Security and Connectivity

HEX@™ and HEX@GRID

HEX@™ and HEX@GRID vacuum controllers, from Atlas Copco, are changing the landscape of the industrial vacuum market. Featuring improved control and functionality, they are supported by top tier security and connectivity.

For Atlas Copco, our customer is the highest priority. Whether we are developing a new product, introducing a service or launching an initiative, our customer remains at the heart of our concerns. Because of this, our industry 4.0 enabled intelligent products are compatible with all major industrial communication protocols. Integrating efficiently and, just as important, securely.

SECURITY

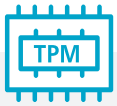
Digital security is an ever increasing concern in the modern industrial workplace. To meet the highest standards, it is no longer possible to have a single layer of security or a single measure in place to safeguard against data breaches.

Atlas Copco fully understands this and makes use of specialists in this field to ensure our products do not represent a weak spot in our customers' infrastructure.

These are some of the key security measures that are used by HEX@™ and HEX@GRID:

Data transfer certificates make use of Elliptic Curve Cryptography – ECC. A highly efficient and robust security standard within the digital marketplace

All data communication to HEX@TM enabled products to and from the cloud also makes use of encryption and private key protocols



Private keys used for decoding are stored on our tamper-proof and robust Trusted Platform Module 2.0 – TPM2

Software Validation 2 layered:

- Our products use software that is signed and encrypted
- Secure boot – software ID is validated each time the controller boot sequence runs

This means that our controllers will only run with our software. This software is given an identity and that is checked each time the contr oller runs. Third-party operating systems cannot be installed and used to control the platform.

Data on the controller is labelled as sensitive or not. If identified as sensitive, it is stored within it's own partitioned memory – which is encrypted to ensure the data is kept safe

Data ports are closely controlled at all times using iptables protocol. This means that where other devices can leave data ports open when not in use, our controllers limit this to an absolute minimum, restricting the access points a threat could use.

Operating system code is only accessible using verified certificates that are given short lifetime validity. This means that the controller code itself cannot be accessed using leaked passwords or as a result of data breaches elsewhere.

User access is tiered with appropriate security levels according to access type.

- User access limited to randomized passwords generated during the pump production – not a generic password that grants access to deeper pump settings
- Admin access for programing changes requires a short lived Json Web Token – JWT – to be downloaded by the user from our secure cloud portal

CONNECTIVITY

In our ever more connected world, connectivity is key. Our pumps have different options when it comes to levels of connectivity as well as communication protocols that can supported.

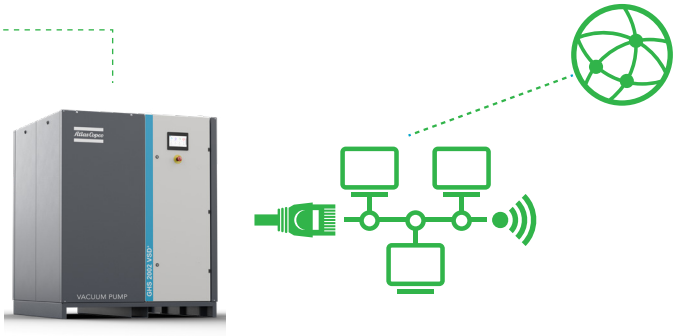
Fully connected pump

When a pump is fully connected it is integrated into the local site IT network and from there also given permission to securely connect to the Atlas Copco Cloud service. An example of this is shown below:

Here the pump is connected to the site LAN using ethernet cable (or WiFi bolt). The pump is then established on the network and can be accessed by any other device on the network such as a PC, laptop, tablet or smartphone (like a network printer or storage drive).

This set up allows the following possibilities:

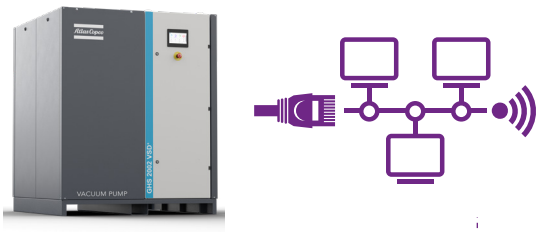
- Full remote access to the pump via the site network (including global access by site owner if VPN is in place)
- Cloud access allows automatic software updates for the pump controller with every new release (quarterly). No need for physical interaction as well as remote Atlas Copco support in the event of a problem



Network connected pump

This is when a pump is connected only to the Local Area Network (LAN), it is integrated into the local site IT network but is not given permission to securely connect to the Atlas Copco Cloud service. An example of this is shown below:

Here the pump is connected to the site LAN using ethernet cable (or WiFi Bolt). The pump is then established on the network and can be accessed by any other device on the network such as a PC, laptop, tablet or smartphone (like a network printer or storage drive).



This set up allows the following possibilities:

- Full remote access to the pump via the site network (including global access by site owner if VPN is in place)

If the pump needs to be updated with the latest software release, then the applicable software pack for this pump must be downloaded from the secure Atlas Copco cloud service and then manually uploaded to the vacuum pump. User authentication will be required to access the package.

Disconnected pump

When the pump is not connected to the network in any way, then access to pump controls or settings is possible using the optional HMI or by connecting a local device (Laptop, smartphone, etc) to the pump.

Remote access to the pump is not possible and like the partially connected pump, applicable software update packs for this pump must be downloaded from the secure Atlas Copco cloud service and then manually uploaded to the vacuum pump. User authentication will be required to access the package.

Site integration and BUS communications

In all three of the cases described, the pump can also additionally communicate with local bus and network protocols for further site integration. This can include:

EtherNet/IP™ EtherCAT® Modbus-RTU

Modbus TCP PROFINET® PROFIBUS® PROCESS FIELD BUS OPC UA

Feature	Fully connected pump	Network connected pump	Disconnected pump
Local control of the pump using front panel of optional HMI	✓	✓	✓
Local access to the pump settings using optional HMI or locally connected device	✓	✓	✓
Remote access to pump controls and settings via LAN	✓	✓	✗
Software updates (new features and bug fixes)*	✓	*Manually each time*	*Manually each time*
Optional remote support from Atlas Copco*	✓	✗	✗
User authenticated access to pump information (including operating data) without network access	✓	✗	✗
Email notification of pump failures	✓	✗	✗
Additional integration into local BUS or site communication network	✓	✓	✓

*Note: this feature is not available via Genius box connection.

Rest assured that when it comes to connectivity and security, the Atlas Copco HEX@™ platform places customer safety and convenience highest on our list of considerations.

For more information, please contact your local Atlas Copco representative.

6996 0072 93 – EN HEX@™ is a trade mark of Atlas Copco AB, Stockholm, Sweden. Production: Atlas Copco Brand Studio. September 2021.

Atlas Copco

Atlas Copco AB

atlascopco.com/vacuum