Circuit Protection is Key in Maintaining Growth for The Internet of Things

WHITE PAPER

INTRODUCTION

The Internet of Things (IoT) promises a future that networks billions of smart, connected devices. The value of this diverse new world of intelligent systems is the sharing of actionable, real-time data that can be accessed across a range of industries such as healthcare, manufacturing, utilities and transportation. Connected, intelligent systems require a greater level of system reliability to be most useful, ensuring ongoing data capture and analysis. This white paper provides an overview of how the IoT ecosystem is developing. It also highlights the IoT-enabling technologies that Bourns provides for circuit protection, circuit conditioning and motion control to help ensure high reliability in the essential link between networked devices and the decision maker.

DEFINING THE INTERNET OF THINGS

The Internet of Things (IoT) is a term applied to the business proposition of increasing communication between integrated, sensor-enabled physical objects via the Internet. It is recognized as the wave of the future for virtually any networked device in a variety of markets and applications including factory automation, building automation systems, safe cities, intelligent homes, wearables, smart meters, smart grid energy systems, and much more. The basic premise relies on connecting any device with an on/off switch to the Internet or to each other, creating large-scale networks of intelligent devices communicating in real-time to enable significant business advantages.

IoT is not relegated to a single sector or market, but is a trend that has an effect on all markets on a global basis with the power to change every aspect of our lives. It goes beyond what we typically think of as communication devices and can include everything from coffee makers, washing machines, and wearable fitness devices to vending machines and medical diagnostic equipment. Almost any machine can be transformed from a standalone device into a smarter, more connected system. Adding intelligence to the network(s) of sensors (increasingly used for gathering information from machines, objects and people) results in more meaningful and actionable data that can be used for smarter asset management which also helps to increase productivity and reduce costs.

The trend toward connectivity and control has been around for more than 50 years, initially in the form of factory automation. The need for integrated or "smart" sensors and connectivity in the factory was driven by the requirement to boost productivity while reducing energy consumption and improving quality. By streamlining processes and enhancing communications on the factory floor, the industry illustrated the great potential that connectivity could bring to other markets. Combining the explosion of low-cost, high-speed communications technologies, smart sensors and data analytics with the ability to ensure higher device reliability with advanced circuit protection technologies is the foundation IoT needs to ensure its future successful adoption and growth.

BOURNS®
09/15 • e/K1557

Circuit Protection is Key in Maintaining Growth for The Internet of Things

WHITE PAPER

INTELLIGENT IoT DEVICES

The billions of connected devices streaming information that can be used to make decisions work in much the same way the human nervous system provides information to the brain. Various electronic sensors communicate with a local hub, a central location or a server; software analyzes the data received and either makes a decision based on programmed logic or notifies an operator to initiate some action. Some of these decisions can be optimized for automation. From driverless cars acting on multiple sensors detecting and controlling speed, lane position, direction, and braking to street lights that can automatically detect traffic while illuminating and darkening as needed to save electricity, the IoT will pervasively infiltrate the markets. Smart and connected industrial equipment can be employed to monitor individual machines and provide failure or error messages allowing field maintenance the opportunity to alleviate the issue, thus, eliminating unplanned factory downtime that can lead to reduced revenues. For example, IoT-ready equipment can be used to detect an imminent malfunction by monitoring temperature or vibration in a motor and notifying maintenance prior to catastrophic failure.

Fulfilling the promise of IoT mandates that applications be developed that ensure network efficiency, interoperability and security. The mandate for connectivity is also affecting data communication devices, which include networking equipment, servers and "Software as a Service" (SaaS). Therefore, the IoT ecosystem will be made up of numerous supporting technologies and is characterized as an extension of the existing Internet. The node or sensor segment, for example, will require multiple solutions to collect and disseminate data to make these solutions IoT-ready. As with all devices connected to the Internet, there is the need for components to ensure protection and conditioning of the circuit. The primary intelligent edge devices that comprise IoT include:

End points

End points are comprised of environmental, physical property, position or chemical sensors that act as the data collection point with information to be analyzed. They are the components responsible for monitoring systems for changes, as well as providing the prompt feedback used to make adjustments that keep systems performing at optimal levels.

Gateways

Gateways provide a range of functions including data aggregation and real-time analysis to and from an IP network. They also support reliable publish/subscribe mechanisms, and provide IoT data buffering in situations where the cloud is temporarily unavailable.

Hubs

Hubs are communications gateways themselves, such as switches, routers, or modems that facilitate connectivity. Simple hubs are devices that connect endpoints to broader networks; by integrating hubs, simple hubs can be connected with the outside world via the Internet. These relatively complex devices work together to provide a diverse array of services that fit together seamlessly.

INTELLIGENT IoT DEVICES *(Continued)*

Infrastructure

A network infrastructure is used to bring data from gateways and enterprise sources together. Infrastructure is what manages and monitors devices and services information, transforming it into actionable intelligence. Reliability is a very real concern to keep the network infrastructure running smoothly.

Network and Cloud Services

The IoT is all about communication. Data communication moves via LAN or WAN technology from hubs to servers; systems can function either locally or remotely and may be wired or wireless. This concept provides the overall infrastructure for the IoT.

Enhanced Services

Big data initiatives, analytical software and data servers or cloud storage are some of the enhanced services enabled by an IoT framework. To offer the greatest and most tangible business value, systems make use of the information collected in real-time – analyzing it for clues to company performance, equipment maintenance requirements, product preferences, and a range of new interactive services that can distinguish market leadership.

INTEGRATED RELIABILITY

More connected devices create more opportunity for system failure, which is certainly not an option for always-on, smart devices. As IoT systems will be used to generate new and innovative infrastructure systems, reliable performance is a critical factor. A smart grid or intelligent transportation application, for instance, must perform with extreme reliability and remove the threat of data tampering. Further, many devices are located away from the relative safety of an established server farm where they may be placed in remote locations, outdoors, in public infrastructure settings or perhaps worn by individuals. Transients such as lightning, burst or electrostatic discharge (ESD) are a constant threat to devices in remote or exposed locations.

Systems optimized for IoT deployment need to be designed with advanced surge and circuit protection to ensure sensitive circuits operate with the highest reliability. Rugged position sensors further aid in reliability, keeping systems suited for harsh computing environments. Customized magnetics and trimmers support efficient power management that also extends the life of IoT systems. Bourns' advanced circuit protection devices, such as the company's Multifuse® products, can be used to avoid catastrophic failure by monitoring and managing overheating inside motors and pumps. The Bourns® TBU® High-Speed Protector (HSP), a low conductive in-circuit protection device, can also add all-important current protection for data lines in exposed networks including lighting, power cross, or power surge events.. As IoT systems continue to proliferate, systems integrated with these circuit protection technologies increase reliability while reducing Bill of Materials (BoM) costs.

IoT GROWTH REQUIRES ROBUST CIRCUIT PROTECTION

It is estimated that the broad adoption of IoT will correlate to the growing need for circuit protection technologies. Technavio, an independent tech-focused global research firm, recently predicted the global circuit protection market to grow at a Compound Annual Growth Rate of 5.49 % during the period of 2014-2019[1]. Growth is based on the rising demand for electricity that is predicted to align with an increase in IoT deployments. Consider just one market as an example: automotive manufacturers today are designing intelligent, connected vehicles, which are much more complex and high performance. This change requires consistent circuit protection to the extent of adding protection to every wire.

Another IoT scenario shows that mobile device users typically interact with their device via touchscreens. These and other interfaces such as push buttons, switches or connectors can create ESD events on the device's supporting circuitry. Protecting against ESD failure requires protection devices such as ESD suppressors or TVS diodes. When the device supports higher throughput in the gigabit per second (Gbps) range, ESD protection requires smaller device capacitance and faster response times. For example, Bourns' current generation of ESD protection devices provide sub-picofarad channel capacitance and nanosecond response times.

When a mobile device uses one or more radio frequency (RF) signal chains, it is particularly susceptible to ESD disruption and may require integrated ESD technology as well as external circuit protection. Further, because mobile batteries are often hot swappable, they too may be subject to short circuit or overloads. These overcurrent conditions are managed with sophisticated resettable fuses such as Bourns® Multifuse® products. Made of conductive polymer, these devices become highly resistant when a fault occurs and return to their low resistive state when the fault is resolved. Longer battery life and increased power efficiency results directly from these low resistance resettable fuses.

[1] *Technavio, Global Circuit Protection Market 2015-2019, July 2015*

Circuit Protection is Key in Maintaining Growth for The Internet of Things

WHITE PAPER

RELIABILITY AND THE FUTURE OF IoT

"By enabling devices to communicate with each other independently of human interaction, the Internet of Things will open up new revenue streams, facilitate new business models, drive efficiencies and improve the way existing services across many different sectors are delivered."[2] Energy conservation, the growth of integrated sensors, and connectivity to the Internet are changing the way people and systems interact with the environment and the world. A case in point is that even as energy consumption rises worldwide in response to economies expanding their infrastructures, utilizing the IoT ecosystem reduces the strain on natural resources. IoT devices help smart meters provide the utility with real-time consumption information enabling intelligent transmission strategies. Energy providers now have the ability to optimize energy distribution and provide clean, reliable power. Medical and industrial fields are capitalizing on the IoT trend as well, as personal comfort, health, and safety have become more important on a global basis.

The number of IoT connections is expected to continue its exponential growth rate. New communication protocols and system architectures will support the bandwidth and computing performance needed to continue growth. "Smart sensors" will fuel data collection and dissemination through integration and communications. Analyzing IoT-provided data, whether it is environmental or social, will enable us to increase production capability, reduce energy consumption and improve the quality of life.

For IoT OEMs and system designers working to fulfill the IoT promise, circuit protection needs to be a high priority early in the design phase. With efficient circuit protection, one worry of system reliability in a connected work is removed. With its broad line of circuit protection, circuit conditioning and motion control products, Bourns enables the reliability that is the vital bond between networked devices and the decisionmaker, allowing the vast Internet of Things to deliver useful information anytime and anywhere it is needed.

[2] *GSMA, Understanding the Internet of Things (IoT), July 2014*

ADDITIONAL RESOURCES

For more information about Bourns' complete line of products, please visit:

www.bourns.com

BOURNS®

09/15 • e/K1557

Americas: *Tel* +1-951 781-5500
Fax +1-951 781-5700

EMEA: *Tel* +36 88 520 390
Fax +36 88 520 211

Asia-Pacific: *Tel* +886-2 256 241 17
Fax +886-2 256 241 16