IoT DEVICE MANAGEMENT
Are you ready to manage the millions?

SPONSOR

ADVANTECH

Enabling an Intelligent Planet

Device management seeks differentiation as market matures

As the long wait for the volume of IoT devices in deployment to grow from millions to billions starts to end, renewed attention is focusing on device management. It's now well-understood that the more devices deployed, the greater the management requirement has become and, like everything in IoT from computing power to connectivity, the cost must match the business case of the IoT service itself. It's entirely possible to have effective IoT device management with providers of platforms, systems and services proliferating. However, it's more difficult to achieve this within the cost constraints imposed by ensuring IoT services are profitable, writes IoT Now managing editor George Malim

Device management is not a nice-to-have, it's an essential, enabling IoT organisations to operate profitably, efficiently and securely, while complying with regulation and legislation. In addition, device management provides the flexibility and affordable upgrade path for many types of devices, making it a critical ingredient of the IoT lifecycle. Devices that were deployed earlier in IoT need to be able to access new functionality and new versions of software in cost-effective ways. Physical engineer visits cannot be sustained by many business cases so automated, over-the-air software upgrades are one aspect that has a significant impact on viability in the future.

Importantly, the variety of IoT devices is now enormous and ranges from near-disposable sensors, such as low cost soil analysis probes for smart agriculture, to hard wired, high-speed cellular connected items such as smart meters which may have operational lives of more than two decades. Devices managed by organisations in both these categories will number in the millions as energy companies, householders and farmers all derive significant value from their connected devices. For this reason, momentum has been behind device management for several years as organisations consider their device capabilities at the design stage of their deployments.

The growing number of connected devices in the IoT ecosystem and the associated IoT applications and business models demonstrate the need for IoT device management

Market conditions

How large volumes of devices will be managed has become an important ingredient for IoT success and projections for the IoT device management market have been encouraging. **Mordor Intelligence** in **Figure 1** reports that the IoT device management market is expected to register a CAGR of 28.7% over the period 2020 to 2025. The firm says IoT device management encompasses connected device provisioning, administration, monitoring and diagnostics necessary for trouble replication and corrective measures. The overall IoT device management market is driven by overall growth of IoT networks and systems, growing concerns over network security, as well as an increased need to monitor the health of IoT devices. That health involves the vital signs of IoT: power, security, on-off status and connectivity.

Further stimulation of IoT adoption is being accelerated by the arrival of 5G networks, which add ultra-low latency and very high speed mobile broadband to the connectivity arsenal, and adoption of multi-access edge computing (MEC), which is bringing processing and acting upon live data into reality. IoT device management systems enable the collection and analysis of data, so this is another factor that is anticipated to fuel market growth.

The growing number of connected devices in the IoT ecosystem and the associated IoT applications and business models demonstrate the need for IoT device management. This proliferation will lead to far larger device estates and the devices themselves are becoming more complex to manage, with more features and dependencies. The definition of device management describes the process of authenticating, provisioning, configuring, monitoring and maintaining device firmware and the software that provides its functional capabilities. Through device management, an IoT platform can deliver complete lifecycle support that includes security patching, alerting, firmware upgrades and provision of performance metrics.

Research by **Stanford University** and **Avast** has found that 66% of homes in North America already have at least one IoT device, suggesting that the typical household will have an average of nine devices by 2022, and nearly half (48%) of total devices and connections will be capable of video. Mordor Intelligence therefore concludes growing adoption of IoT devices is leading to increased need for IoT device management. However, IoT growth in general does not mean all the device management challenges have been addressed. In fact requirements continue to become more stringent. Exposure of confidential information concerning the privacy concerns, real-time complexity, dynamic environment, and lack of compatibility and connectivity along with the absence of uniform IoT standards for interoperability is a crucial challenge for the market to address.

Source: Mordor Intelligence

Figure 1: IoT device management market growth 2020-2025

Pandemic impacts

In addition, IoT is undergoing disruption thanks to the COVID-19 pandemic, which has hit the pace of adoption. IoT will be integral to the long-term recovery plans of the post-COVID-19 economy worldwide although some facets of IoT itself will be negatively impacted in the short-term. A combination of manufacturing shut-downs, supply chain interruptions and changes in connected product availability and demand are expected to cause an 18% drop in the net addition of IoT devices in 2020, according to **ABI Research**. This equates to the loss of 66 million potential wide area network (WAN) connections over previous forecasts.

Proportionally, the most heavily impacted markets will be fleet and other heavy vehicles or equipment, the firm says. These are expensive assets that enterprises are buying less of in the interests of cost control. Fixed assets, digital signage and kiosks also face impacts, as

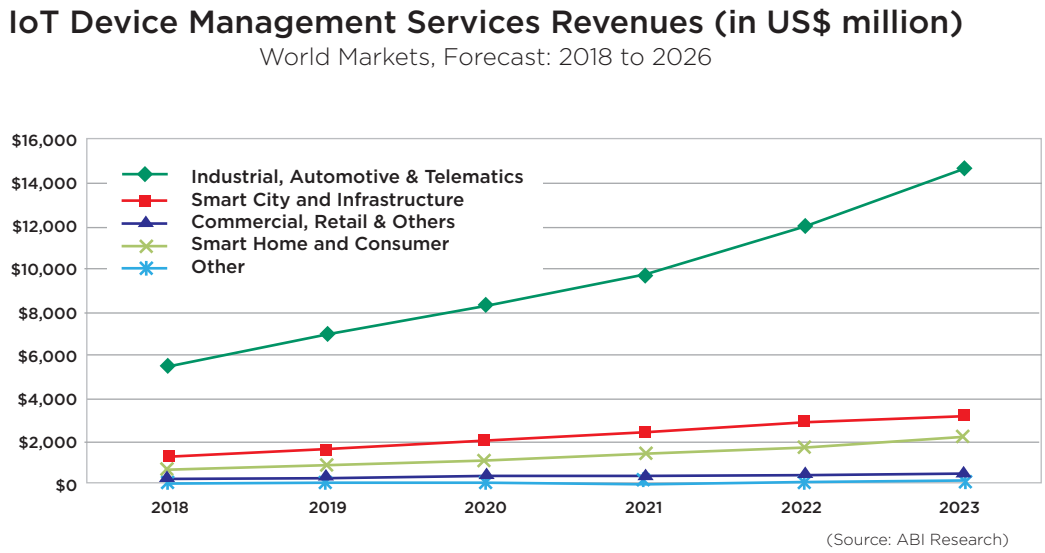


Figure 2: IoT device management services revenues (US$ million) 2018-2026

In the consumer markets, passenger vehicle and connected car markets are suffering considerably as people stay in one place

they are driven by the entertainment and retail sectors which have been effectively paused by the massive reduction in personal mobility and footfall.

In the consumer markets, passenger vehicle and connected car markets are suffering considerably as people stay in one place. Conversely, with people spending more time at home, improving the functionality and comfort of there is expected to boost smart home revenues. In the enterprise market, while utility metering initiatives face delays as home visits are temporarily prohibited, these are expected to bounce back quickly. At the same time, asset tracking, inventory managementand condition-based monitoring are all expected to attract greater long-term investment to enable companies to allow people to do more with less and to reliably run things remotely.

Jamie Moss, the research director for M2M, IoT and IoE at ABI Research, explains: "COVID-19's impact on the IoT is three-fold. Some applications will experience a decline in shipments during 2020, ergo a reduction in the expected growth rate to their installed base," he says. "Yet, with no intrinsic change to their desirability and utility, they will return to expected growth in subsequent years. Some will experience a temporary stall in 2020 that will be compensated for by increased activity immediately after, to bring installed base expectations back into line. Others will experience fundamental shifts in demand, both positive and negative, for years to come as consumer and enterprise priorities shift in the light of COVID-19."

Mordor Intelligence sees similar dynamics, reporting that retail, healthcare, fleet management, heavy transport utilities, transportation and logistics, fixed assets, vehicles or equipment, and digital signage are the hardest hit IoT applications. The flipside is that IoT will be fundamental to the long-term recovery plans of the post-COVID-19 economy. Even so, some facets of IoT will be negatively impacted in the short term before returning to expected growth in subsequent years.

Pre-COVID projections therefore are likely to get back on track in 2021 or 2022. ABI Research had previously predicted that device management services, which include device provisioning, software and firmware updates, and device monitoring, were projected to generate revenues of US$20.5 billion by 2023. The firm forecasts in **Figure 2** that IoT device management services will be a necessary component of any significant IoT solution, with 70% of revenues being generated within the industrial, automotive and telematics verticals.

The need for enterprises to manage a growing number of diverse IoT devices has led to the emergence of various platforms over the years

The search for differentiation

The variety of applications and industries that rely on device management is large and this is reflected in the number of vendors that serve the market either as technology, platform or service providers. Some of the major players include **Advantech**, **Aeris**, **Arm**, **DevicePilot**, **IBM**, **Microsoft**, **Oracle**, **PTC**, **Smith Micro Software**, **Software AG** and **Wind River**, among many others. This has led to a competitive and innovative market.

However, there is a perceived lack of differentiation in the market place, according to a recent study by **Analysys Mason**. Partly because of the growth of IoT, organisations need to manage a diverse range of devices and this has seen adoption of various device management platforms that all apparently match the main market needs. The analyst firm advocates that device management platform provider demonstrate and communicate their differentiating features, focusing on developing distinct features and developing vertical sector specific capabilities.

The need for enterprises to manage a growing number of diverse IoT devices has led to the emergence of various platforms over the years. This, in turn, has made it increasingly difficult for suppliers to differentiate their offerings and for customers to identify the key strengths of each supplier. However, much attention has been devoted to addressing the baseline device management capabilities.

These include device onboarding, monitoring, troubleshooting, software updates and device disconnections. More recently security and resilience have become important device management capabilities, along with further automation of device management processes. Although the latest additions have widened device management capability, they have not created substantial differentiation. Analysys Mason says that, while businesses are increasingly deploying device management platforms to automate the lifecycles of their connected assets and to improve the resilience and security of their IoT device estates, such platforms are overlapping with connectivity management platforms and application enablement platforms and this is complicating the selection process for customers.

There were 87 key IoT platforms in the market at the end of 2019 according to Analysys Mason's IoT platform contracts tracker, up from 53 in May 2017, 63 of which supported device management. Vendors sell device management platforms directly to enterprises, as well as to telecoms operators that then resell them as managed services. Enterprises then use device management to address the technical challenges that they encounter when deploying IoT solutions.

The growing role of IoT in mission-critical processes mean secure IoT infrastructure is a priority

The analyst firm interviewed several operators and vendors that provide device management platforms during its research and found three key technical capabilities that can be used as a basis for differentiation.

- **Security** The growing role of IoT in mission-critical processes mean secure IoT infrastructure is a priority. Growing volume and sophistication of cyberattacks and the potential financial losses due to liabilities, regulatory fines and loss of business mean device management can prove its value by helping organisations achieve compliance. Analysys Mason says suppliers can distinguish their platforms by implementing strong end-to-end security measures to detect and prevent breaches.

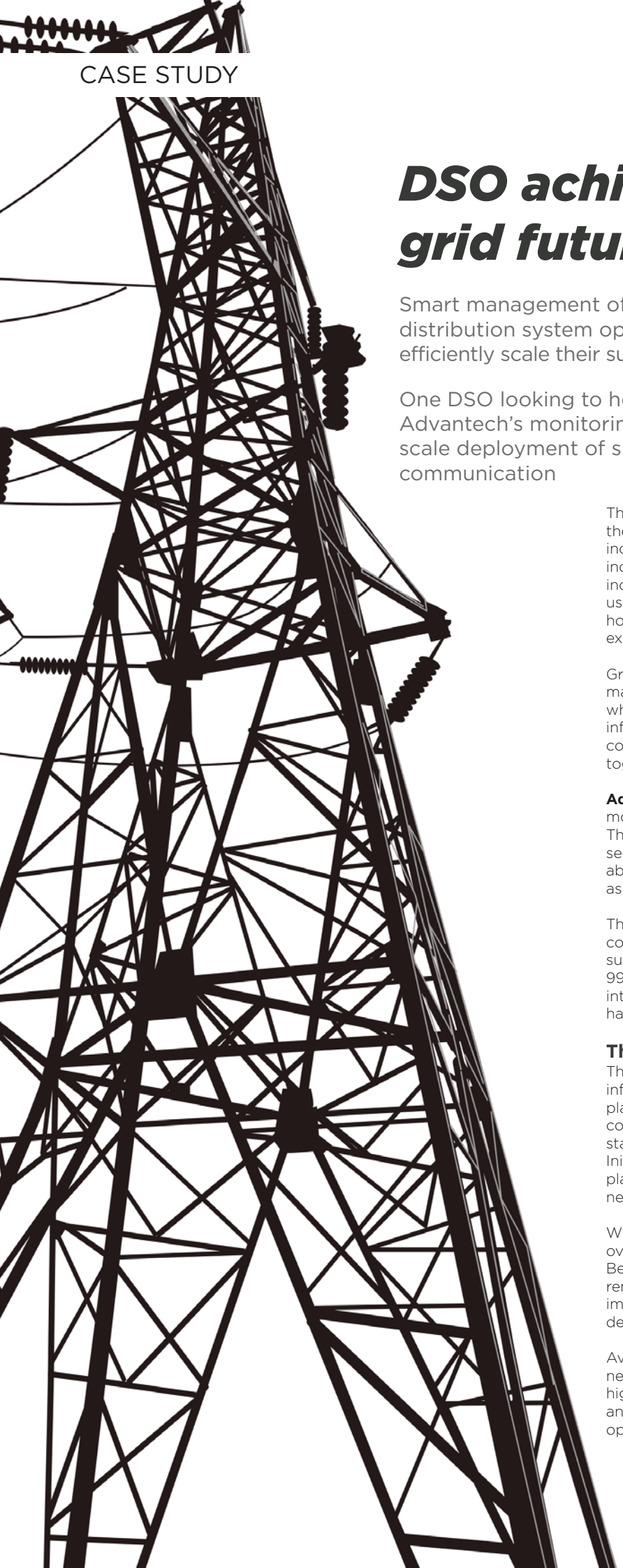
- **Flexibility** The lifecycle of IoT devices means that management should be continuous and flexible to support changed requirements as markets develop. A key requirement is to plan for compatibility with a growing number of as-yet-unknown devices. Suppliers can differentiate by having a larger number of certified devices in their catalogues or demonstrate flexibility in the number of standard or proprietary protocols that their platforms support.

- **Specialisation** Developing distinctive features and addressing the technical requirements of specific verticals or user groups has the potential to set vendors apart from the crowd. By doing so they can segment the market and target customers that have a particular level of interest in a set of capabilities.

Conclusion

IoT implementation, in common with the wider economy, has been rocked by the pandemic and this has also affected device management adoption. Businesses now face a series of unique challenges but IoT-enabled machines, sensors and devices answer many of these. However, to do so cost efficiently, securely and without downtime, device management performs a vital task. Effective device management is now more widely understood to be critical to establishing and maintaining the health, connectivity and security of IoT devices. Decision makers are therefore looking more closely than ever before at device management capabilities and placing these as part of the foundations of their IoT solutions. ■

CASE STUDY



DSO achieves electricity grid futurability

Smart management of power supply demands is helping distribution system operators (DSOs) around the world efficiently scale their supply to our ever-changing requirements.

One DSO looking to hone performance recently implemented Advantech's monitoring communications system for its large-scale deployment of smart wireless routers for substation communication

The demands placed on electricity grid operators by their customers, suppliers and regulators grow increasingly stringent. One major challenge for the industry is to reduce urban and total pollution, while increasing renewable energy sources and electric vehicle use. When it comes to reducing energy consumption, however, the key is automating the complex and extensive distribution grid.

Grid operators are now upgrading their monitoring and management systems to ensure resilience and reliability whilst balancing generation and demand. Part of the infrastructure necessary to support such automation and control is the wide area communication system to link together all the important points in the grid.

Advantech has recently provided a complete grid monitoring communications solution for a major DSO. The solution ensures high reliability, easy expansion, security, simple installation and, critically, scalability: the ability to roll out hundreds, even thousands of systems as easily as the first ten.

This DSO needed to upgrade its grid management communication system to maintain its high electricity supply security at more than 99.9% and try to reach 99.99%, which equates to less than one hour of service interruption a year for each customer. The DSO has over half a million customers and 100,000km of cables.

The challenges

The upgrade to its existing telecommunications infrastructure needed to reflect the demands being placed on electrical grids. It would offer: high-reliability communications to various substations, switching stations, interconnect sites and distribution locations. Initially, the project included 1,000 remote sites, with plans to extend this to a further 4,000 sites over the next ten years.

With any project like this, a decision needs to be made over whether to use wired or cellular communications. Because many of the sites identified for connection were remote, a wired connection would be difficult to implement and to maintain. A fully-wireless solution was decided upon.

Availability would be critical. The wireless solution needed to offer a high degree of resilience and specific high priority sites, for example the switching stations and substations, needed even greater availability. When operational, the whole system needed monitoring to ▶

ADVANTECH
Enabling an Intelligent Planet

ensure system performance and availability. Security is also paramount. The communications solution would need to support a robust cyber security protocol that would protect the network and conform to the most stringent security audits for critical infrastructure.

Lastly, there was the major issue of installation and provisioning. The solution had to be simple and easy for the DSO's field engineers to install, without any special training for device configuration or commissioning.

The Advantech proposal

Three different Advantech wireless routers would be deployed to provide the connectivity for grid monitoring:

For the high priority stations, an Advantech SmartMotion router would be deployed, offering two simultaneously-active cellular connections from two different providers with two different SIMs. This would ensure the highest possible availability. In addition, a wired connection to a satellite (VSAT) link was also deployed at these high priority sites to provide a failsafe link. The SmartMotion router would therefore provide three differing communications links to the central monitoring sites.

For the lower priority sites, and depending on the physical connections to the local monitoring systems, either a SmartStart or SmartFlex router would be deployed offering one active cellular connection but again utilising dual SIM cards to allow failover to the backup operator in case of availability issues with the primary operator.

Ensuring physical communication was one challenge, but bigger challenges were security, monitoring, managing and provisioning the network. Each physical site would communicate via dual encrypted links with two central management sites.

The health of the routers at remote sites would be monitored via widely-used Zabbix software to ensure that the agreed service level agreement (SLA), would be met. Advantech's software development team modified the standard router software to support two active encrypted links using the Simple Certificate Enrolment Protocol (SCEP) to ensure regular certificate renewal, integrating the routers into an SNMP-based Zabbix monitoring system to provide the necessary data for SLA monitoring.

Advantech proposed to meet the challenge for simple installation with a zero-touch provisioning system which automatically linked the router on first power-up to our central management system. This would avoid any need for configuration on-site, minimise errors and therefore would lower installation costs.

Advantech proposed to use WebAccess/DMP, its provisioning application. WebAccess/DMP, which offers a full suite of deployment and management tools: zero touch deployment, site specific configuration and an additional layer of monitoring and diagnostics. WebAccess/DMP can be cloud based, but with the stringent security requirements demanded by an operator of critical infrastructure an on-premise version was deployed so ensuring the entire network, including the data, management and device provisioning and maintenance, was "air-gapped" from the public Internet.

Implementation

This challenging distribution grid operator trusted Advantech to provide its resilient and secure wireless communications network. Advantech's proposed solution helped it to roll out communications systems in 1,000 substations in just 12 months without a hitch, proving the value of the simplified installation process. Service in the field is proving the value of the redundant communication channels. ■