CHERITech'26 CONFERENCE

12-13 Nov 2026
Munich, DE

Located at semi | SEMICON EUROPA

Opportunities for CHERI in the Energy Industry

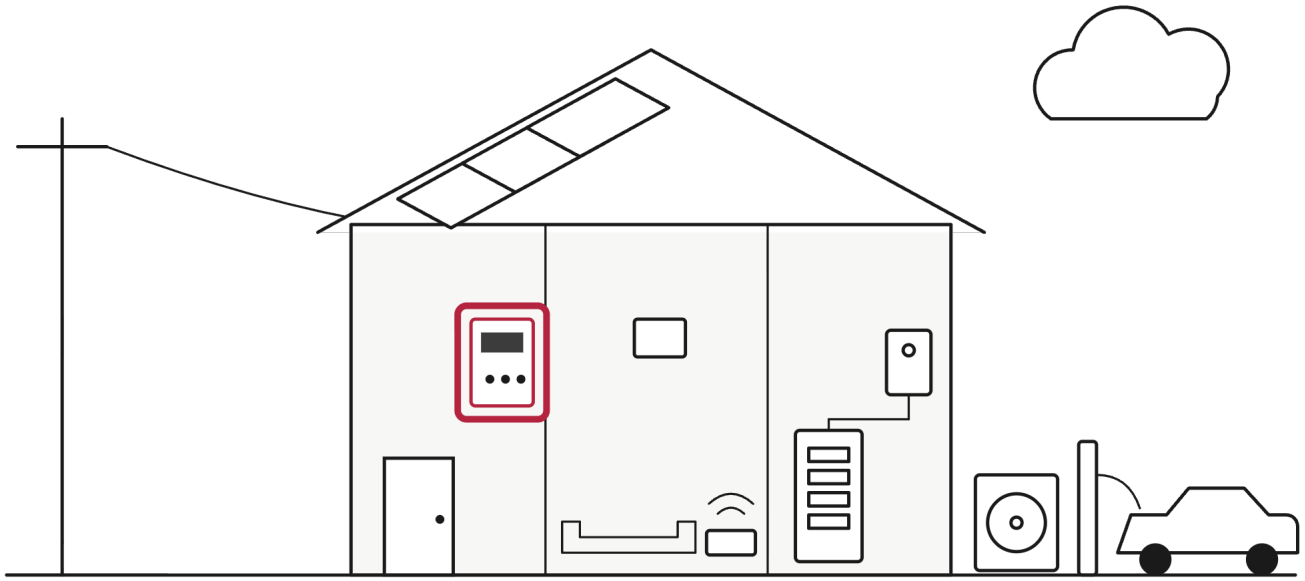
The grid's new front door

Joshua Cooper
CEO
Hildebrand Technology Limited



The grid’s new threat

Securing consumer energy from the silicon up

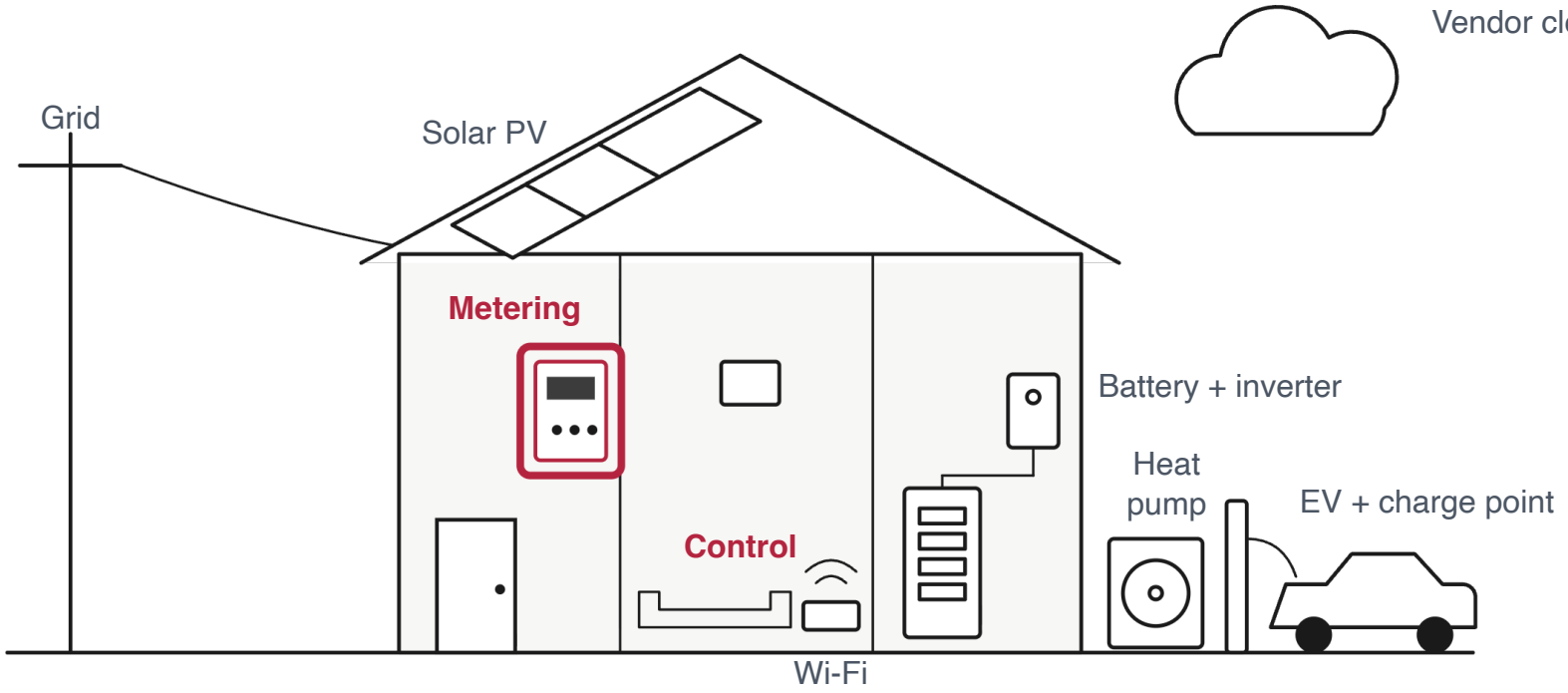


Joshua Cooper

Hildebrand Technology Limited

hildebrand

The metering and control devices decide what the house does



38 million smart meters in Great Britain. More than 20 million homes able to earn from time-of-use tariffs, export and flexibility.

Every one of them is now a **control point** on the grid.

hildebrand

The front door is governed. The back doors are not.

FRONT DOOR · SMART METERING HAN

- Zigbee Smart Energy Profile
- Keys managed through the DCC
- Supplier switch swaps the keys
- Certified, specified devices

BACK DOORS · WI-FI AND VENDOR CLOUDS

- Batteries, inverters, chargers, heat pumps
- One app and cloud per vendor
- Firmware patched when the vendor gets round to it
- Remote control is the feature

hildebrand

A bad day at one address

06:05 **A malformed cloud message hits the comms parser**
Buffer overflow. The attacker now runs the control device.

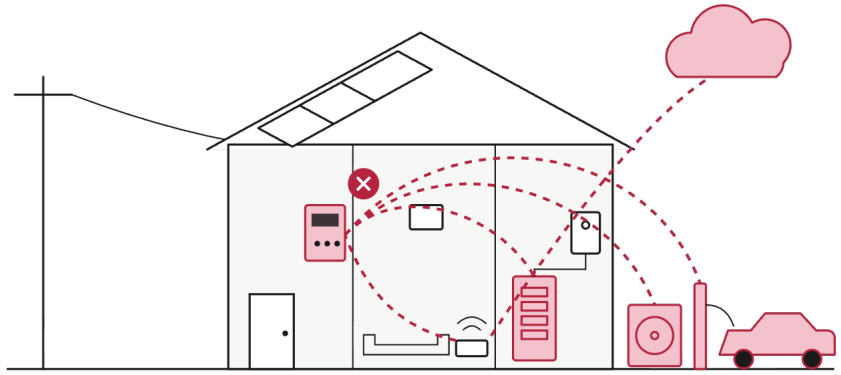
06:10 **Heat pump switched off**
By evening the house is at 14 °C. It is January.

07:00 **Battery emptied into the grid at 4p**
Then refilled at 17:30 on the peak rate. About £5 lost today.

08:10 **Consumption drops to standby**
Whoever is watching knows the house is empty until 18:40.

18:45 **Car plugged in, charger locked**
22% in the morning. The school run is in doubt.

21:00 **Message in the app**
Pay to get your home back.



Every step is a published capability: cloud takeover, settings tampering, data exposure and cyber-physical ransomware were all demonstrated in the 2025 SUN:DOWN research.

hildebrand

One bad day in 900,000 homes is a national event

900,000 → **4.5 GW** → **49 Hz**

homes at 5 kW, acting at once

sudden swing on the continental grid

where automatic load shedding begins

80% of hybrid-inverter flaws disclosed over three years were rated high or critical

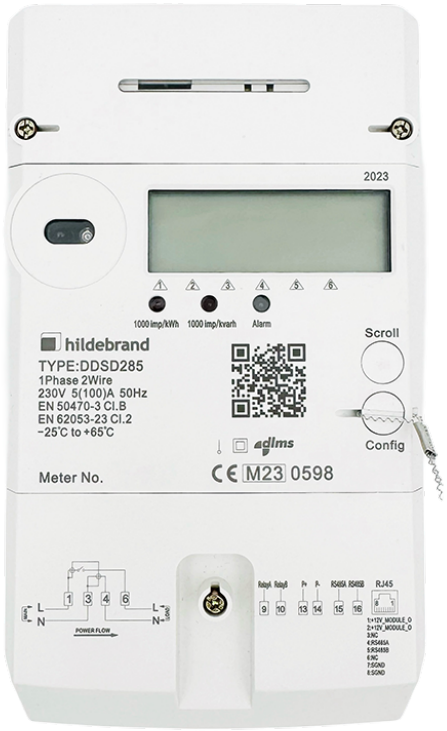
Undocumented radios reported in some imported inverters and batteries

GB wants **10–12 GW** of consumer-led flexibility by 2030, up from 2.5 GW in 2023

hildebrand

The first CHERI enabled product is a smart meter

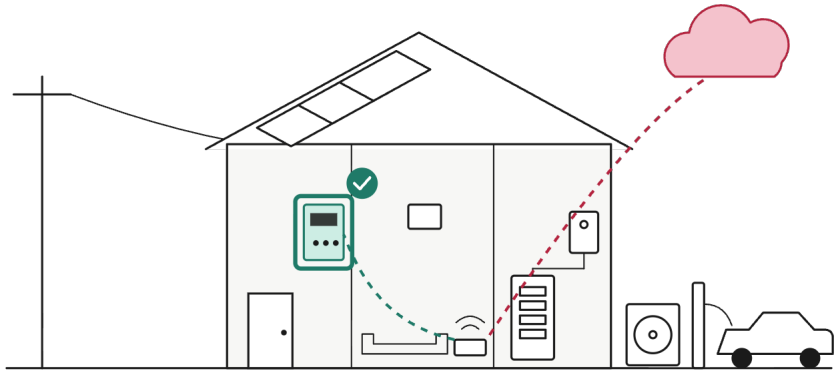
Manufactured by Hildebrand for UK and European markets



Using SCI Semiconductor ICENI to secure the front door of the grid.

hildebrand

The exploit fails at the door



Same 06:05 message. The out-of-bounds write hits a capability check and traps. The comms compartment restarts clean; the rest of the day is normal.

Comms Faults and restarts	**Metrology** No capability to reach it
Control Relay and inverter untouched	**AI inference** Control decisions intact

Glow CHERI meter · single-phase, 3-phase, 3-phase CT · SCI Semiconductor **ICENI**, CHERIoT-Ibex RISC-V · existing C recompiled with about **1–3% overhead**

Glow CHERI AI · controller · Codesip **PRIME**, RISC-V · existing model

Both on the stand today.

hildebrand

The bad command is refused

17:30 INCOMING

“Every battery: discharge now”

well-formed, signed, from a compromised aggregator

→

EDGE AI PLAUSIBILITY GATE

Checks the command against this home’s forecast, state of charge, tariff and recent history

→

Plausible: act

it fits what this home can do now

Implausible: refuse

fall back to the home’s own schedule

Decide locally

Forecast, optimise and control run on the device, so the home behaves sensibly without the cloud

Trust the meter

Settlement comes from the meter’s measurement, not from what a device reports

hildebrand

Memory safety stops the exploit. Local intelligence stops the instruction.

Attack on the home	Conventional device	Glow CHERI meter	CHERI + edge AI
Firmware takeover	Cold house, £5 lost, car at 22%	Normal day	Normal day, attempt logged
Rogue dispatch	Battery dumped, car late	Same: no memory bug involved	Refused; home keeps its plan
Privacy harvest	Attacker knows when you're out	Read blocked	Blocked; less data leaves anyway

Only the second layer stops a well-formed malicious instruction.
Only the first stops the exploit that would disable the second. You need both.

Built for the rules that are coming

11 Sep 2026

EU CRA: 24-hour reporting of actively exploited flaws begins

Today

First CHERI-secured smart meter on show

End 2026

GB load control licence applications open (planned)

11 Dec 2027

EU CRA applies in full, with CE marking

End 2027

GB licence required to control household load (planned)

GB Energy Smart Appliance rules add minimum cyber security and grid-stability requirements for chargers, heating and batteries.

CHERI gives an auditor evidence that a whole class of bugs cannot be exploited.

hildebrand

Come and break it

Pilot

Utilities, suppliers and housing providers: trial the Glow CHERI meter

Partner

Silicon, RTOS and device makers: put CHERI and edge AI in inverters, chargers and batteries

Policy

Regulators and standards bodies: name hardware memory safety in device requirements

Run the bad day yourself

hildebrand.co.uk · Joshua Cooper



THANK YOU

Contact contact@cheri-alliance.org

Web www.cheri-alliance.org

Located at semi | SEMICON EUROPA

CHERI™ and the CHERI logo are protected trademarks. Use of these marks is subject to the CHERI Alliance Trademark Policy – https://cheri-alliance.org/legal-and-policies/trademark/

This work © 2026 by CHERI Alliance is licensed under CC BY-SA 4.0 (Creative Commons Attribution-ShareAlike 4.0 International) – https://creativecommons.org/licenses/by-sa/4.0/