HALO FastHub Internet Access

Executive Summary

Reliable internet connectivity is as critical to HALO FastHub as the electrical supply is – it underpins a seamless user experience and enables user and payment authorisation, remote monitoring, over-the-air [OTA] updates, reactive maintenance and remote fault resolution.

3ti's recommended configuration is for Primary connectivity to be via a site-hosted wired WAN paired with Secondary (failover) connectivity provided by a 3ti cellular SIM card (mobile network).

Where a wired connection is unavailable, BT broadband, StarLink, or WiFi can serve as the primary channel; SIM-only operation is not recommended for permanent use.

This document details the connectivity requirements: in short: HALO FastHub needs a simple IP network with outbound (egress) access to several internet hosted services; there is no need for any inbound port or service mapping. This can be provided easily using an existing guest network or dedicated VLAN.

Contents

Executive Summary 1
1 Background 2
2 HALO FastHub Implementation 3
3 Primary WAN Technical Requirements 5
4 Primary Connectivity Alternatives 5
4.1 Business Broadband (fixed-line) 6
4.2 StarLink (satellite) 6
4.3 WiFi (+SIM) 6
4.4 Dual-SIM (NOT recommended) 7
5 Service Ports 8
5.1 Group 1: Basic Networking 8
5.2 Group 2: Maintenance 8
5.3 Group 3: Operations 8
5.4 Group 4: Payments (CPI) 8
5.5 Group 5: Payments (PAX) 8
5.6 Group 6: Display Screens 9
6 Security 9

HALO FastHub Internet Access

1 Background

The delivery of HALO services requires reliable internet connectivity. It is very much aligned with the modern "internet of things", taking advantage of simple cloud connectivity over zero-trust, zero-config networks.

HALO FastHub's internet connection is used to:

- Provide EV charging user authentication and payment authorisation
- Provide remote session and fault monitoring and data logging
- Keep track of solar generation and battery energy use for monthly performance reporting
- Update display screen media / display content (if present)
- Provide OTA software updates (e.g. product & security upgrades and configuration changes)
- Remotely access locally stored CCTV recordings
- Monitor fire and security alarm systems
- Monitor smart lighting and control systems, provide system warnings and fault notifications
- Enable remote resolution of faults, avoiding system downtime and engineering callouts

The #1 problem affecting EV charge point up-time and reliability is communications, all too often based on Cellular (mobile) networks which frequently drop out. Whilst such interruptions are only a minor nuisance for mobile phone users, it can be a major disruptor for EV drivers, causing difficulties starting, maintaining or finishing a charge session.

Temporary connectivity issues typically cause time-outs and delays while charging or starting a charge, and permanent / lasting faults require engineering call-outs which take time and operational cost to arrange, during which charge points may still be powered but unavailable for use. This frustrates drivers who simply want to plug in and charge, and risks lost revenue through poor reviews and reduced repeat visits.

WiFi signals can also suffer from interference, device contention or configuration changes, and while even fixed WAN/LAN cables are not 100% reliable 100% of the time, they are absolutely the best choice for reliability, cost and convenience by far.

Furthermore, legal requirements for internet connectivity and data recording were introduced with *The Electric Vehicles (Smart Charge Points) Regulations 2021* (SCPR)[1], and mandatory uptime and availability reporting requirements were introduced with *The Public Charge Point Regulations 2023*[2]. These regulations were introduced

[1] https://www.legislation.gov.uk/uksi/2021/1467/contents/made
[2] https://www.legislation.gov.uk/uksi/2023/1168/contents/made

into the statute for the UK on 30th June 2022 and 24th November 2023 respectively, and build upon the obligations within the *Automated and Electric Vehicles Act 2018*[3].

Whilst these regulations do not specifically mandate *non-cellular* internet access for EV charge points, it is increasingly difficult for SIM-only facilities to meet the necessary performance, representing single-point and/or multiple single-points of failure.

2 HALO FastHub Implementation

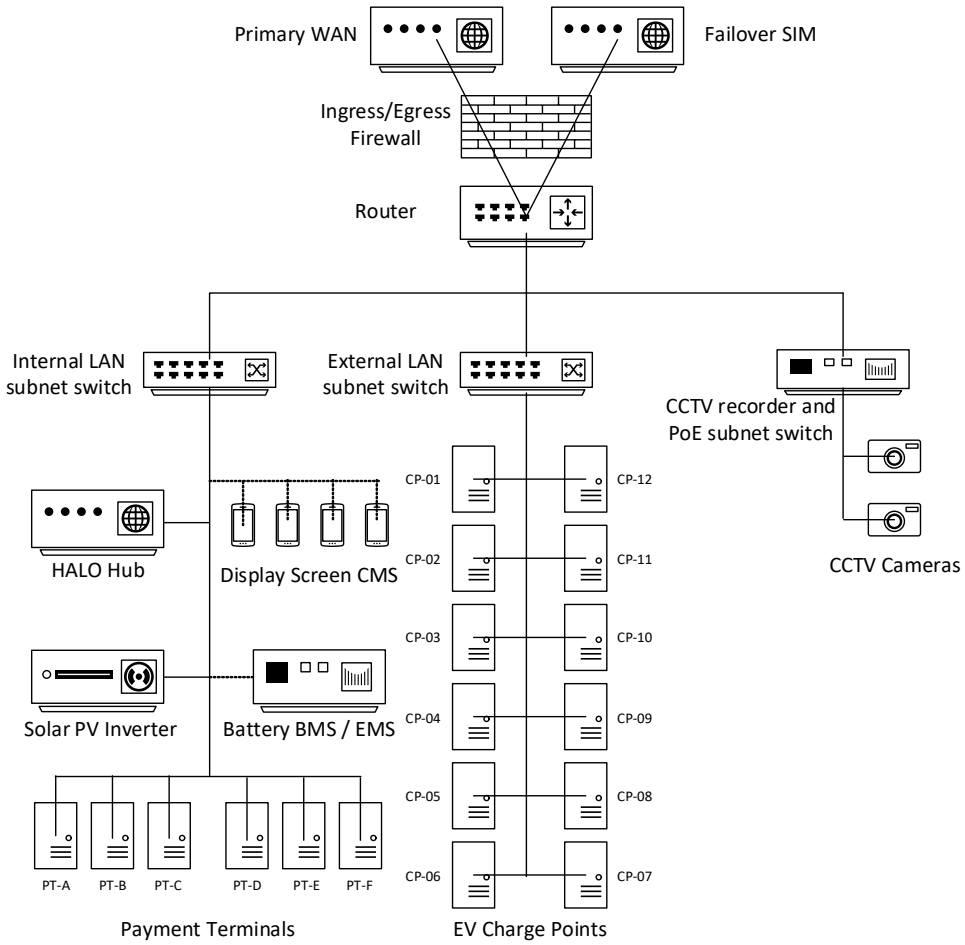
HALO FastHub operates dual-channel failover communications: if the primary channel is lost, it automatically switches to the backup and will notify 3ti's O&M[4] team, keeping EV drivers able to start and pay for a charge whilst the fault is resolved.

The drawing below shows the typical internal network arrangement:

[3] https://www.legislation.gov.uk/ukpga/2018/18/contents

[4] O&M is short for Operation and Maintenance, see the Halo FastHub Operation and Maintenance Service document.

HALO FastHub Internet Access



For maximum reliability, HALO FastHub uses *non-homogeneous*[5] connectivity channels to minimise the risk of a simultaneous outage impacting both channels – for example, a dual-SIM solution, even if different networks, doesn't solve the problem if a shared cell tower loses power or upstream connectivity. This is why 3ti's preferred configuration is as follows:

- Use a client-hosted wired LAN/WAN as the *primary* communications channel.
- Use a 3ti-hosted multinetwork[6] cellular SIM as the *secondary* communications channel.

Wired LAN/WAN links are typically the fastest, most reliable, and most cost-effective channel, delivering the best overall EV driver experience. When installed at the same time as grid connection groundworks, a wired connection is a relatively inexpensive additional step.

[5] Non-homogeneous in this context means using different and distinct hardware and software channels.

[6] Multinetwork sims "roam" to whichever cellular network provides the best connectivity. 3ti use non-steered SIMs which connect to the strongest signal. They are not appropriate for long-term primary connectivity.

If client-hosted WAN/LAN isn't possible, 3ti can arrange, install and manage alternative primary communication channels – see §4, below.

3 Primary WAN Technical Requirements

HALO FastHub requires a straightforward WAN connection. It presents as a single IP client device to the host network via an internal NAT firewall, with no inbound routing requirements.

WAN connection requirements:

- TCP/IP v4 or v6 network connected to the internet delivered to HALO FastHub either from nearby feeder pillar (max 100m) or via a fibre media converter (for longer runs). Within the unit it connects to a standard RJ45 / CAT5 WAN port.
- Single WAN IP interface using either Static- or Dynamic (DHCP)- IP addressing (as preferred client); HALO FastHub can also be a direct internet-facing IP / Port, hosted in a DMZ or given private network range or VLAN with an upstream gateway.
- Upstream routers, firewalls and NAT are all acceptable provided they do not block outbound service ports (for example, by limiting to HTTP(s) 80/443 only). See §5 below.
- Minimum bandwidth 1-2 MBit/s. Typical data consumption ~40 GB/month[7].

For security, it is strongly recommended that primary connectivity is provided via an isolated VLAN or BYOD guest network, segregated from internal corporate networks.

4 Primary Connectivity Alternatives

Where a client site cannot provide a direct hard-wired WAN connection via an existing site network, subject to site-survey the following primary connectivity alternatives are supported (in order of descending preference). All are *less* preferable from a reliability and cost standpoint. 3ti will always provide a backup SIM as a secondary connectivity solution regardless of the chosen primary channel.

All additional costs for primary connectivity are payable by the client and will be added to monthly HALO FastHub service fees if 3ti provides them. Prices herein are indicative, exclude VAT, and a full quotation is available on request.

[7] Monthly data usage can vary considerably from ~ 1 GB/month to ~80 GB month depending on site utilisation and/or the use of additional services such as payment terminals, advertising screens, CCTV, grid flexibility and battery storage systems.

4.1 Business Broadband (fixed-line)

This option uses a dedicated FTTC / FTTP business broadband line (e.g. BT Business / OpenReach) to HALO FastHub, avoiding data traversal of client networks. A dedicated connection (particularly FTTP) is highly reliable but may involve additional siteworks and periodic renewal overheads.

Installation costs vary significantly and can be covered by the client, or 3ti can install and optionally amortise the cost over the HALO FastHub service contract. Where practicable the service router / connection hub should be installed building-side to facilitate future flexibility.

Estimated cost: £40/month broadband, plus installation (typically £50–£150/month if amortised over the HALO FastHub contract length).

4.2 StarLink (satellite)

Whilst StarLink is occasionally vulnerable to service interruptions, these tend to happen for a few minutes overnight whilst satellites reposition. When paired with 3ti's failover SIM this provides sufficiently reliable, independent primary internet connection at reasonable cost.

Estimated cost: £100–£300/month depending on location, inclusive of hardware. Where practicable, StarLink should also be installed building-side using a wired WAN connection from HALO FastHub; this provides a fixed service address and adds future flexibility to replace with alternative primary communication channels. If this is not practicable, StarLink can be mounted directly to HALO FastHub.

4.3 WiFi (+SIM)

When paired with 3ti's failover SIM communication WiFi can provide a sufficiently reliable, independent primary internet connection at near-zero monthly cost, although less reliably than fixed line or StarLink.

A strong WiFi signal can be used in place of a hard-wired internet connection, perhaps using parabolic / high-gain antennas at one or both ends of the link. WiFi Access control must be via a fixed SSID/PSK only, without any captive portal / hotspot landing / login / payment access pages. DHCP is essential in this configuration, although MAC filtering can be reliably applied if required.

The estimated cost for this is £500 for hardware/installation with no ongoing monthly costs. Similar to StarLink, it is recommended that the WiFi link distance is minimised using a wired network bridge if possible; e.g. a wired WAN connection

provided from the HALO FastHub to the building, and WiFi bridge installed building-side closer to the network it is bridging to.

If this is not possible, an external WiFi-WAN antenna can be mounted to HALO FastHub, ideally at an elevation where it will not be frequently interrupted e.g. by delivery lorries.

4.4 Dual-SIM (NOT recommended)

It is *possible* for 3ti systems to operate using only an additional 4G/5G data SIM; however this creates a complete dependency on cellular networks, which are prone to interference, operator-side reconfiguration, upstream outages and issues with signal strength, latency, throughput and reliability. This is especially problematic for sites with contactless payments enabled, where connectivity drops can cause failed or stuck transaction pre-authorisations, driving customer dissatisfaction and additional support calls.

Such issues are especially likely during periods of high demand, such as public events or locations when large numbers of visitors are present within a cell – which often coincide with times lots of visitors want to charge.

Even with failover multi-network SIMs (as used by 3ti), SIM-only installations have a poor reliability record compared to other solutions; 4G/5G cellular towers are shared between multiple providers and networks and often, the issue causing one SIM or network to fail causes the others to fail too – they lack the data channel and infrastructure independence of recommended non-homogeneous solutions.

Whilst operating SIM-only is acceptable for short durations (e.g. during initial commissioning, or where there is a temporary problem with the primary internet channel), this solution is NOT recommended as a permanent solution:

1. Reliability and resilience are reduced.
    a. For public sites subject to PCPR[8], single-source connectivity is unlikely to meet uptime requirements and can result in failed / stuck credit-card preauthorisation issues.
    b. For private sites, EV charging can become unreliable and frustrating at peak times.

2. Engineering call-out costs; where SIM-only (even dual-SIM) is chosen, 3ti requires acceptance of additional on-site call-out charges for visits caused by SIM connectivity losses.

[8] PCPR: The Public Charge Point Regulations 2023 (see Background, above).

Consequently, 3ti will not offer 4G/5G-only as a connectivity solution for public sites subject to PCPR. For private sites, 4G/5G-only will be considered only following a site survey confirming reliable signal quality across multiple networks.

Estimated costs: £40–50/month for data charges and £400-500/visit for on-site call-outs. 3ti accepts no liability for financial penalties arising from PCPR uptime non-compliance.

5 Service Ports

Whilst there are no *inbound* port mapping requirements, HALO FastHub must be able to communicate *outbound* on a wide range of services. The following is a list of outbound service ports and services which should be accessible. The 3ti team will be able to advise which groups within this list are relevant to your installation – most commonly 1, 2, 3 and 5.

5.1 Group 1: Basic Networking

- **ICMP ECHO** (optional, but recommended for diagnostics)
- TCP Port 53 (DNS fallback)
- TCP Port 853 (DoT)
- TCP Port 80 (HTTP)
- TCP Port 8080 (HTTP)
- **UDP** Port 53 (DNS)
- **UDP** Port 123 (NTP)
- TCP Port 443 (HTTPS)
- TCP Port 8443 (HTTPS)

5.2 Group 2: Maintenance

- TCP Port 1194 (OVPN)
- **UDP** Port 1194 (OVPN)
- **UDP** Port 51820 (WireGuard)
- TCP Ports 15009-15011 (RMS Mgmt.)
- TCP Ports 15039-15040 (RMS Mgmt.)
- TCP Ports 15041 – 15100 (RMS Maint.)
- **UDP** Ports 30000-59999 (RMS VPN)
- TCP Port 20022 (RMS Connect)
- TCP Port 20080 (RMS Connect)
- TCP Port 20100 (RMS Connect)
- TCP Port 23389 (RMS Connect)

5.3 Group 3: Operations

- TCP Port 1433 (HALO)
- TCP Port 15003 (HALO)
- TCP Port 9998 (Fuuse WS)
- TCP Port 9999 (Fuuse WSS)
- TCP Port 1883 (MQTT)
- TCP Port 8883 (MQTTS)
- TCP Port 5671 (AMQPoT)
- TCP Port 8081 (Clenergy WSS)

5.4 Group 4: Payments (CPI)

- TCP Port 10101 (CPI OTA)
- **UDP** Port 10101 (CPI OTA)
- TCP Ports 9527-9528 (SST SBC)
- **UDP** Port 3479 (SST QUIC)
- TCP Port 6783 (SST SBC)

5.5 Group 5: Payments (PAX)

- TCP Port 3000 (PAX MSG)
- TCP Port 7275 (PAX GPS)
- TCP Ports 8089 (PAX RMT)

5.6 Group 6: Display Screens

- TCP Port 5500 (MIS)
- TCP Port 7001 (MIS)
- TCP Port 21 (MIS)
- TCP Port 990 (MIS)
- TCP Port 5901 (MIS)
- TCP Port 7002 (MIS)
- TCP Port 22 (MIS)

3ti reserve the right to amend both the service port and destination server lists throughout product life as those services and endpoints evolve.

It is strongly recommended that there are NO outbound (egress) port filtering[9] firewalls on the client connection: it adds minimal CyberSecurity benefit and creates disproportionate IT overhead for both Client and 3ti's IT team. Hostile firewalls also cause installation delays, performance issues and ongoing support requirements.

NOTE: The above list is the target server ports only. Full endpoint IP/DNS can be provided on request, however this is strongly discouraged as it creates a significant ongoing maintenance / update overhead.

Many services run on servers with dynamic IPs (e.g. AWS, Azure); client firewalls with egress filters restricting by destination IP or hostname will likely result in occasional service interruptions until IT teams are able to trace and implement the necessary changes. Allowlisting should be implemented via wildcard DNS ranges – nodal DNS and/or IP filtering in particular should be avoided.

Some services also use multiple parallel TCP connections for resilience; egress restrictions may force sequential / serialised communications and degrade system responsiveness and the EV driver experience. Firewall configuration practices which "snoop" traffic and only enable observed ports often fail after a period of a few weeks or months due to server-side load balancing and port hopping.

6 Security

3ti holds and maintains NCSC CyberEssentials certification[10], which includes annual review of our security posture and ensuring system software and firmware remains up to date. Teltonika IoT routers within HALO FastHub are within scope and remotely monitored and managed for maximum up-time and security. 3ti's third-party cloud and managed IT service providers are additionally ISO27001 and CyberEssentials+ certified.

HALO FastHub uses SSL/TLS via HTTP(S), WS(S), SSH, etc for all external communications; outbound VPN / secure tunnels are established as needed.

[9] Note: HALO FastHub's egress firewall will automatically block common insecure egress ports such as SMTP, Telnet, TFTP, NetBIOS, RDP, RPC, SMB, etc. No inbound ports are mapped, even during remote maintenance operations. Secure tunnels are short-lived destroyed by default after 1 hour.

[10] https://www.ncsc.gov.uk/cyberessentials/overview

Current Version (as amended): 3rd July 2026