Howden
A Chart Industries Company

White paper

Howden Uptime
Security

Revolving Around You™

www.howden.com

Abstract

This document will give you a brief overview of the security concepts deployed throughout the Howden Uptime technology stack.

The Howden Uptime data journey consists of four parts. The first part is the “Asset” which represents the equipment that delivers operational data via sensors which are stored in the DCS (distributed control system), the PLC (programmable logic controller) or delivered directly to the Edge.

The second part is the “Edge” device, which can be an edge gateway (industrial pc) or a virtual machine. The third part is the “Communication”, which realises the data transmission from the customer site to the Howden Uptime “Cloud”, which represents the fourth part of the data journey.

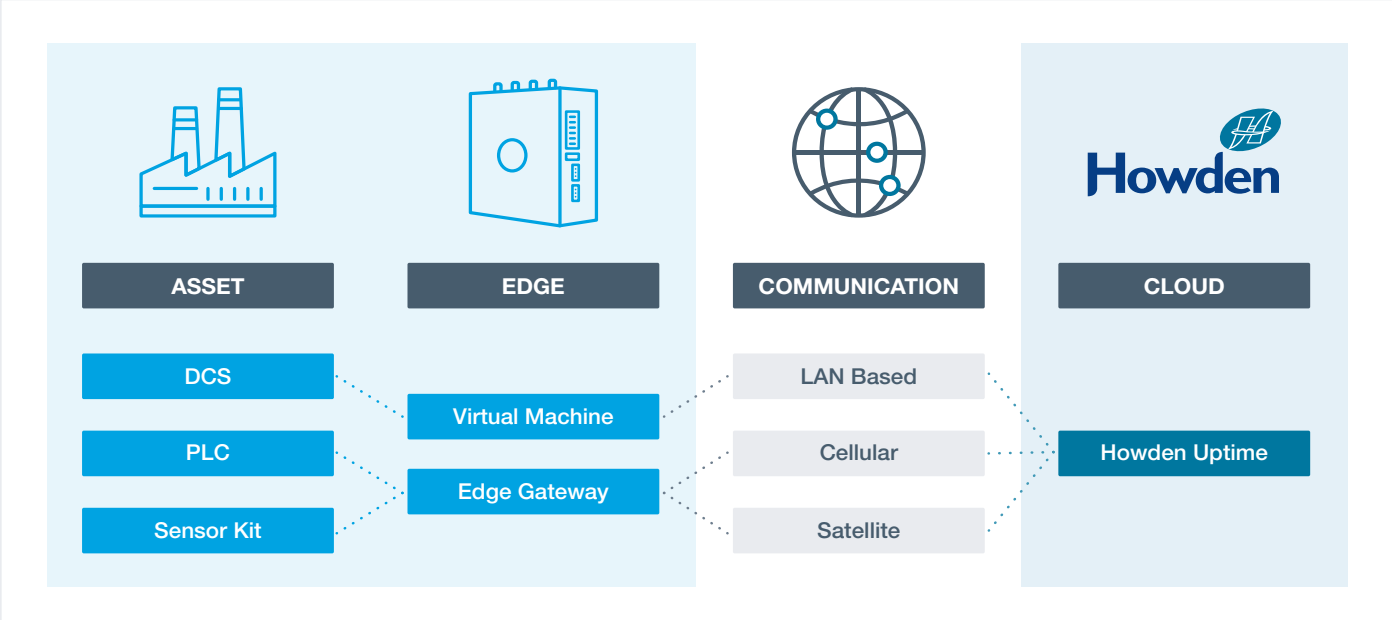

Figure 1: Howden Uptime Overall Architecture.

Asset

The equipment (“Asset”) is equipped with a set of sensors, which gather the operational data of the machine. Depending on the installation, the operational data is streamed from the PLC or the DCS.

There is an additional solution that exists for equipment without any monitoring, which is to connect a special sensor kit directly to the edge gateway.

In a case where the data resides in the DCS, a replication of the data relevant to the asset is stored in a data mirror, then from there the replicated data is transmitted to Howden Uptime.

This ensures a separation of the control system layer from the transmissions layer. The Howden Uptime server never actually connects to the real historian database as it is only connected to the replicated one, mitigating any risk.

Edge

The Edge is the device used to receive the data from the control system and to send the data to the Howden Uptime ThingWorx model residing in the Microsoft Azure cloud.

Hardware

There is a 24x7x365 support contract in place with Microsoft and PTC to support this application. In the event of a hardware failure, a replacement Edge will be dispatched with an image of the configuration pre-installed, within 24 hours.

Patch management for Windows 10 IoT, ThingWorx Industrial Connectivity and Edge Firmware are all updated and managed by Howden, in partnership with PTC and Microsoft, via the established internet connection to ensure that all operating systems and software are kept up to date. Crowdstrike Falcon next generation protection is preinstalled on the Edge to ensure depth in defence, detection and response.

Many national agencies around the world are now specifying that the industrial communication components and systems deployed in national infrastructure projects must meet a certain level of security.

For instance, in order to achieve a particular IEC 62443 security level target, an IT-OT bridge may be required to physically isolate the two networks, one critical and one open, from each other. In these instances, a data diode unit can be placed between the two networks in order to achieve this. The diode unit is purely passive with no influence on the critical network and importantly there is no possibility of introducing external data into the critical network.

On all hardware deployed specific to Howden Uptime applications any unused serial, USB or RJ45 ports are disabled or otherwise secured to prevent unauthorised access.

Additionally there is an option to provide a “virtual Edge”, which is a virtual machine image running the same OS and software like the normal Edge. The “virtual Edge” is an appliance, which is installed in the client environment.

Edge (cont.)

Software

Every OPC Unified Architecture (UA) product, client, or server gets an X509 certificate called an application instance certificate. This certificate consists of three things: a public key that is known to the world, a private key that is only known to the application, and identity information that enables applications to know who owns the certificate.

With ThingWorx Industrial Connectivity (former KEPServerEX) installed on the Edge, the Security Policies advanced plug-in is included with all licenses. The Security Policies plug-in allows administrators to assign security access permissions on individual objects (such as channels, devices, and tags) based on the role of the user interacting with the Runtime project. It is used in conjunction with the server's User Manager, which enables management of user groups, users, and default security settings.

This enables only those signed in with the correct privileges to modify the communications settings between the Edge and the control system further down the ISA 95 model and the supervisory systems further up the model.

ThingWorx Industrial Connectivity has many industrial drivers allowing connection to older retrofit applications that used propriety protocols but thanks to the convergence of IT and OT applications many modern control systems use more modern and secure protocols. Typically, the protocol of choice on modern industrial IoT platforms is OPC Unified Architecture (UA). OPC UA was designed with security in mind. One of the key ways OPC UA protects the integrity and confidentiality of messages is through message encryption and signing.

OPC UA uses an IT technology called X509 certificates for message signing and encryption. Message signing means when your application receives a message, you can know exactly who sent it by checking the message signature. This protects against rogue entities sending your client or server bogus requests, or man in the middle attacks. Message encryption provides confidentiality by guaranteeing that only the receiver is able to read a message.

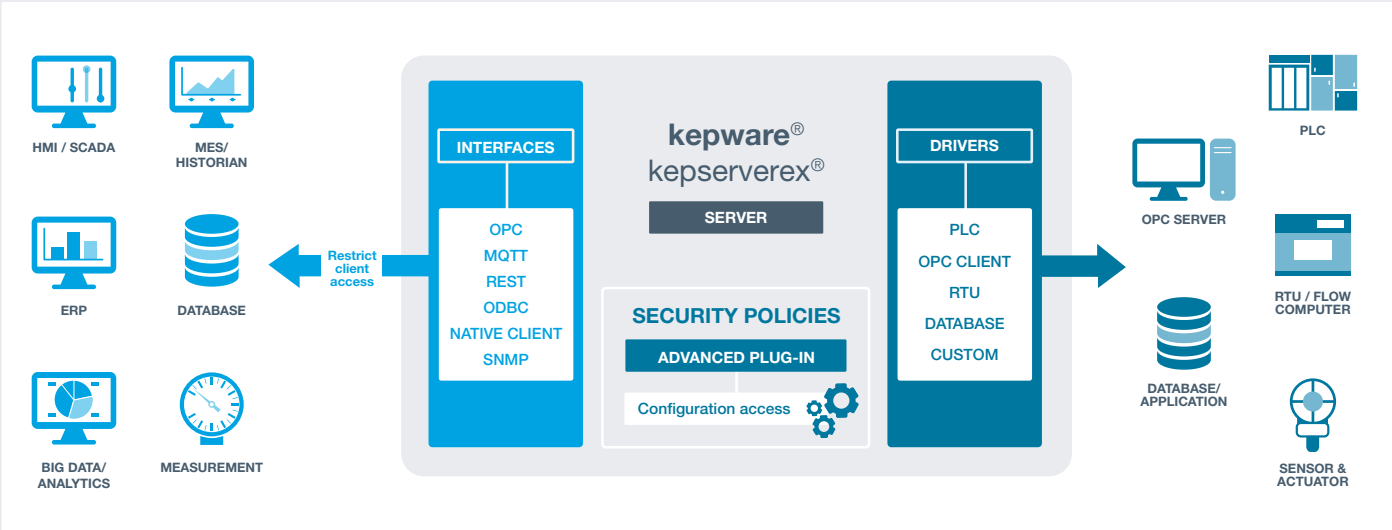

Figure 2: OPC Architecture (PTC).

Communication

Cellular/Satellite

A range of cellular options are available from AT&T. The standard connection uses cellular connectivity over a private APN that interfaces with Azure over a dedicated private MPLS cloud, so traffic will not touch the public internet. In addition a VPN or IPSecVPN connection is available, but additional charges will apply.

The Edge has a static IP address to connect to the control system local area network but connects using dynamic IP addresses to the cellular network. Our partner AT&T also provide a range of satellite communication options either for remote locations or for offshore-based applications.

Local Area Network (LAN) based

Another communications option that is available, especially on assets that are DCS controlled, is the communication option via LAN based internet connection. In this case the communication runs through a client managed firewall.

Cloud

Azure

Microsoft Azure runs in datacenters managed and operated by Microsoft. These geographically dispersed datacenters comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. The datacenters are managed, monitored, and administered by Microsoft operations staff. The operations staff have years of experience in delivering the world's largest online services with 24x7 continuity.

Howden use the shared responsibility model where it's important to understand the division of responsibility between the end user and Microsoft.

On-premises, the end users own the whole stack, but as operations move to the cloud, some responsibilities transfer to Microsoft. Figure 3 illustrates the areas of responsibility, according to the type of deployment of the stack (software as a service [SaaS], platform as a service [PaaS], infrastructure as a service [IaaS], and on-premises).

As end users, Howden are always responsible for the following, regardless of the type of deployment: Data, endpoints, account and access management.

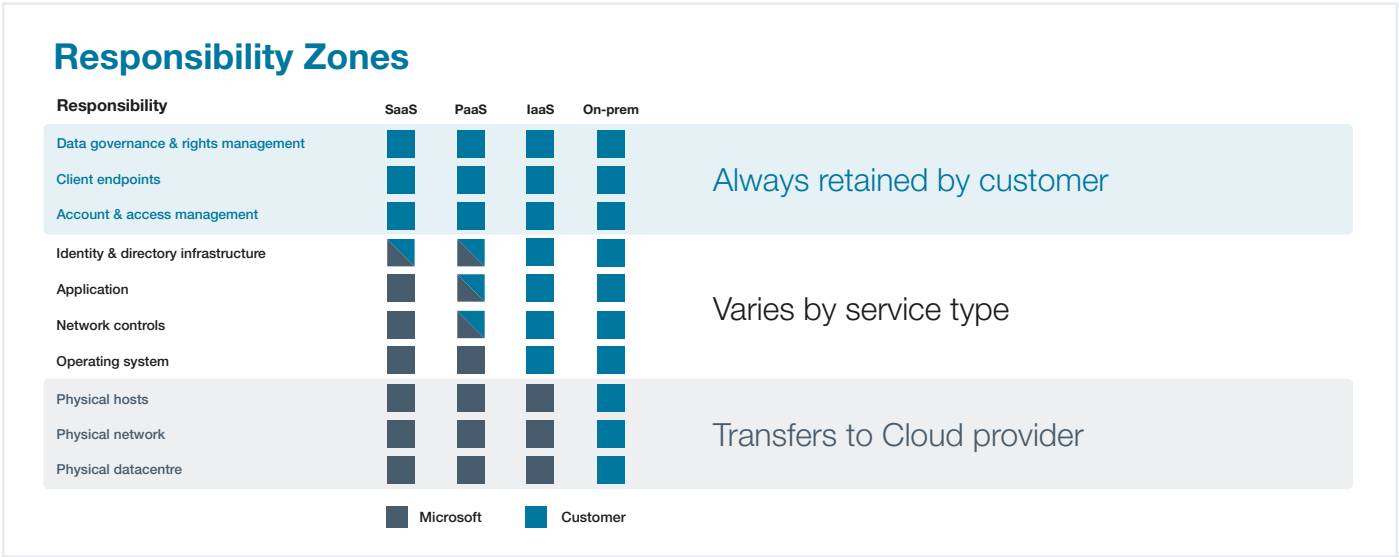

Figure 3: Microsoft Azure responsibility areas.

Cloud (cont.)

Thingworx

The ThingWorx Platform has an extremely granular security model to enable data isolation and service execution at any required level. The ThingWorx Platform supports HTTPS authentication, which requires a user to establish a web session using a username and password.

In addition, The ThingWorx Platform has a pluggable authentication model which allows customers and partners to implement their own business process specific authentication model. This extensibility also enables the ThingWorx Platform to release new authentication modules independently of major releases. The ThingWorx Platform can support standard industry mechanisms such as SAML, and SSO integration from other tools such as Salesforce.com, SAP and others.

The ThingWorx Platform has an Access Control List (ACL) model that allows administration of ThingWorx Platform authorization to a very detailed level.

The ThingWorx Platform has overlaying levels of security that can be applied. Access control can be granted or denied at the most granular level, such as specific read or write access to a single 'Thing Property'. This allows Howden to assign clients access to their assets and after that the clients can then allow their 3rd party maintenance contractors, for instance, access to those assets as well.

If the client has multiple sites the client administrator can allow the users on one site, 'A', access to the site A assets and then similarly allow the users on one site, 'B', access to the site B assets, but the administrator gets to see all of site A and B assets. There are separate permission settings for Design-Time and for Run-Time. Both Design-Time and Run-Time permissions can be set for any entity in the system. Only Howden application designers have access to any Design-Time environment features.

Vulnerability testing

Each year, the Howden Uptime technology stack is put through a vulnerability assessment to ensure it remains robust and up to date against an ever changing threat environment.

This involves contracting a third party to test each aspect of the system, aiming to identify security issues that could negatively affect business or reputation if exploited.

The type of testing used in this case is known as Grey Box testing, which involves the testers knowing some internal aspects of the system, but not everything.

Conclusion

In conclusion, all four parts of the Howden Uptime technology stack have highly robust and verified security options in place to manage the transmission of your data all the way through the data journey, safely.

Further reading on each of the separate parts of the technology stack is available on request, following the completion of a non-disclosure agreement.

Author: Dr Billy Milligan, Solutions Development Lead - DDA, Howden
Co-Author: Frank Scherz, Team Lead Automation & Controls R&D - Howden

e: uptime@howden.com
w: www.howden.cloud/uptime

Revolving Around You™