VARIASS B.V. &
PLASMAMADE B.V.

28-03-2019

PLASMAMADE AIR FILTER FAIL-SAFE CONSTRUCTION.

AUTHOR & PERFORMANCE:

Document written by: Variass B.V. .

Text and figures converted to the usual template: Sander van Gameren, PlasmaMade B.V. .

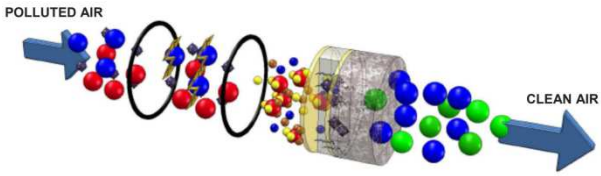
SUMMARY AND FRAMEWORK:

The Air filter fail-safe construction is explained in this document. The air filter fail-safe is a circuit that can be seen between the power adapter and the internal power supply, see figure 2 in this document. This document has been supplied by Variass B.V. and by PlasmaMade B.V. put in the usual template.

INDEX:

1 INTRODUCTION.

The main function of the PlasmaMade ‘Air filter’ is to purify contaminated air in the kitchen industry. The filter can be seen as four different systems. See figure 1 below.



Figuur 1: Weergave van de werking van het plasmafilter systeem van PlasmaMade.

First two passive filters, a fiberglass and carbon filter. In addition, two active systems, an ozone generator and an electrostatic filter.
The active part of the "Air filter" is controlled via software on a microcontroller (MCU). The main function of the MCU is to switch on both active filters when there is sufficient air flow and to switch off the ozone generator when the desired ozone is reached. The MCU with its software ensures that the amount of ozone generated cannot exceed the desired and set value.

From a "fail-safe" point of view, it is desirable that an independently functioning safety circuit is applied in addition to the MCU to prevent a situation from arising that more than the desired amount of ozone is generated and ends up in the room.

Hereby the Carbon cannot be seen as a 'fail-safe' construction because carbon cannot be guaranteed as a workable substance over time, carbon will always decrease because it is an absorbent material and therefore absorbs substances and can therefore be saturated and therefore cannot be classified as 'fail-safe',.

2. RESULT (OACS, ozone active control system)

2.1Watchdog stage 1 (software)

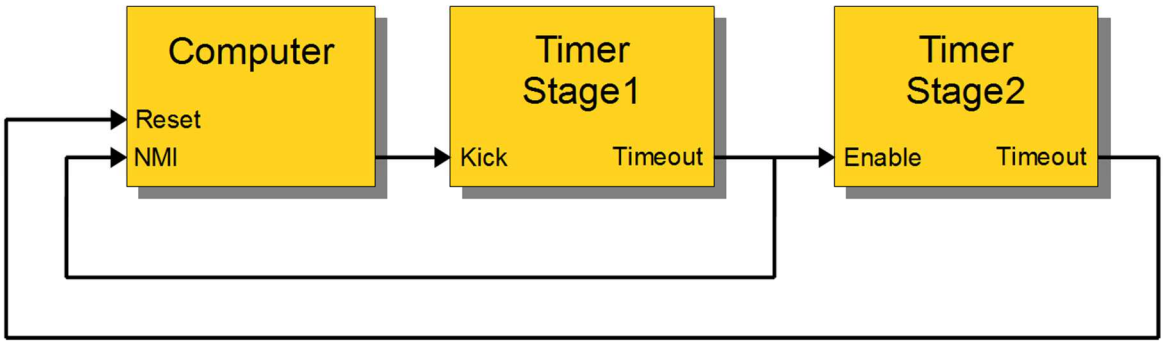
The first safety feature of the PlasmaMade system is the so-called Watchdog, A watchdog timer (sometimes called a *computer operating properly* or *COP* timer, or simply a *watchdog*) is an electronic timer that is used to detect and recover from computer malfunctions. During normal operation, the computer regularly resets the watchdog timer to prevent it from elapsing, or "timing out". If, due to a hardware fault or program error, the computer fails to reset the watchdog, the timer will elapse and generate a timeout signal. The timeout signal is used to initiate corrective action or actions. The corrective actions typically include placing the computer system in a safe state and restoring normal system operation.

Watchdog timers are commonly found in embedded systems and other computer-controlled equipment where humans cannot easily access the equipment or would be unable to react to faults in a timely manner. In such systems, the computer cannot depend on a human to invoke a reboot if it hangs; it must be self-reliant. For example, remote embedded systems such as space probes are not physically accessible to human operators; these could become permanently disabled if they were unable to autonomously recover from faults. A watchdog timer is usually employed in cases like these. Watchdog timers may also be used when running untrusted code in a sandbox, to limit the CPU time available to the code and thus prevent some types of Bug's in the system a reset will be done.

A watchdog timer may initiate any of several types of corrective action, including maskable interrupt, non-maskable interrupt, processor reset, fail-safe state activation, power cycling, or combinations of these. Depending on its architecture, the type of corrective action or actions that a watchdog can trigger may be fixed or programmable. Some computers (e.g., PC compatibles) require a pulsed signal to invoke a processor reset. In such cases, the watchdog typically triggers a processor reset by activating an internal or external pulse generator, which in turn creates the required reset pulses.[3]

In embedded systems and control systems, watchdog timers are often used to activate fail-safe circuitry. When activated, the fail-safe circuitry forces all control outputs to safe states (e.g., turns off motors, heaters, and high-voltages) to prevent injuries and equipment damage while the fault persists. In a two-stage watchdog, the first timer is often used to activate fail-safe outputs and start the second timer stage; the second stage will reset the computer if the fault cannot be corrected before the timer elapses.

Watchdog timers are sometimes used to trigger the recording of system state information—which may be useful during fault recovery[3]—or debug information (which may be useful for determining the cause of the fault) onto a persistent medium. In such cases, a second timer—which is started when the first timer elapses—is typically used to reset the computer later, after allowing sufficient time for data recording to complete. This allows time for the information to be saved, but ensures that the computer will be reset even if the recording process fails.



the above diagram shows a likely configuration for a two-stage watchdog

For example, the above diagram shows a likely configuration for a two-stage watchdog timer. During normal operation the computer regularly kicks Stage1 to prevent a timeout. If the computer fails to kick Stage1 (e.g., due to a hardware fault or programming error), Stage1 will eventually timeout. This event will start the Stage2 timer and, simultaneously, notify the computer (by means of a non-maskable interrupt) that a reset is imminent. Until Stage2 times out, the computer may attempt to record state information, debug information, or both. The computer will be reset upon Stage2 timeout.

2.2 Fail-safe PCBA (Hardware)

For a correct "fail-safe" function on the ozone generator, it was decided to design a totally independent functioning safety circuit. The following functional requirements have been drawn up for this:

- The "fail-safe" circuit must work completely independently. So no action or interaction with MCU or air-flow sensor.
- After intervention of "fail-safe" the total "Air filter" must be permanently disabled. It should not be possible for the end user to use the "Air filter" again.
- Since the "fail-safe" function can be seen as a safety circuit, it is desirable to include it in the production test procedure.

Based on these requirements, it is decided to develop a circuit with which it can be independently established that the ozone generator is active longer than desired. After this, the system hardware must be moderately disabled.

Fail-safe Solution

To meet the above requirements, the following improvement has been chosen:

- Detection that ozone generator is active longer than desired.

    o By measuring the supply current, it is detected that the ozone generator is active. A time constant and current limit determine that the ozone generator is active for longer than desired.

- Permanent system shutdown.

    o By activating the fuse in the primary power supply system, the total "Air filter" is permanently disabled.
    o Because the fuse is not a replaceable part of the PCBA, it is not possible for the end user to reactivate the 'Air filter'.

- Test of "fail-safe" function.

    o The "fail-safe" function is included in the functional production test procedure.

Below, in figure 2, the block diagram overview of the "Plasmamade" Air filter.

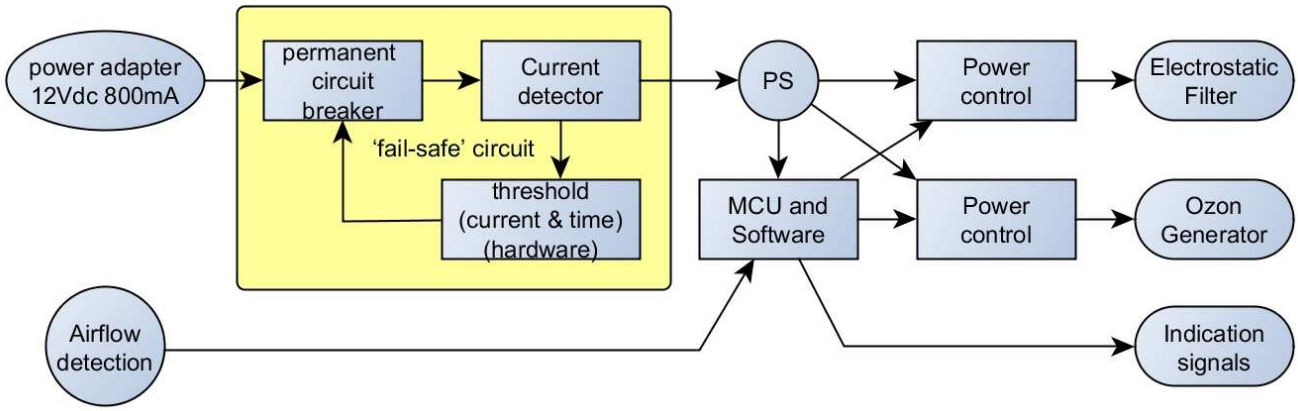


Figure 2: Block diagram overview of the "PlasmaMade" Air filter.

We call this system OACS ozone active control system and IACS ionization active control system.

3. CONCLUSION.

- The ozone generator is controlled via two separate systems, the MCU with watchdog and the "fail-safe" circuit.
- The watchdog prevents the MCU for a bug and will reset the MCU to his first program and will start again in his first setting program mode.
- The "fail-safe" circuit prevents the ozone generator from being active for longer than desired (error situation).
- If the "fail-safe" circuit has intervened within an Air filter, this spoiling system is permanently disabled. There is no possibility to restore the system for the end user.

  The "fail-safe" function is included in the functional EoL production test procedure, for 100% security.

EoL End-of-Line

End-of-line (EoL) testers are responsible for testing the overall functionality of the product during the manufacturing process. Under the harsh conditions of the manufacturing environment, test systems must simulate all the relevant conditions, whilst at the same measuring the responses of the equipment being tested.
In series production, a high testing throughput rate is crucial. For this reason, the test procedures developed in prototype testing are optimised in order to achieve a short cycle time.
A stable electromechanical design is every bit as important here as high-performance hardware and software architecture.

4. References.

1 "The Grenade Timer: Fortifying the Watchdog Timer Against Malicious Mobile Code" by Frank Stajano and Ross Anderson (2000).

2 *Lamberson, Jim. "Single and Multistage Watchdog Timers" (PDF). Sensoray. Retrieved 10 September 2013.*