IoT Software Distribution and Services

Accelerate Your Application Development

- IoT Cloud Services
- IoT Gateway Software Solutions
- RTOS for Sensor Node
- Microsoft Windows Embedded OS
- Linux and Android Solutions
- Wind River VxWorks
- Acronis Backup and Recovery
- Intel Security Solutions
- WISE-PaaS/RMM
- Software APIs
Complete IoT Software Solutions

The Internet of Things connects all kinds of electronic devices via the Internet. It is a web-enabled data exchange that empowers devices with “smartness”. In other words, the IoT aims to integrate the physical world with the virtual world by using the Internet as the middleware to communicate and exchange information.

Due to the sheer number of products and devices, some of which use non-standard specifications, there are often unconventional requirements demanded of IoT devices and the environments that support them. For instance, many problems emerge from the limited form-factors and power available to IoT devices. Others issues arise from the way in which IoT devices are manufactured and operated.

The best approaches are much more like traditional consumer product design, combined with existing best practices for server-side and Internet connectivity that need to be factored in. We can summarize the overall requirements into some key categories:

- Connectivity and communications
- Device Management
- Scalability
- Security and Privacy
- Data collection, analysis, and actuation

The Advantech IoT Software Structure

Advantech supports ARM/x86 systems in general and not specific sets of technologies. We support the most popular open source projects and leading technologies to provide the best solutions. We also provide APIs, Operating Systems, applications, and cloud services to help developers easily implement more IoT solutions in the field.

Advantech IoT Software Architecture consists of a set of layers. Each layer performs a clear function and layers can be instantiated by specific technologies. There are also additional functions supplied by 3rd party cloud and security solutions.
IoT Cloud Services

Cloud Services consist of three elements: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Solution as a Service (SaaS).

Advantech’s IoT Cloud Services focus more on the PaaS, providing the necessary and useful building blocks to support customer solutions and leveraging IaaS to provide computing, storage, and networking services.

Advantech is partnering with Microsoft® Azure as the IaaS and also PaaS solution provider through the Microsoft CSP (Cloud Solution Provider) Program, in order to offer more diverse functions for IoT applications. (WISE-PaaS, Advantech’s IoT platform, also provides a total solution from devices to cloud services as an evolution via CSP. WISE-PaaS helps customers build their new generation products and services for the IoT era.)

We have prepared pre-configured software solutions for the Azure marketplace. It only take few minutes to connect Advantech devices to an Azure virtual machine, which already has all the needed services installed and well configured. Advantech software for Azure helps customers fill their IoT solution deployment gaps and focus on core vertical services.

We also provide IoT devices which have already passed Azure certification. These devices are pre-integrated with an Azure IoT suite and complete data connections. Customers can design IoT solutions easier and take advantage of machine learning for data analysis that boosts efficiency and reduces cost.

Advantech provides Azure subscriptions as a CSP. We provide technical support and design-in services that reduce trial iterations and optimize development.
IoT Gateway Software Solutions

The Gateway layer supports the connectivity of all devices and there are multiple potential protocols for communication between the devices and the cloud. The four most well-known potential protocols are:

- HTTP/HTTPS (and RESTful approaches on those)
- MQTT 3.1 / 3.1.1
- AMQP
- Constrained Application Protocol (CoAP)

We chose MQTT as the preferred device communication protocol, with HTTP as an alternative option. The reasons for selecting MQTT and not CoAP at this stage are:

- Better adoption and wider library support for MQTT; 24 different programming language libraries have been provided on the official web site.
- Simplified bridging into existing event collections and event processing systems.
- Simpler connectivity over firewalls and NAT networks.

One important aspect with IoT devices is not just for the device to send data to the cloud/server, but also to receive data from the cloud/server. This is one of the benefits of the MQTT specification: because it is a brokered model, clients connect via an outbound connection to the broker, whether or not the device is acting as a publisher or subscriber. This usually avoids firewall problems, because this approach works even behind firewalls or via NAT networks. We think the gateway software stack should cover OS, connectivity, security, and manageability.

- Operating Systems: specific for gateway solutions, such as Windows 10 IoT Core, Wind River Intelligent Device Platform, Wind River Pulsar, Open source Yocto, Unbuntu Snappy Core, and Red Hat Jboss.
- Connectivity: covers the cloud uplink via the Internet through MQTT, AMQ, and downlink with Wire/Wireless PAN with Legacy I/O, BLE, Zigbee, SubG, IBM LoRa, or Sigfox.
- Security: includes open SSL, TLS, and also Intel Security for each device.
- Manageability: WISE-PaaS/RMM allows the gateway to be controlled and monitored with pre-configured actions or alerts to administrator.
Real Time Operating Systems for the Sensor Node

The bottom layer of the architecture is the device layer. Devices can be of various types, but in order to be considered IoT devices, they must have some communication protocols that either indirectly or directly attaches to the Internet. Advantech platforms provide the capacity to connect to the Internet either indirectly or directly. WISE-devices typically use System-on-Chips (SoC), such as ARM cortex M series or microprocessors integrated with low power consumption protocols; the objective being to provide long battery life and long-term data observation. WISE-devices are usually resource limited and typically have no operating systems, or run embedded Linux platforms such as OpenWRT, or dedicated real-time embedded operating systems such as mbed OS, Wind River Rocket or FreeRTOS. All IoT devices need to be compatible with the IETF and IPSO alliance, and with CoAP for certified interoperability and communication between devices.

Real-Time OS

Built for the Demands of Small, Smart, Connected IoT Devices

A rocket application combines application-specific code with a custom configured kernel to create a single binary that is loaded and executed on a system’s hardware. Both the application code and kernel code execute in a single shared address space.

The Rocket kernel provides the following extensive suite of services

- **Multi-threading**
  - Including both priority-based, non-preemptive fibers, and preemptive tasks (with optional round robin time-slicing).

- **Interrupt**
  - Including both compile-time and run-time registration of interrupt handlers, which can be written in C or assembly language.

- **Power Management**
  - Including tickless idle and an advanced idling infrastructure.

- **Inter-thread Data Passing**
  - Including basic message queues, enhanced message queues, and byte streams.

- **Memory Allocation**
  - Including dynamic allocation and freeing of fixed-size or variable-size memory blocks.

- **Inter-Thread Synchronization**
  - Including binary semaphores, counting semaphores, and mutex semaphores.

ARM mbed OS

mbed OS accelerates the process of moving from initial idea to deployed product by providing a core operating system, robust security foundations, standards based communication capabilities, and drivers for sensors, I/O devices and connectivity. mbed OS is built as a modular, configurable software stack so that you can readily customize it to the device you’re developing for, and reduce memory requirements by excluding unnecessary software components.

mbed OS forms the client-side portion of the mbed IoT Device Platform on microcontrollers, and is designed to work in concert with mbed Device Connector, mbed Device Server, and mbed Client. Together this platform lets you deliver comprehensive IoT solutions.

Microcontrollers and IoT devices have diverse hardware features and requirements. mbed OS includes a low level hardware abstraction layer (HAL) as well as higher level abstract drivers for common hardware peripherals like SPI and I2C ports, GPIO pins and timers. Hardware abstraction and drivers in mbed OS also provide deeply integrated support for power management, which together with energy-awareness in the scheduler helps mbed OS address demanding applications where power efficiency is critical to operation.
Microsoft Windows Embedded OS

Customized Service
We offer a ready to use embedded OS image. It provides a complete set of components that enable rapid prototyping and application development.

- Windows CE4.2, 5.0, 6.0, and Windows Embedded Compact 7 and 2013.

Board Support Packages (BSP) Services
We work with silicon and component vendors to get the latest embedded drivers. We integrate them with modified kernels, boot loader and SW API SUSI to produce a fully verified BAP. With Advantech BSP, customers can build up their solutions on Win CE, QNX, and VxWorks and customized HW.

Innovation Utility Service
- OS Enhance Tool: A utility for setting embedded lockdown features.
- WES Language Adding Tool: A utility to quickly add languages packs.

Product Family
**Microsoft Windows 10 IoT**

Windows 10 IoT powers a range of intelligent connected devices from smaller equipment such as gateways or mobile point-of-sale units, to industrial devices like robots and specialty medical equipment. Designed to connect through Azure IoT Services, Windows 10 IoT offers enterprise-grade security along with native connectivity for machine-to-machine and machine-to-cloud scenarios.

**Connecting to Azure Cloud Services**

Azure IoT Suite is an integrated offering that takes advantage of all relevant Azure capabilities to connect devices and other assets (i.e. “things”), capture the data they generate, integrate and orchestrate the flow of that data, and manage, analyze, and present it as usable information that either helps people to make better decisions or boosts intelligent automation of operations. The offering, while customizable to fit the unique needs of organizations, will also provide finished applications to speed deployment of common scenarios we see across many industries, such as remote monitoring, asset management and predictive maintenance, while providing the ability to grow and scale solutions to cover millions of “things.”

**Seamless Sensor/Gateway Communications**

The success of IoT totally depends on the quality of communication between devices. Within proprietary Windows 10 IoT networks, establishing that communication is fairly easy with AllJoyn. AllJoyn is an open source software framework and set of services that aims to enable interoperability among connected devices, regardless of the underlying proprietary technology or communications protocols. By implementing AllJoyn in Windows 10, Microsoft is joining with more than 80 alliance members to support interoperability across a variety of platforms and at scale, advancing the development and vision of IoT.

**Key Features**
- One Core OS - Universal Driver
- IoT Ready - AllJoyn Library + Azure IoT Suite
- Flexible Activation
- One App Platform - Universal App (UAP)
- Built-in Embedded Lockdown Features

**SKUs and Target Devices**

<table>
<thead>
<tr>
<th>Features</th>
<th>Windows 10 IoT Enterprise</th>
<th>Windows 10 IoT Mobile Enterprise</th>
<th>Windows 10 IoT Core</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Main difference</strong></td>
<td>• Full version Windows w/advanced lockdown capabilities.</td>
<td>• Target IoT gateway device</td>
<td>• Target IoT gateway device</td>
</tr>
<tr>
<td></td>
<td>• Win32 and UAP support</td>
<td>• Single universal app experience</td>
<td>• Single universal app experience</td>
</tr>
<tr>
<td><strong>Activation</strong></td>
<td>• Activation works both online and offline</td>
<td>• Universal app &amp; uni-driver support</td>
<td>• Universal app &amp; uni-driver support</td>
</tr>
<tr>
<td></td>
<td>• OAI3.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5x5 single/multi activation key</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Lockdown Features</strong></td>
<td>• EWF &amp; overlays</td>
<td>• USB filter</td>
<td>• USB filter</td>
</tr>
<tr>
<td></td>
<td>• USB filter</td>
<td>• Dialog and notice filters</td>
<td>• Shell and app launcher</td>
</tr>
<tr>
<td></td>
<td>• Dialog and notice filters</td>
<td>• Input filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Input filter</td>
<td>• AppLocker and layout control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• AppLocker and layout control</td>
<td>• Shell and app launcher</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Shell and app launcher</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Target Devices</strong></td>
<td>• Industrial/Medical/ATM</td>
<td>• Mobile POS</td>
<td>• IoT gateway</td>
</tr>
<tr>
<td></td>
<td>• Thin client</td>
<td>• Handheld</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Traditional POS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Industrial tablet</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Digital signage/kiosk</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Linux and Android Solutions

Linux

Linux is a popular OS in the embedded market, and the fastest growing area in IoT is the move toward open source Linux. Therefore, Advantech works with a wide range of Linux partners for the integration.

Key Features

General Linux Distribution Consulting Service
We offer installation and verification for Yocto, Ubuntu, SUSE/openSUSE, Red Hat Enterprise, Fedora, and CentOS, depending on customer requirements. We also provide technical consultation for Application layer development by project request, and optimized kernels with simple applications for quick evaluation on RISC platforms.

Linux Driver Modification & Configuration Services
We offer SUSI software API/Driver development service based on the customer’s defined Linux Kernel or Distribution, including APIs for Watchdog, Timer, GPIO, SMBus, I2C, Backlight On/Off, and Brightness. For RISC platforms, we can also help configure the right parameters for graphic drivers, and network drivers, etc. In addition, value-added software support such as boot-up logo customization, AP integration and burn-in customized image support are provided.

Application Ready Platform
Advantech leverages Wind River Linux with Intelligent Device Platform, Wind River Pulsar, Ubuntu Snappy Core, and Yocto Linux with a gateway software stack to provide gateway ready solutions. Among them all, Yocto Linux is our standard offering for RISC platforms, including boot loader, kernel with integrated drivers, and AP layer services and libraries. An Ubuntu image is available for GUI evaluation.

Embedded QT Package
Advantech provides a reliable QT solution, a cross-platform application, and an open-source UI framework, supporting mainstream Linux dev projects such as Yocto for customers to easily integrate QT into their build environment, speed up QT installation and enhance QT usability. Advantech QT package includes modules like GUI, Networking, XML, OpenGL and APPs like GStreamer testing and UART testing, with source code.
Third Party Solutions for Linux
We leverage Intel Security (McAfee) and Acronis technologies for several Linux distributions to provide security and backup/recovery solutions.

<table>
<thead>
<tr>
<th></th>
<th>SUSI Driver</th>
<th>Security Solution (Powered by McAfee)</th>
<th>Backup/Recover Solution (Powered by Acronis)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux</td>
<td>5.x – 7.x</td>
<td>5.x – 7.x</td>
<td>4.x – 7.x</td>
</tr>
<tr>
<td>SUSE Linux Enterprise</td>
<td>11-SP3 – 12</td>
<td>SLES 10, 11</td>
<td>10 – 12</td>
</tr>
<tr>
<td>SUSE Linux Enterprise</td>
<td>11.x – 13.x</td>
<td>SLED 11</td>
<td></td>
</tr>
<tr>
<td>CentOS</td>
<td>5.x – 7.x</td>
<td>5.x – 7.x</td>
<td>5.x – 7.x</td>
</tr>
<tr>
<td>openSUSE</td>
<td>11.x – 13.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>12.04(LTS)</td>
<td>12.04(LTS)</td>
<td>9.10 - 15.04</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>14.04(LTS)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ubuntu</td>
<td>15.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Debian</td>
<td>6.0 – 8.0</td>
<td></td>
<td>4 – 8.1</td>
</tr>
<tr>
<td>Fedora</td>
<td>18, 23</td>
<td></td>
<td>11 – 22</td>
</tr>
<tr>
<td>Yocto</td>
<td>1.7.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>5.x – 7.x</td>
<td>5.x - 7.x</td>
<td></td>
</tr>
</tbody>
</table>

Only for reference and support level depends on HW model. Please check with your local contact for more details and the latest information.

Android

Android has become one of the fastest-growing embedded operating systems for its openness, customizable features, and robust ecosystem. But growing competitive pressures make it difficult for many companies to meet time-to-market deadlines with the differentiated features and quality levels demanded by their customers.

Android gives you everything you need to build best-in-class app experiences. It gives you a single application model that lets you deploy your apps broadly to hundreds of millions of users across a wide range of devices—from phones to tablets and beyond.

Android also gives you tools for creating apps that look great and take advantage of the hardware capabilities available on each device. It automatically adapts your UI to look its best on each device, while giving you as much control as you want over your UI on different device types.
Wind River VxWorks

The stakes are high for real-time embedded systems and failure is not an option. Wind River® has a long history of consistently supporting your key requirements for high performance, absolute determinism, and minimal footprint—a history that has kept VxWorks® the market-leading real-time operating system (RTOS) year after year. As the first RTOS with 32-bit and 64-bit processing with multi-core and multi-OS support, VxWorks provides you with the functionality and support you require to stay competitive. And as your plans evolve to take advantage of next-generation processor capability, we continue to stay ahead of the technology curve, continually expanding VxWorks’ proficiency to extract maximum performance from the new multi-core landscape.

VxWorks’ unique combination of high speed and scalability with trusted safety and security capabilities will keep your platforms running at the leading edge of the latest embedded technology.

Key Features

Lower system development costs with a single RTOS that scales.
VxWorks is the RTOS foundation for successful development of very small devices, large intelligent connected systems, and everything in between. It is scalable to meet your project’s unique memory footprint, functionality, and processing power requirements.

Broad connectivity
VxWorks adds connectivity protocols such as USB, CAN, Bluetooth, and Continua, as well as the modularity that can help bring many previously disconnected devices online without reworking the core of their embedded software.

Complete security for connected devices
IIoT demands pervasive connectivity that exposes devices and systems to more security risks than ever before. VxWorks allows you to design your embedded system to the necessary level of security by leveraging a comprehensive set of built-in security features for the development of boot and execute, operation, transmission, and idle power down stages.

Ensure Compliance with Safety and Security Requirements
VxWorks trusted system platforms have a proven track record in safety- and security-certified environments. A high reliability RTOS, VxWorks provides hard real-time performance and determinism along with the certification evidence required by the highest safety and security standards. You can count on VxWorks to run forever, error-free.

Expandable and upgradable architecture
The modular, future-proof architecture of VxWorks separates the core kernel from protocols, applications, and other packages, which enables you to enrich your products with new features and capabilities as standards and market requirements evolve without retesting or recertifying the entire system.
Restart your system in the shortest time and protect valuable data

Acronis provides a quick, effective and easy-to-operate backup and recovery solution. Acronis can back up the operating system, applications, settings and all of your data. With Acronis Backup and Recovery Solution, you can reduce expensive, disruptive downtime cost, and lower the risk of permanent data loss after a crash.

The installation and configuration process is hassle free. Even though you may not be an IT expert, you can restore an entire system when needed. With Acronis Startup Recovery Manager, the recovery process becomes more intuitive by selecting the F11 key and following the step-by-step guide.

Acronis also provides many ways to backup and store data to satisfy a variety of users’ needs, such as incremental and differential backups, backup of the whole system or selected disks/partitions, or only the changes. It also allows backup to local drives, external storage, FTP, or on the system drive using a separate and secure partition (Acronis Security Zone). Acronis makes backup and recovery not only more convenient but altogether safer.

- Protect workstations from hardware failure, viruses/malware, and file corruption
- Recover the entire system even if the OS crashes

**Acronis True Image Personal/OEM**
- Many different backup methods
- Many different storage methods
- Create Bootable DVD, or USB media with backup file
- Acronis Startup Recovery Manager
- Bare-metal restore

**Acronis True Image Premium with all functions**
- Incremental and differential backups
- Non-stop backups and backup over FTP
- Universal restore
- Acronis Secure Zone
- NAS support
- Scheduling
- Disks/partition cloning
- Personal image encryption with Advanced encryption
- Standard (AES)

**For clients’ Windows OS**

**For Windows server**

- Avoid expensive downtime and get back up and running in minutes
- Comprehensive backups and fast, flexible recovery

**Acronis Server Backup of running system (hot backup)**
- Full image backups
- Disk and partition backups
- Incremental backups
- Browsing and mounting backups
- Scheduling
- Backup password protection
- Bare-metal restore
- Bootable recovery media
- Restore individual files and folders
Intel Security Solutions

In the IoT era, more and more devices are being connected together and security has become a significant issue. So why not enjoy a tailored security solution that meets the specific design requirements for your data, with better device protection in for your embedded applications. We will be launching more security solutions in the near future but below are some of the current available solutions.

McAfee Embedded Security Solutions (whitelisting)

99% of embedded devices suit the Whitelisting Solution
With built-in application whitelisting and change control technology to lock down devices, protecting against unauthorized malware and changes that could take a system offline is now much simpler. With security integrated into your device, you and your customers stay compliant and avoid incidents that can result in high maintenance and service costs, such as zero-day exploits, high support costs related to device security, and high field maintenance costs tied to unauthorized changes.

Our solution has low impact on system performance, and requires low CPU and memory utilization. The small overhead makes you enjoy the benefits of low ownership cost.

Key Features

Application Control
● Protects against zero-day-attack
● Prevents all unauthorized applications from being executed
● Automatically accepts new software added through authorized process

Change Control
● Sets access rights for who or which application can access protected data
● Prevents outages resulting from unplanned changes

ePolicy Orchestrator
● Protects against zero-day-attack  ● Fast time to remote deployment/configuration
● Reporting  ● Central management  ● Compliance requirements  ● Monitors data of managed clients

Benefits
● Minimized desktop footprint  ● Zero-impact scanning  ● Intelligent trust  ● Significantly reduce pattern updates

level 1- McAfee Application Control
Application Control is McAfee’s fundamental product to provide an effective way to block unauthorized applications and code on fixed-function devices.

level 2- McAfee Embedded Control
McAfee Embedded Control combines Application Control and Change Control, providing advanced protection by only allowing authorized code to run and only authorized changes to be made.

level 3- McAfee Integrity Control
McAfee Integrity Control combines McAfee Embedded Control and McAfee ePolicy Orchestrator® providing integrated audit and compliance reports to help satisfy multiple compliance regulations.
**McAfee Endpoint Protection for OEM (Blacklisting)**

Today’s competitive landscape makes differentiating OEM systems an increasingly difficult yet imperative mandate. How do you meet customer needs and deliver ongoing value to make your systems stand apart? The solution is pretty obvious: make your devices more secure while reducing ongoing security management costs. Security remains the No 1 concern of company executives who understand the security risks endpoints pose to their brand reputation and bottom line. McAfee® Endpoint Protection for OEMs is an affordable way to build advanced security capabilities and greater value into your devices and solutions.

McAfee Endpoint Security 10 provides integrated protection, performance and simplicity for OEM systems. It provides an affordable way to build advanced security capabilities and greater value into your devices and solutions. It combines industry-leading firewall protection, threat prevention, and web control modules into a flexible, easy-to-manage security solution that works as one to protect your devices from cyberattacks. This new integrated architecture allows firewalls, threat prevention, and web control modules to share common services. As a result, McAfee threat defenses work together to more effectively learn, talk, analyze, and act on potential malware and advanced threats in real time.

**Key Features**

McAfee Endpoint Protection for OEMs unites three powerful security modules. Select the modules for your specific devices based on the system type and environment while maintaining the flexibility to update modules at any time—during installation or once deployed.

- Threat Prevention Module: Includes several new, advanced malware-scanning features to defend against emerging and targeted attacks
- Web Security Module: Prevents users from browsing to malicious or unauthorized websites and serves as a replacement for McAfee Site Advisor Enterprise.
- Firewall Module: Stops malicious inbound and outbound network traffic.

**Benefits**

- Industry-leading firewall protection, threat prevention, and web control in a tightly integrated, high-performance architecture.
- Comprehensive protection against cyberthreats with McAfee Global Threat intelligence.
- Simplified management from the cloud or locally.
WISE-PaaS/RMM
IoT Remote Monitoring and Management

WISE-PaaS/RMM serves as one part of Advantech’s IoT software solutions, focusing on IoT device remote monitoring and management, and bridging the layers in Advantech’s IoT Platform Architecture. Advantech strives to integrate collaborative partnership solutions with Intel, Microsoft, Windriver, McAfee, Acronis and others by providing pre-integrated, pre-validated hardware and software building blocks to enable seamless and secure data flows from the sensor to the cloud and back.

Centralized Management
WISE-PaaS/RMM provides a Console/Server/Agent web-based structure for centralized management. Administrators can perform equipment status and maintenance checks on WISE-PaaS/RMM’s console through any web browser using any connected device. The Server/Agent connection has been enhanced to fit the MQTT communication protocol. This improves connection security and stability, and also decreases development time for integration. WISE-PaaS/RMM not only provides a comprehensive device monitoring and control system that includes both hardware and software, but also provides distributed connectivity that solves the challenges encountered with large-scale or multi-site device management.

High Availability
WISE-PaaS/RMMs support hierarchical server structure view to allow the administrator to manage services/devices across different subnets at the same time (logically) without compromising network segment privacy. Also, RMM allows a server to set 1 or 2 redundant servers, with which all data will be synced continuously and a redundant server will take over when the primary server is down to ensure service availability.

Sensor/ Device Connectivity
WISE-PaaS/RMM connects with a variety of devices from IPCs, to gateways and sensors, and supports secure data setting, acquisition, aggregation, and storage for further analysis. It also integrates different protocols to ensure seamless and secure communication.
WISE-PaaS/RMM Structure

Web-based User Interface
- System Monitoring
  - Device Monitoring
  - Automatic Alerts
  - Dashboard Builder
- Remote Control
  - Remote KVM
  - Power On/Off
- System Security
  - System Recovery
  - System Protection

Web Service
100+ RESTful APIs

Core Platform
- Device Management
- Database Management
- Event Management
- System Management

WISE Agent
- MQTT
  - IoT Protocol
- Software Handlers
- Handler SDK

Benefits for IoT
Accelerated time-to-value
Capitalize on Advantech’s investments in back-end infrastructure and pre-built connections to many popular platforms.
Robust development environment
Utilize built-in APIs and SDK to easily extend IoT software services across platforms and systems supporting C language
Cross-platform applicability
Leverage RMM’s cross-platform interoperability to integrate with virtually any connectable endpoints.
Scalable management
Extend built-in management modules and widgets to create compelling business and operational intelligence and IoT device management solutions.

Accelerated Time-to-value
- IoT SDK Packages
  - Web Services APIs
  - Sensor/Device SDK (WISE Agent)
  - Device BSP

Standard Protocols
- MQTT
- TR-069
- OMA
- OSGi

Security
- Intel McAfee Security
- OpenSSL
Software APIs (SUSI API + iManager)

SUSI APIs: Secure & Unified Smart Interface

If you are software developer or a system integrator you are all too familiar with the following problem: you are writing an application that requires direct hardware access. Unfortunately, that access is no longer available in modern operating systems. So you have to locate and study reams of specifications to write the appropriate drivers, and that is a complex and time-consuming job. To ease the burden, Advantech has created SUSI (Secure and Unified Smart interface), a suite of application program interfaces that allows users to directly monitor and control digital I/O, 12C, CPU stepping speed, watchdog timers, smart fans and access hardware monitoring sensors.

Benefits

Time to market
Not having to delve into chipset hardware specs and develop drivers for each new board and application reduces the overall project effort and means quicker time to market and therefore profit.

Enhance hardware reliability
Use of SUSI APIs can help reduce heat and power consumption, resulting in increased reliability. This allows the setup of warning mechanisms, event triggers, display adjustments, and other critical settings and actions that enhance overall system reliability and lower maintenance requirements.

Flexible upgrades
New functions and settings can easily be implemented via SUSI and new versions of SUSI; no need to rewrite an entire application.
iManager APIs: Intelligent Self-Management

To fulfill the ever-changing specialized demands of various industrial applications, Advantech designed an intelligent self-management firmware agent. iManager is a built-in solution chip with a standardized API, integrating several unique platform consolidating functions needed by embedded system integrators to help improve consistency, lighten the development effort and speed-up your product's time-to-market.

**iManager 3.0 (coming soon)**

**System on Chip**
- Integrate EC, Super IO, SPI and EEPROM

**Powerful CPU & High Speed Peripheral**
- 8051 → 8086 (IC, SMBus, GPIO, CANBus)

**New Device Functions**
- RS-232/485, Parallel, CANBus, CaseOpen

**Supports three kinds of host interface**
- LPC, eSPI and PCIe

**eSPI implementation**
- Sideband pins and scalable bandwidth
- Medium bandwidth
- Pin count reduction: 5 to 7 pins
- Low voltage I/O: only 1.8V mode

**Benefits**

- **OS-independent**
  - Cross-platform programming
- **Self-Management**
  - Intelligent resource management
  - Real-time response
  - Auto-protection and system restore
  - Plug and play
  - Security enhancements
Application Stories

Transforming Retail Business with Advantech Embedded Software Services

Introduction and Application Requirements
With IoT and cloud technology, customer information from different sources and different sites can be collected and accumulated into a large database for valuable business intelligence extraction. For example, when a global retail chain deploys an IoT system across its retail sites, it can implement market analyses to determine and predict customer interests in different countries and areas and adjust inventory distribution accordingly. This can help policy makers develop deep overall insights into their business and improve business management and overall strategies.

System Solutions

Benefits
- Robust and total software solutions provide secure systems for POS machines and data acquisition gateway management
- Remote data acquisition and environmental sensors monitor each branch store
- Seamless connection to Microsoft Azure cloud service helps users gain better business intelligence
Protecting Intelligent Automation Systems with Advantech Embedded Security Solution

Introduction and Application Requirements

With the coming of the IOT era, manufacturing has become more and more computerized. Interconnected, ‘networked’, machines have become the norm, and they provide great convenience and increases in productivity in factories. However, as factory networking increases, there is also an increased security risk from viruses entering through data sharing via the internet or USB memory devices, and consequently an increased need for IT security.

Industrial customers face unique new challenges including a wider range of cyber threats than ever before. Any connected device can be a potential target for cyber-attack, and industrial controls are being targeted as they become IP enabled. Industrial customers often lack the resources necessary to respond efficiently to security incidents, and downtime while servers are reinstalled causes major disruptions to manufacturing operations. In addition to malware and virus attacks, industrial customers are also concerned about data security. Industrial customers needed a way to address clear inefficiencies in their backup and recovery regimes.

System Solutions

Advantech leverage Intel® Security and Acronis to provide an embedded security solution that works on industrial equipment. It covers most existing systems; the user does not have to undertake system replacements.

Benefits

- Whitelist approach provides complete security without affecting system performance.
- This comprehensive solution protects systems against different types of security threats
- Lower operational cost and no manual effort
- Quick and easy system restoration in case of system failure or disaster
- Clone OS/data for redeployment in hours, not days
- Maintains the operation of the production line