AVNET SILICA

THE ROUTE TO MASSIVE IoT

From proof-of-concept to as-a-service IoT deployment with IoTConnect on AWS

powered by aws

EXECUTIVE SUMMARY: THE ROUTE TO MASSIVE IoT

Connectivity is now truly ubiquitous. All verticals, without exception, are converging on a future where productivity becomes universally data driven. The devices that will enable these intelligent and connected endpoints will be hugely diverse in their design but share many common features. This combination of uniformity and uniqueness is both an opportunity and a challenge for OEMs looking to leverage the massive IoT.

In its simplest form, the massive IoT will comprise many endpoints communicating through microservices provided and maintained in a cloud platform. Standard protocols provide the interface mechanism, but the OEM must take control of the implementation.

Connecting IoT endpoints to a cloud platform is becoming simpler. All major semiconductor providers now supply their own development kits that connect quickly to leading IoT cloud providers, such as Amazon Web Services (AWS).

These kits offer fast proof-of-concept (PoC). OEMs moving from PoC to large-scale deployment will be faced with diversity in the hardware targets they use in their endpoints. They may standardize on a single supplier, but they may find the most optimal designs require products from multiple suppliers.

The real design work starts after PoC. Real-world IoT solutions may not have the benefit of standardizing on just one semiconductor supplier. Avnet understands the need for choice and works closely with the embedded industry's leading semiconductor vendors. Each of those vendors is focused on IoT. Each offers easy on-ramps to AWS.

Design teams within OEMs will be looking to avoid compromises when choosing the right hardware components for their solution. With so much support coming from competing vendors, it becomes important to understand where those compromises arise.

IoT solutions are complex. Often, the real value comes from leveraging the IoT data. This is where AI and cloud services offer a real difference. PoC solutions provide the initial experience, but the long-term value to the OEM's end-customer comes from how the total solution is configured, how relevant data is extracted, and how value from the data is delivered.

Avnet is the only electronics component distributor offering a smooth transition from PoC to large-scale deployment leveraging multiple semiconductor vendors, IoTConnect® is unique in the market. Avnet distributes the hardware and has developed the middleware to connect cloud platforms to endpoints. Avnet's technology has been endorsed and integrated into key hardware components from all the major semiconductor vendors. This includes pre-integration and board support for wired/wireless communications, microcontrollers, and security ICs. Avnet calls this technology IoTConnect.

This whitepaper provides the context behind real-world IoT solutions. It explains the design effort required to move from PoC to large-scale deployment. The need for security and maintainability will be discussed. Best practices in managing large-scale IoT solutions as a service will also be provided.

TABLE OF CONTENTS

/STARTING YOUR IoT JOURNEY

Leveraging PoC solutions from leading semiconductor vendors

The proof-of-concept stage is important for any project. In IoT applications, the concept will inevitably involve capturing data and sharing it with other services.

At a high level, these two functions are unrelated. Embedded developers will be familiar with implementing control systems that use sensors and actuators to effect real-world changes. Connectivity is also a common feature in embedded systems. At its heart, IoT is the convergence of these two functions.

Determining what should go into the payload of the communications channel is where this convergence takes shape. It will be defined by the application and the way it operates in the larger system.

This is a rapidly evolving design requirement. The trend toward using artificial intelligence (AI) at the edge will also determine how much data and what kind of information needs to be in the payload.

Payload definition is why the PoC stage is critical when developing new endpoints, either for greenfield installations or the continued extension of an existing solution. Every new endpoint developed will need to provide new value. That value comes from whatever is put into the payload.

Finding the fastest on-ramp to IoT

Design flexibility at the early stages of a project means the PoC can take many forms. The final design may use a different hardware solution, or it may become apparent that it requires the specific features of the selected platform.

It is important for OEMs to move efficiently at this early stage. Engineering teams cannot afford to evaluate several platforms; certain assumptions and decisions need to be made early. Semiconductor vendors focus their efforts on enabling those platforms designed to best fit many endpoint profiles.

This focus has created faster on-ramps to IoT PoC. Manufacturers appreciate how enabling it can be to move quickly from an idea to a demonstrable solution. This is even more apparent when targeting IoT applications. For many developers, the effort required to connect an endpoint to a cloud service can be an unknown.

The learning curve will cover understanding how the cloud platform is configured, what services are available and how to access them. A significant part of that effort

will need to be applied to comprehending the security measures available and how they are implemented. Many semiconductor vendors are working collaboratively with Avnet and cloud providers to flatten this curve.

An overview of PoC acceleration solutions

Creating an "out-of-the-box" experience can accelerate a project's development phase. These experiences normally take the form of a development kit and associated firmware, coupled to a cloud platform with the necessary pre-enablement for establishing a connection to some useful features.

The transferable knowledge that comes from this phase will vary. If the hardware platform is fixed at this point, the knowledge will include low-level design choices. The configuration of the data payload will be defined. The capabilities and complexity of the cloud platform will be abstracted but apparent.

The overview below covers some of the cloud-enabled development platforms already available from Avnet and its leading semiconductor partners. Avnet is working with all its component supplier partners to onboard more of their products to cloud services through IoTConnect. This journey will continue as new solutions emerge.

ST Microelectronics

STMicroelectronic's B-U5851-IOT02A Discover Kit demonstrates the capabilities of the STM32U585AI, which features an Arm® Cortex®-M33 microcontroller at its core. This powerful processing resource comes with Arm® TrustZone® and ArmV8-M mainline security extensions.

The Discovery Kit features Wi-Fi and Bluetooth, and a wide range of sensors including microphone, temperature and humidity, magnetometer, accelerometer, gyroscope, pressure, time-of-flight, and gesture detection.

The STM32U5 is ST's successor to the STM32Lx in terms of low-power operation. For IoT applications, low power can be critical. Avnet recently announced that IoTConnect is now available for the STM32U5.

Daniel Colonna, STM32 marketing director, STMicroelectronics, said: "Adding support for Avnet's IoTConnect can be of great benefit to our customers developing applications using the STM32U5. Avnet created and industrialized the tool to support scalable deployment, making it ideal for large-volume IoT applications."

As a member of ST's partner program, Avnet is continuing to add IoT support for ST's processors, wireless SoCs, sensors, and security solutions. The partnership is focused on expanding support for IoTConnect through the STM32Cube Expansion Packages.

Microchip Technologies

Microchip's WFI32-IoT board comes with a certified WFI32E01PC module, featuring a PCB antenna and Trust&GO hardware secure element.

The board also includes a PICkit On-board 4 (PKOB4) debugger interface, and a mikroBUS™ Click™ header. On-board sensors include temperature and light, and the board integrates a Li-Ion/LiPo battery charger with Power Path Management. A header is also included to make power measurement simpler using a multimeter.

Avnet and Microchip recently announced co-developed methods to simplify IoT security for full lifecycle secure device management (SDM). It comprises pre-integration of IoTConnect to Microchip's CryptoAuthentication® ICs.

Nuri Dagdeviren, corporate vice president of Microchip's secure computing business unit, said: "Integrating Avnet's IoTConnect SDM technology with our Trust&GO platform allows removal of customer touchpoints requiring setup of certificates and provisioning of associated keys securely in an embedded system. This removal enabled by our partnership with Avnet facilitates customer deployment towards another level of scale with enhanced security."

STARTING YOUR IoT JOURNEY

Renesas Electronics

The Renesas CK-RX65N Cloud Kit is based on the RX65N MCU group . It has been designed for IoT applications running real-time operating systems and middleware stacks, so offers plenty of processing performance. Connectivity is provided through the RYZ014A PMOD CAT-M1 cellular module and included SIM card, as well as Ethernet.

Many sensors are integrated on the board, including indoor and outdoor air quality sensors, a 9-axis motion sensor, and temperature and humidity. In addition, it offers two MEMS microphone and compatibility with Arduino through an Uno R3 connector.

Renesas and Avnet are strong IoT partners. The Renesas Quick-Connect Studio is delivering online, cloud-based development. Engineers can use a graphical interface to build hardware and software prototypes that accelerate product development. As it matures, Avnet will provide deeper integration into Quick-Connect Studio. This will give developers targeting IoT the ability to abstract firmware and streamline designs based on custom hardware.

Avnet

IoTConnect is Avnet's software solution that provides an easy path to deploying large IoT applications and associated services. It includes libraries and SDKs that integrate into both the endpoint and the cloud platform.

Avnet is already working with the market leaders from both IoT vectors: the endpoint and the cloud platform. IoTConnect has been architected to simplify, through standardization, the design effort required to connect endpoint hardware to cloud software.

Steven Detloff, Avnet's IoT solutions manager, explains how Avnet is working with manufacturers to help OEMs move from PoC to production: "In a general sense, enablement refers to taking reference code provided by microcontroller suppliers and pre-integrating the IoTConnect SDK. The resultant releases on GitHub allow the development boards to connect and communicate with IoTConnect."

Access the IoTConnect Quick Start Demo pages:

- ST Discovery Kit for IoT node with STM32U5 series
- Microchip WFI32-IoT Development Board
- Infineon XENSIV™ Kit with PAS CO2 sensor
- Avnet MaaXBoard SBC based on NXP i.MX 8M
- Renesas CK-RX65N Cloud Kit Based on RX65N MCU Group

Avnet complements the code with robust documentation, which ensures customers can reuse code snippets in their own implementations of the reference designs.

Providing reference enablement code reduces the time and effort required to create demonstrations and PoCs. It accelerates the development of a production design leveraging the IoTConnect platform.

Integrating multiple PoCs at the cloud level

A large scale IoT solution will include multiple hardware targets and, possibly, several IoT cloud platforms. OEMs will need to move freely through the landscape to quickly evaluate the right solutions for their applications. Integrating multiple hardware platforms, even on the same cloud platform, can be a challenge and incur multiple development cycles.

IoTConnect has been architected to provide a common abstraction layer between the hardware target and the cloud platform. This layer provides more than abstraction from the underlying hardware. It provides a simpler way to add security and access the features of an endpoint and the microservices of a cloud platform.

Using IoTConnect, OEMs can move quickly from the PoC stage towards developing complete heterogeneous IoT solutions that leverage the most optimal hardware solution from almost any semiconductor vendor. IoTConnect enables full integration into the AWS IoT cloud platform, while making it simpler to move between hardware targets.

/UNDERSTANDING THE CHALLENGES AHEAD

The PoC stage is an important phase in development. The PoC will likely be the first time an OEM can demonstrate the purpose of their IoT solution. Bringing multiple development and evaluation kits together helps to demonstrate how a concept becomes a strategy.

Scaling up from PoC will require more than integrating multiple evaluation kits. Inevitably, there will be design requirements that dictate changes be made to both hardware and software.

While evaluation kits are well positioned to get OEMs to the PoC stage, moving forward they will also need design support. Using abstraction in the way offered by IoTConnect can streamline the design phase by accessing support that will be applicable to diverse endpoint designs based on almost any vendor's silicon.

There are many touchpoints where modification and design refinement will be necessary. Functionally, the OEM will be well equipped to make those changes. In terms of the communication channel, standards and modules provide the ideal starting point. The main effort will be required at the point where these two functions converge.

Beyond defining what goes into the payload, OEMs will need to focus on security. Ensuring the security of the data, the endpoint, and the overall connection will be a high priority

Security in endpoints and the cloud

It took a long time and many publicized security breaches to move security up the IoT priority list. For too long, manufacturers were willing to take the view that small IoT devices were too obscure to be targeted by malicious actors. In truth, the digital footprint of the smallest smart sensor is the same size as the largest connected utility plant. All it takes is one unsecured IP address.

In the IoT timeline, IoTConnect is relatively new. Because it was conceived and developed while securing IoT connections became a priority, IoTConnect has SDM baked in.

Wherever IoTConnect is used, SDM is present. Instigating security becomes easier when the technology is inherent. And as outlined earlier, Avnet is working hard with semiconductor vendors to put IoTConnect and SDM directly into silicon solutions. This puts security where it needs to be: everywhere.

Hardware-secure elements provided by silicon manufacturers for microcontroller products, such as Microchip's Trust&Go, still need to be managed in the cloud. Avnet's SDM, found in Avnet IoTConnect's console, creates a user interface to easily manage device security in the cloud, which includes such things as identifying the devices, verifying certification or authentication, and storing certificates. SDM works in conjunction with the hardware-secure element providing a simple interface to manage security for connected devices over their entire lifecycle.

IoT system deployment

Security plays a less apparent but just as crucial role in the deployment phase of an IoT application. As each new endpoint is integrated into the system architecture, the cloud application must recognize the endpoint and attach it to the network. A similar process needs to take place as endpoints reach their end-of-life.

This is termed provisioning and decommissioning. It represents a serious security threat. Allowing devices onto a network gives them access to parts of the network. When endpoints are removed from a network they need to be removed securely, otherwise a malicious actor may acquire the endpoint and, with it, access to the network.

UNDERSTANDING THE CHALLENGES AHEAD

Provisioning and decommissioning endpoints

Provisioning is the process of adding an endpoint to a network. Doing this securely involves identification and authentication before issuing a certificate that allows the device to become part of the network.

For many OEMs, this can be the most demanding phase. It is complex, necessarily, which adds to the challenge. Understanding how secure provisioning works in an IoT application involves another learning curve.

Typically, this phase is abstracted away at the PoC stage when using an evaluation or development kit. Moving to production will require understanding and implementing the provisioning methods available from the chosen IoT cloud platform.

AWS supports several approaches to provisioning, including using pre-installed certificates and provisioning by a trusted user.

Decommissioning requires the certificate to be securely removed from the device before it can be released from the network. Devices that are not correctly decommissioned present a security risk if their identification is not removed from the cloud platform's list of trusted devices.

Provisioning and decommissioning involve a deeper understanding of public key infrastructure and transport layer security. IoTConnect has SDM built-in, which can help abstract away the complexity of secure provisioning and decommissioning.

/LONG-TERM SUSTAINABILITY IN IoT

IoT endpoints are typically hardware devices defined in large part by software. It is possible, but uncommon, to redefine the hardware after the device is deployed. It is common, and often part of the OEM's strategy, to redefine the software while the device is in service.

There are two main reasons for in-service software updates. The first is to support feature development or unlock hardware features after the device has been deployed. This may be to support new revenue generation, or as part of the long-term product strategy.

For example, an endpoint may be equipped with cellular connectivity through the integration of a subscriber identity module (SIM). In embedded devices, like an IoT endpoint, a common approach is to use an embedded universal integrated circuit card, or eUICC, or eSIM (embedded SIM). If an endpoint is intended for use across multiple geographic regions, it is common to configure and activate an eSIM in the field.

The second reason to support in-service software updates is to improve or repair the device at the software level. The software update may be to remove a bug that was discovered after shipping or to mitigate a potential security risk found in the software. Devices based on popular operating systems such as Linux may also need to be updated after deployment for the same reasons.

Over-the-air (OTA) updates are the recommended way to support in-service software updates. OTA requires its own security measures. The connection needs to be authenticated, but so does the source of the software update. Attack methods such as man-in-the-middle can be used to intercept new firmware. By inserting a small amount of code, the firmware update can become the doorway for bad actors.

There are well-defined and practical precautions that should be implemented when using OTA. Most PoC platforms include some form of OTA, which can help OEMs understand how to implement it correctly.

Long-term, large-scale endpoint maintainability

Moving from PoC, the OEM needs to implement a strategy for using OTA across a large-scale deployment of perhaps thousands of devices. Also, there will be contiguous updates over the lifetime of the IoT application.

Keeping track of the latest firmware versions used across multiple endpoint types is one aspect of the long-term sustainability. At an implementation level, OTA updates need to be carefully scheduled and controlled.

In the massive IoT, OTA becomes the most significant aspect of maintenance. It is unrealistic to plan any IoT solution that does not support OTA.

IoTConnect was designed to support wide-scale secure OTA. The features include a cataloger and scheduler specifically configured as a deployment mechanism for OTA updates. These features enable OTA updates to be managed and deployed at scale, to diverse endpoints across a wide area network, without interruption to service. The synchronization of wide-scale OTA updates is critical, due to the potential dependencies between devices.

EXPLORING THE FUTURE OF XAAS (AS-A-SERVICE) IN IoT

The "as-a-service" suffix can be applied to many things. That is largely thanks to IoT, connectivity, and OTA technology. It is most often called SaaS (software as-a-service). It can also be applied to hardware if access to that hardware incurs an ongoing fee.

We can differentiate in terms of product and service simply if we assume the sale of a product is a single financial transaction, and a service has a recurring financial transaction. However, this obscures the cost of supporting a product long after that single transaction has taken place.

According to Michael Lamp, director of Global IoT Enablement at Avnet, OEMs should think about SaaS as a product line, not just software. There needs to be a good business strategy behind offering anything as-a-service. There will be ongoing maintenance costs associated with a service, just as there are with a product. But to fully leverage the XaaS model, the features of the service also need to improve over time.

By standardizing on IoTConnect, OEMs are positioning themselves to explore and leverage the XaaS paradigm as it develops.

What is XaaS?

Many companies offering something as-a-service follow a subscription-based model. If the customer stops paying, they stop receiving the service. This can work for some services, like streaming the latest movies, but it does not work in IoT.

A subscription model does not map well to a multitiered service. In IoT, there can often be multiple tiers involved. Each partner will provide additional value to the end-customer. Using SaaS as a subscription would put all the financial burden on the consumer and make it difficult to attribute the revenue appropriately between the partners.

In the context of IoT solutions, XaaS becomes simpler to administer when it uses an independent intermediary, such as Avnet, with services running over IoTConnect.

What could XaaS mean to your IoT solution?

Data is at the heart of IoT. Data ownership becomes one of the main challenges involved with a multitiered XaaS solution. Knowing where the data was generated, who can use it and who retains ownership can become contested when the value of the data is inherent to the application.

Avnet's IoT services have been developed with multitiered services in mind. Avnet can act as the intermediary to harvest and store data in the cloud. Access to these services can be managed through the features offered by IoTConnect running on the AWS IoT cloud platform.

IOTCONNECT'S SOFTWARE SOLUTION ACCELERATORS

The software solution accelerators developed by Avnet for IoTConnect are focused on the cloud application. In terms of enablement, they are comparable to – and complement – the endpoint-centric PoC hardware kits developed by semiconductor manufacturers.

Each accelerator integrates the cloud services needed by a specific end application. This provides a foundation for the OEM, giving them access to around 70% of the cloud functionality their IoT solution needs.

The accelerators are designed to be further enhanced and optimized. They can also be combined for applications that need features from more than one accelerator.

Avnet's engineers achieve this by implementing application programming interfaces (APIs) into IoTConnect that communicate directly to the microservices offered by AWS IoT. The APIs make it simpler to access the services, as the OEM does not need to devote engineering resources to understanding how the microservice works.

Using IoTConnect's software solution accelerators, OEMs can move quickly from PoC to creating business value. The accelerators provide a template for complete IoT solutions targeting the most in-demand applications across all verticals. OEMs and systems integrators are already leveraging this capability to deliver complete customized services built on proven standard foundations.

ALL INDUSTRY OFFERINGS


Smart Factory


Smart Healthcare


Smart Office


Asset Monitoring


Air Quality Monitoring


Smart Warehouse

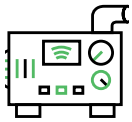

Connected Workforce

Smart Retail


Smart Fleet Management

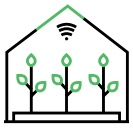

Cell Tower Monitoring


Smart City


Mobile Energy Generator Monitoring


Energy Monitoring


Facility Monitoring


Smart Agriculture


Fresh Produce Monitoring

/CONCLUSION

The business opportunities presented by connectivity are boundless. Invariably, they all depend on good data. Wide area networking and cloud platform providers have created the infrastructure to explore these opportunities.

The responsibility of implementation cannot be outsourced entirely. But by standardizing on IoTConnect, OEMs can remove many of the pain points associated with building an IoT solution.

Through IoTConnect, access to the growing infrastructure of IoT technologies becomes simpler. IoTConnect is the scalable and secure way to build IoT solutions and deliver dependable business services.

/ OFFICES

AUSTRIA
Vienna
Phone: +43 186 642 300
Fax: +43 186 642 350
wien@avnet.eu

BELGIUM
Merelbeke
Phone: +32 9 210 24 70
Fax: +32 9 210 24 87
gent@avnet.eu

BULGARIA
Sofia
sofia@avnet.eu

CZECH REPUBLIC (SLOVAKIA)
Prague
Phone: +420 234 091 031
Fax: +420 234 091 030
praha@avnet.eu

DENMARK
Herlev
Phone: +45 432 280 10
Fax: +45 432 280 11
herlev@avnet.eu

ESTONIA
(LATVIA, LITHUANIA)
Pärnu
Phone : +372 56 637737
paernu@avnet.eu

FINLAND
Espoo
Phone: +358 207 499 200
Fax: +358 207 499 280
helsinki@avnet.eu

FRANCE (TUNISIA)
Rennes
Phone: +33 299 838 485
Fax: +33 299 838 083
rennes@avnet.eu

Illkirch
Phone: +33 390 402 020
Fax: +33 164 479 099
strasbourg@avnet.eu

Massy Cedex
Phone: +33 164 472 929
Fax: +33 164 470 084
paris@avnet.eu

Toulouse
Phone: +33 05 62 47 47
toulouse@avnet.eu

Vénissieux Cedex
Phone: +33 478 771 360
Fax: +33 478 771 399
lyon@avnet.eu

GERMANY
Berlin
Phone: +49 30 214 882 0
Fax: +49 30 214 882 33
berlin@avnet.eu

Freiburg
Phone: +49 761 881 941 0
Fax: +49 761 881 944 0
freiburg@avnet.eu

Hamburg
Phone: +49 40 608 235 922
Fax: +49 40 608 235 920
hamburg@avnet.eu

Holzwickede
Phone: +49 2301 919 0
Fax: +49 2301 919 222
holzwickede@avnet.eu

Kaarst
Phone: +49 2301 919 0
Fax: +49 2301 919 222
kaarst@avnet.eu

Lehrte
Phone: +49 5132 5099 0
hannover@avnet.eu

Leinfelden-Echterdingen
Phone: +49 711 782 600 1
Fax: +49 711 782 602 00
stuttgart@avnet.eu

Leipzig
Phone: +49 34204 7056 00
Fax: +49 34204 7056 11
leipzig@avnet.eu

Nürnberg
Phone: +49 911 24425 80
Fax: +49 911 24425 85
nuernberg@avnet.eu

Poing
Phone: +49 8121 777 02
Fax: +49 8121 777 531
muenchen@avnet.eu

Wiesbaden
Phone: +49 612 258 710
Fax: +49 612 258 713 33
wiesbaden@avnet.eu

HUNGARY
Budapest
Phone: +36 1 43 67215
Fax: +36 1 43 67213
budapest@avnet.eu

ITALY
Cusano Milanino
Phone: +39 02 660 921
Fax: +39 02 660 923 33
milano@avnet.eu

Firenze
Phone: +39 055 428 2301
Fax: +39 055 431 035
firenze@avnet.eu

Modena
Phone: +39 059 348 933
Fax: +39 059 344 993
modena@avnet.eu

Padova
Phone: +39 049 807 368 9
Fax: +39 049 773 464
padova@avnet.eu

Turin
Phone: +39 011 204 437
Fax: +39 011 242 869 9
torino@avnet.eu

Roma
Phone: +39 02 660 921
roma@avnet.eu

LITHUANIA
Kaunas
lithuania@avnet.eu

NETHERLANDS
Breda
Phone: +31 765 722 700
Fax: +31 765 722 707
breda@avnet.eu

NORWAY
Asker
Phone: +47 667 736 00
Fax: +47 667 736 77
asker@avnet.eu

POLAND
Gdansk
Phone: +48 58 307 81 51
Fax: +48 58 307 81 50
gdansk@avnet.eu

Katowice
Phone: +48 32 259 50 10
Fax: +48 32 259 50 11
katowice@avnet.eu

Warszawa
Phone: +48 222 565 760
Fax: +48 222 565 766
warszawa@avnet.eu

PORTUGAL
Vila Nova de Gaia
Phone: +35 1 223 779 502
Fax: +35 1 223 779 503
porto@avnet.eu

ROMANIA (BULGARIA)
Bucharest
Phone: +40 21 528 16 32
Fax: +40 21 529 68 30
bucuresti@avnet.eu

SLOVAKIA
Bratislava
Phone: +421 232 242 211
Fax: +421 232 242 210
bratislava@avnet.eu

SLOVENIA
(BOSNIA AND HERZEGOVINA, CROATIA, MACEDONIA, MONTENEGRO, SERBIA)
Ljubljana
Phone: +386 156 097 50
Fax: +386 156 098 78
ljubljana@avnet.eu

SPAIN
Barcelona
Phone: +34 933 278 530
Fax: +34 934 250 544
barcelona@avnet.eu

Galdàcano. Vizcaya
Phone: +34 944 572 777
Fax: +34 944 568 855
bilbao@avnet.eu

Tres Cantos
Phone: +34 913 727 100
Fax: +34 916 369 788
madrid@avnet.eu

SWEDEN
Sundbyberg
Phone: +46 8 587 461 00
Fax: +46 8 587 461 01
stockholm@avnet.eu

SWITZERLAND
Rothrist
Phone: +41 62 919 555 5
Fax: +41 62 919 550 0
rothrist@avnet.eu

TURKEY (GREECE, EGYPT)
Kadikoy Istanbul
Phone: +90 216 528 834 0
Fax: +90 216 528 834 4
istanbul@avnet.eu

UNITED KINGDOM (IRELAND)
Maidenhead
Phone: +44 1628 512 900
Fax: +44 1628 512 999
maidenhead@avnet.eu

Stevenage, Herts, Meadway
Phone: +44 1438 788 310
Fax: +44 1438 788 250
stevenage@avnet.eu

ISRAEL
Tel-Mond
Phone: +972 (0)9 7780280
Fax: +972 (0)3 760 1115
avnet.israel@avnet.com

SOUTH AFRICA
Cape Town
Phone: +27 (0)21 689 4141
Fax: +27 (0)21 686 4709
sales@avnet.co.za

Durban
Phone: +27 (0)31 266 8104
sales@avnet.co.za

Johannesburg
Phone: +27 (0)11 319 8600
Fax: +27 (0)11 319 8650
sales@avnet.co.za