

Connecting Automation Systems to the IoT via HMIs

Many human-machine-interface (HMI) software solutions enable Internet of Things connectivity in a variety of ways. Here's a look at how to do it, along with instructions for configuring an HMI.

Machine builders are connecting their automation systems to the Internet of Things (IoT), and many human-machine-interface (HMI) software solutions enable IoT connectivity in various ways.

HMI software has evolved in form, capabilities, characteristics, expectations, and purpose. While providing a graphical interface for local operators and the process are the leading HMI requirements, modern HMI software based on open standards goes way beyond this basic functionality to provide many other features.

SMART HMI FEATURES

A modern HMI can be either embedded or PC-based. An embedded HMI



runs on a dedicated platform powered by an operating system such as Windows Embedded or Linux, and a PC-based HMI typically runs on a full-featured Windows operating system. PC-based HMIs are more powerful and more expensive, while embedded HMIs often provide sufficient capability, and are always lower in cost and simpler to setup and maintain. With either type of HMI, functionality beyond a simple operator interface can transform it into a smart HMI.

SMART HMI FEATURES

HERE IS A LIST of some of the features found in smart HMIs, many of which are integral to IoT implementations:

- Open architecture
- Built-in drivers for connection to a wide variety of field devices and controllers
- Integration tools for network and Internet connections
- Platform-agnostic runtime
- Integration with legacy and proprietary systems
- Browser-based access via the HTML5 standard

Smart HMIs have open architectures, enabling use of a variety of off-the-shelf hardware and software. They work with an array of operating systems and allow use of open technologies, such as ActiveX, Extensible Markup Language (XML), and .NET to visualize documentation and videos, and to listen to audio messages. The ability to open, edit, and save spreadsheets, documents, and Adobe files is another feature of open-architecture HMIs.

ISO/TS 16949
MADE IN THE U.S.A.

TRIM-LOK

TRIMS AND SEALS

Our products use
3M Automotive Attachment Tapes

EPDM SPONGE RUBBER TUBING
HIGH STRENGTH BOND
INDIVIDUAL METAL CLIPS RETAIN A PERMANENT GRIP
PVC (VINYL) TRIM WITH METAL CLIP

AND SO MUCH MORE!

CALL US FOR A **FREE** CATALOG
800-853-4489 • www.trimlok.com

PI

Micro Stages: Linear, Rotary, XYZ, 6D

FOR ALL POSITIONING & AUTOMATION APPLICATIONS

Brushless DC Motors

Stepper & DC Motors

Voice Coil, Flexures

Ultrasonic Motor

Piezo Inertia Motor

Learn more ▶ pi.ws/micro
PI (Physik Instrumente) 508.832.3456

PI: The Broadest and Deepest Portfolio of Precision Motion Technologies

Vacuum Stages

Flexure Stages

Air Bearings

Piezo Mechanics

Hexapods

Beam Steering

Mini Stages

Fiber Alignment

BUILDING BLOCKS OF AUTOMATION



Cut-To-Length



Punch Assembly



Knife Assembly



Unwind-Rewind



Rotary Knife



Slitter Station

Smart HMIs

This openness also allows development of a single application deployed on many different platforms, including Microsoft standard, embedded, and mobile Windows. Some smart HMIs also support versions of Linux, VxWorks, and other embedded operating systems.

These HMIs must connect to a wide variety of controllers and devices. Although some limit the types of connections available to their proprietary controllers and other components, other HMI suppliers support hundreds of drivers for programmable logic controllers (PLCs), Object Linking and Embedding for Process Control (OPC, client and server), TCP/IP, and other connections.

Smart HMIs also include built-in integration tools for quick connections to networks and the Internet. These tools are typically menu-driven and create connections by filling in the blanks with information with respect to the device to be connected and to the type of network.

These smart HMIs can easily tie into enterprise resource planning (ERP) and “back-office” systems using built-in relational database connectivity. These drivers and open architecture also make integration with legacy and proprietary systems fast and reliable.

Platform-agnostic, full-featured HMI software provides the opportunity to reshape automation-system architectures and eliminate constraints imposed for decades by closed systems. For example, it is now possible to deploy the HMI software on the same hardware where the real-time control software is running, such as a PC.

Smart HMIs with platform-independent “thin client” visualization based on HTML5 are a good choice, considering the wide variety of PCs, tablets, and smartphones available that support this standard.

HMI SECURITY AND CONFIGURATION

When creating a networked HMI application, a good place to start is with cybersecurity and system configura-

tion. As with all network and Web-based automation-system connections, well-planned and robust security is necessary.

Whether the HMI access is via a PC connecting to an in-plant network or a mobile device accessing the HMI via the cloud, all users must be required to go through an authentication process where they enter a user ID and a strong password. This authentication process is an industry standard and built in to the HTTP protocol.

Here's how to set up an HMI to ensure cybersecurity:

Limit remote device functionality.

Many security concerns involve access to the main HMI application from remote devices. The more remote the device, the less access it should be given. For example, an in-plant thin client will have a wide range of functionality, while a smartphone should probably be limited to viewing a small subset of data.

Provide proper password protection.

A strong password is just the start. Smart HMIs allow setting a minimum password size with certain required characteristics, such as the use of letters, numbers, and symbols—thereby increasing password strength. Once securely logged on, it is a good idea to enable an auto log-off after a period of inactivity.

Carefully configure network. Cybersecurity incidents frequently involve an automation system or HMI connected to a corporate or business network, so the industrial automation network must be properly segmented from the business network. The automation network should not be directly connected to the Internet. Instead, there should be a proxy server, an intermediate network, or access controls such as a virtual private network. Blocking all other network connections is part of a well-designed cybersecurity configuration.

Create a whitelist to restrict access to known devices. Smart HMIs allow password protection of screens, objects, and editing. It is not uncommon to have up to 256 user or group levels of security available. It may also be possible to inde-

pendently secure capabilities in the HMI development and runtime environments.

Configure the HMI to protect the development and the runtime platforms. Securing the development environment with smart HMIs is a good way to control access. Project settings, driver configuration, data sources, and network configurations can be secured via passwords and user-access methods. Even creation and modification of tags, screens, and tasks can be controlled.

Once cybersecurity is established, it is time to move to the next steps for developing a smart HMI application.

HMI DEVELOPMENT AND PUBLICATION

A smart HMI provides a variety of tools to create the application, design screens, and publish data to PCs and other displays.

The collection of automation tools needed to develop HMIs screens is often provided right out of the box, and screen design is one of the areas of primary focus during HMI application development. If the HMI supports HTML5, much of this time can be saved because this standard provides “develop once and deploy too many” capability. This capability is commonly deployed with the main HMI acting as the Web server, and the remote devices accessing and displaying information via any Web browser supporting the HTML standard.



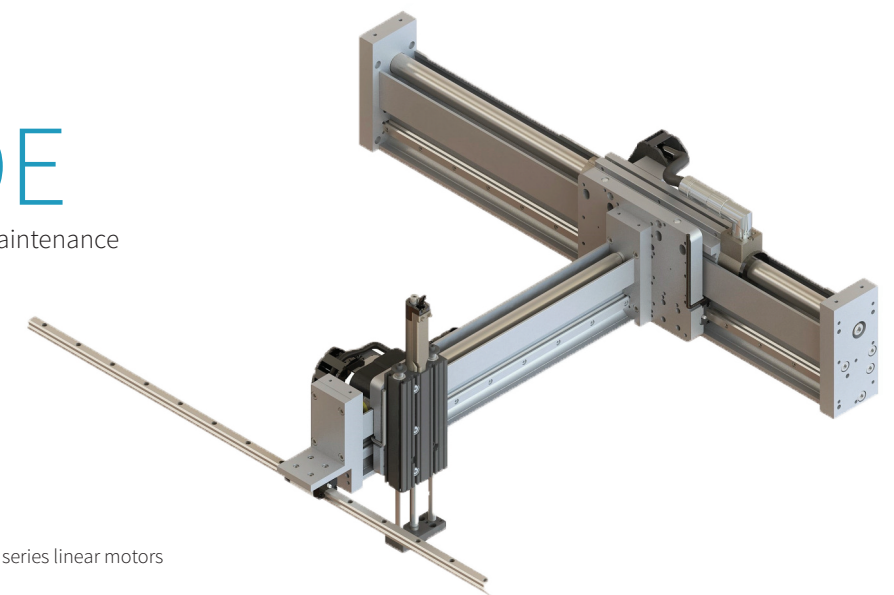
Smart HMIs allow deployment to a wide variety of mobile and fixed devices, as well as provide built-in tools to maintain proper cybersecurity.

Even with this capability, it is still important to consider how the HMI will be used on the remote device. A PC hosting the main HMI application displays comprehensive machine data and graphics, while a smartphone may just be used for a quick check of information.

In general, HMI screens intended for display on a tablet or smartphone should be developed to show a limited amount of data. Showing the operator information that can be quickly viewed on these small devices can reduce operator information overload and eliminate or make it difficult to see information.

Introducing LinMot's new F GUIDE

High Performance & Low Maintenance



Semi gantry shown with 48, 37, & 23 series linear motors

precision

and

dynamics

LinMot®

linmot.com linmotusa.com
262-743-2555

Durable • Precise • Flexible Superior Flexible Shaft Couplings

ISO 9001:2008 Certified

Performance & Reliability.....
a Win, Win Combination!

- Thinnest high strength walls
- Zero backlash
- Superb flexibility
- Customization
- Extremely low elastic windup
- Seamless construction
- Low to moderate torque
- High cycle life



SHOP Online!

Servometer
buy.servometer.com



Smart HMIs



Along the same lines, it is not necessary to make all screens developed for viewing on the main PC or embedded platform available for viewing on smaller devices such as tablets and smartphones. Instead, developers should just provide access to a limited number of carefully considered screens.

With smart HMI development systems, downloadable HMI runtime applications target platforms via a variety of connections. For example, a specific application for a remote computer can be downloaded, started, and stopped remotely. Locally or via a wired or wireless Ethernet connection, the HMI application can be published and run using simple menu-driven steps.

Many HMI software development packages have built-in download tools to make deployment easy and fast. HMIs with these built-in tools do not require USB memory sticks or other devices to download applications to remote stations. Instead, these tools allow download and upload of project files, run/stop control of remote applications, and runtime licensing. These tools are usually menu-driven, and only require the user to fill in the blanks as to the target device's location on the network.

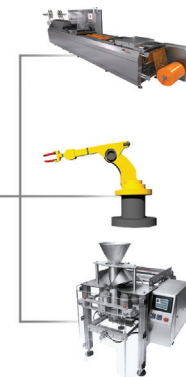
IoT CONNECTIVITY

How does this all tie into the IoT? It starts with HMI connections to a wide variety of sensors and other field devices, which are what makes up the IoT. Many types of machines and other parts of industrial facilities house these devices. Once connected, these devices have access to the Internet through networks and clouds via the HMI.

The HMI connects to a local, in-plant automation network for communication to field devices on a single line, cell, or system via a controller. Smart HMIs also offer the ability to directly connect to intelligent field devices, such as motor drives, multi-variable instruments, and analyzers.

As the connection moves outside the plant to distribute data to remote platforms, proper security steps should be taken as discussed above. In some configurations, these remote or mobile HMI platforms connect to the main HMI via the cloud. These clouds can be public, private, or hybrid. Public clouds must be carefully configured to protect data.

More appropriate cloud-storage methods for industrial applications are private and hybrid, as both offer better protec-



Whether inside the factory or out, local and remote HMIs are the window into the machine, production, and factory floor.

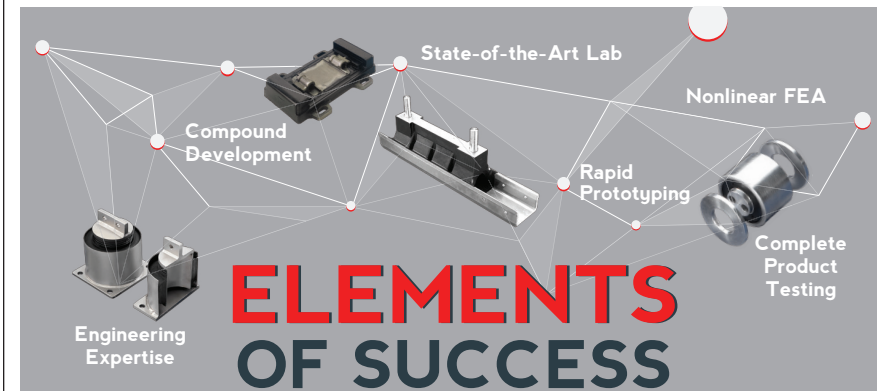
tion of the data. These include firewalls, better passwords, or encryption methods. Private clouds are on-premises networks, and as such, can offer in-house staff the ability to carefully and continuously monitor a high level of security of all connections.

Although there are many different types of hybrid clouds, the most common for an HMI deployment would be a dedicated and secure network deployed off premises and administrated by a staff of IT personnel, many charged with maintaining cloud security. Security procedures such as whitelisting can be implemented with a private cloud, but this will require close cooperation with the firm hosting the cloud.

Smart HMIs support browser-based mobile access via the cloud, providing instant access to equipment and production data. The open-system authentication process on these HMIs helps users maintain data security without the need to become cybersecurity experts.

CONCLUSION

Smart HMIs provide built-in tools and menu-driven instructions to allow connection to a wide variety of field devices, either through controllers or directly. Once data is collected, it can be securely distributed through networks and the cloud to many different types of platforms, including thin clients, tablets, and smartphones. The HMI should be equipped with the tools and menus to enable data distribution in a secure manner without the need for custom programming. **md**



ELEMENTS OF SUCCESS

INNOVATIVE ELASTOMERIC SOLUTIONS

Corry Rubber Corporation is an ISO-9001:2008, ISO-14001:2004 and ISO/TS-16949:2009 certified manufacturer equipped with an ISO-17025 certified laboratory specializing in the engineering, development, on-site mixing and manufacturing of highly engineered elastomeric and plastic components and systems.

LET US DEVELOP THE RIGHT
SOLUTION FOR YOU!



sales@corryrubber.com | 814.664.2313 x226 | corryrubber.com

TRUST REELL

Solutions

- ✓ Precise positioning
- ✓ 1000+ configurations from 0.0 to 11.0 N-m
- ✓ Motion variety Symmetric, One-way and Differential
- ✓ Presale engineering support

Reell creates
a perfect solution



REELL

Innovative Torque Solutions
Our promise – A perfect fit and feel

PLUG AND PLAY

When Accuracy and Speed Matters

MICROTRAK™ 4

- 0.03% FSO
- 40kS/sec. sensor frame rate
- USB for power and data
- All digital output

mti instruments

www.mtiinstruments.com
1800-342-2203
sales@mtiinstruments.com