Brownout protection

The most dangerous moment in a flight computer's life is the one it creates itself: firing an output. A charge can demand tens of amps from the battery whenever your configuration fires it, and if that demand drags the supply down far enough, an unprotected computer resets in mid-air, at precisely the moment it must not. Jupiter's answer is a system with a strong claim behind it: firing an output, any output, into any load, on any battery, cannot brown out the computer. This page explains how that claim is engineered, from the measurement underneath it to the regulator that acts on it to the hard floor beneath everything.

In plain English: this system lets the outputs consume as much power as the battery can provide, after the power the computer itself needs has been set aside. The computer's share is never negotiable; everything beyond it goes to the fire.

The reservoir is also the measurement

As covered on the Power supply page, a 0.1 F supercapacitor sits on the main 4.2 V rail, backing the board, never the outputs. During a fire it does two jobs at once. It is the board's energy reserve, holding the electronics up through the disturbance. And it is a live instrument: when an output loads the battery, the way this capacitor's voltage moves under that load reveals, moment by moment, what the battery can actually deliver, not its label, not its age, its real capability right now, with this igniter, at this temperature. Everything else on this page is built on reading that signal well and acting on it correctly.

Reading it well is its own discipline. The capacitor voltage is sampled at 50 Hz continuously, firing or not, and no decision anywhere in the system is ever made from a single raw sample, because during protection the capacitor voltage is a sawtooth and one sample only tells you where in the ripple you happened to look. Instead, every sample becomes a damped working value, the mean of the last 300 milliseconds, and that is the only number the protection logic sees. Alongside the level, the system measures the trend, which way the capacitor is heading over the last half second, because as you'll see, level and trend can disagree, and when they do, the trend is usually telling the truth.

The scale, honestly drawn

The capacitor's charge is expressed as a percentage with a deliberately honest zero: 100 percent is the full 4.2 V rail, and 0 percent is 3.5 V, which is not where the board dies but where risk begins, the voltage at which the 3.3 V regulator that feeds the processor and sensors starts to lose its grip. Every threshold in this system is placed relative to that meaning of zero.

First, the igniter gets its chance

When a fire begins and the capacitor first dips below the protection threshold, nothing is rationed for the first 150 milliseconds. That grace window is unconditional, and it exists because most igniters fire well within it: protection that beat the igniter to the punch would be worse than no protection at all. A capacitor collapsing fast through the window is exactly the case the window is for, the match gets its full-current run, and the systems below stand ready the moment the window closes.

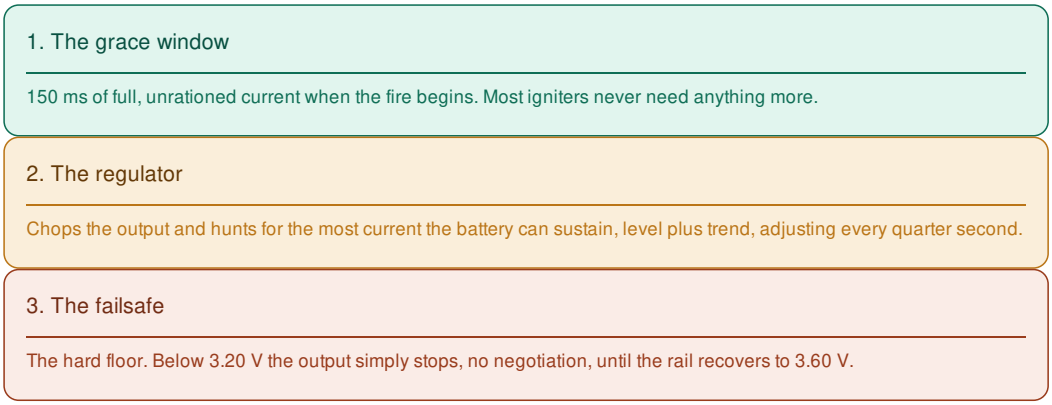
The regulator: spending exactly what the battery can afford

If the capacitor is still below the protection threshold when the grace expires, the output is chopped: switched rapidly on and off, 10 times a second by default, and the fraction of each cycle spent on, the duty, becomes the knob the system turns. What follows is best understood as an optimiser rather than a limiter: its goal is to find and hold the most firing current the battery can actually sustain.

Its logic runs on the capacitor's level and trend together, deciding every quarter of a second. While the capacitor is holding steady or climbing, the battery is proving it can give more, so the duty steps up, four percent at a time, spending that proven headroom into the igniter. While the capacitor is falling, the duty holds where it is and lets the situation declare itself: raising into a fall would chase the capacitor down, and cutting a fire that may be about to stabilise would throw away current for nothing. Only when the capacitor has been spent right down to its low reserve, and is still not recovering, do the cuts begin, and then they keep coming while it keeps dropping, stepping down twice as fast once the reserve is genuinely low. On a battery with headroom, the practical result is a duty that ramps back up and a fire that completes at or near full current with the capacitor never approaching the reserve. On a battery at its limit, the duty settles wherever supply meets demand. Only a fire the battery genuinely cannot afford ever walks the capacitor down to the reserve line, and that spending is deliberate: charge held back

during a fire is current denied to the igniter for no benefit, because the capacitor refills for free the instant the output stops.

The trend's veto works both ways. Below the reserve but already climbing? The recovery is happening by itself, and cutting duty would slow the fire to speed up something needing no help, so the cut is vetoed. Level and trend together, every quarter second: direction from where the capacitor is, permission from where it's going. Two more courtesies round it out: the duty never drops below 10 percent, because a slow ignition beats none at all, and in the last second of a timed fire the regulator simply holds flat and lets the fire have whatever remains, since the capacitor refills the moment it ends anyway.



Three independent layers: the failsafe does not negotiate with the regulator, and neither waits for the other

The failsafe underneath

The regulator is deliberately measured and patient, which is right for finding an operating point and wrong for a last line of defence, so beneath it sits something with no patience at all. If the damped working voltage falls below 3.20 V, the output stops outright, no ramp, no duty, no negotiation, and does not resume until the rail has recovered above 3.60 V. It is fully independent of the regulator on purpose: a fire can start with a healthy capacitor at full duty and collapse it inside the grace window, before the regulator has even engaged, and a failsafe that waited for the regulator would miss the fastest collapse there is. It also keeps evaluating after the output stops, because the output stopping is exactly how the rail recovers and the failsafe clears itself.

Settings

Three settings shape the system, and the defaults suit almost everyone. supercap_protect sets the charge percentage below which protection is armed, 50 to 80 percent, default 80. supercap_pwm sets the duty the chop starts at before the regulator takes over, default 50 percent. supercap_pwm_hz sets the chop frequency, default 10 Hz; the upper end of its range exists for bench experimentation with what your igniters and wiring tolerate rather than as a free upgrade, since duty resolution coarsens as the frequency climbs.

Seeing it work

None of this is invisible. Every test fire is recorded at 50 Hz to a trace you can fetch from the website: capacitor voltage, battery voltage, the 4.2 V rail, duty, output and power-good state, starting half a second before the output comes on so you see the rail at rest, and running ten seconds after it stops, because the recovery is half the story, how fast the capacitor climbs back tells you what headroom the battery actually had, which the fire itself cannot show. In flight, the capacitor, battery and rail are all in the flight log at 50 Hz alongside the chop duty, so every flight carries the complete power story. The practical meaning of the whole system is simple: a tired battery or a heavy igniter shows up as a slower, chopped fire in the data, never as a computer that wasn't there for the rest of the flight.