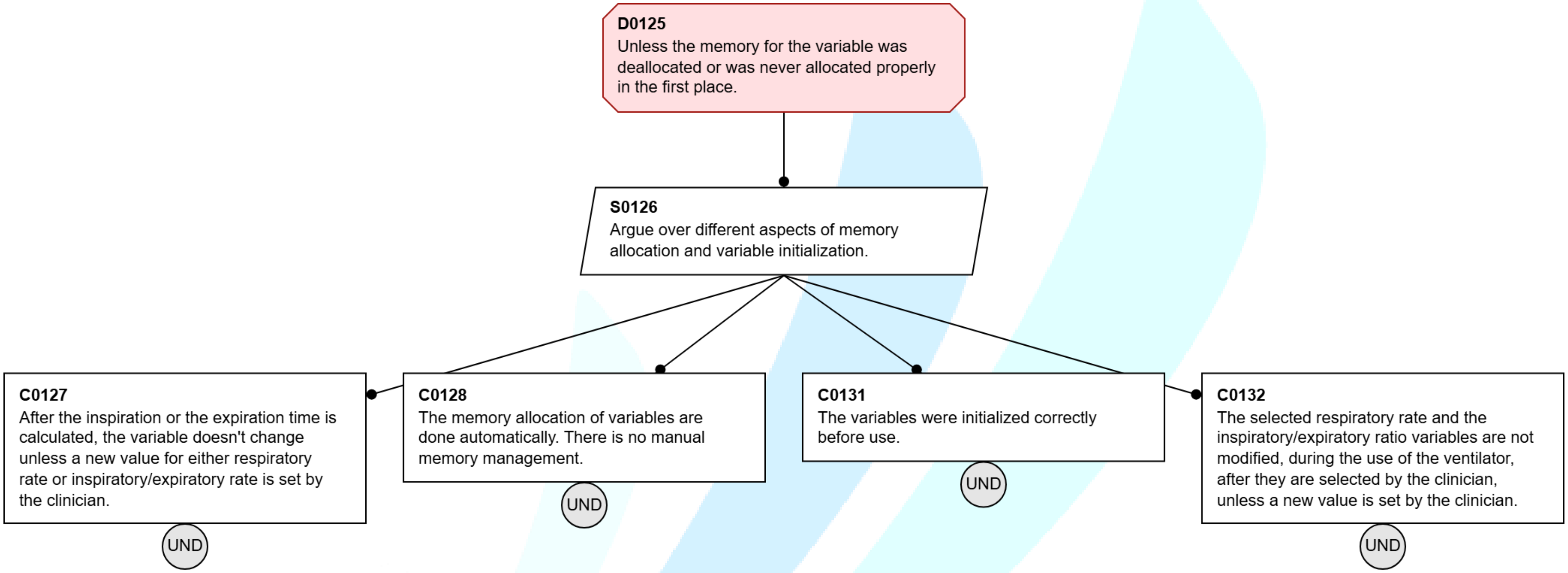
C0158
The respiratory rate and expiratory/inspiratory ratio displayed on the screen to the clinician is the same as the values stored in those variables in the Microcontroller.

IR0120
If the time, memory, computation and communication aspects of the software works as intended, the software is able to control the three way valve according to the requirements.

C0105 - The variables selected respiratory rate, inspiratory:expiratory ratio and inspiration time are safely stored in heap memory in the Arduino a...			
Parent subtree(s)	S0101	**Descendant subtree(s)**	D0125, D0133
Glossary Terms	None		


C0105
The variables selected respiratory rate, inspiratory:expiratory ratio and inspiration time are safely stored in heap memory in the Arduino and can be retrieved when needed.
A0145
The inspiration time is calculated properly.
D0125
Unless the memory for the variable was deallocated or was never allocated properly in the first place.
D0133
Unless there is heap memory corruption affecting/ overwriting the variable in the heap memory in the Microcontroller.
X0144
The inspiratory time is calculated based on the following inputs: respiratory rate and inspiratory/ expiratory ratio.

D0125 - Unless the memory for the variable was deallocated or was never allocated properly in the first place.			
Parent subtree(s)	C0105, C0165, C0377	**Descendant subtree(s)**	None
Glossary Terms	None		



D0125
Unless the memory for the variable was deallocated or was never allocated properly in the first place.

S0126
Argue over different aspects of memory allocation and variable initialization.

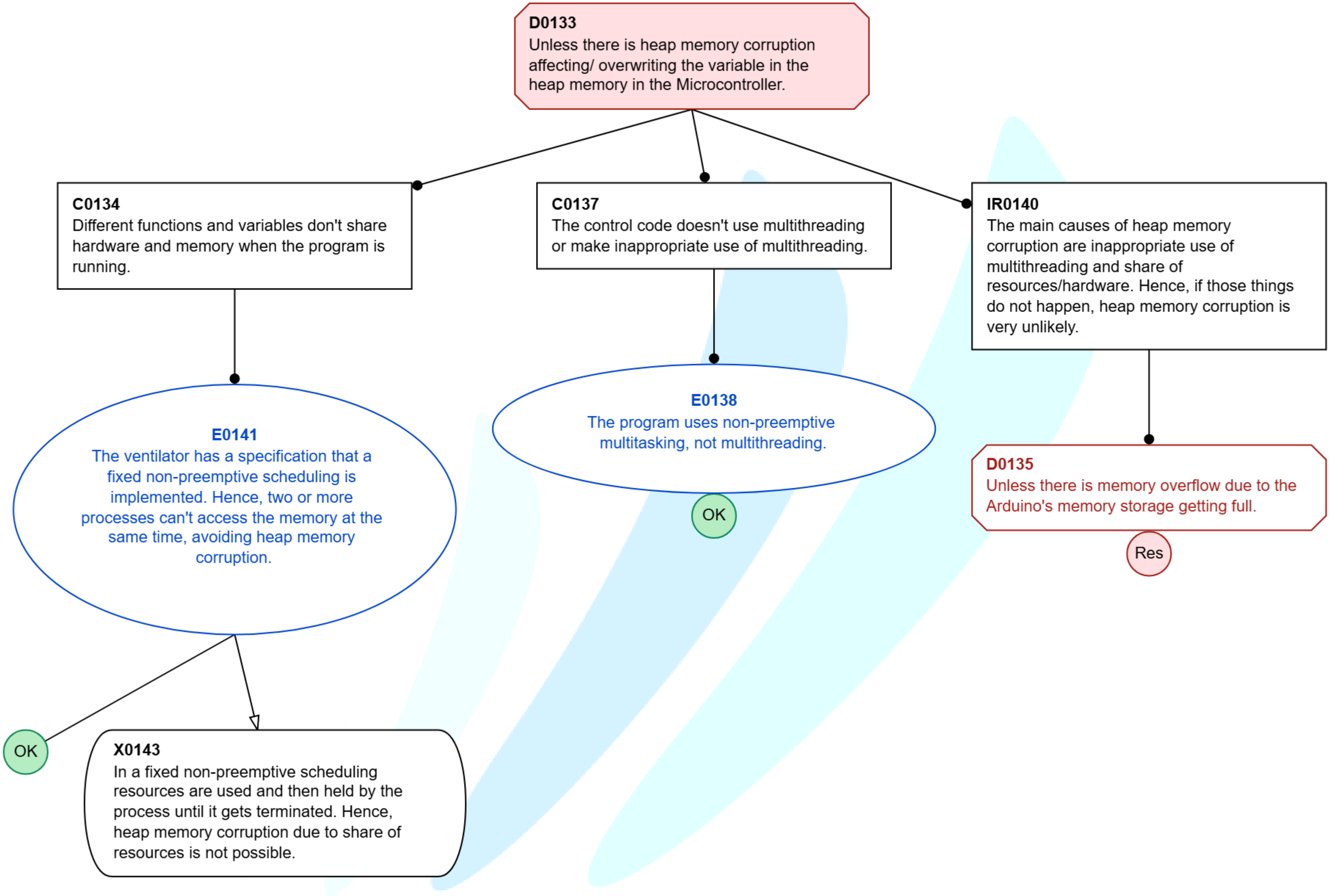
C0127
After the inspiration or the expiration time is calculated, the variable doesn't change unless a new value for either respiratory rate or inspiratory/expiratory rate is set by the clinician.

C0128
The memory allocation of variables are done automatically. There is no manual memory management.

C0131
The variables were initialized correctly before use.

C0132
The selected respiratory rate and the inspiratory/expiratory ratio variables are not modified, during the use of the ventilator, after they are selected by the clinician, unless a new value is set by the clinician.

D0133 - Unless there is heap memory corruption affecting/ overwriting the variable in the heap memory in the Microcontroller.			
Parent subtree(s)	C0105, C0165, C0377	**Descendant subtree(s)**	None
Glossary Terms	None		



D0133
Unless there is heap memory corruption affecting/ overwriting the variable in the heap memory in the Microcontroller.

C0134
Different functions and variables don't share hardware and memory when the program is running.

C0137
The control code doesn't use multithreading or make inappropriate use of multithreading.

IR0140
The main causes of heap memory corruption are inappropriate use of multithreading and share of resources/hardware. Hence, if those things do not happen, heap memory corruption is very unlikely.

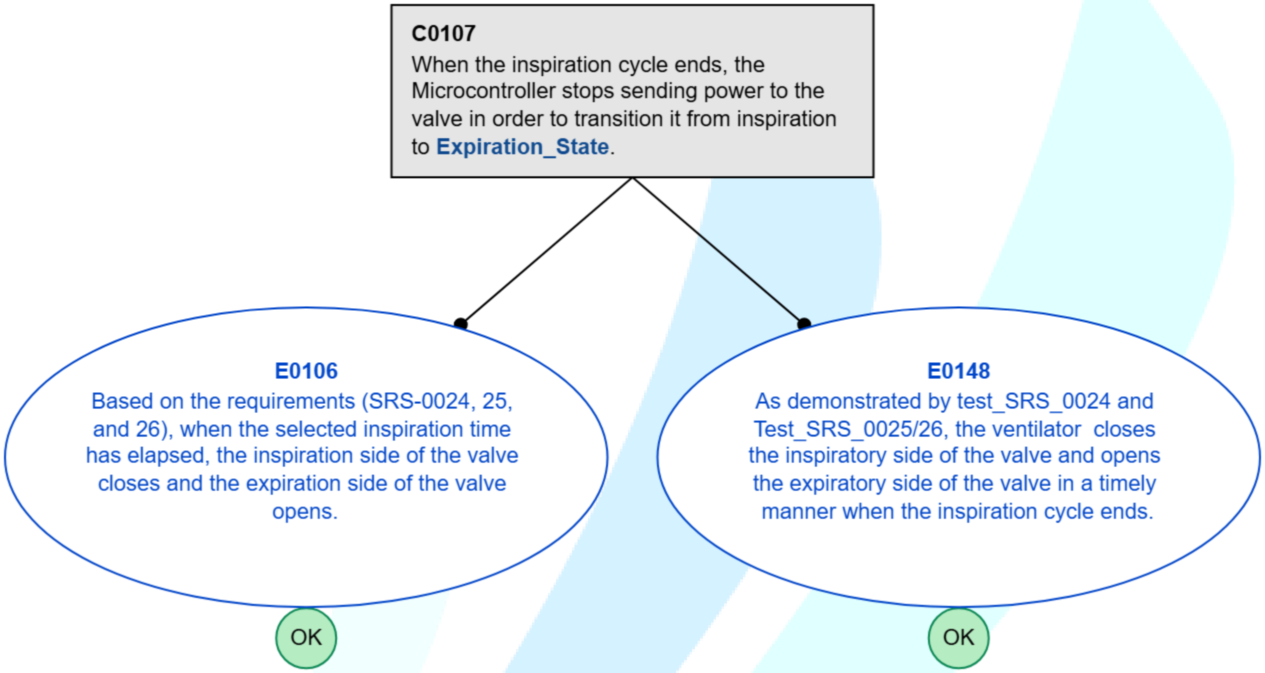
E0141
The ventilator has a specification that a fixed non-preemptive scheduling is implemented. Hence, two or more processes can't access the memory at the same time, avoiding heap memory corruption.

E0138
The program uses non-preemptive multitasking, not multithreading.

D0135
Unless there is memory overflow due to the Arduino's memory storage getting full.

X0143
In a fixed non-preemptive scheduling resources are used and then held by the process until it gets terminated. Hence, heap memory corruption due to share of resources is not possible.

C0107 - When the inspiration cycle ends, the Microcontroller stops sending power to the valve in order to transition it from inspiration to Expirati...			
Parent subtree(s)	S0101	**Descendant subtree(s)**	None
Glossary Terms	Expiration_State		

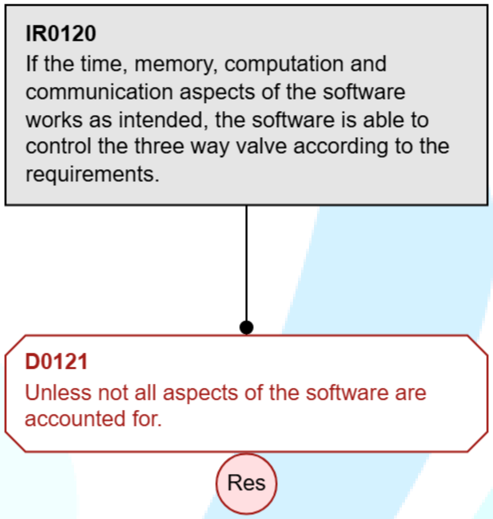


C0107
When the inspiration cycle ends, the Microcontroller stops sending power to the valve in order to transition it from inspiration to **Expiration_State**.

E0106
Based on the requirements (SRS-0024, 25, and 26), when the selected inspiration time has elapsed, the inspiration side of the valve closes and the expiration side of the valve opens.

E0148
As demonstrated by test_SRS_0024 and Test_SRS_0025/26, the ventilator closes the inspiratory side of the valve and opens the expiratory side of the valve in a timely manner when the inspiration cycle ends.

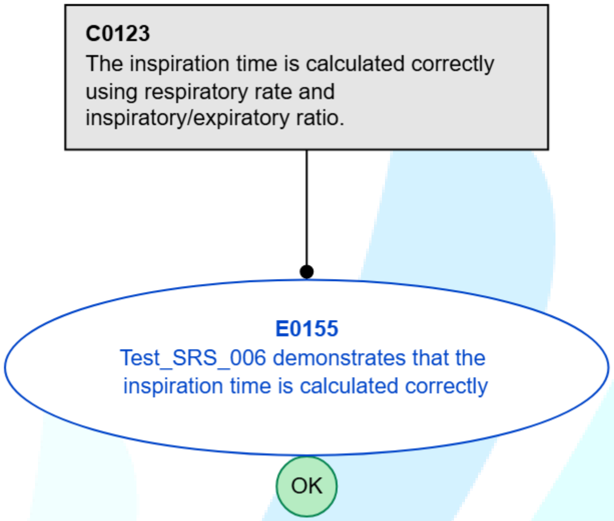
IR0120 - If the time, memory, computation and communication aspects of the software works as intended, the software is able to control the three way ...			
Parent subtree(s)	S0101, C0022	**Descendant subtree(s)**	None
Glossary Terms	None		



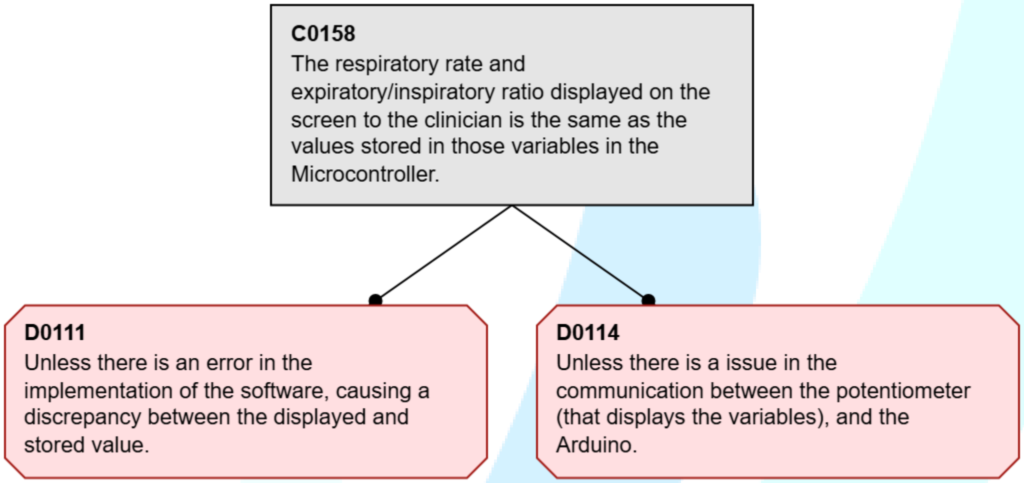
IR0120
If the time, memory, computation and communication aspects of the software works as intended, the software is able to control the three way valve according to the requirements.

D0121
Unless not all aspects of the software are accounted for.

C0123 - The inspiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.			
Parent subtree(s)	S0101	**Descendant subtree(s)**	None
Glossary Terms	None		


C0123
The inspiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.
E0155
Test_SRS_006 demonstrates that the inspiration time is calculated correctly
OK

C0158 - The respiratory rate and expiratory/inspiratory ratio displayed on the screen to the clinician is the same as the values stored in those var...			
Parent subtree(s)	S0101, C0022	**Descendant subtree(s)**	D0111, D0114
Glossary Terms	None		

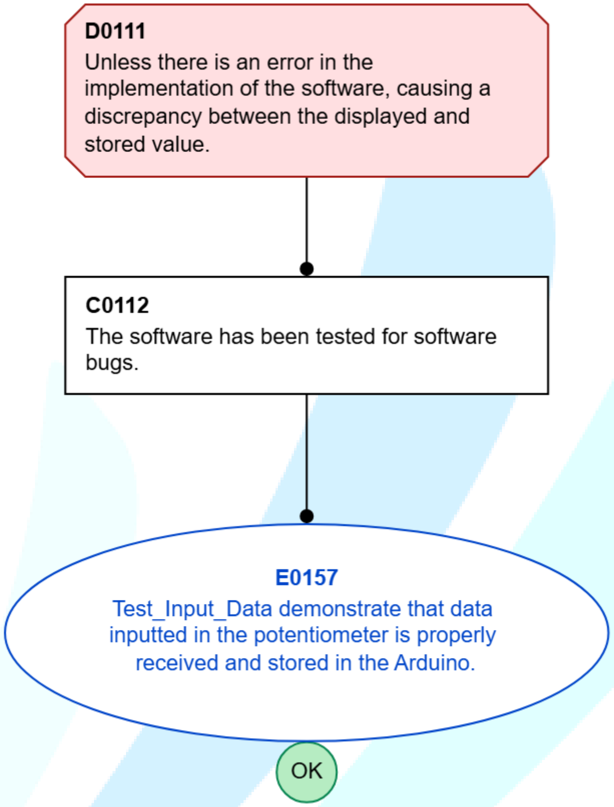


C0158
The respiratory rate and expiratory/inspiratory ratio displayed on the screen to the clinician is the same as the values stored in those variables in the Microcontroller.

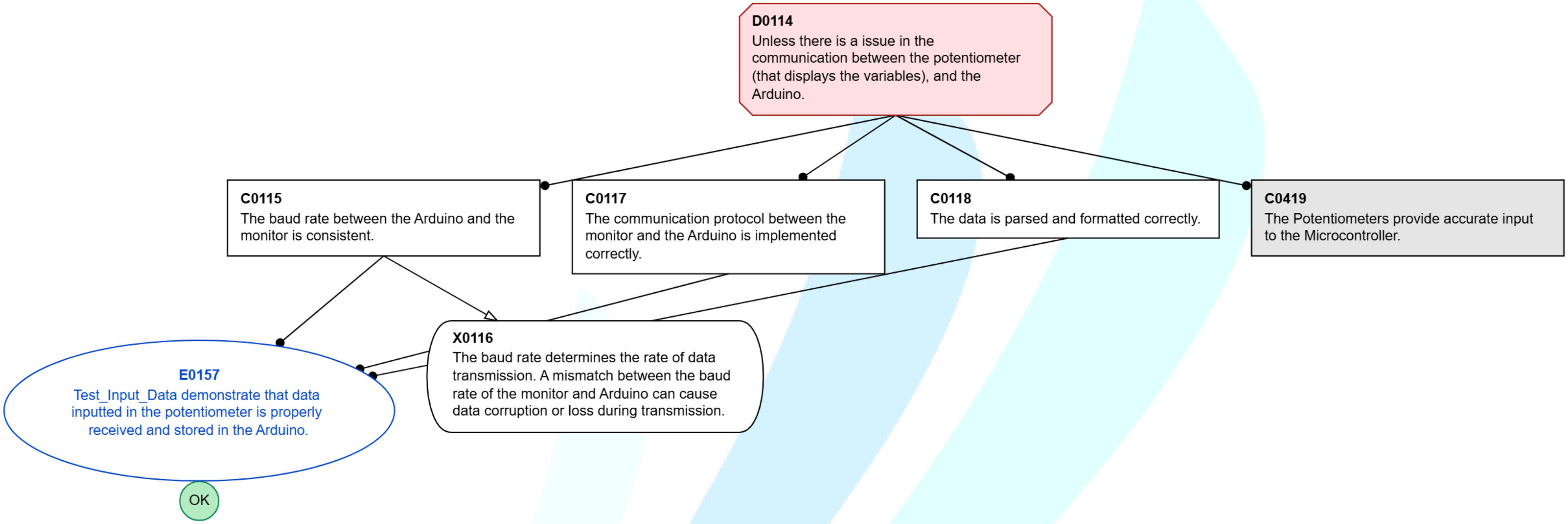
D0111
Unless there is an error in the implementation of the software, causing a discrepancy between the displayed and stored value.

D0114
Unless there is a issue in the communication between the potentiometer (that displays the variables), and the Arduino.

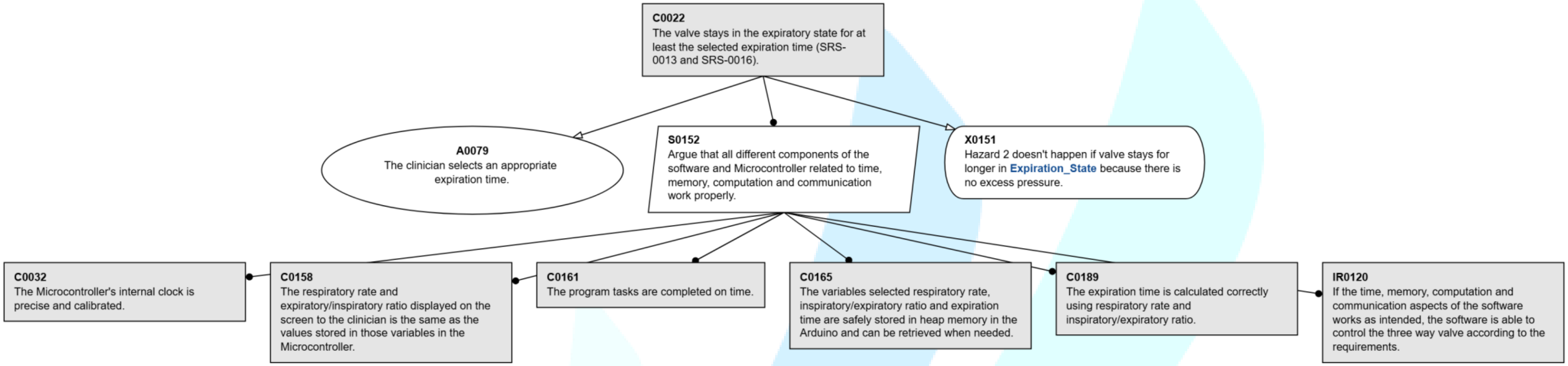
D0111 - Unless there is an error in the implementation of the software, causing a discrepancy between the displayed and stored value.			
Parent subtree(s)	C0158	**Descendant subtree(s)**	None
Glossary Terms	None		


D0111
Unless there is an error in the implementation of the software, causing a discrepancy between the displayed and stored value.
C0112
The software has been tested for software bugs.
E0157
Test_Input_Data demonstrate that data inputted in the potentiometer is properly received and stored in the Arduino.
OK

D0114 - Unless there is a issue in the communication between the potentiometer (that displays the variables), and the Arduino.			
Parent subtree(s)	C0158	**Descendant subtree(s)**	C0419
Glossary Terms	None		


D0114
Unless there is a issue in the communication between the potentiometer (that displays the variables), and the Arduino.
C0115
The baud rate between the Arduino and the monitor is consistent.
C0117
The communication protocol between the monitor and the Arduino is implemented correctly.
C0118
The data is parsed and formatted correctly.
C0419
The Potentiometers provide accurate input to the Microcontroller.
X0116
The baud rate determines the rate of data transmission. A mismatch between the baud rate of the monitor and Arduino can cause data corruption or loss during transmission.
E0157
Test_Input_Data demonstrate that data inputted in the potentiometer is properly received and stored in the Arduino.
OK

C0022 - The valve stays in the expiratory state for at least the selected expiration time (SRS-0013 and SRS-0016).			
Parent subtree(s)	S0020	**Descendant subtree(s)**	C0032, IR0120, C0158, C0161, C0165, C0189
Glossary Terms	Expiration_State		



C0022
The valve stays in the expiratory state for at least the selected expiration time (SRS-0013 and SRS-0016).

A0079
The clinician selects an appropriate expiration time.

S0152
Argue that all different components of the software and Microcontroller related to time, memory, computation and communication work properly.

X0151
Hazard 2 doesn't happen if valve stays for longer in **Expiration_State** because there is no excess pressure.

C0032
The Microcontroller's internal clock is precise and calibrated.

C0158
The respiratory rate and expiratory/inspiratory ratio displayed on the screen to the clinician is the same as the values stored in those variables in the Microcontroller.

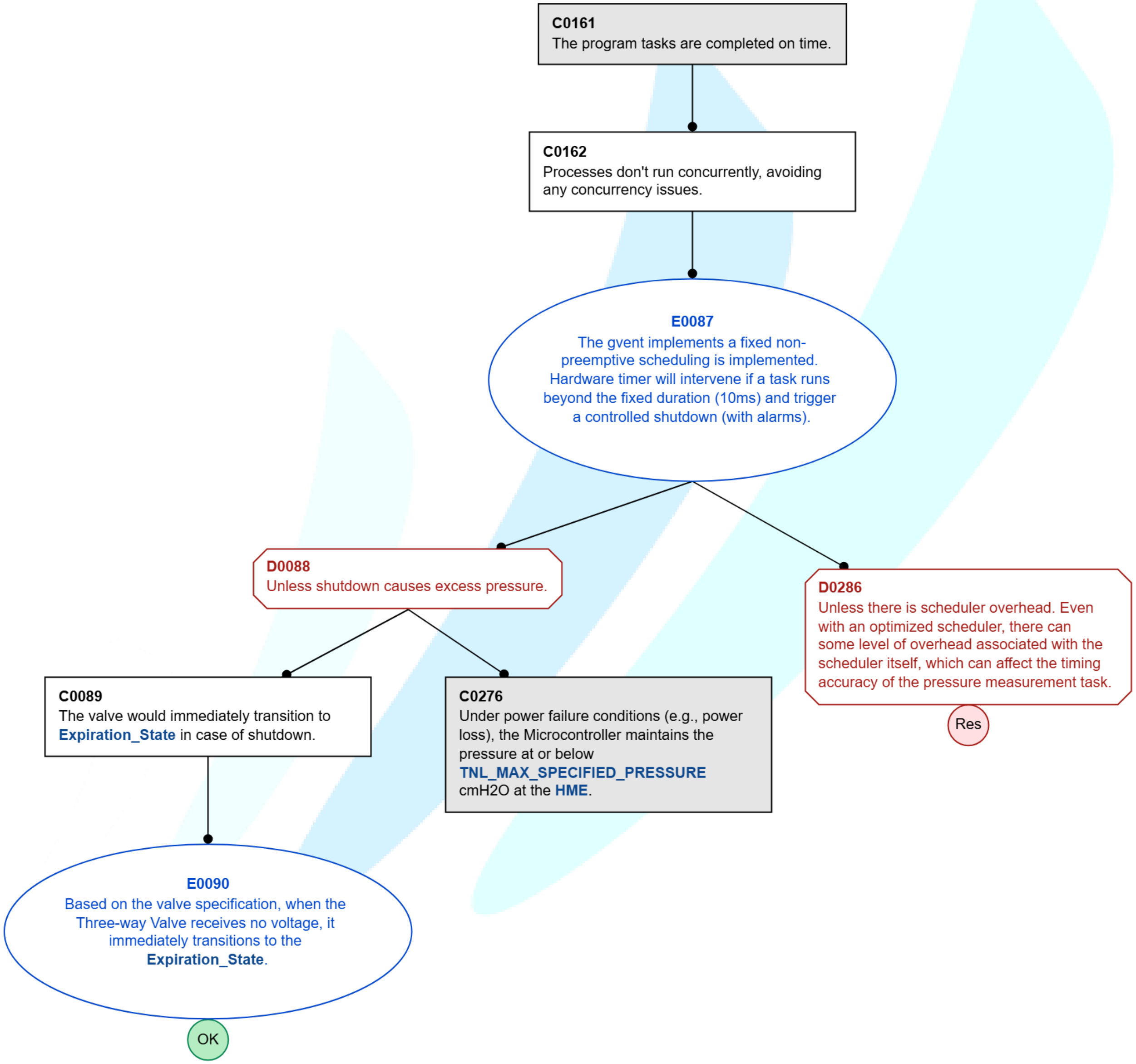
C0161
The program tasks are completed on time.

C0165
The variables selected respiratory rate, inspiratory/expiratory ratio and expiration time are safely stored in heap memory in the Arduino and can be retrieved when needed.

C0189
The expiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.

IR0120
If the time, memory, computation and communication aspects of the software works as intended, the software is able to control the three way valve according to the requirements.

C0161 - The program tasks are completed on time.			
Parent subtree(s)	C0022	**Descendant subtree(s)**	C0276
Glossary Terms	Expiration_State, TNL_MAX_SPECIFIED_PRESSURE, HME		



C0161
The program tasks are completed on time.

C0162
Processes don't run concurrently, avoiding any concurrency issues.

E0087
The gvent implements a fixed non-preemptive scheduling is implemented. Hardware timer will intervene if a task runs beyond the fixed duration (10ms) and trigger a controlled shutdown (with alarms).

D0088
Unless shutdown causes excess pressure.

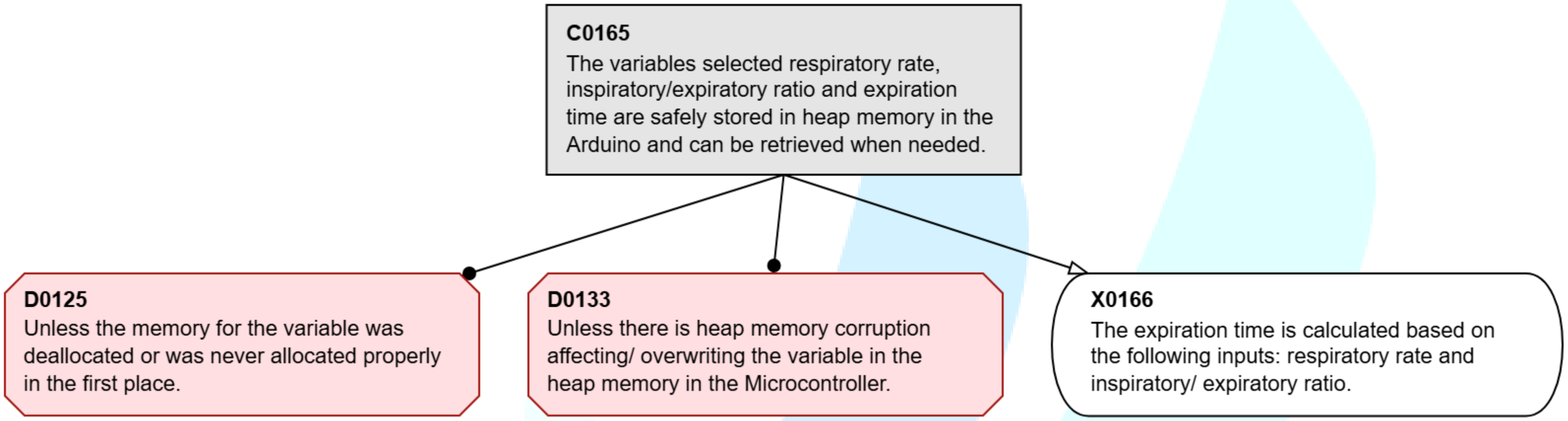
D0286
Unless there is scheduler overhead. Even with an optimized scheduler, there can some level of overhead associated with the scheduler itself, which can affect the timing accuracy of the pressure measurement task.

C0089
The valve would immediately transition to **Expiration_State** in case of shutdown.

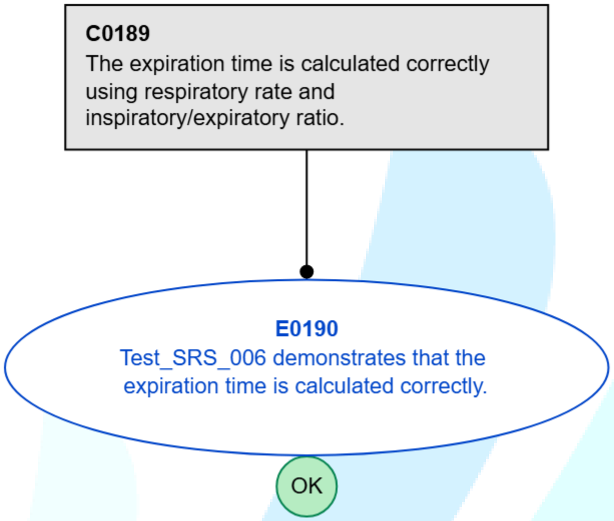
C0276
Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

E0090
Based on the valve specification, when the Three-way Valve receives no voltage, it immediately transitions to the **Expiration_State**.

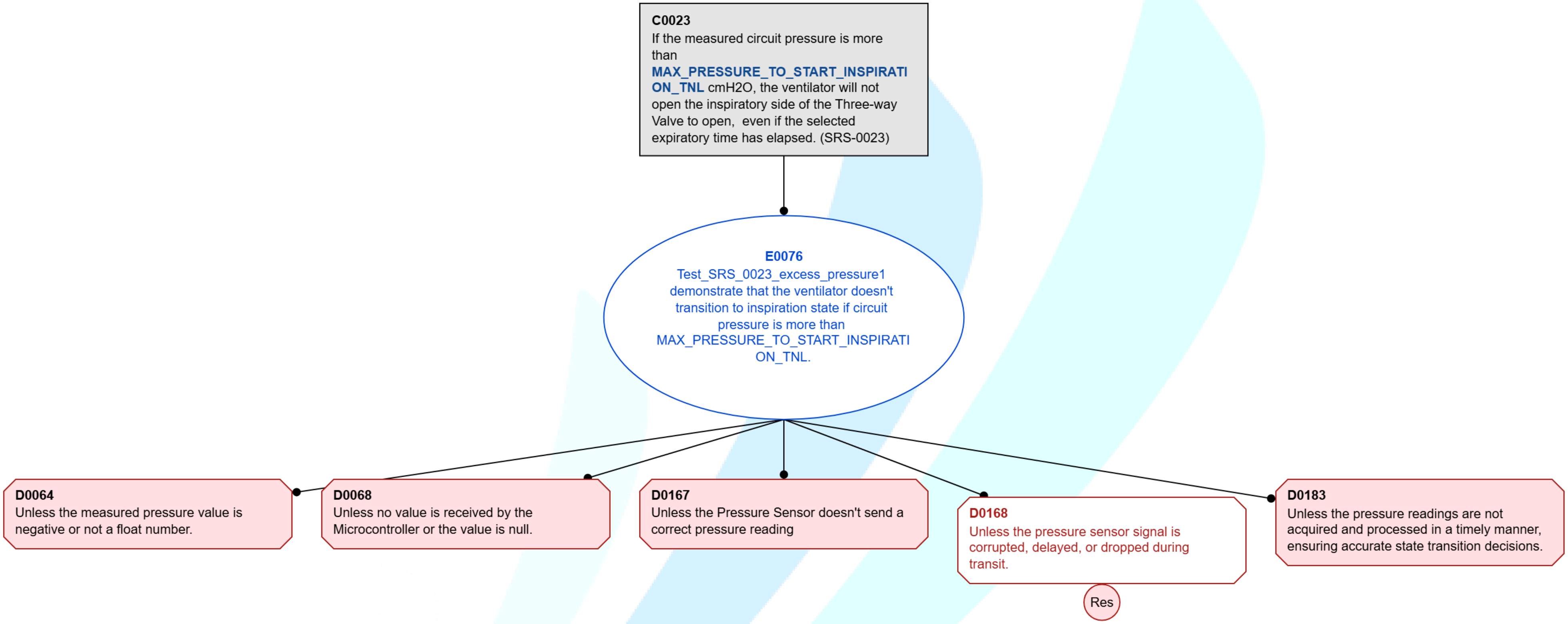
C0165 - The variables selected respiratory rate, inspiratory/expiratory ratio and expiration time are safely stored in heap memory in the Arduino an...			
Parent subtree(s)	C0022	**Descendant subtree(s)**	D0125, D0133
Glossary Terms	None		


C0165
The variables selected respiratory rate, inspiratory/expiratory ratio and expiration time are safely stored in heap memory in the Arduino and can be retrieved when needed.
D0125
Unless the memory for the variable was deallocated or was never allocated properly in the first place.
D0133
Unless there is heap memory corruption affecting/ overwriting the variable in the heap memory in the Microcontroller.
X0166
The expiration time is calculated based on the following inputs: respiratory rate and inspiratory/ expiratory ratio.

C0189 - The expiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.			
Parent subtree(s)	C0022	**Descendant subtree(s)**	None
Glossary Terms	None		


C0189
The expiration time is calculated correctly using respiratory rate and inspiratory/expiratory ratio.
E0190
Test_SRS_006 demonstrates that the expiration time is calculated correctly.
OK

C0023 - If the measured circuit pressure is more than MAX_PRESSURE_TO_START_INSPIRATION_TNL cmH2O, the ventilator will not open the inspiratory side...			
Parent subtree(s)	S0020	**Descendant subtree(s)**	D0064, D0068, D0167, D0183
Glossary Terms	MAX_PRESSURE_TO_START_INSPIRATION_TNL		



C0023
If the measured circuit pressure is more than **MAX_PRESSURE_TO_START_INSPIRATION_TNL** cmH2O, the ventilator will not open the inspiratory side of the Three-way Valve to open, even if the selected expiratory time has elapsed. (SRS-0023)

E0076
Test_SRS_0023_excess_pressure1 demonstrate that the ventilator doesn't transition to inspiration state if circuit pressure is more than MAX_PRESSURE_TO_START_INSPIRATION_TNL.

D0064
Unless the measured pressure value is negative or not a float number.

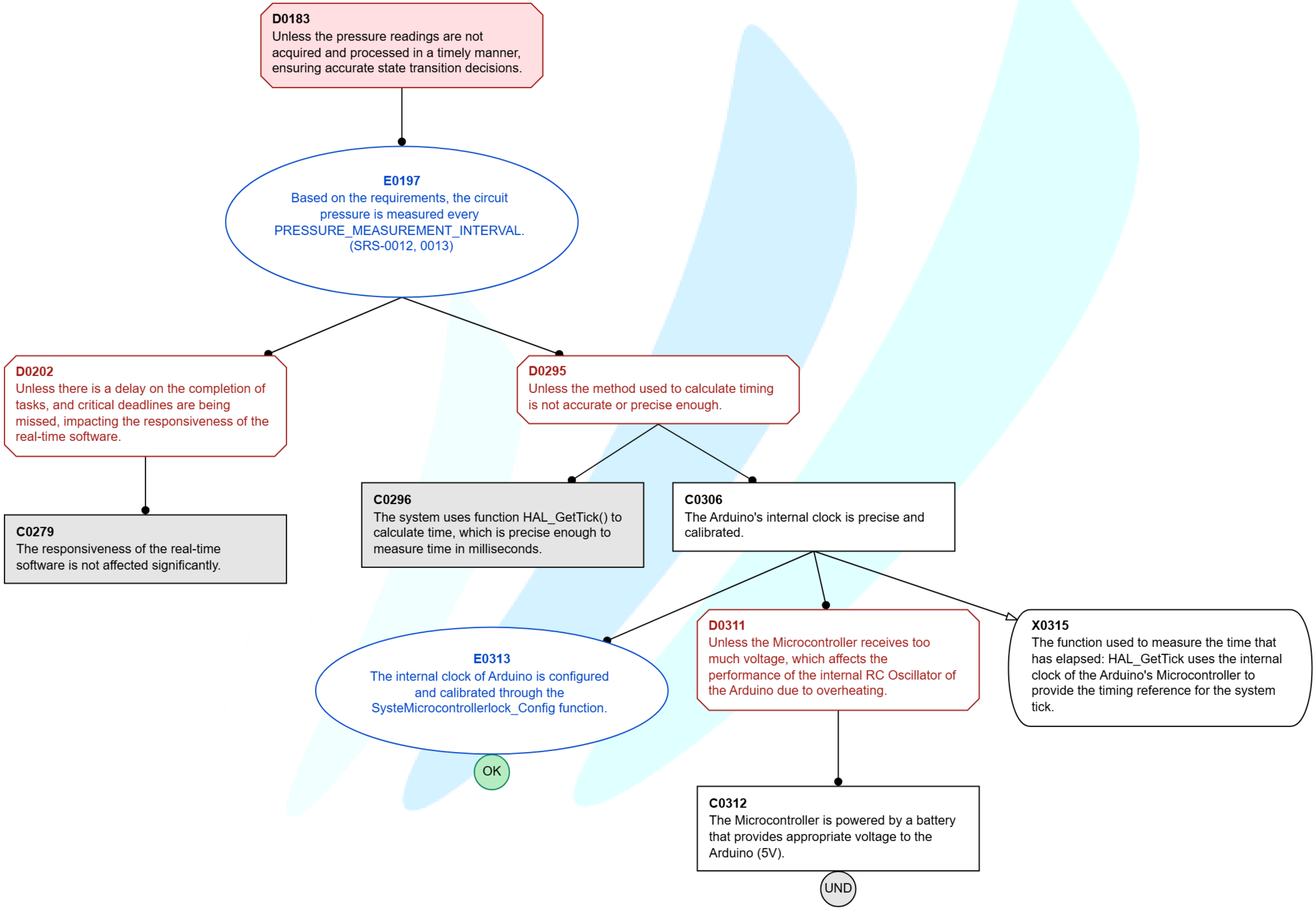
D0068
Unless no value is received by the Microcontroller or the value is null.

D0167
Unless the Pressure Sensor doesn't send a correct pressure reading

D0168
Unless the pressure sensor signal is corrupted, delayed, or dropped during transit.

D0183
Unless the pressure readings are not acquired and processed in a timely manner, ensuring accurate state transition decisions.

D0183 - Unless the pressure readings are not acquired and processed in a timely manner, ensuring accurate state transition decisions.			
Parent subtree(s)	C0023	**Descendant subtree(s)**	C0279, C0296
Glossary Terms	None		



D0183
Unless the pressure readings are not acquired and processed in a timely manner, ensuring accurate state transition decisions.

E0197
Based on the requirements, the circuit pressure is measured every PRESSURE_MEASUREMENT_INTERVAL. (SRS-0012, 0013)

D0202
Unless there is a delay on the completion of tasks, and critical deadlines are being missed, impacting the responsiveness of the real-time software.

C0279
The responsiveness of the real-time software is not affected significantly.

D0295
Unless the method used to calculate timing is not accurate or precise enough.

C0296
The system uses function HAL_GetTick() to calculate time, which is precise enough to measure time in milliseconds.

C0306
The Arduino's internal clock is precise and calibrated.

E0313
The internal clock of Arduino is configured and calibrated through the SysteMicrocontrollerlock_Config function.

OK

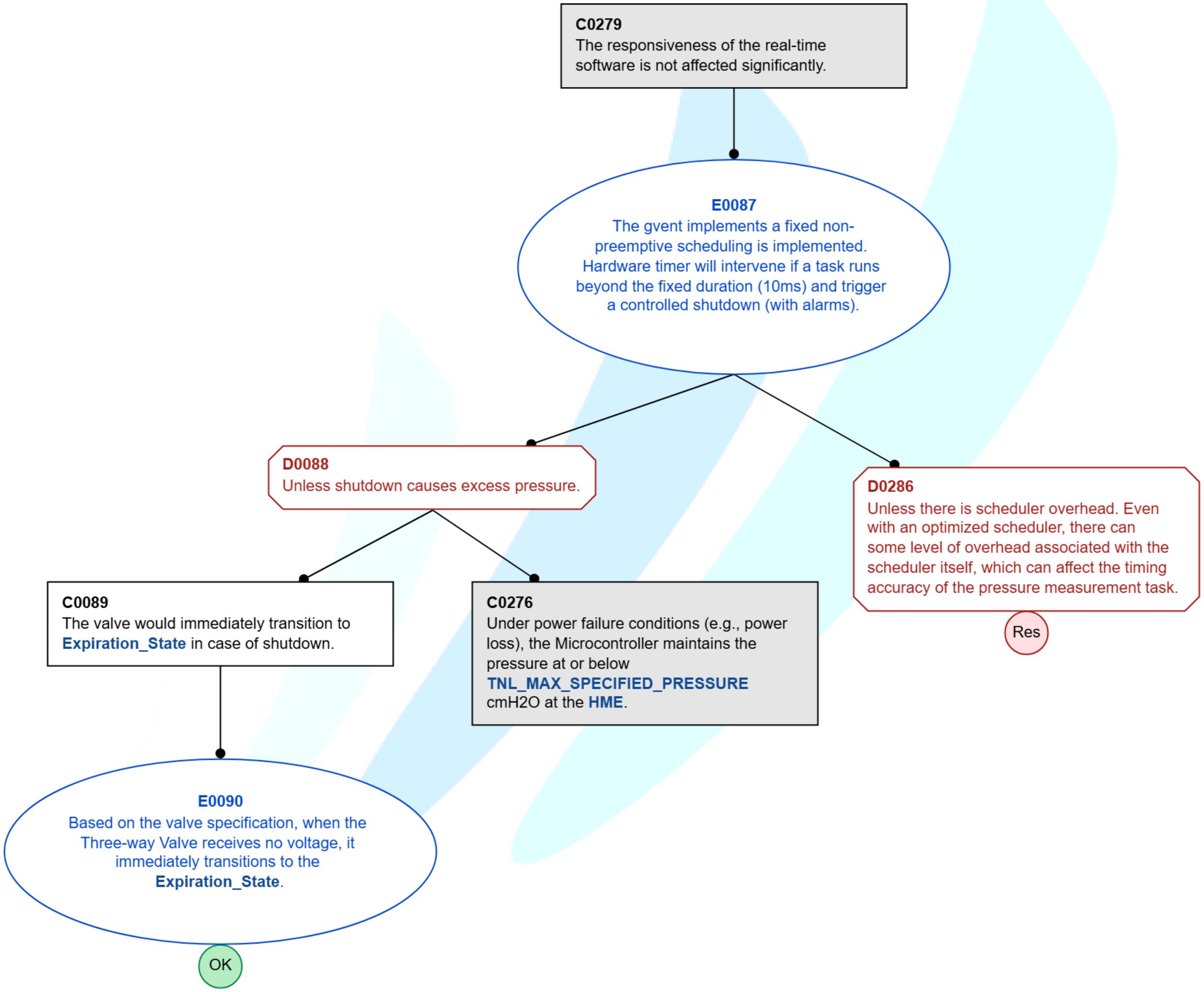
D0311
Unless the Microcontroller receives too much voltage, which affects the performance of the internal RC Oscillator of the Arduino due to overheating.

C0312
The Microcontroller is powered by a battery that provides appropriate voltage to the Arduino (5V).

UND

X0315
The function used to measure the time that has elapsed: HAL_GetTick uses the internal clock of the Arduino's Microcontroller to provide the timing reference for the system tick.

C0279 - The responsiveness of the real-time software is not affected significantly.			
Parent subtree(s)	C0196	**Descendant subtree(s)**	C0276
Glossary Terms	Expiration_State, TNL_MAX_SPECIFIED_PRESSURE, HME		



C0279
The responsiveness of the real-time software is not affected significantly.

E0087
The gvent implements a fixed non-preemptive scheduling is implemented. Hardware timer will intervene if a task runs beyond the fixed duration (10ms) and trigger a controlled shutdown (with alarms).

D0088
Unless shutdown causes excess pressure.

D0286
Unless there is scheduler overhead. Even with an optimized scheduler, there can some level of overhead associated with the scheduler itself, which can affect the timing accuracy of the pressure measurement task.

Res

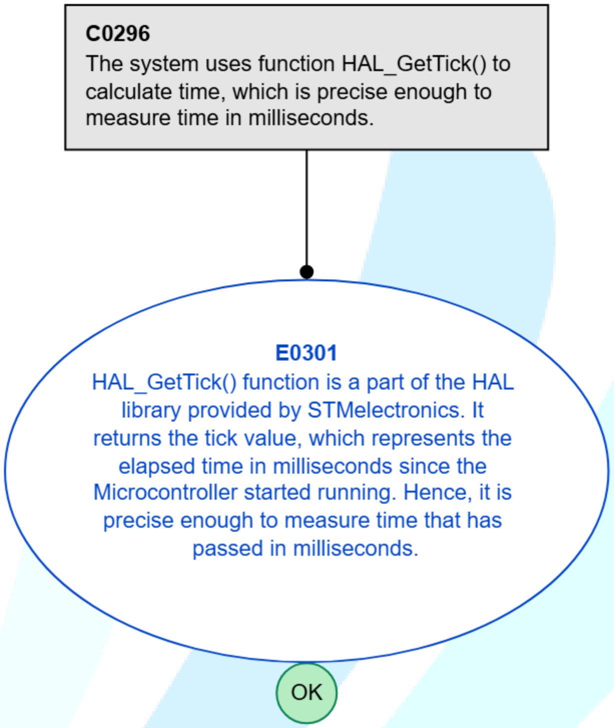
C0089
The valve would immediately transition to **Expiration_State** in case of shutdown.

C0276
Under power failure conditions (e.g., power loss), the Microcontroller maintains the pressure at or below **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

E0090
Based on the valve specification, when the Three-way Valve receives no voltage, it immediately transitions to the **Expiration_State**.

OK

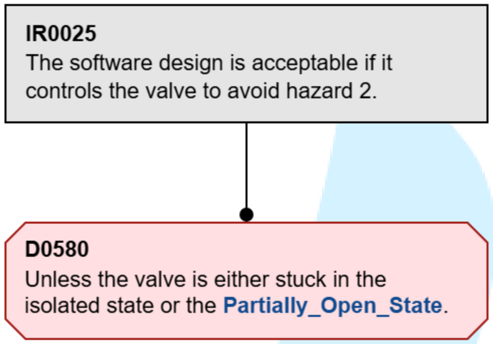
C0296 - The system uses function HAL_GetTick() to calculate time, which is precise enough to measure time in milliseconds.			
Parent subtree(s)	C0196, C0466	**Descendant subtree(s)**	None
Glossary Terms	None		



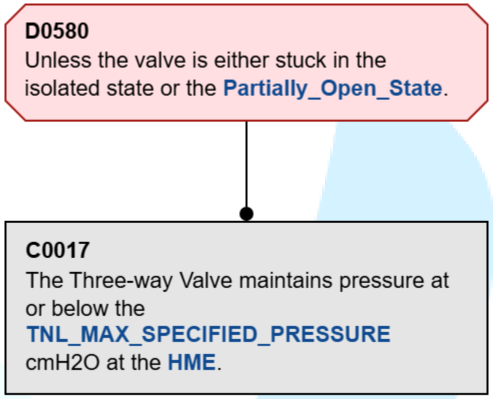
C0296
The system uses function HAL_GetTick() to calculate time, which is precise enough to measure time in milliseconds.

E0301
HAL_GetTick() function is a part of the HAL library provided by STMelectronics. It returns the tick value, which represents the elapsed time in milliseconds since the Microcontroller started running. Hence, it is precise enough to measure time that has passed in milliseconds.

IR0025 - The software design is acceptable if it controls the valve to avoid hazard 2.			
Parent subtree(s)	S0020	**Descendant subtree(s)**	D0580
Glossary Terms	Partially_Open_State		


IR0025
The software design is acceptable if it controls the valve to avoid hazard 2.
D0580
Unless the valve is either stuck in the isolated state or the Partially_Open_State.

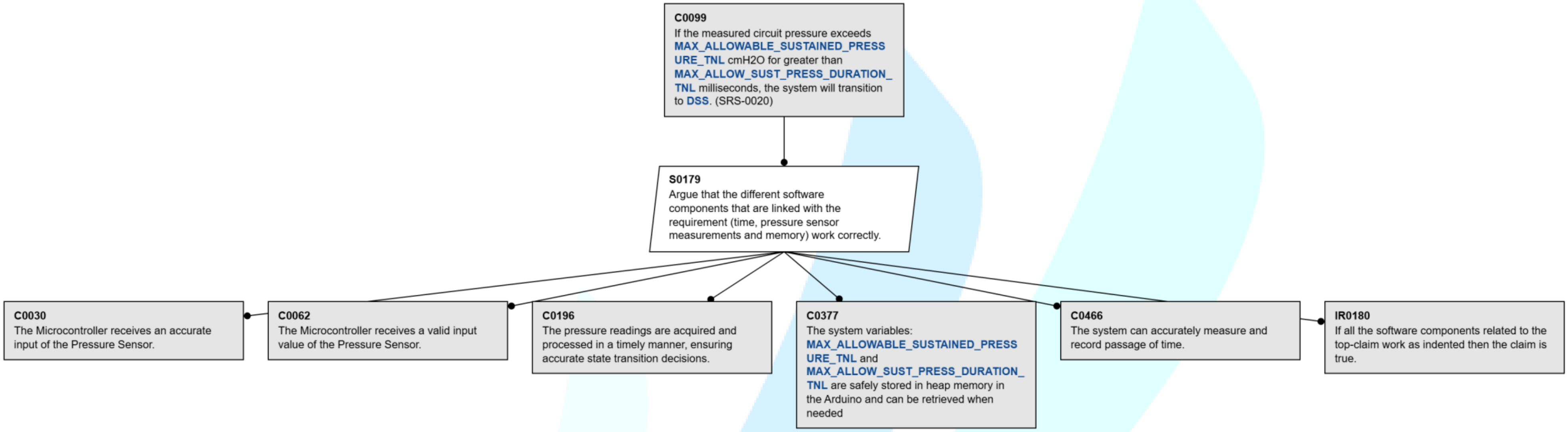
D0580 - Unless the valve is either stuck in the isolated state or the Partially_Open_State.			
Parent subtree(s)	IR0025	**Descendant subtree(s)**	C0017
Glossary Terms	TNL_MAX_SPECIFIED_PRESSURE, HME, Partially_Open_State		



D0580
Unless the valve is either stuck in the isolated state or the **Partially_Open_State**.

C0017
The Three-way Valve maintains pressure at or below the **TNL_MAX_SPECIFIED_PRESSURE** cmH2O at the **HME**.

C0099 - If the measured circuit pressure exceeds MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL cmH2O for greater than MAX_ALLOW_SUST_PRESS_DURATION_TNL milli...			
Parent subtree(s)	S0020	**Descendant subtree(s)**	C0030, C0062, IR0180, C0196, C0377, C0466
Glossary Terms	MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL, MAX_ALLOW_SUST_PRESS_DURATION_TNL, DSS		



C0099
If the measured circuit pressure exceeds MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL cmH2O for greater than MAX_ALLOW_SUST_PRESS_DURATION_TNL milliseconds, the system will transition to DSS. (SRS-0020)

S0179
Argue that the different software components that are linked with the requirement (time, pressure sensor measurements and memory) work correctly.

C0030
The Microcontroller receives an accurate input of the Pressure Sensor.

C0062
The Microcontroller receives a valid input value of the Pressure Sensor.

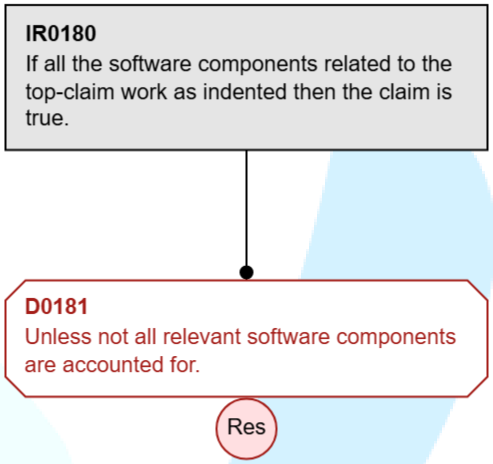
C0196
The pressure readings are acquired and processed in a timely manner, ensuring accurate state transition decisions.

C0377
The system variables: MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL and MAX_ALLOW_SUST_PRESS_DURATION_TNL are safely stored in heap memory in the Arduino and can be retrieved when needed

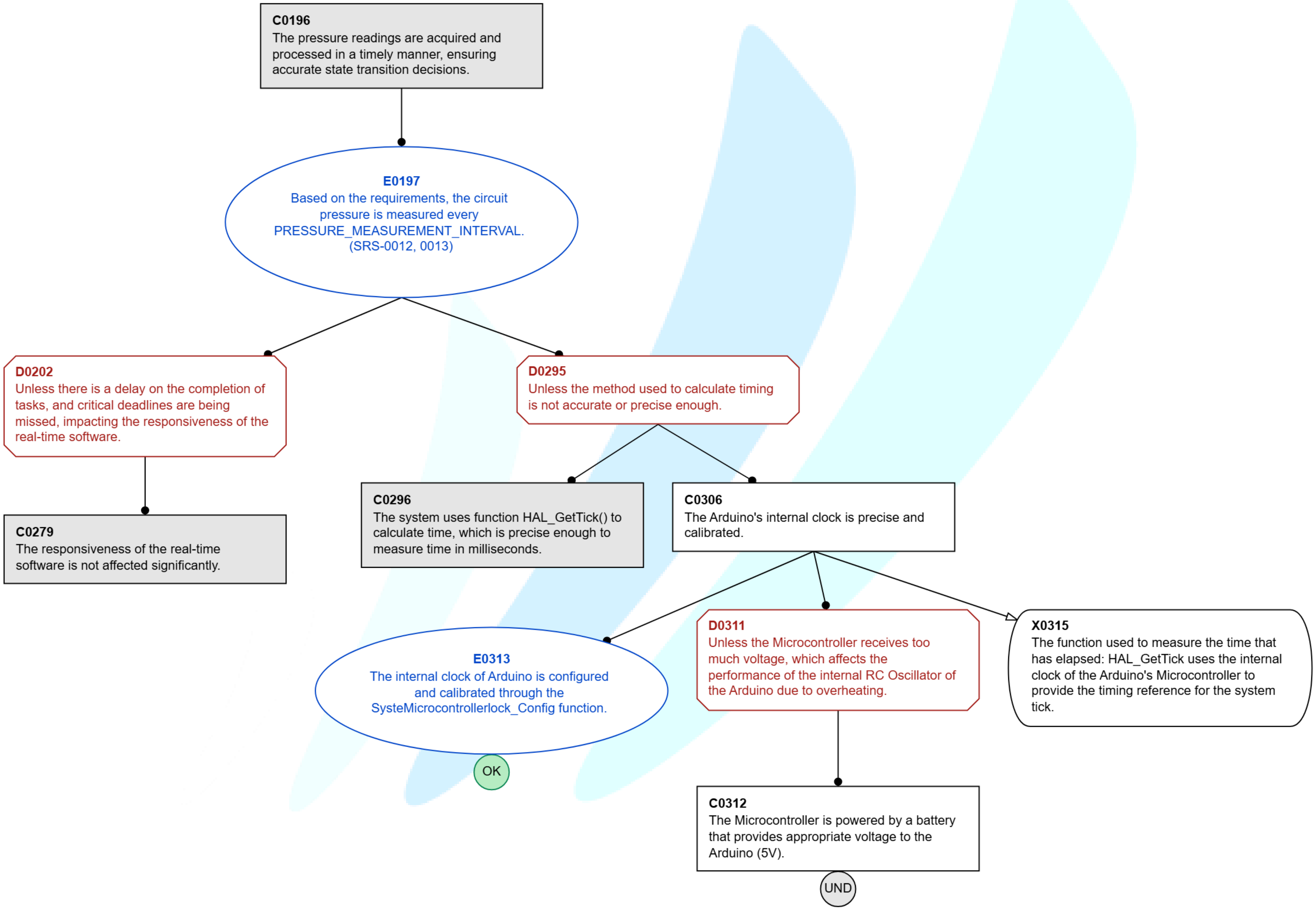
C0466
The system can accurately measure and record passage of time.

IR0180
If all the software components related to the top-claim work as indented then the claim is true.

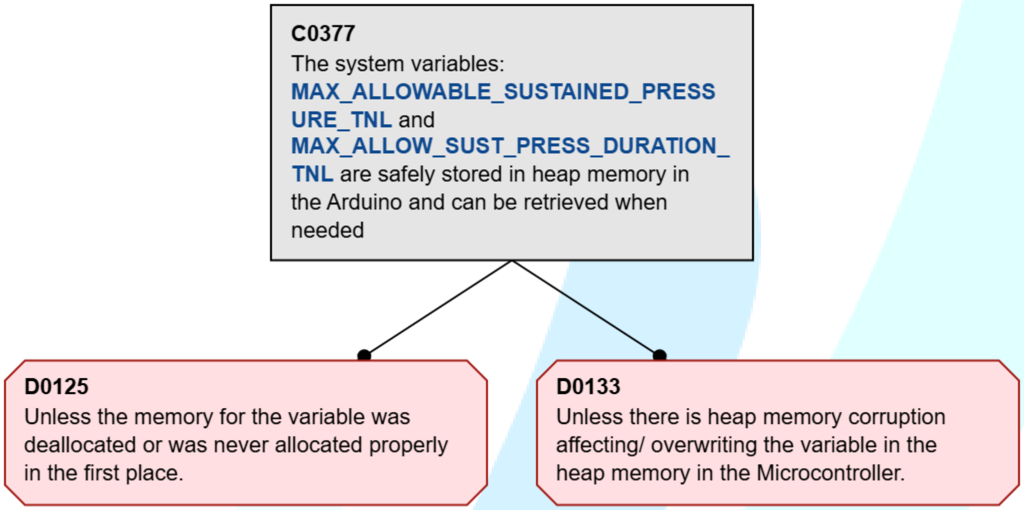
IR0180 - If all the software components related to the top-claim work as indented then the claim is true.			
Parent subtree(s)	C0099	**Descendant subtree(s)**	None
Glossary Terms	None		


IR0180
If all the software components related to the top-claim work as indented then the claim is true.
D0181
Unless not all relevant software components are accounted for.
Res

C0196 - The pressure readings are acquired and processed in a timely manner, ensuring accurate state transition decisions.			
Parent subtree(s)	C0099	**Descendant subtree(s)**	C0279, C0296
Glossary Terms	None		


C0196
The pressure readings are acquired and processed in a timely manner, ensuring accurate state transition decisions.
E0197
Based on the requirements, the circuit pressure is measured every PRESSURE_MEASUREMENT_INTERVAL. (SRS-0012, 0013)
D0202
Unless there is a delay on the completion of tasks, and critical deadlines are being missed, impacting the responsiveness of the real-time software.
D0295
Unless the method used to calculate timing is not accurate or precise enough.
C0279
The responsiveness of the real-time software is not affected significantly.
C0296
The system uses function HAL_GetTick() to calculate time, which is precise enough to measure time in milliseconds.
C0306
The Arduino's internal clock is precise and calibrated.
E0313
The internal clock of Arduino is configured and calibrated through the SysteMicrocontrollerlock_Config function.
OK
D0311
Unless the Microcontroller receives too much voltage, which affects the performance of the internal RC Oscillator of the Arduino due to overheating.
X0315
The function used to measure the time that has elapsed: HAL_GetTick uses the internal clock of the Arduino's Microcontroller to provide the timing reference for the system tick.
C0312
The Microcontroller is powered by a battery that provides appropriate voltage to the Arduino (5V).
UND

C0377 - The system variables: MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL and MAX_ALLOW_SUST_PRESS_DURATION_TNL are safely stored in heap memory in the Ard...			
Parent subtree(s)	C0099	**Descendant subtree(s)**	D0125, D0133
Glossary Terms	MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL, MAX_ALLOW_SUST_PRESS_DURATION_TNL		

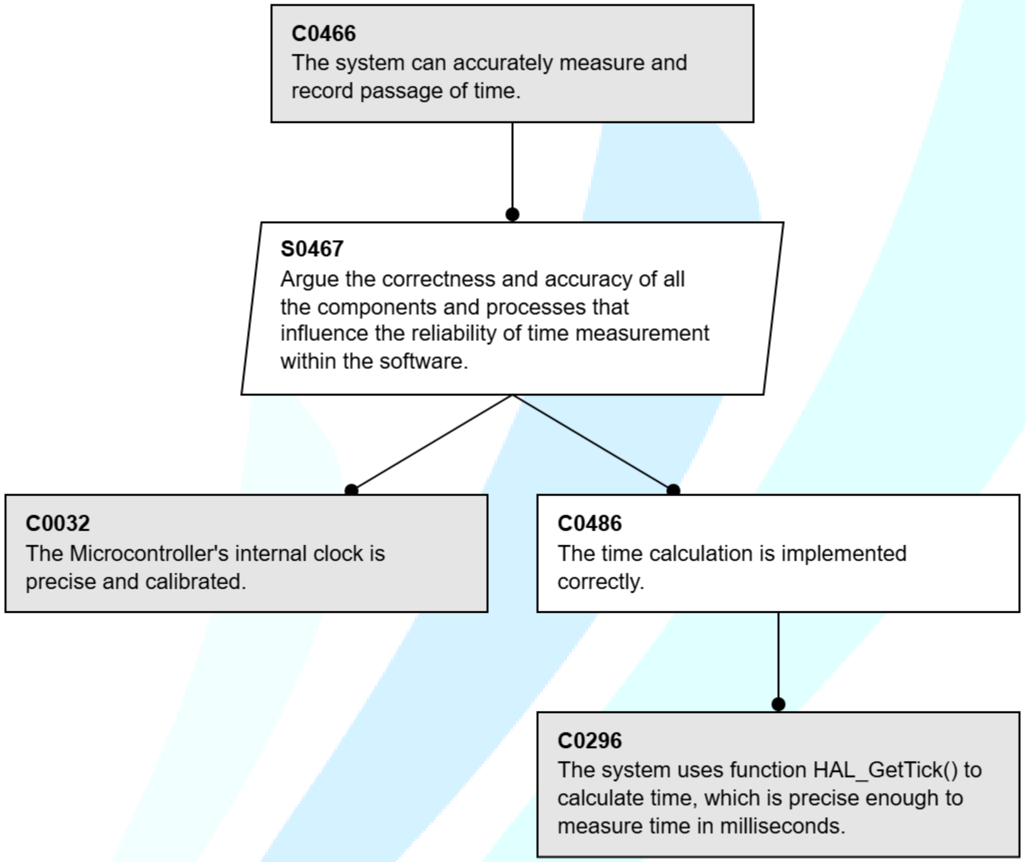


C0377
The system variables: **MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL** and **MAX_ALLOW_SUST_PRESS_DURATION_TNL** are safely stored in heap memory in the Arduino and can be retrieved when needed

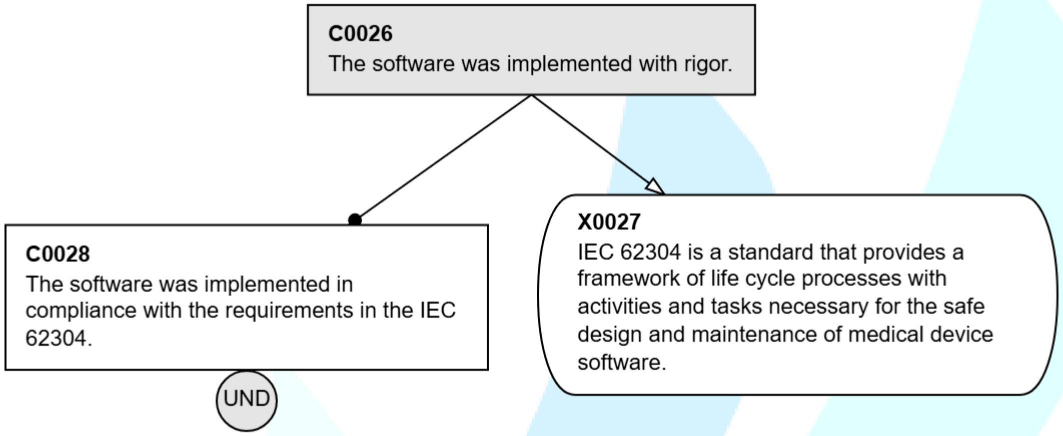
D0125
Unless the memory for the variable was deallocated or was never allocated properly in the first place.

D0133
Unless there is heap memory corruption affecting/ overwriting the variable in the heap memory in the Microcontroller.

C0466 - The system can accurately measure and record passage of time.			
Parent subtree(s)	C0099	**Descendant subtree(s)**	C0032, C0296
Glossary Terms	None		


C0466
The system can accurately measure and record passage of time.
S0467
Argue the correctness and accuracy of all the components and processes that influence the reliability of time measurement within the software.
C0032
The Microcontroller's internal clock is precise and calibrated.
C0486
The time calculation is implemented correctly.
C0296
The system uses function HAL_GetTick() to calculate time, which is precise enough to measure time in milliseconds.

C0026 - The software was implemented with rigor.			
Parent subtree(s)	C0005	**Descendant subtree(s)**	None
Glossary Terms	None		



C0026
The software was implemented with rigor.

C0028
The software was implemented in compliance with the requirements in the IEC 62304.

X0027
IEC 62304 is a standard that provides a framework of life cycle processes with activities and tasks necessary for the safe design and maintenance of medical device software.

Glossary

Term	Definition
DSS	*Design Safety State - In this state the expiratory side of the Three way valve is open. The state persists until the system is power cycled.*
MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL	*The maximum pressure (cmH2O) the patient's airways can withstand without being harmed irrespective of the duration of the over-pressure condition.*
TIME_TO_TRANSITION_TO_DSS_TNL	*The amount of time (ms) required for the ventilator to transition to Design Safety State.*
HME	*Heated Moisture Exchanger*
MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL	*the circuit pressure (cmH2O) setpoint that if exceeded for MAX_ALLOWABLE_SUSTAINED_PRESSURE_DURATION_TNL ms, would be considered unsafe by the operator.*
MAX_ALLOW_SUST_PRESS_DURATION_TNL	*MAX_ALLOWABLE_SUSTAINED_PRESSURE_DURATION_TNL – the maximum time (ms) that the circuit pressure can be at or above TNL_MAX_ALLOWABLE_SUSTAINED_PRESSURE_CSP cmH2O before being considered unsafe by the operator.*
H-1	*H1 occurs when the pressure at the HME momentarily exceeds MAX_ALLOWABLE_MOMENTARY_PRESSURE_TNL cmH2O for any period of time.*
H-2	*H2 occurs when the pressure at the HME exceeds MAX_ALLOWABLE_SUSTAINED_PRESSURE_TNL cmH2O for a period of time exceeding MAX_ALLOWABLE_SUSTAINED_PRESSURE_DURATION_TNL milliseconds.*
TNL_MAX_SPECIFIED_PRESSURE	*The current maximum pressure set-point that the operator (e.g., doctor) has set.*
MAX_PRESSURE_TO_START_INSPIRATION_TNL	*The maximum pressure (cmH2O) in the circuit so that the inspiratory side of the Three-way valve may be opened.*
Inspiration_State	*When (air can move between the Gravity Chamber and the HME) and (air cannot move between the HME and the PEEP valve).*
Expiration_State	*When (air can move between the PEEP valve and the HME) and (air cannot move between the Gravity Chamber and the PEEP valve)*
PEEP	*Positive End Expiratory Pressure*
TNL_MAX_PEEP_PRESSURE	*The set-point selected by the operator for the Positive End Expiratory Pressure. This is the pressure in cmH2O that the patient's lungs will dissipate to during the Inspiration_State*
V&V	*Verification and Validation*

Partially_Open_State	*The “partially open state” occurs when the Three-way Valve is not in fully Inspiratorion_State or Expiration_State.*
Isolated_State	*The "isolated state" occurs when air cannot flow into nor out of the HME. This occurs when either: a) the HME port of the 3-way valve is blocked or b) both the inspiratory and expiratory ports of the 3-way valve are blocked.*
RMVS	*Rapidly Manufactured Ventilator Systems*
FMEA	*Failure Mode and Effects Analysis*
STPA	*System-Theoretic Process Analysis*

END