Bsides 2025 Badge
Preliminary Hardware Failure Analysis Report

Focus: Analysis of IC (IP5305T / U2) and Power Stage Failures

Report Type: Preliminary

Revision: 3
Updated on: 05 February 2026, by posix

1. Overview

This is a preliminary report on the analysis of the root cause for the failure of the Bsides 2025 Badge device.

Multiple devices failed during the Bsides 2025 event, some due to reversed polarity from the chemical power source, others due to what could be consistent with a thermal runaway event.

It was found that the device is subjected to current and voltage transients that may lead to internal damage of the selected Power Converter / Battery Charger IC (IP5305T, refereed to simply as “IC” and/or “U2” throughout the report) under certain operating conditions, that are expected to occur during normal use of the device.

Key findings

- The selected inductor is prone to core saturation in the DUT, allowing a large current to flow through the internal IP5305T (U2) switching node FET when this occurs.
- It was observed that the switching node ringing is prone to higher-than-expected peak voltage overshoot during the FET turn-off.
- The IP5305T (U2) was not designed for applications that impose rapid, high-frequency transient load demands (such as Wi-Fi transmission bursts), even though the average load current remains within the U2 nominal operating limits.
- There is no snubber network between the switching node and a low-impedance reference node.
- There is no reverse-polarity protection for the chemical power source (although the correct polarity is properly marked on the PCB).
- The bypass diode D2 is unnecessary and can be removed from the circuit.

2. DUT

- Bsides Lisbon 2025 Badge
- PCB revision: 1.0
- Relevant subsystem: Regulator (U3), Boost / Battery Charger (U2/L1), ESP MCU (U1)
- Firmware version: 1.0

3. Failure

There are two distinct reported failure modes:

- IC5305T (U2) failure, most likely caused by a thermal runaway event. The reasons and exact conditions that led to this (possible) thermal runaway event could not be replicated under controlled conditions. Nevertheless, FET degradation was observed during testing. This is the focus of this preliminary report.
- AMS1117-3.3 (U3) failure, most likely caused by the chemical power source being inserted with its polarity reversed relative to the PCB polarity markings. This event was replicable under controlled conditions.

4. Test Setup

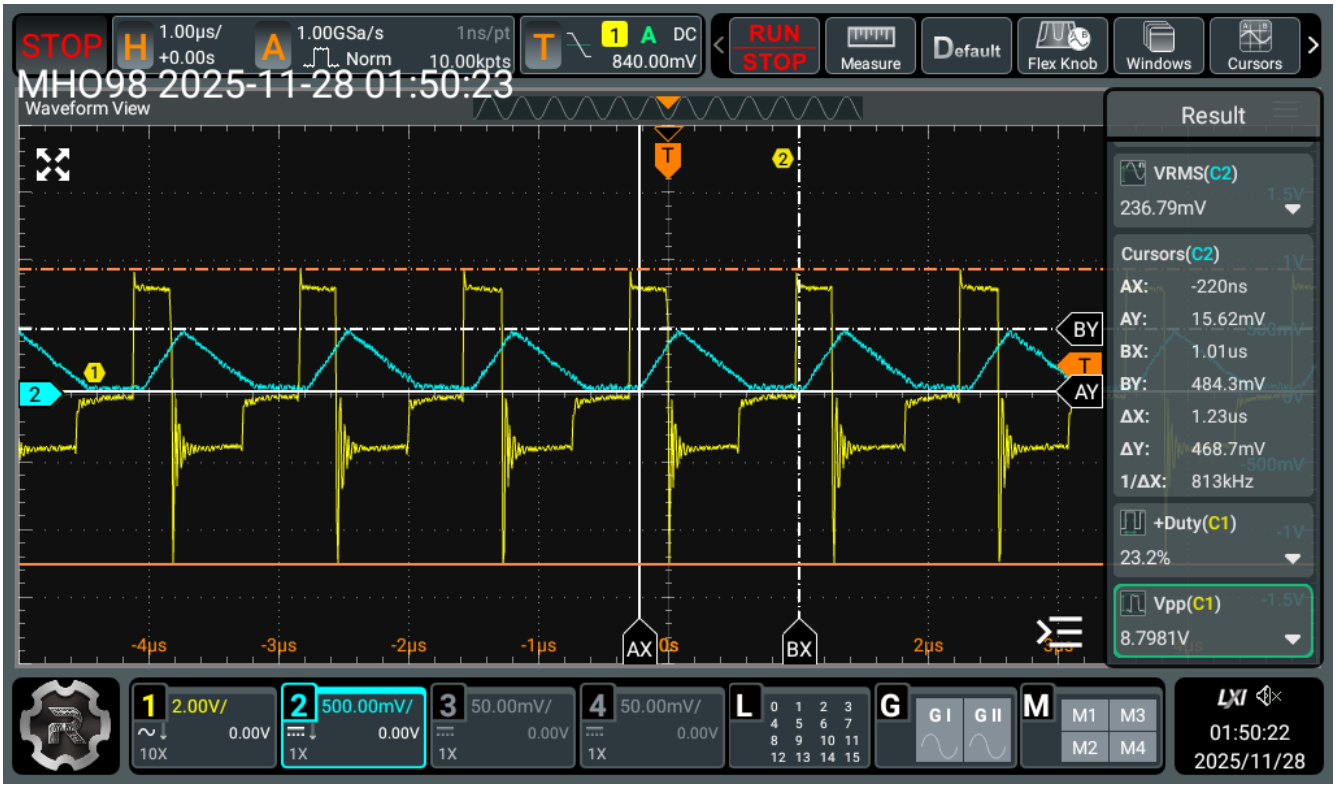
- Power supply: CPX200, TTi (all tests were set @ 3.4V, with current limit set @ 8A)
- Oscilloscope: MHO98, Rigol
- Voltage probes: SQ350, Sensepeek
- Current probe: I-prober 520, Aim-TTi
- Electronic Load: 2280, PeakTech
- DMM: SDM4065A-SQ, Siglent
- Thermal Imaging: 279FC, Fluke
- Temperature / Humidity: 23 C / ~60%
- DC Load patterns (@Vout): Continuous; Pulsed (10ms);

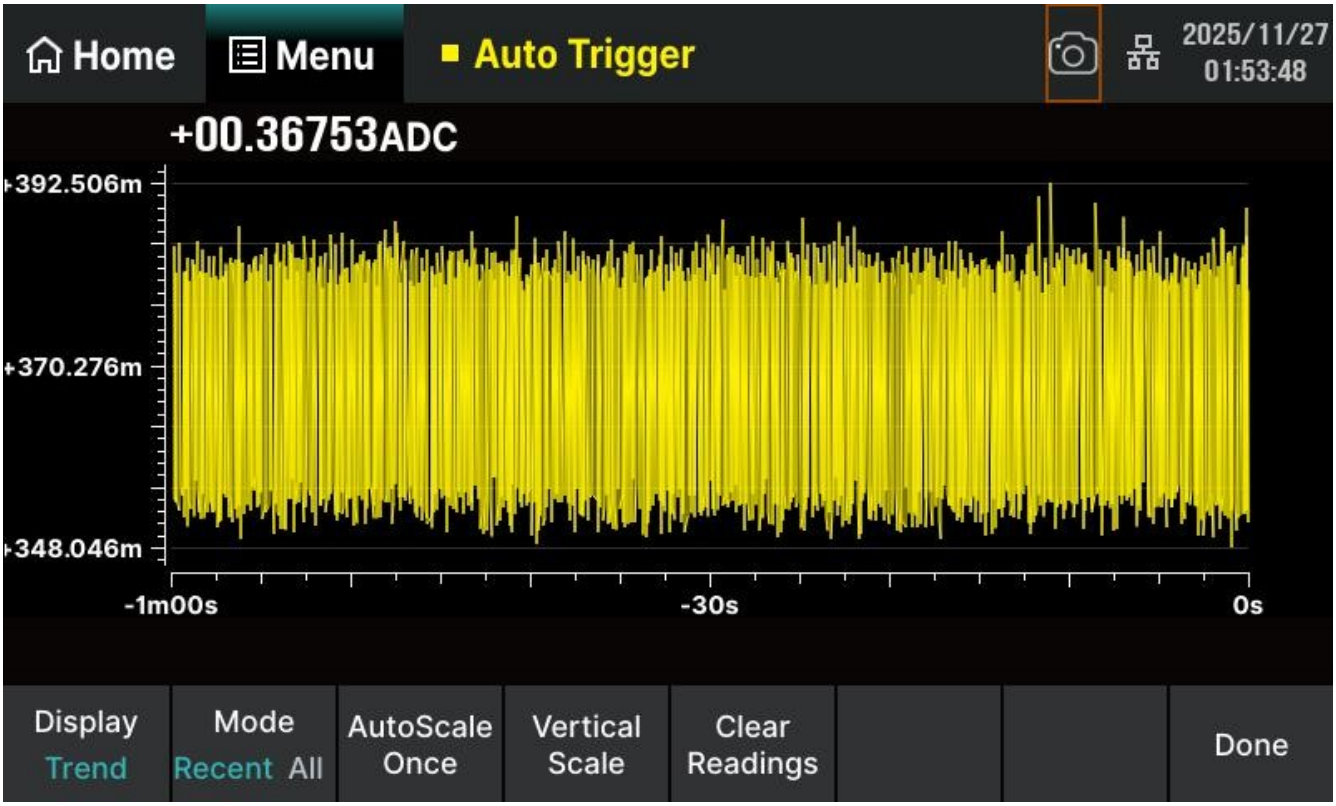
5. Measurements

There are five (5) key categories of measurements of interest:

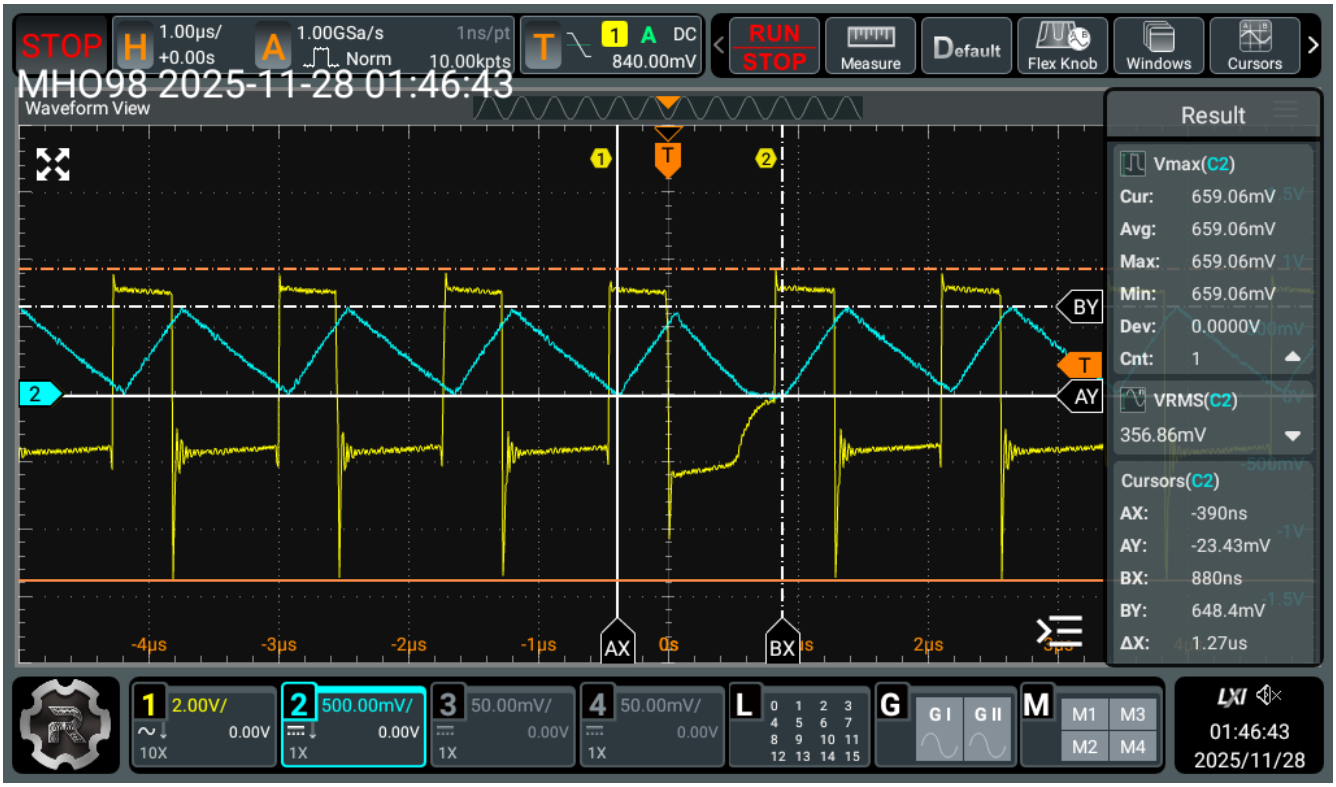
- Current across the inductor (L1) under boost DCM, Boundary, CCM and Saturation conditions.
- Peak voltage overshoot at the switching node and respective duty cycles.
- Peak output current at which the device shuts down.
- Peak temperature observed at the IP5305T (U2) case.
- I-V curve traces for the IP5305T (U2) switching node, comparing unused vs. tested units.

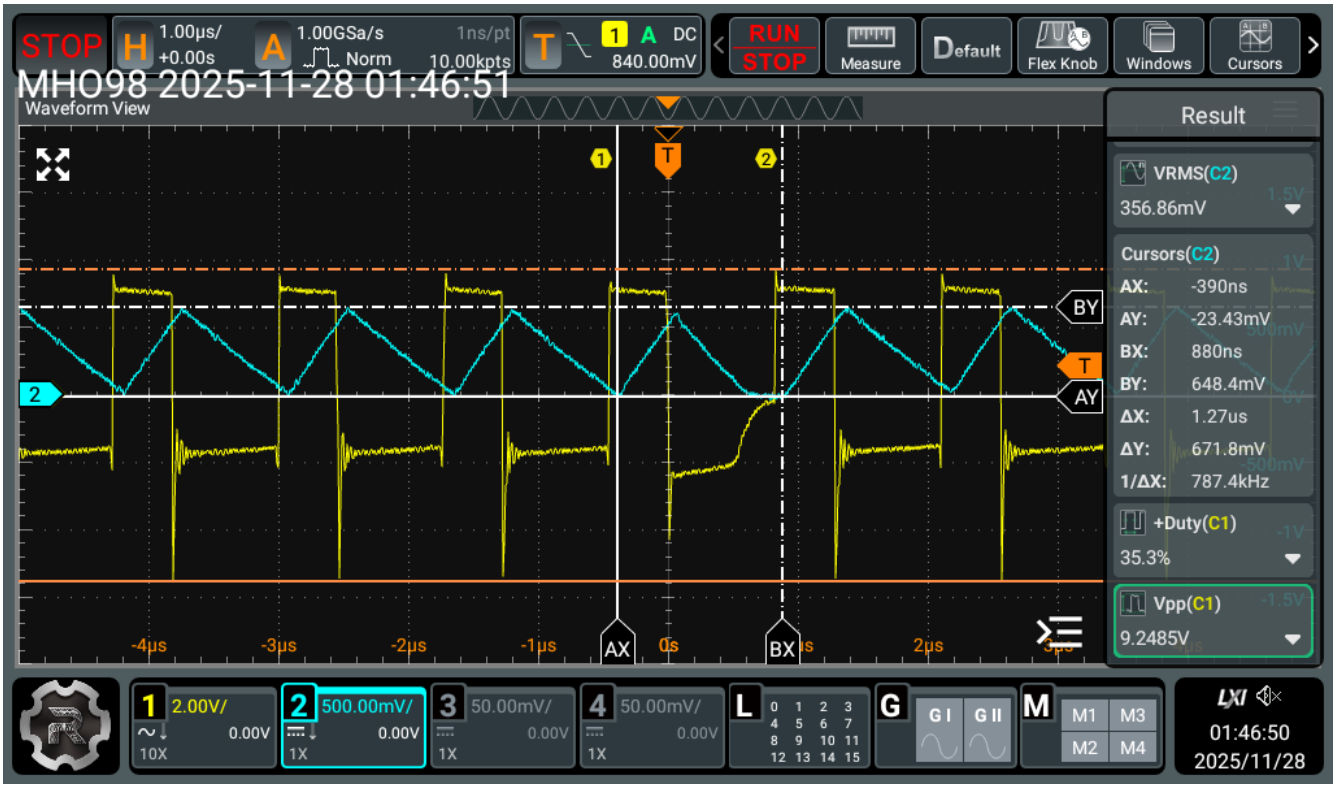
5.1. Inductor Vpp and Current @ DCM (Iload: 100mA):

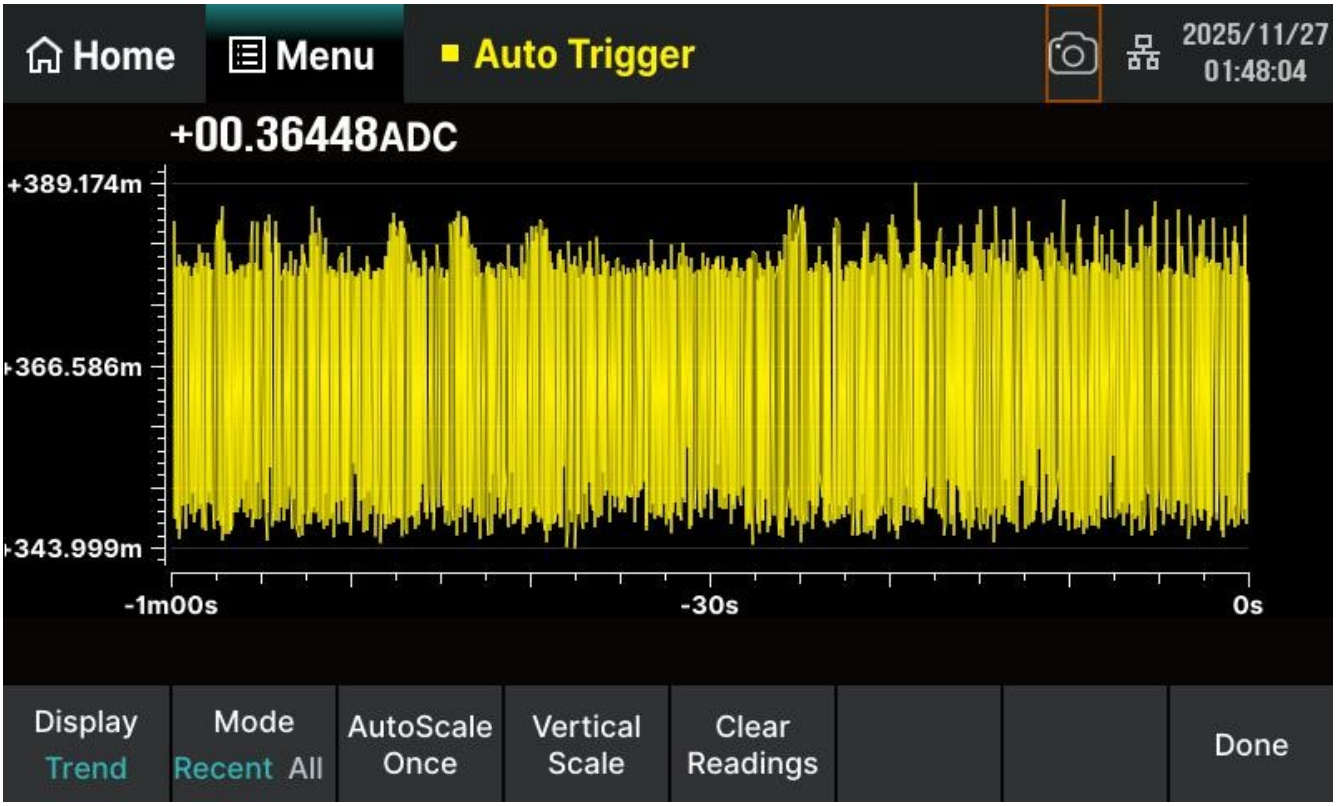



Home
Menu
Auto Trigger
2025/11/27
01:53:48
+00.36753ADC
+392.506m
+370.276m
+348.046m
-1m00s
-30s
0s
Display
Trend
Mode
Recent All
AutoScale
Once
Vertical
Scale
Clear
Readings
Done

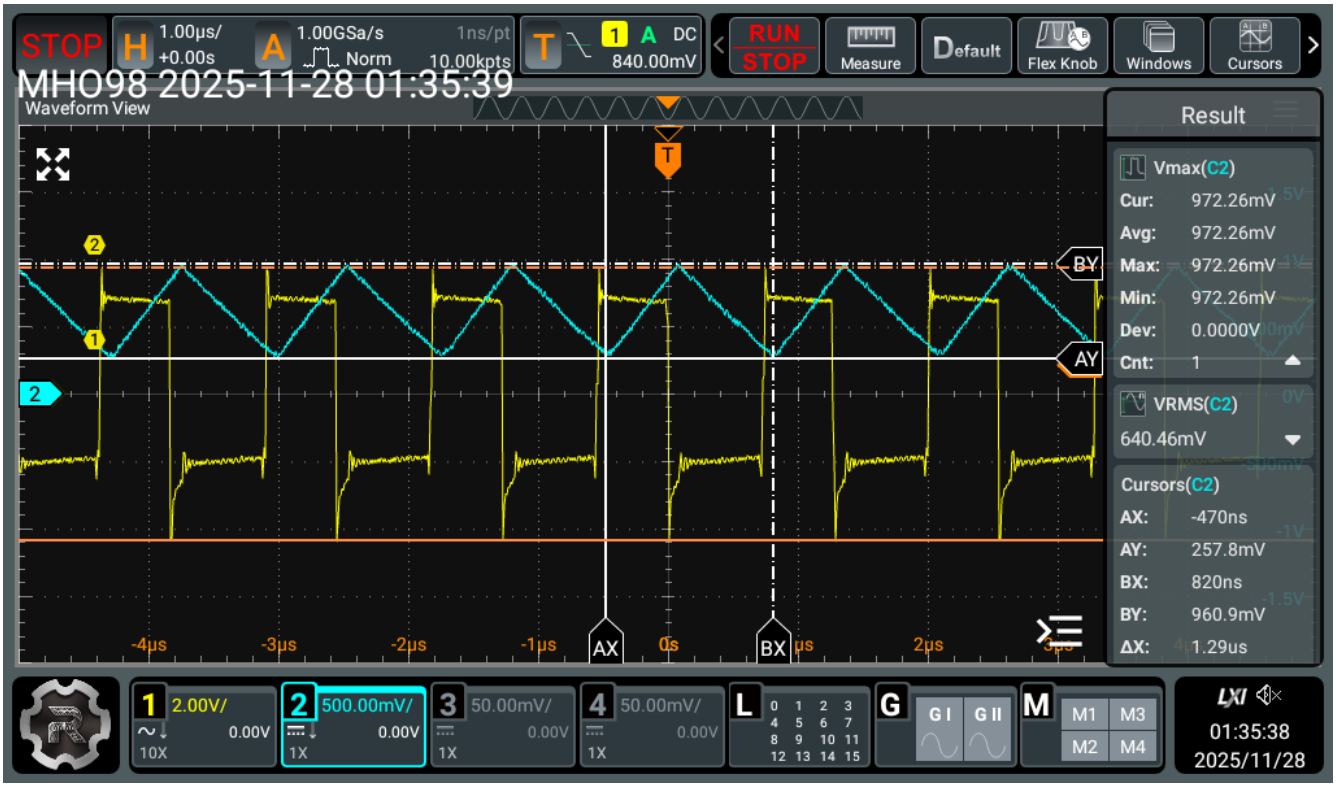
5.2. Inductor Vpp and Current @ DCM/CCM boundary (Iload: 213mA):

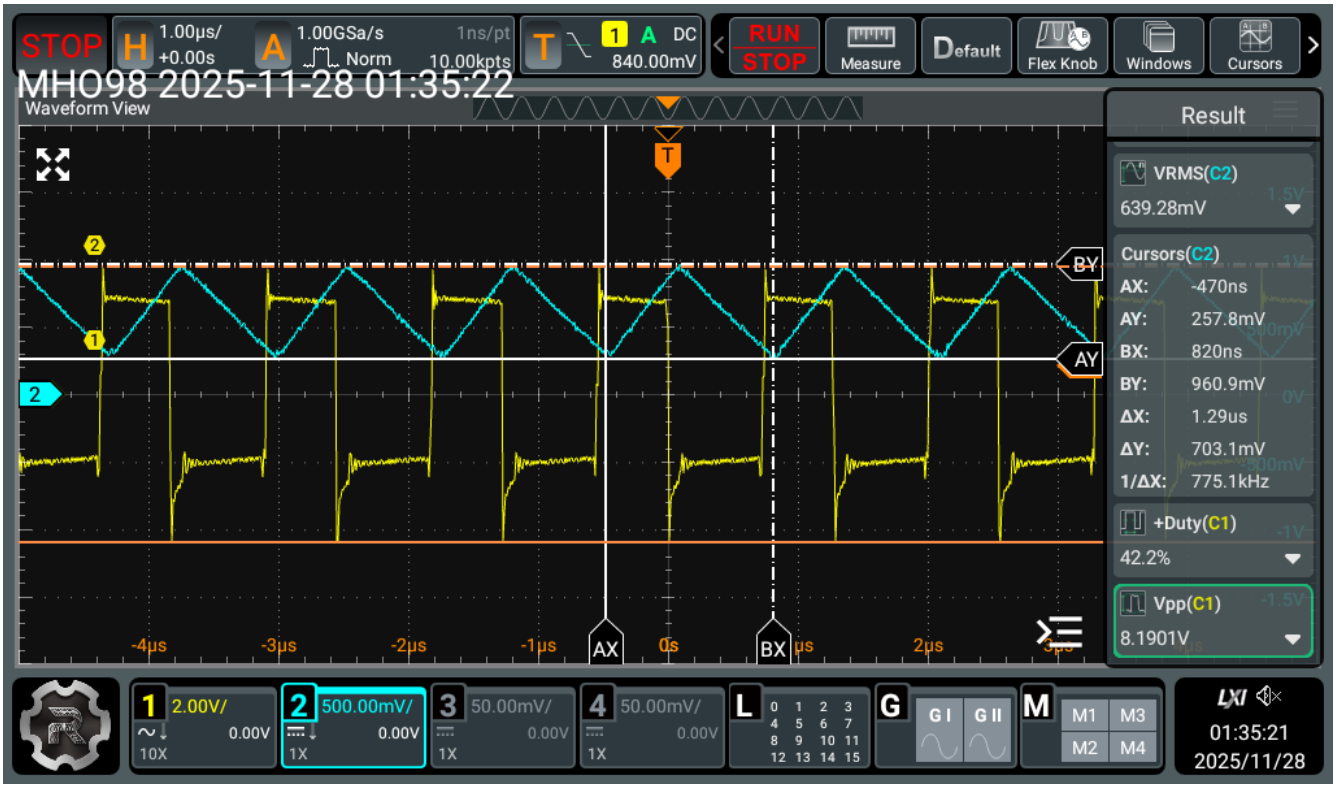


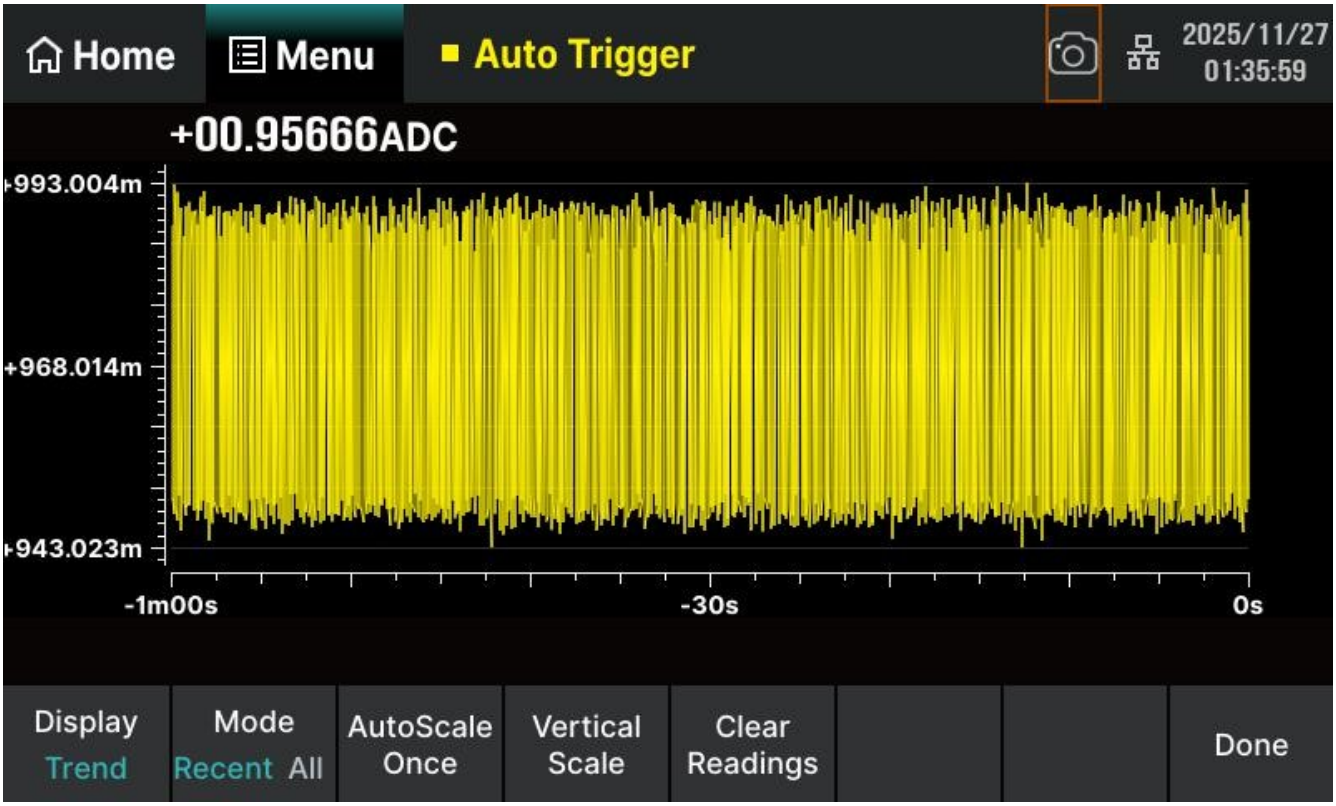



Home
Menu
Auto Trigger
2025/11/27
01:48:04
+00.36448ADC
+389.174m
+366.586m
+343.999m
-1m00s
-30s
0s
Display
Trend
Mode
Recent All
AutoScale
Once
Vertical
Scale
Clear
Readings
Done

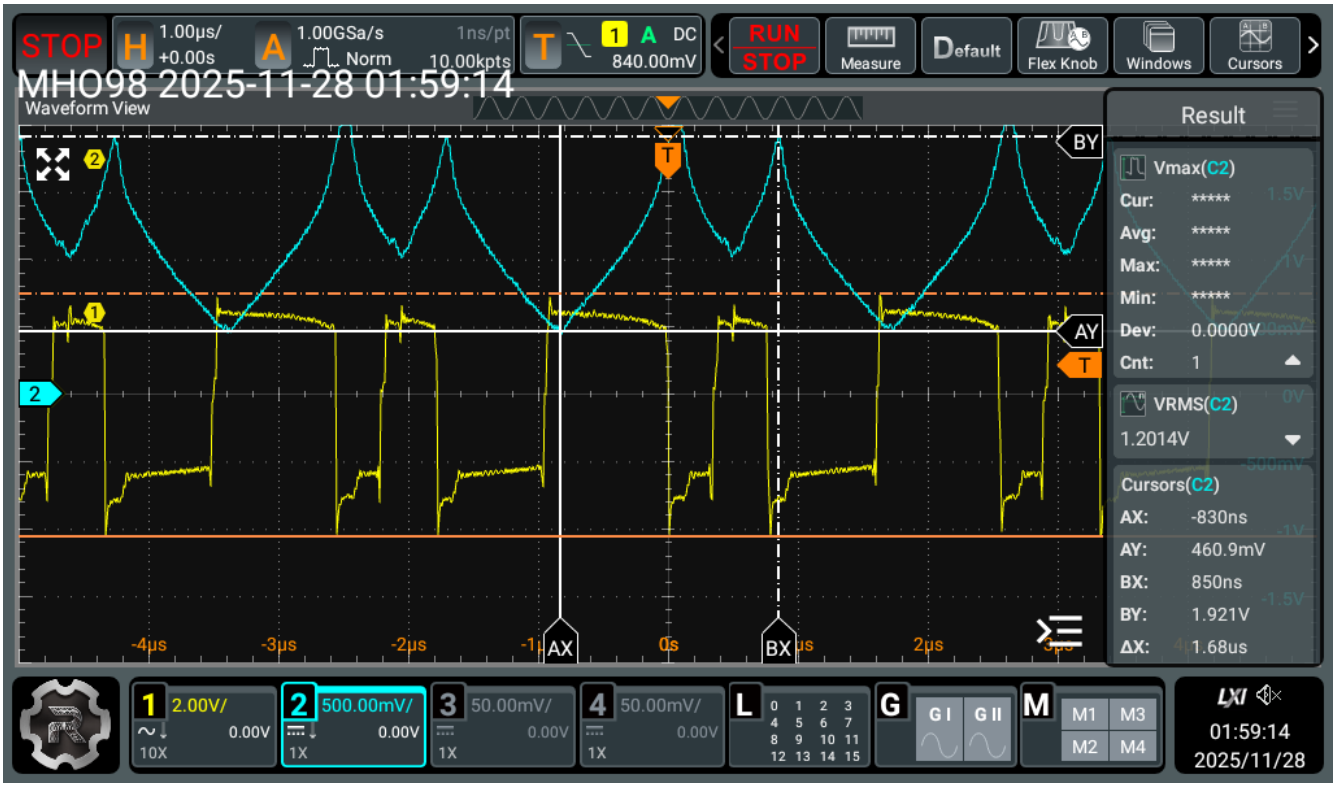
5.3. Inductor Vpp and Current @ CCM (Iload: 500mA):

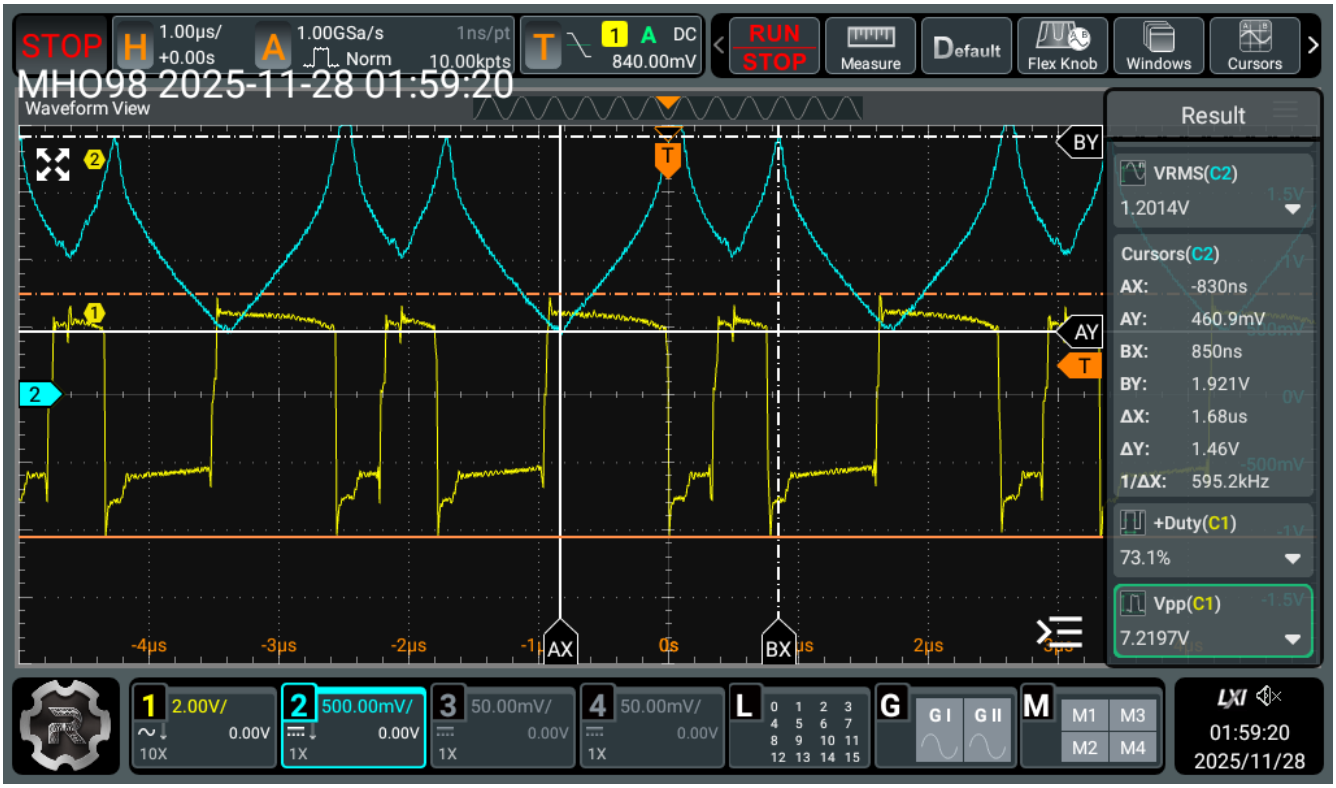


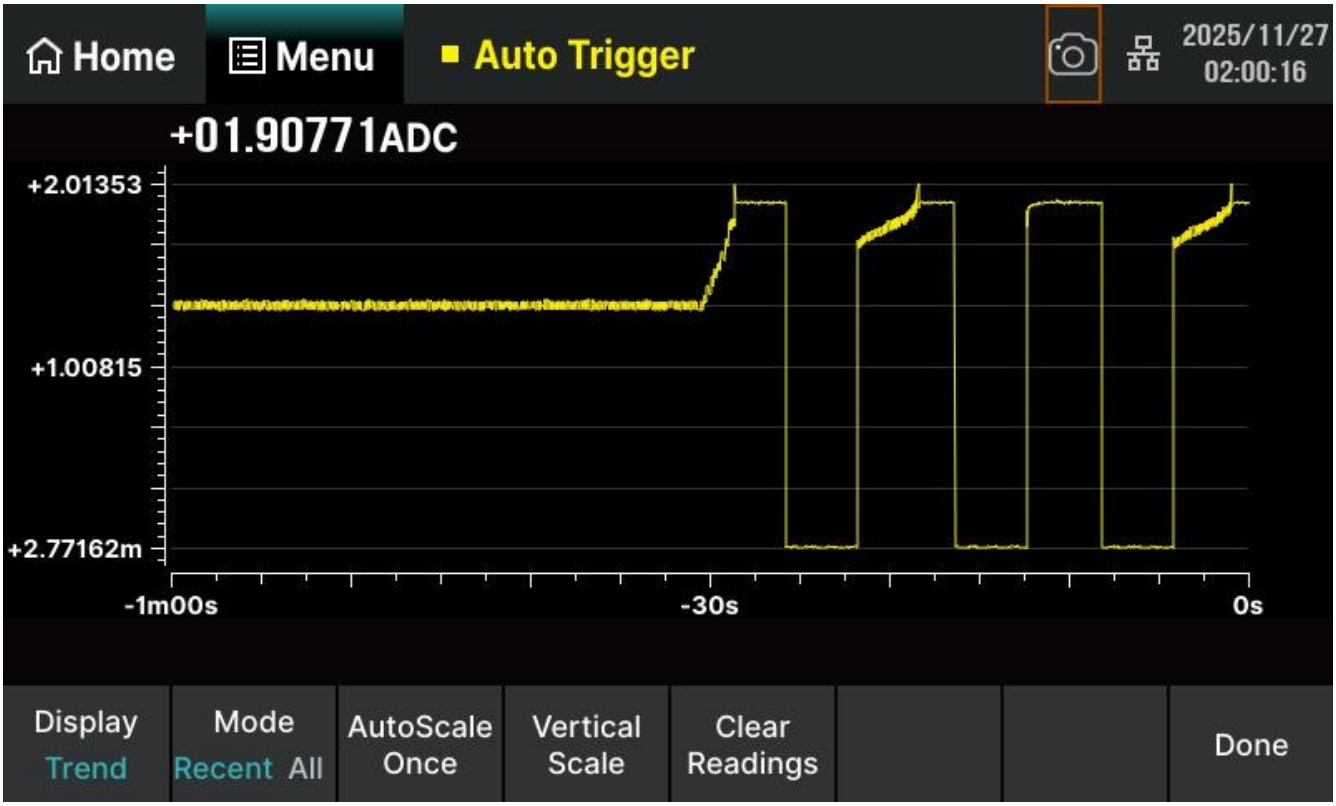



Home
Menu
Auto Trigger
2025/11/27
01:35:59
+00.95666ADC
+993.004m
+968.014m
+943.023m
-1m00s
-30s
0s
Display
Trend
Mode
Recent All
AutoScale
Once
Vertical
Scale
Clear
Readings
Done

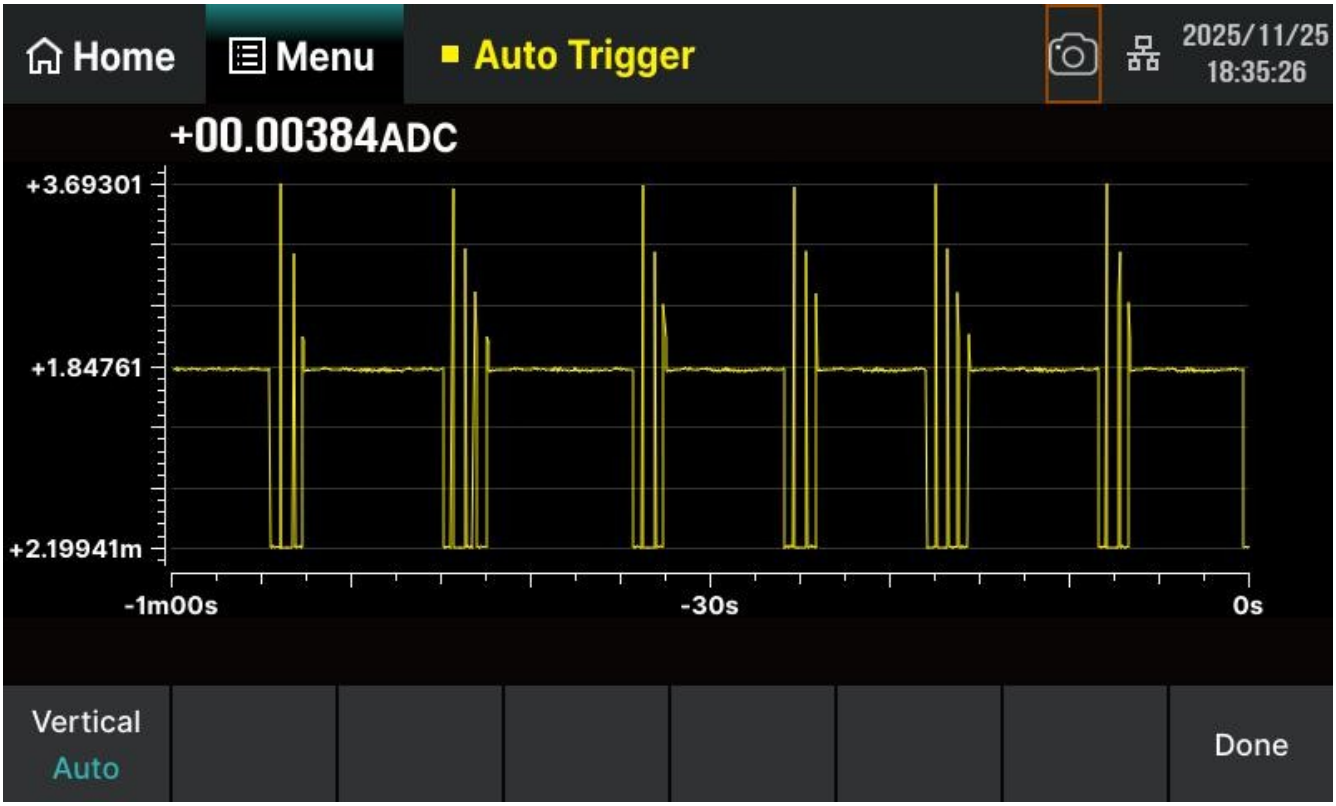
5.4. Inductor Vpp and Current @ Isat (Iload: 680mA – Device shuts down):






Home
Menu
Auto Trigger
2025/11/27
02:00:16
+01.90771ADC
+2.01353
+1.00815
+2.77162m
-1m00s
-30s
0s
Display
Trend
Mode
Recent All
AutoScale
Once
Vertical
Scale
Clear
Readings
Done

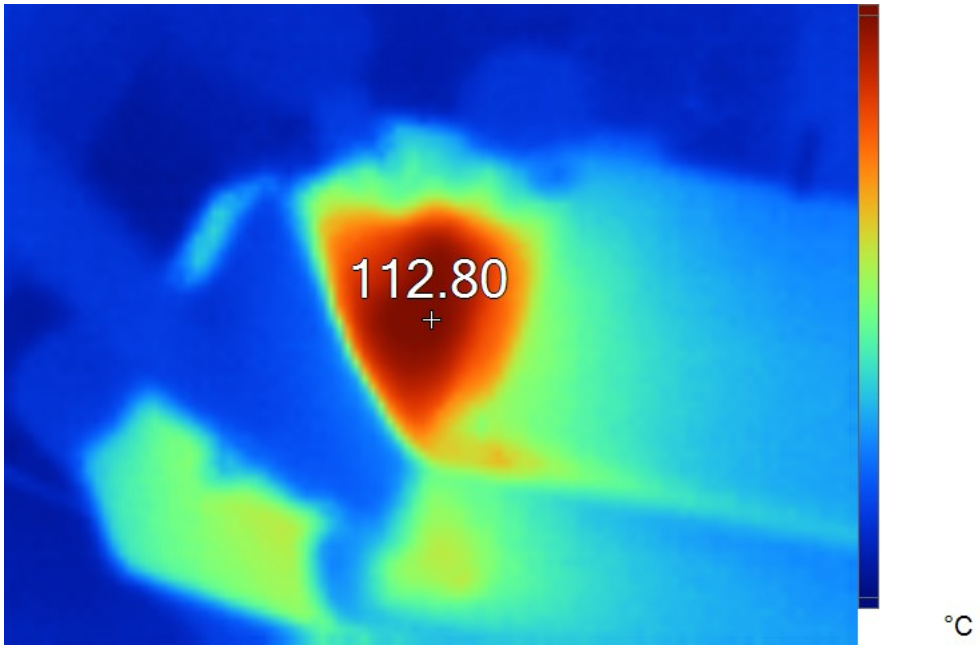
5.5. Current transients @ 800mA Iload power cycles (note the ~3.7A peaks):



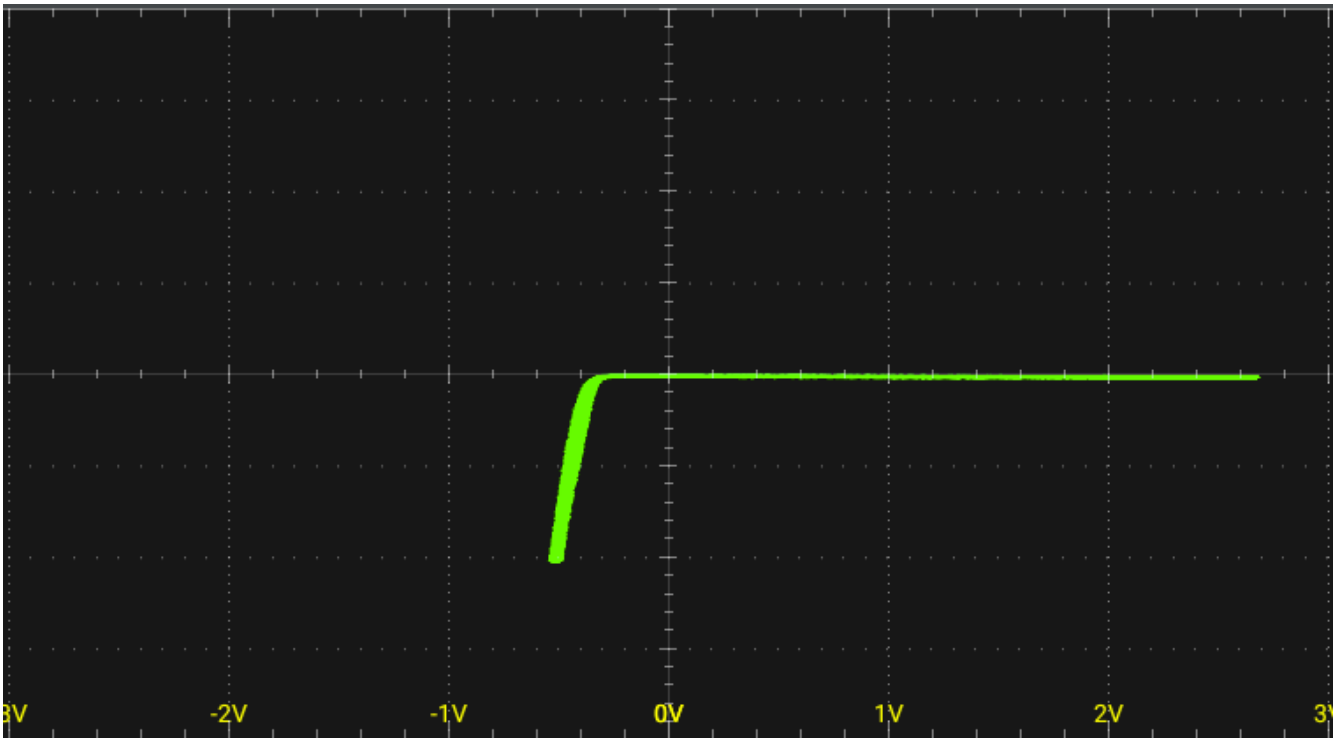
5.6. Switching-node ringing @ 800mA Iload power cycles (note the Vpp ~11V):

5.7. Peak Temperature observed @ 780mA Iload (pulsed, 10ms, 50% duty cycle):

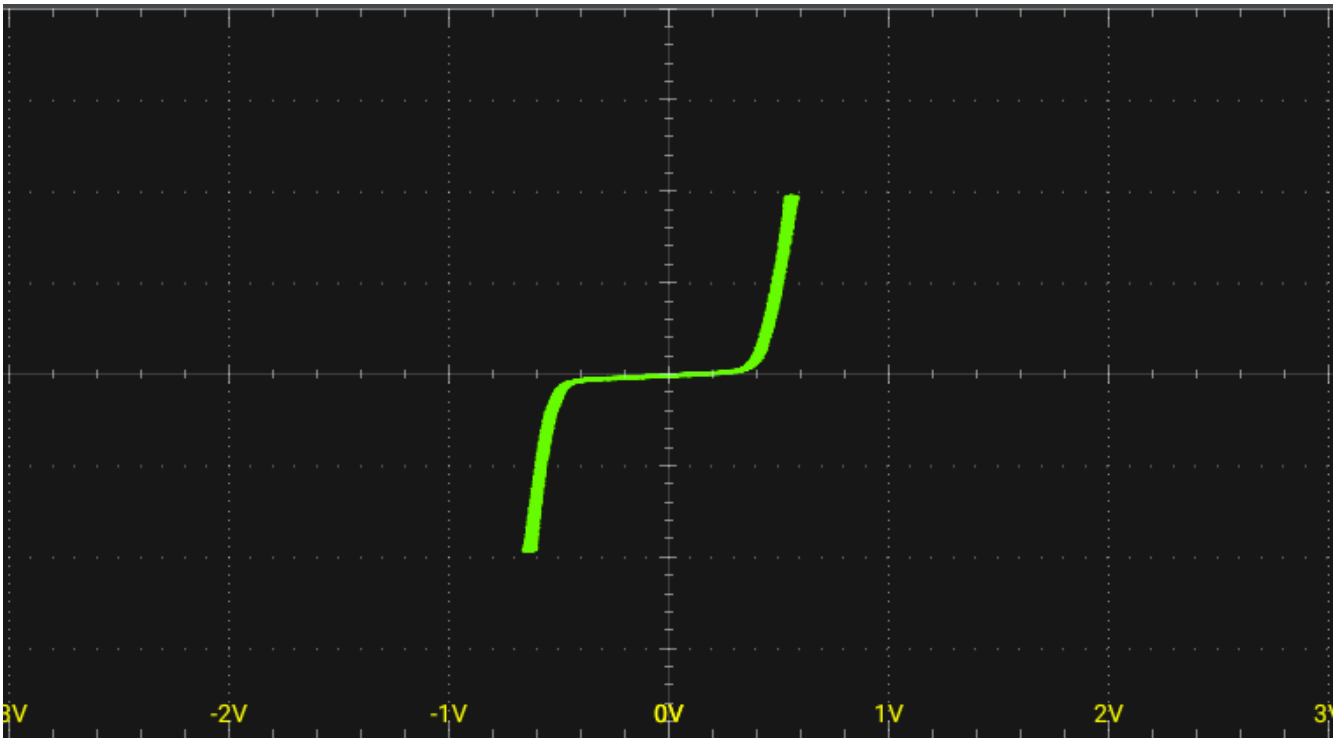
- 112.8 Celsius (assumed junction temperature to be between 20 to 50 Celsius higher).



5.8. I-V Curve trace for a unused IP5305T (picked directly from a reel):



5.9. I-V Curve trace for a IP5305T after being subjected to the previous tests:



6. Analysis

Based on the measurements performed in section five (5), we can now theorize about the probable causes for the first failure mode described in section three (3) that might lead to the failure of the DUT.

6.1. Excessive* current in the U2 FETs / switching node (*Excessive: above safe operating limits.)

- When the inductor core saturates (5.4), excessive* current may flow through the U2 FET and the switching node.
- Excessive* current may flow through the U2 internal FET during Wi-Fi transmissions from the ESP MCU (U1), as short, high *di/dt* pulses draw current from the power source and through the boost stage.
- Pulsed current and/or sub-millisecond current transients may render the IC internal protections ineffective (delayed response), leading to localized excessive heating in the U2 FET.
- Manufacturing variations of the ICs (U2) and/or inductors (L1) may result in slightly different electrical characteristics, increasing current transients and potentially stressing or damaging the IC (U2). Tolerances in RDS(on) (U2), gate charge (U2), Isat (L1) may be a contributing factor.
- Repetitive pulsed operation may gradually degrade the IC (U2) and/or inductor (L1), particularly when current the peaks approach the inductor (L1) saturation current (Isat, 5.4).

The IC (U2) and inductor (L1) combination in the DUT was subjected to large current peaks (3.7A) during the tests (5.5), which may have contributed to the degradation of the IC (U2), as seen in (5.9).

Even minor degradation of the internal FET in the IC (U2) may reduce the effectiveness of its internal protections and/or (other) internal circuits, potentially leading to thermal runaway.

Further testing is required to confirm or refute this hypothesis.

6.2. Large transient voltage overshoot at the switching node during FET turn-off

- Power cycling the device with the DC electronic load set to 800mA causes large currents to flow through the IC (U2), leading to higher-than-expected peak voltage overshoot when the internal FET turns off. The highest measured Vpp was ~11V (5.6), which is unusual for an IC designed to operate at nominal 5V. Nevertheless, the absolute maximum ratings for the internal FET are not specified in the IC (U2) datasheet, so it might still be within tolerance.
- Higher switching transients might occur with different IC (U2) / Inductor (L1) combinations in different devices, potentially degrading the FET and subsequently causing them to fail shorted between drain and source, leading to a thermal runaway due to uncontrolled current flow.

The lack of a snubber network between the switching node and a low-impedance reference node contributes to higher-than-expected peak voltage overshoot during FET turn-off.

Further testing is required to confirm or refute this hypothesis.

6.3. FET degradation during testing

Even though a catastrophic failure of the DUT was not observed during testing, a potential degradation of the internal FET in the switching node of IC (U2) was observed.

The IC (U2) was de-soldered from the DUT and an I-V curve trace was performed between the SW and PowerPAD connections. The resulting curve for the suspected degraded IC (U2) can be seen in (5.9) and compared with the I-V curve of an unused IC in (5.8).

These results indicate that, for the suspected IC (U2), a current conduction path exists between SW and PowerPAD when a positive voltage is applied across the terminals. Although the exact degradation mechanism cannot be determined from this measurement alone, the observed behavior is consistent with degradation of the internal silicon structures associated with the switching FET. As conduction begins at lower applied voltages, the effective resistance between SW and PowerPAD is reduced. This can lead to increased static current and higher power dissipation during operation, increasing the risk of thermally induced failure.

It is difficult at this stage to conclude which specific test contributed the most to this degradation, as the IC (U2) was traced after testing, rather than between each test. It is, however, suspected that the degradation occurred during the measurements shown in (5.6) and (5.7), which subjected the IC (U2) to the highest combined thermal and electrical stress.

Further testing is required to confirm or refute this hypothesis.

7. Recommendations

A different design is recommended for future iterations of this device, especially regarding component selection for the power stage and battery management circuitry. The inclusion of a snubber network and the use of an inductor with higher Isat margins are strongly recommended.

7.1 Short-Term Mitigations

It remains unclear, given the inability to replicate the failure in controlled conditions, which short-term mitigations for the already assembled devices could reduce the risk of failure. Using an inductor with a higher maximum Isat could result in higher-than-expected peak voltage overshoot at the switching node, due to the absence of a snubber network. Preventing inductor saturation under the current design may therefore increase transients voltage stress at the IC (U2) FET, potentially causing internal degradation.

There is, however, the possibility of finding an alternate IC that is pin-compatible with U2 and designed to operate under the conditions and requirements of this application without additional protection circuitry. Such an IC might or might not exist and further investigation is required.

7.2 Hardware Redesign Recommendations

- Select an inductor (L1) with a higher current saturation margin (Isat).
- Include a snubber network between the switching node and a low-impedance reference node to limit the peak amplitude of voltage overshoot during FET turn-off.
- IC (U2) selection must consider the device-s actual power usage. The currently used IC (U2), the IP5305T, is primarily designed for power banks, which typically demand a stable, low-transient current supply. In contrast, the DUT operates with Wi-Fi transmission bursts, requiring an IC capable of handling fast, high *di/dt* load transients.
- Bypass diode D2 is not required.
- Implement reversed-polarity detection or protection for the chemical power source.
- Include thermal vias in the PCB power pads to improve heat transfer.
- Whenever possible, match the Vout of the first power stage to the load to avoid boosting the chemical power source only to step it down to 3.3V with a linear regulator (U3), which would dissipate excess energy.