BRIEF
Internet of Things
Federal

Harnessing the Power of IoT

Components of a successful solution design

Gateways – such as the Intel® DK300 Series – help customers to securely compute, aggregate, and share data.

"The world is in the midst of a dramatic transformation from isolated systems to Internet-enabled devices that can network and communicate with each other and the cloud. Commonly referred to as the Internet of Things (IoT), this new reality is being driven by the convergence of increasingly connected devices, compute and data economics, and the proliferation and acceleration of cloud and big data analytics. This shift in technology is generating unprecedented opportunities for the U.S. public and private sectors to develop new services, enhance productivity and efficiency, improve real-time decision making, solve critical societal problems, and develop new and innovative user experiences."[1]

For Federal agencies, implementation of an IoT solution offers many benefits:

- Reduced time to information
- Reduced cost of information systems (data transmission and storage)
- Reduced infrastructure investments
- Increased quality of information
- Increased security of information
- New approaches for data transmission during limited network bandwidth

Within the Federal environment, significant benefits from IoT can be realized through innovative solution designs spanning from simple to complex systems. New technology, such as the Intel® Gateway shown on the left, is at the heart of these IoT systems. In an example of a simple system, a wearable heart rate monitor performs condition-based monitoring utilizing a single sensor to capture a single data type before transmitting data anomalies with a gateway to alert a doctor's office. In an example of a complex system, predictive maintenance alerts are derived by streaming data from multiple types of sensors from multiple systems into compute algorithms on a gateway that will populate dashboards to support smart building management decision making.

Intel's Approach to an IoT Solution

Intel's IoT approach, illustrated in Figure 1 on the next page, is to create a solution comprised of multiple components that provide end users with analytical capabilities that drive informed decisions. An IoT foundation begins with connectivity, manageability, and security. The physical components of the solution are edge devices, gateways, networks, and public and private clouds. A data interoperability framework supports data transfer between IoT components, while analytics capabilities, integrated into both the edge and cloud, change data into information.

"Data interoperability is one of the core challenges that needs to be addressed when designing IoT solutions."

Tiffany Sargent
IoT Senior Solutions Architect,
Intel Federal LLC

Successful approaches for IoT solution designs result in information that can be shared with end users who use data computed either at the edge or the cloud, or both. Design approaches require that information be viewed and interacted with across multiple platforms such as phones, handhelds, tablets, machine dashboards, and control centers. Interaction requirements can include both people-to-machine and machine-to-machine communications. To ensure IoT system resources are optimized for the desired operations and usage models, compute models and data flows are created and integrated with physical components to maximize edge-to-cloud overall performance.

Connectivity, Manageability, and Security

Intel's IoT solution is based on the foundational elements of connectivity, manageability, and security that anchor the physical components. These elements are accomplished by using McAfee and Wind River products. Using high-performance messaging, connectivity spans multiple device and data protocols across different networks. Manageability supports both devices and APIs. Security is a cornerstone of IoT that spans devices, clients, servers, clouds, data, and APIs. A security model must be both robust and adaptable to support multiple types of use cases and usage models across a variety of infrastructures. Combining a security model with manageable endpoints and secured communications powered by policy provides a robust solution that helps enable autonomy in the endpoints and decision making at the edge.

How the IoT Solution is Enhanced by Gateways at the Edge

From a physical perspective, the first point of data collection is an "edge" device or "thing." Things sense, compute, and respond to data requests at the edge. Gateways can be physically placed between the edge device and the cloud. Gateways aggregate data, compute data, and control data at the edge. The network dynamically scales and connects

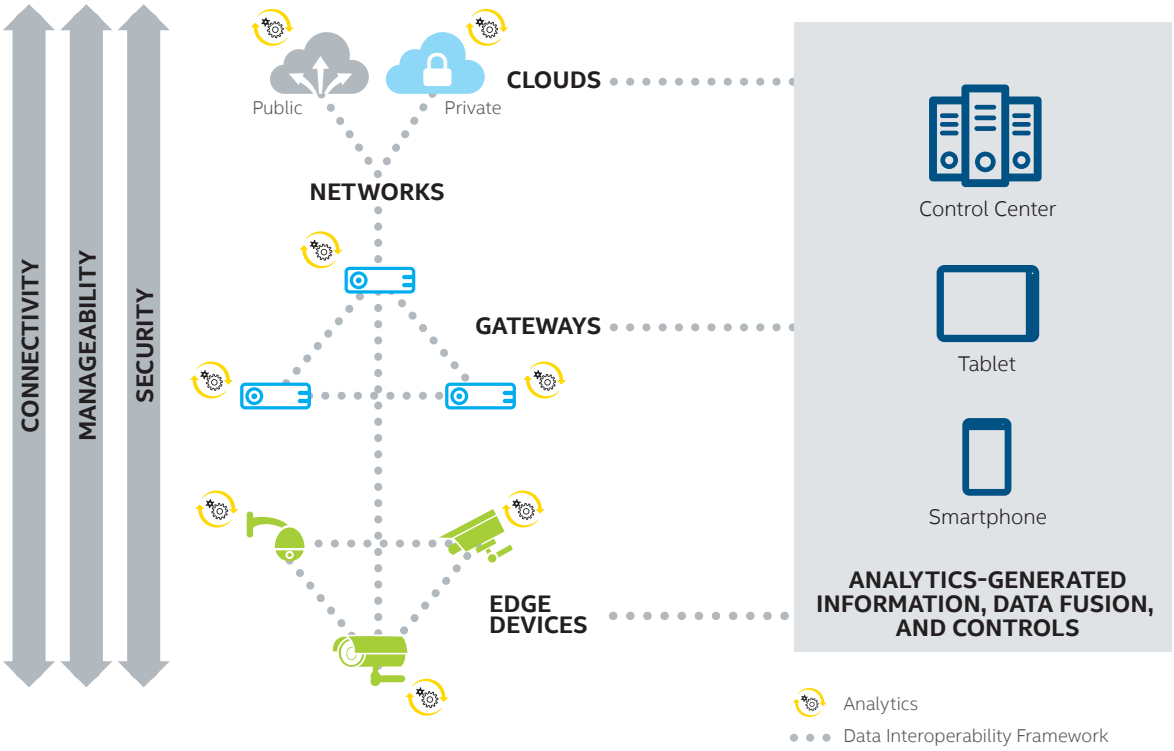

Figure 1. An IoT solution is comprised of physical components (edge devices, gateways, networks, and clouds), a data interoperability framework, and compute capabilities (analytics).

the IoT solution starting from the edge to a server or cloud. Within either a private or public cloud environment, the cloud runs software, manages both the platform and infrastructure, and computes. As IoT systems mature, the industry can expect to see distributed and shared compute across the physical components that will begin to recognize smart edge devices, gateways, and servers as interoperable nodes.

IoT solutions make existing devices more intelligent because data can be computed and managed locally at the edge where the data is first collected and ingested into the system. As data moves through an IoT solution, it can seamlessly integrate with other data (data fusion), systems, and infrastructure. Significant benefits result when compute begins at the edge and only the desired data is moved for additional processing in the cloud or shared in real time with an end user. These benefits include lower cost to move and store data and faster compute velocity during post-edge data processing. Compute location and data movement rely on the foundation of security designed to support the IoT system edge-to-cloud.

As Intel creates its IoT solution comprised of silicon, hardware, and software, solutions must interoperate across multiple government agency segments and technology domains. The desired architecture is based on a flexible and modular set of platforms, hardware, software, and analytical models. These new interoperable modular blocks can support multiple kinds of data flows both across edge devices and bidirectionally between the edge and the cloud. As interoperability is a cornerstone of an IoT ecosystem, some key design and implementation considerations are explored in more detail in the next section.

Interoperability Is Key to Successful IoT Solutions

A certain level of interoperability is necessary to achieve a successful IoT ecosystem. A significant difference in the IoT ecosystem from previous technology ecosystems is that data exchange or data fusion will be desired across domains or verticals versus previously when data was managed under specific standards within a single domain. Imagine integrating all the data from various sensors and systems of a Smart City such as environmental, transportation, infrastructure, energy, and industrial. An interoperability solution approach needs to span many aspects of the IoT solution ranging from systems to software to data to communications to network and beyond. Although positive actions through standards and individual vertical community frameworks have made great strides, the IoT ecosystem will require convergence and commonalities that are applicable across domains and verticals.

Interoperability for Legacy Systems

Developing and implementing an IoT solution requires integration of both new technology and existing legacy systems. It is unrealistic to believe that implementation of IoT will be accomplished as a systemic overhaul, but rather as a time-phased implementation of new IoT technologies, such as a gateway, that would support incremental benefits. The phased implementation approach will create significant benefits, but introduce new complexities with interoperability.

To address an environment with legacy systems, existing embedded sensors and instrumented machines on the edge will require a simple, scalable configuration data ingress strategy to be able to support broad-scale IoT implementation. In addition to the legacy

The Relationship between Cyber-Physical Systems and IoT

In the Federal Government, Cyber-Physical Systems (CPS) are often discussed concurrently with IoT systems and sometimes the terms are used interchangeably. CPS research, programs, and collaborative initiatives are funded and supported across the Federal Government. There are several overlaps between the IoT and CPS. Multiple, but similar definitions of CPS exist.

The National Institute of Standards and Technology (NIST) Engineering Laboratory, through its Cyber-Physical Systems and Smart Grid Program Office, is leading a NIST-wide program to advance CPS. NIST defines CPS or "smart" systems as "co-engineered interacting networks of physical and computational components."[2]

The Networking and Information Technology Research and Development (NITRD) program includes a cross-agency Cyber-Physical Systems Senior Steering Group, which defines CPS as "a generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities. The ability to interact with, and expand the capabilities of, the physical world through computation, communication, and control is a key enabler for future technology developments."[3]

There is a strong relationship between CPS and IoT – in fact, CPS is a physical manifestation of IoT. Therefore, the benefits and challenges associated with IoT apply equally to CPS.

environment, implementing new sensors requires interaction with a gateway or server in a specific manner to support extensibility. The development of interoperability strategies will require partnerships and open standards to facilitate IoT interoperability and provide a coordinated technology evolution path.

Data Interoperability

Data interoperability is the most significant aspect of IoT interoperability, because much effort and cost is associated with reconciling data formats or performing data transformations within and across systems. Additionally, from an operations perspective, managing cross-system data connections and modifications as done today will not be sustainable in the future IoT ecosystem. For example, how to manage timing and synchronization will become an even more complex issue within and across systems. Furthermore, the risk of compromised data quality increases with multiple cross-system data changes. The formation of an overarching IoT data interoperability framework is required to allow data to move through an IoT ecosystem and to support robust data quality; manage data governance, security, and policy; and have some minimum agreed-upon data structures or metadata.

A data interoperability framework will lower the barriers for data to move seamlessly within the IoT ecosystem and could be utilized, for example, in the management of critical infrastructure comprised of cross-domain systems.

Conclusion

The IoT ecosystem holds great potential, creating opportunities for innovation and partnership. New Federal IoT usage models are emerging every day within the public sector, many as the result of collaborative discussions with technologists to explore the art of the possible. With the availability of new technology, thought leadership, and establishment of consistent IoT policies and global standards that support interoperability, both the public and private sectors can continue to explore new ways to harness the power of IoT technologies, such as edge compute, creating a world that is more efficient and productive.

For more information visit **www.intel.com/federal**

Author

Tiffany Sargent
IoT Senior Solutions Architect
Intel Federal LLC

Contributors

Marjorie Dickman
Global Director of IoT Policy
Intel Corporation

Chris Hunt
IoT Solutions Architect
IoT Center of Excellence

Follow the conversation: **#intelfederal**

[1] Marjorie J. Dickman, "Policy Framework for the Internet of Things," Intel Corporation – Global Public Policy (2014).

[2] For more information about CPS go to www.nist.gov/cps/cpspwg.cfm

[3] The Networking and Information Technology Research and Development (NITRD) program researches and develops information technology capabilities to empower Federal missions; support U.S. science, engineering, and technology leadership; and bolster U.S. economic competitiveness. www.nitrd.gov/nitrdgroups/index.php?title=Cyber_Physical_Systems_%28CPS_SSG%29#title