Response to Commerce Department's Request for Comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"(RIN 0660–XC024)

by Dr Robert Marcus
Co-Chair of NIST Big Data Public Working Group
CTO of ET-Strategies
robert.marcus@et-strategies.com

Response to US Commerce Department's Request for Comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things"(RIN 0660–XC024)

by Dr Robert Marcus
CTO of ET-Strategies (robert.marcus@et-strategies.com)
Co-Chair of NIST Big Data Public Working Group

Introduction:

This document is a response to some of the questions included in the Commerce Department's Request for Comments on "The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things". The questions addressed are:

1. *Challenges and opportunities arising from IoT*
2. *Definitions of "Internet of Things" and related concepts*
4. *Dividing or classifying the IoT landscape*
5. *IoT research and initiatives*
6. *Technological issues that may hinder the development of IoT.*
7. *Prioritizing Commerce Department and Government IoT activities*
8. *IoT demands on existing infrastructure architectures, business models, or stability*
9. *Preparing to minimize IoT disruptions on existing infrastructures*
13. *Impact of IoT have on industrial practices*
16. *Government response to cybersecurity concerns about IoT*
20. *Factors that Department should consider in its international IoT engagements*
26. *IoT role of the Department of Commerce within the federal government*
27. *Strategy for future Government and private sector collaboration in IoT*

Many reference links and diagrams are included to provide more detailed information on each of these topics.

Executive Summary:

Categories of Internet of Things (IoT) Applications: There are many different types of IoT applications. The appropriate roles of government organizations (e.g. Department of Commerce) depends on the IoT application category. Some examples of categories and possible government response are:

- Research and Testbeds: (Recommendation - Government Funding Support) CPS research and testbeds should be supported by government grants. These grants should be focused on key areas of CPS technology. Some examples include systems of systems implementations, advanced CPS analytics, and interoperability across diverse devices.

- Private industrial: (Recommendation - Government Standardization Support) . CPS industrial applications (e.g. Smart Manufacturing)will usually be privately deployed and managed. However these initiatives will strengthen US economic competitiveness. Government should support standardizations in this area

- Public Consumer: (Recommendation - Government Regulate) CPS consumer applications (e.g. Smart Home) will usually be privately developed. Government should supply regulations guaranteeing factual marketing, privacy and security for consumers. Governments could mandate specific capabilities and standardizations if necessary.

- Public Governmental (Recommendation - Government Managed) CPS governmental applications (e.g. Smart City) should be managed by Government executive leadership. Some technology development and system integration can be performed by commercial vendors using Government specifications.

- Defense and Intelligence (Recommendation - Government Owned) CPS defense and intelligence applications should be owned by the Government and developed under the appropriate security regulations and Government standards . Contractors should be required to meet these regulations and standards and be carefully supervised.

Public Governmental Applications: The most demanding of the Public Governmental IoT applications are the large-scale Smart X systems of systems (e.g. Smart Grid, Smart Cities). This is the area where the Department of Commerce can make the greatest contribution. (There will also be spill-over benefits in other IoT application categories e.g. Smart Manufacturing.) There are many unresolved challenges in technology, architecture, standardization, engineering, security, and policy for robust implementations.

Some of the technology challenges are listed below: All of the presentations are accessible from http://www.slideshare.net/bobmarcus/inventory-of-my-cps-slide-sets

- Interfaces between IoT and Cloud. See http://www.slideshare.net/bobmarcus/diagrams-io-t-interfaces-to-cloud-big-data and http://www.slideshare.net/bobmarcus/iot-to-cloud-middle-layer

- Hierarchical Data Processing. See www.slideshare.net/bobmarcus/data-processing-in-cyberphysical-systems and http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems .

- Hierarchical Real-Time Control. See http://www.slideshare.net/bobmarcus/control-in-cyberphysical-systems and http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems

- Management of Devices including Power, Time, and Networking. See http://www.slideshare.net/bobmarcus/management-for-cps

- Engineering Large-Scale System of Systems. See http://www.slideshare.net/bobmarcus/engineering-large-scale-cyberphysical-systems,and http://www.slideshare.net/bobmarcus/iot-nodesosmiddlewareplatforms

- Security, Privacy and Trust. See http://www.slideshare.net/bobmarcus/security-in-cyberphysical-systems

- Standardization and Interoperability. See http://www.slideshare.net/bobmarcus/standards-and-open-source-for-big-data-cloud-and-iot

- Developing testbeds to support research and testing on Cyber-Physical Systems tools and technologies. See www.slideshare.net/bobmarcus/research-and-testbeds-in-cyberphysical-systems

Some Reference Architecture Challenges and the Role of Hubs:

NIST has taken a leading role in defining Reference Architectures for Cyber-Physical Systems(CPS), Big Data, and Clouds. The current Reference Architectures are based on tightly coupled systems sharing a security and management fabric. To model Smart X applications, it is necessary to extend these architectures to deal with loosely coupled hierarchical multiscale systems of systems. This can be accomplished by considering the current Reference Architectures as models for “Hubs” that process data and commands. The Smart X architectures can then be modeled by linking Hubs with different capabilities. See http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems

Linking Hubs in a CPS systems of system architecture will require interoperability standards for data, messaging, and networking. There are many efforts underway by multiple organizations to develop these standards. (See the list of 30 organization in the answer to question 20). In the future, these standards must be harmonized and be robust enough to support end-to-end monitoring, analytics, and performance..

Engineering CPS systems of systems will require incremental development, deployment, and upgrading of individual systems. Standardized interfaces between Hubs will be necessary but not sufficient. It will also be necessary to utilize more sophisticated modeling, simulations, development tools, and methodologies.

Security and management will be essential for future Smart X applications. Due to the loosely coupled systems of systems architecture, these qualities must be handled in a distributed fashion. Each Hub must handle internal security and management with the ability to support distributed capabilities

Setting detailed policies for systems of systems will be difficult in a multiscale dynamic environment. It will be necessary to have set of core guidelines that can be enforced within and between Hubs.

Recommendations: In the IoT domain, the Department of Commerce should focus on contributing to Smart X applications. These contributions could include:

- Fund ongoing NIST efforts in Smart City/CPS applications such as those at http://www.nist.gov/public_affairs/releases/upload/smartcities_cps_budgetsheet.pdf
- Establish a NIST Public Working Group for Smart X applications combining Cyber-Physical Systems, Big Data, Cloud and domain experts.
- Develop a hierarchical Reference Architecture for CPS systems of systems (e.g. using Hubs) extending current CPS, Big Data, and Cloud Reference Models.
- Promote consensus standardizations for CPS including interoperability among distributed systems and Hubs at multiple scales from IoT to Cloud.
- Encourage collaboration initiatives among vendors in private Smart X applications e.g. Industrial Internet.See http://www.slideshare.net/bobmarcus/iot-use-cases.
- Develop core guidelines for security and privacy in distributed loosely coupled CPS systems of systems
- Support the creation of tools needed to incrementally design, develop, test, and deploy large-scale Smart X applications

My Experience: I have held many senior positions in software, consulting, manufacturing, and research organizations. These include:

* Co-Chair of NIST Big Data Working Group
* Major contributor to Cloud Standards Customer Council's IoT Architecture
* Chief Architect for General Motors Global Information Services
* Director of Colorado Grid Computing Initiative
* Director of Object Technology at AMS Center for Advanced Technology
* CTO with Rogue Wave Software
* VP of Technical Strategy for the MCC Research Consortium
* Coordinator for Object Oriented Standards at Boeing Computing Services
* SRI Senior Research Engineer Consultant on major DoD projects
* In 2002, I published "Great Global Grid: Emerging Technology Strategies" http://www.slideshare.net/bobmarcus/2002-great-global-grid-book
* In 2016, I created over a dozen slide sets related to IoT accessible at http://www.slideshare.net/bobmarcus/inventory-of-my-cps-slide-sets

Questions and Answers

1. Are the challenges and opportunities arising from IoT similar to those that governments and societies have previously addressed with existing technologies, or are they different, and if so, how?

IoT is a pervasive technology that will provide unique new challenges and opportunities. However it is also be an extension of current technology (e.g. devices, Internet, Cloud). See http://www.slideshare.net/bobmarcus/challenges-and-best-practices-for-iot-cloud-and-big-data-systems .Many examples of IoT technical challenges can be found in Table 1 below from "A Gap Analysis for IoT Systems" from Finland at http://arxiv.org/pdf/1502.01181.pdf

Category	Current status	Expectations	Gaps	Problems	Recommendations
Support of heterogeneous devices	Platforms assume smart objects to talk HTTP or require gateway	•Devices must be easily and securely integrable to the IoT platform without a gateway • Unified resources and simplify usability	**G1.1** Support of constrained devices **G1.2** Standardized IoT devices models **G1.3** Secure authentication, identification of management of IoT devices	• Heterogeneous interactions • Protocol standardization	• Relying on standard protocols (e.g., CoAP, LwM2M, MQTT) • Integration of state-of-the-art security and privacy protocols
Data ownership	Mainly given to the end-user but with very simple privacy policies	• Full control given to the owner of the data • Local storage • Fine-grained data visibility model	**G2.1** Manipulation of data in edge devices **G2.2** Self-storage	• Security of the data storage • Device constrains to store data and provide secure access control	Algorithms and mechanisms available to the data owner to limit the access only to a predefined set of the resources
Data processing & sharing	• Nonuniform data sharing format • Sharing is performed via nonuniform REST API	• Uniform data format across multiple platforms. • Pub/Sub mechanism and data catalogs • Edge analytics	**G3.1** Data processing is not well integrated in IoT platforms **G3.2** Efficient processing for data formats and models **G3.3** Data analytics is only available in cloud-based solutions **G3.4** Data catalogs are missing	• Complex identification system to access data • Fusion efficiently data streams from multiple data catalogs • IoT devices have limited computing capabilities	• Data catalogs with semantic indexes • Uniform and interoperable data models • Integration of data processing technologies in platforms • Cloudlet-like solution for edge analytics
Developer support	• REST API to access the data or devices handled by the platform • Applications are for internal use rather than for sharing (except IFTTT)	• Use of a common API to ease the development of cross-platform applications • Domain Specific Language (DSL) dedicated to cross-platform application development	**G4.1** Application mash-up APIs **G4.2** Limited presence of SDKs **G4.3** Absence of DSL with higher abstraction level primitives	• Require standardization of application interactions dedicated to the IoT • IoT app store are missing	IoT platforms must provide SDKs and APIs that maximize the re-usability of the services provided by their platform
Ecosystem formation	Platforms provide useful building blocks, storage and run-time environment for application developers	• Platform easily expandable by the developers and offering them incentives to contribute • Cross-platform sharing of applications and services • Local composition of services	**G5.1** Low platform expandability **G5.2** Limited monetizing possibilities **G5.3** Limited support for cross-platform integration	• Silos of platform-specific solutions • User's using multiple platforms may not be able to aggregate the whole data into a single application	• Financial incentives for developers shall be offered • A broker is needed to ease cross-platform integration • Models to contextually define IoT applications to simplify their discovery by the end-users
IoT marketplace	• Limited applications sharing • Limited (usage-based) charging of the end users of these applications	• Dedicated IoT data catalogs, IoT app store and IoT device store • Ability to advertise, deliver and charge for the use of applications and data • Validate applications against policies	**G6.1** Application, data and device catalogs dedicated to the IoT are generally missing **G6.2** The billing (based on fixed fees, usage, or other metrics) of the end-users of the data is generally missing	An ecosystem of independent application developers, device manufacturers, and end-users all supporting the platform is needed for the demand for marketplace to appear and sustain	The marketplace functionality shall be provided by future IoT platforms

Table 1. Challenges for the Internet of Things

Below is a list of Industrial IoT challenges from Cisco at http://www.slideshare.net/biren_gandhi/get-cloud-resources-to-the-iot-edge-with-fog-computing . Most of these challenges must be addressed in all large-scale Smart X applications

- Data Size/Sources (Velocity, Variety, Volume)
  - Geo-distribution
  - M2M Chatter (status, health, etc.)
- IT meets OT
  - Local Control Loops (deterministic behavior)
  - Cyber Physical Threats/Security
- System-wide View
  - e.g. Smart Traffic Light System
- Cohesive Operations
  - Resource Orchestration & Monitoring
  - Distributed Policy Management
  - Joint/Delegated/Contractual Ownership
- Data Processing & Analytics
  - Balance among Real-time, Semi-real-time and Non-real-time
  - Aggregation and Bandwidth/Compute Cost
- Reliability/Availability
  - Unlike DC, "failure" is a norm
- Complex Greenfield/Brownfield Deployment
  - Longer Life of Critical Infrastructural Systems
  - Huge Deployment/Operational Costs
- Interplay with the Cloud
  - Many Silo'ed "Platforms" (per vendor)
  - Detached Apps (driven from consumer domain)
  - Ecosystem of Tools and Practices

Beyond the above challenges are the issues involved in deploying large-scale public Smart X applications which will have to combine loosely coupled heterogeneous IoT systems and existing technologies (e.g. Clouds, networks, analytics, databases). See http://www.slideshare.net/bobmarcus/iot-use-cases

Some challenging aspects of IoT Applications from Cloud Standards Council's IoT Architecture from the Cloud Standards Customer Council's IoT architecture are listed below. http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf)

- **Scalability**: Scale for IOT system applies in terms of the numbers of sensors and actuators connected to the system, in terms of the networks which connect them together, in terms of the amount of data associated with the system and its speed of movement and also in terms of the amount of processing power required.
- **Big Data**: Many more advanced IoT systems depend on the analysis of vast quantities of data. There is a need, for example, to extract patterns from historical data that can be used to drive decisions about future actions. The extraction of useful information from complex data such as video is another example of analysis requiring large amounts of processing. The ability to mine existing data for new insights and the need to combine different datasets in novel ways are characteristics likely to be part of an IoT system. IoT systems are thus often classic examples of "Big Data" processing.
- **Cloud computing**: IoT systems frequently involve the use of cloud computing platforms. Cloud computing platforms offer the potential to use large amounts of resources, both in terms of the storage of data and also in the ability to bring flexible and scalable processing resources to the analysis of data. IoT systems are likely to require the use of a variety of processing software – and the adaptability of cloud services is likely to be required in order to deal with new requirements, firmware or system updates and offer new capabilities over time.
- **Real time**: IoT systems often function in real time; data flows in continually about events in progress and there can be a need to produce timely responses to that stream of events. This may involve stream processing; acting on the event data as it arrives, comparing it against previous events and also against static data in order to react in the most appropriate way. There is a parallel need to ensure that corrupted data is detected and not used – whether introduced by faulty sensors or malicious action – since the use of corrupted data could cause harm and damage to humans, equipment, and the environment.
- **Highly distributed**: IoT systems can span whole buildings, span whole cities, and even span the globe. Wide distribution can also apply to data – which can be stored at the edge of the network or stored centrally. Distribution can also apply to processing – some processing takes place centrally (in cloud services), but processing can take place at the edge of the network, either in the IoT gateways or even within (more capable types of) sensors and actuators. Today there are officially more mobile devices than people in the world. Mobile devices and networks are one of the best known IoT devices and networks.
- **Heterogeneous systems**: IoT systems are often built using a very heterogeneous set of. This applies to the sensors and actuators, but also applies to the types of networks involved and the variety of processing components. It is common for sensors to be low-power devices, and it is often the case that these devices use specialized local networks to communicate. To enable internet scale access to devices of this kind, an IoT gateway is used.

- **Security and Privacy**: The question of the security and trustworthiness of distributed heterogeneous IoT systems is a hard problem whose solutions must scale and evolve with the systems. Data protection is necessary, including significant privacy concerns regarding data that relate to individuals. Gaining assurance that these systems are safe, secure, resilient and uphold their stakeholders expectations about privacy is especially challenging.
- **Compliance**: Providing confidence about the operation of these IoT systems is necessary both due to the regulations of specific industries, sectors and verticals and also the norms and expectations of the stakeholders of the IoT systems.
- **Integration**: IoT systems do not exist on their own, but need to connect to existing operational technology systems like factory systems, building control systems, and other types of physical management systems as well as existing enterprise systems including enterprise applications and enterprise databases.

The Cloud Context Broker for Smart City from FIWARE.org in Figure 1 from http://www.slideshare.net/fermingalan/introduction-to-fiware-cloud-context-broker captures some of the complexity of CPS systems of systems Architectures.
CKAN = Comprehensive Knowledge Archive Network. See CKAN.org

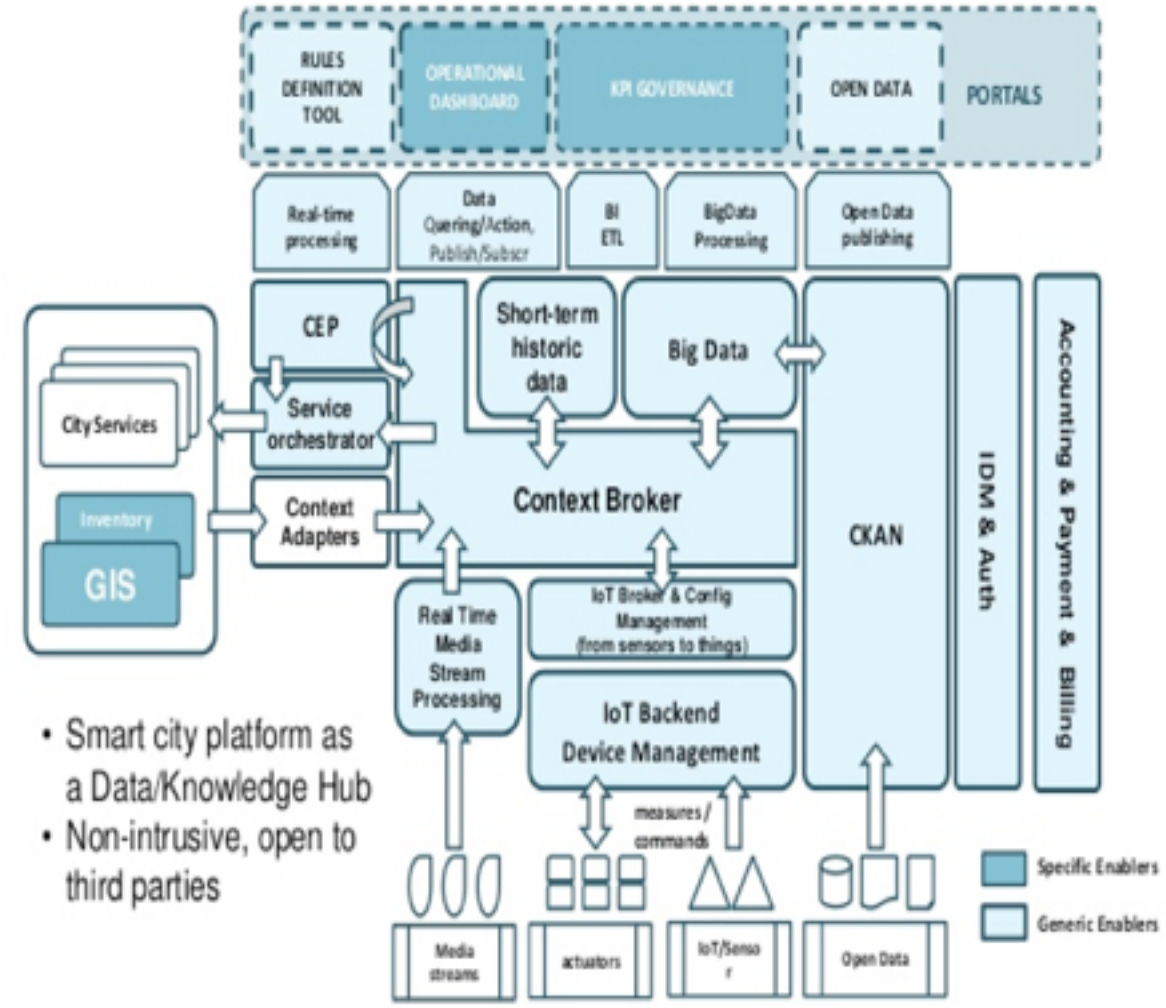


Figure 1. FIWARE.org's Cloud Context Broker for Smart City

a. What are the novel technological challenges presented by IoT relative to existing technological infrastructure and devices, if any? What makes them novel?

Several new challenges exist for large-scale Smart X applications. These include Interfaces between IoT and Cloud, Hierarchical Data Processing, Hierarchical Real-Time Control, Management of IoT Elements (Devices, Power, Time, and Networking), Engineering Large-Scale CPS Systems of Systems, Security, and Privacy.

Challenge 1: Interfaces between IoT and Cloud. See http://www.slideshare.net/bobmarcus/diagrams-io-t-interfaces-to-cloud-big-data and http://www.slideshare.net/bobmarcus/iot-to-cloud-middle-layer.

In large-scale CPS applications, it will often be necessary to have intermediate nodes between devices and Cloud. This layer is sometimes called Fog or Edge Computing as shown in Figure 2 from http://embedded-computing.com/25938-seeing-through-the-fog-computing/ and http://www.slideshare.net/biren_gandhi/get-cloud-resources-to-the-iot-edge-with-fog-computing

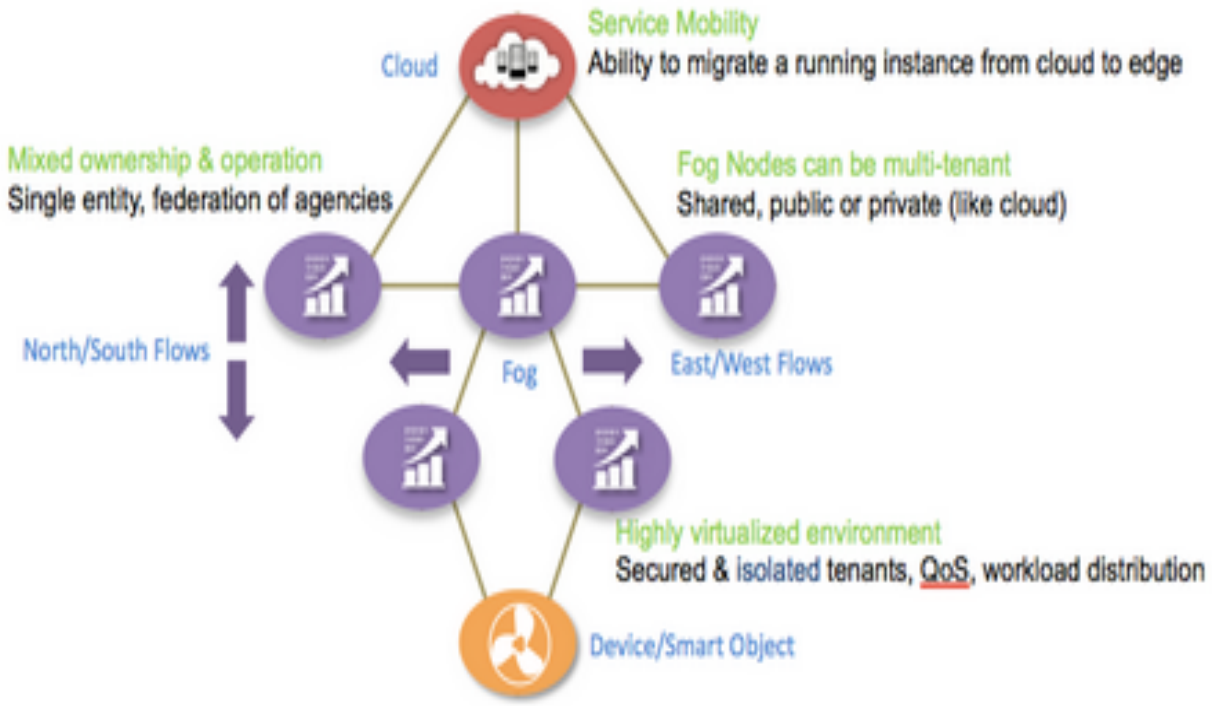


Figure 2. Fog Computing Nodes between Devices and Cloud from Cisco

The University of Florida IoT to Cloud Architecture in Figure 3 from http://www.cise.ufl.edu/~helal/pervasive-fundamentals-cyberphysical.htm shows a multi-layer framework connecting IoT to Cloud processing.

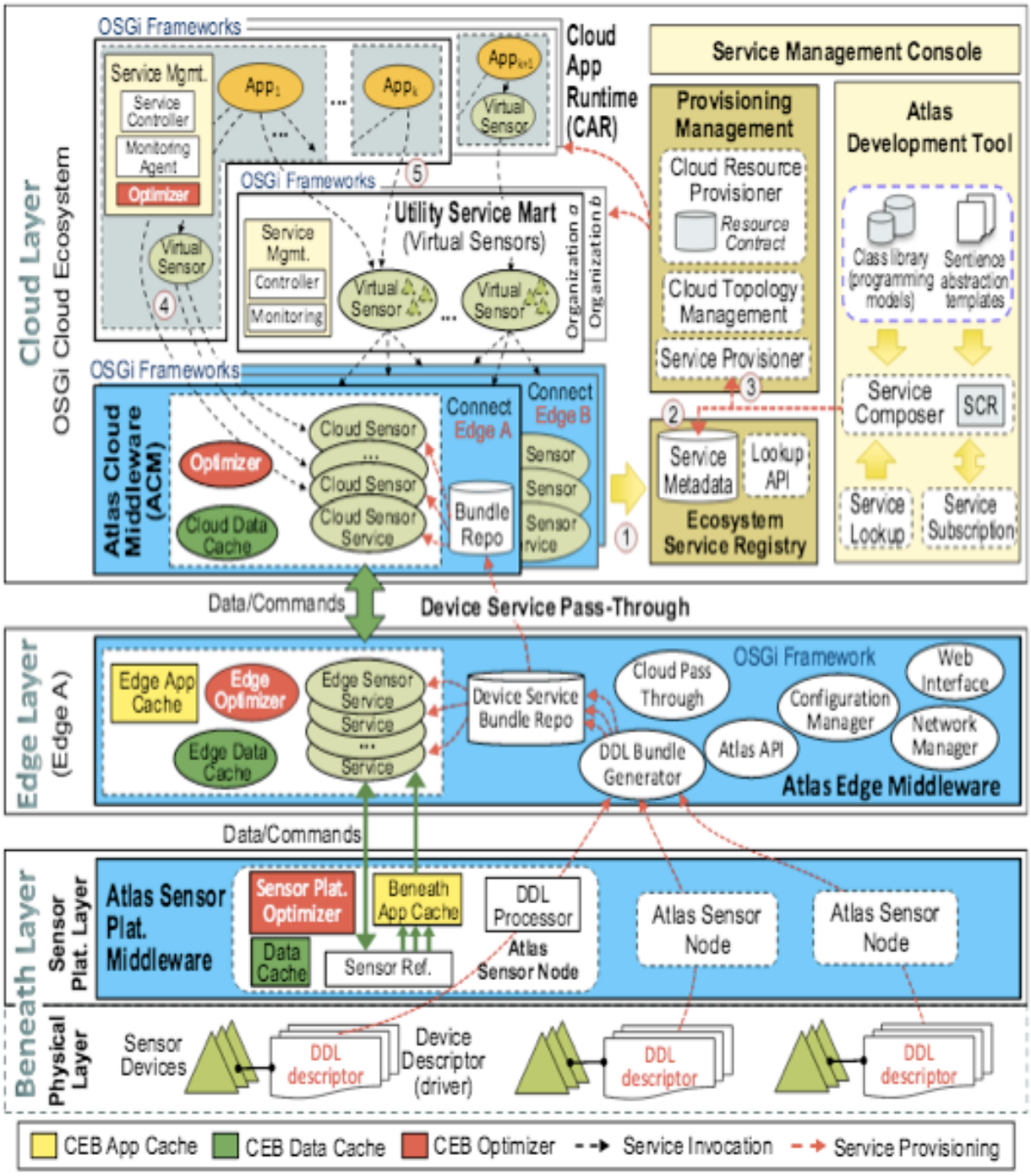


Figure 3. Cloud-Edge-Beneath (CEB) Architecture from the University of Florida

The Edge and and Cloud layers will need many components to deal with IoT as shown iFigure 4 from http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf

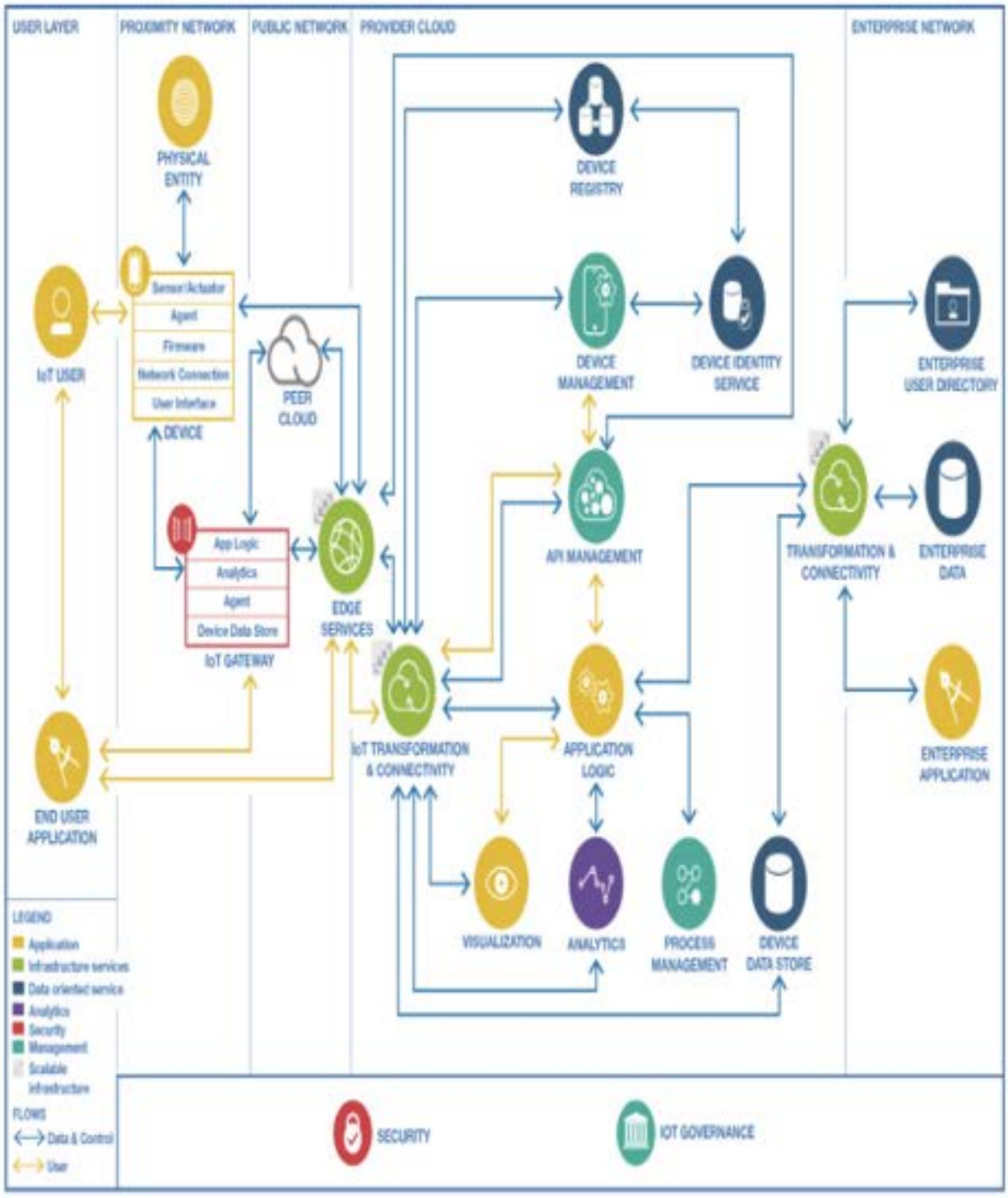


Figure 4. Cloud Standards Council's Architecture for Enterprise IoT

Challenge 2: Hierarchical Data Processing. See www.slideshare.net/bobmarcus/data-processing-in-cyberphysical-systems and http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems .A hierarchical IoT Data Management Framework from the European Research Cluster for the Internet of Things (IERC) at http://tinyurl.com/zs5g8qx is shown in Figure 5.

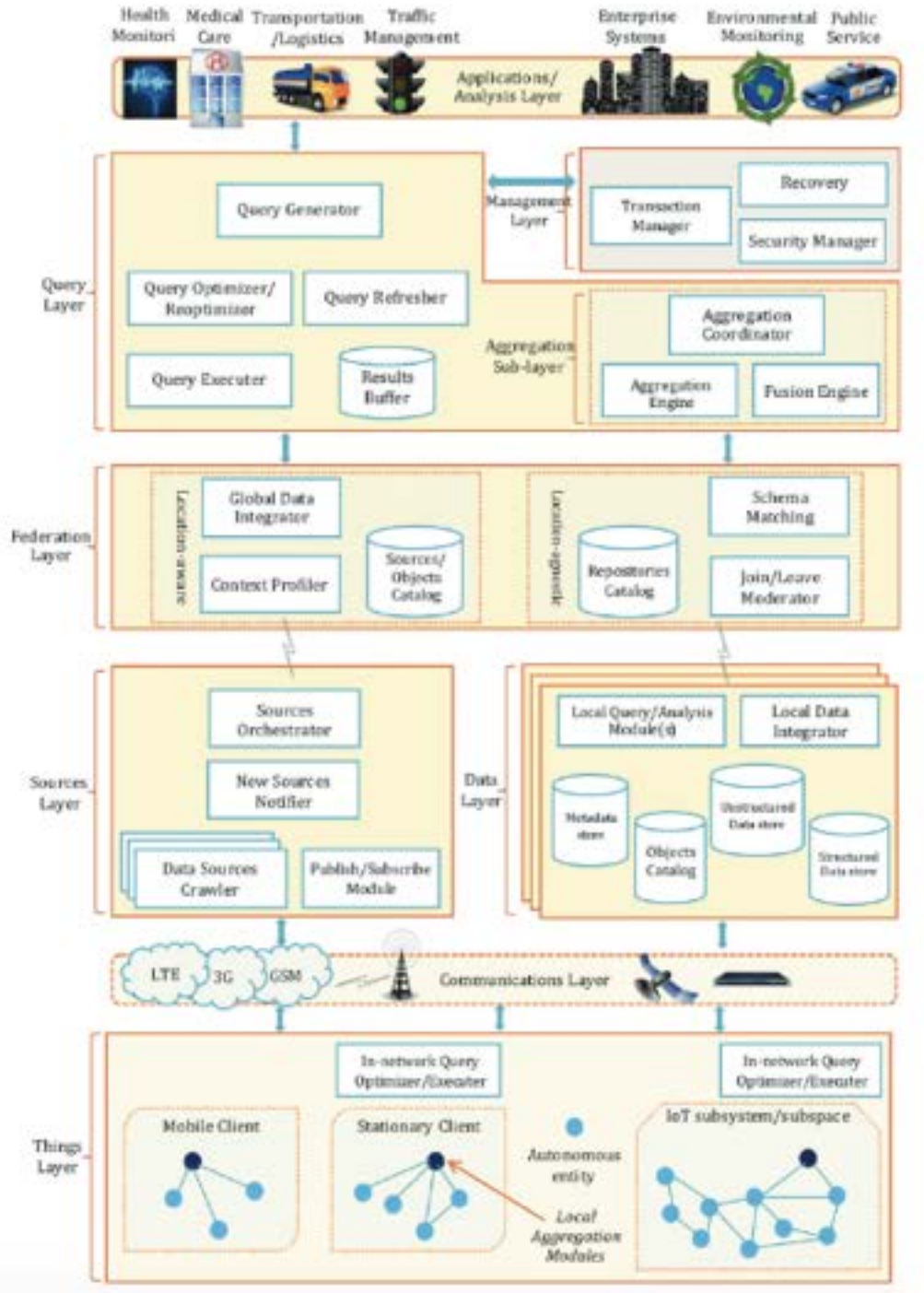


Figure 5. IoT Architecture from the European Research Cluster for IoT (IERC)

A key element in modeling hierarchical multiscale systems of systems is the “Data Hub” pictured in Figure 6 from www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems It is based on the NIST Big Data Reference Architecture at http://bigdatawg.nist.gov/_uploadfiles/M0397_v1_2395481670.pdf

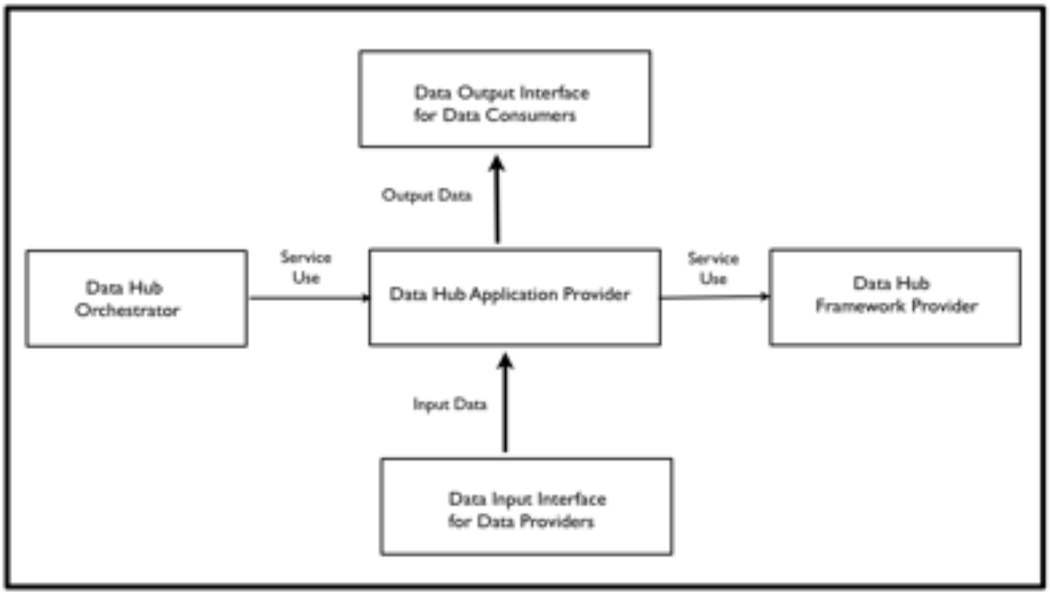


Figure 6. Elements in a Data Hub based on NIST Big Data Reference Architecture

In Smart X applications, Data Hubs at multiple levels are loosely coupled as shown in Figure 7 from www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems

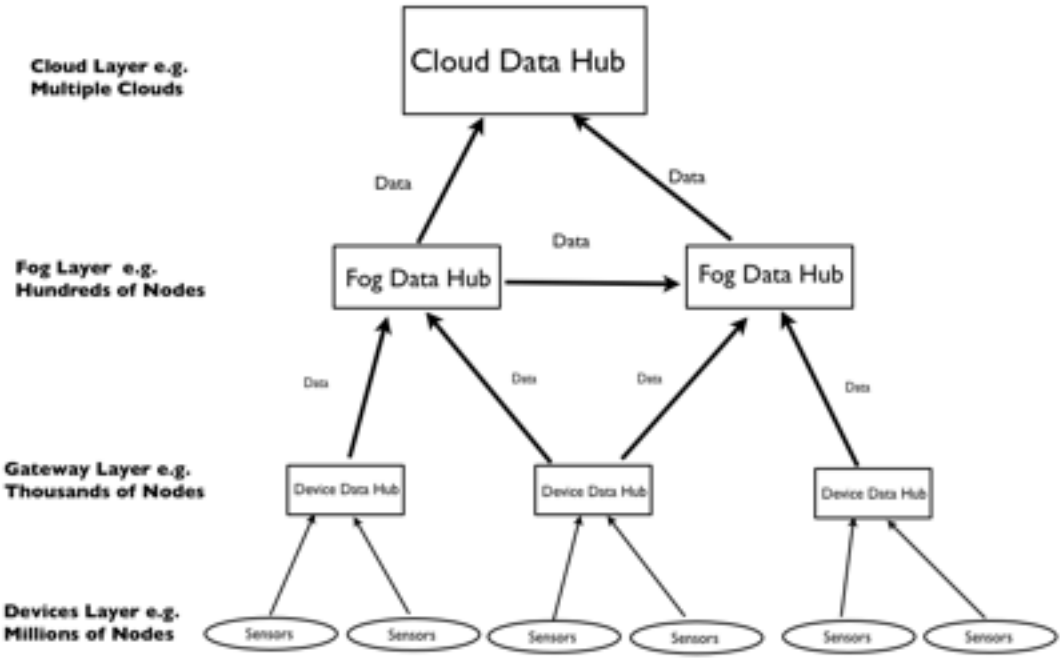


Figure 7. Connected Data Hubs in a Hierarchical Multiscale CPS Architecture

The network requirements for connecting devices, Fog, and Clouds is shown in Figure 8 from Datafloq at https://datafloq.com/read/fog-computing-vital-successful-internet-of-things/1166

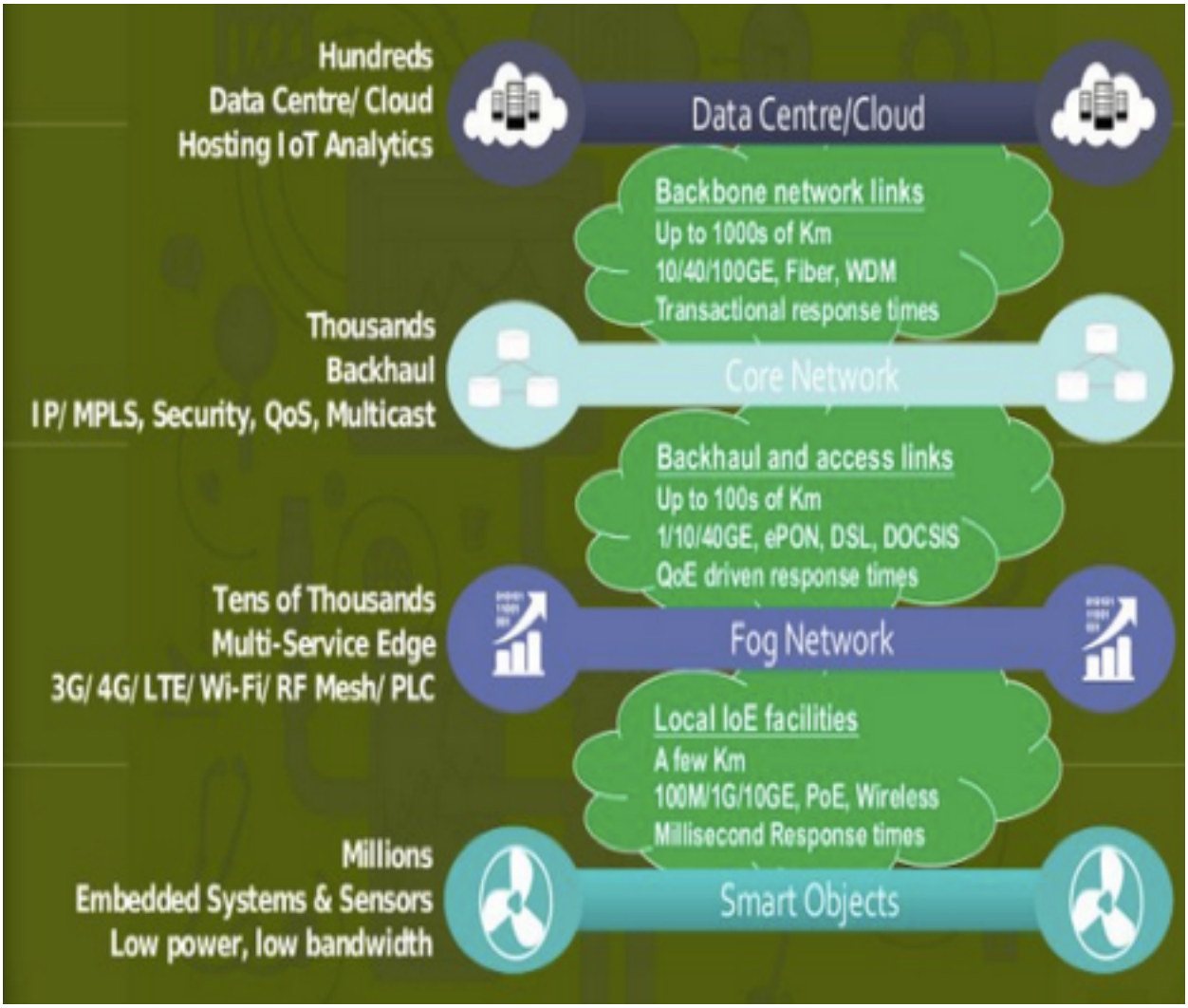


Figure 8. Network Requirements for Connecting Devices, Fog, and Cloud

Challenge 3: Hierarchical Real-Time Control. See http://www.slideshare.net/bobmarcus/control-in-cyberphysical-systems and http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems

Some early work on Hierarchical Control was done by James Albus of NIST. Figure 9 from https://en.wikipedia.org/wiki/Hierarchical_control_system shows his model of a node in a Hierarchical Real-Time Control System.

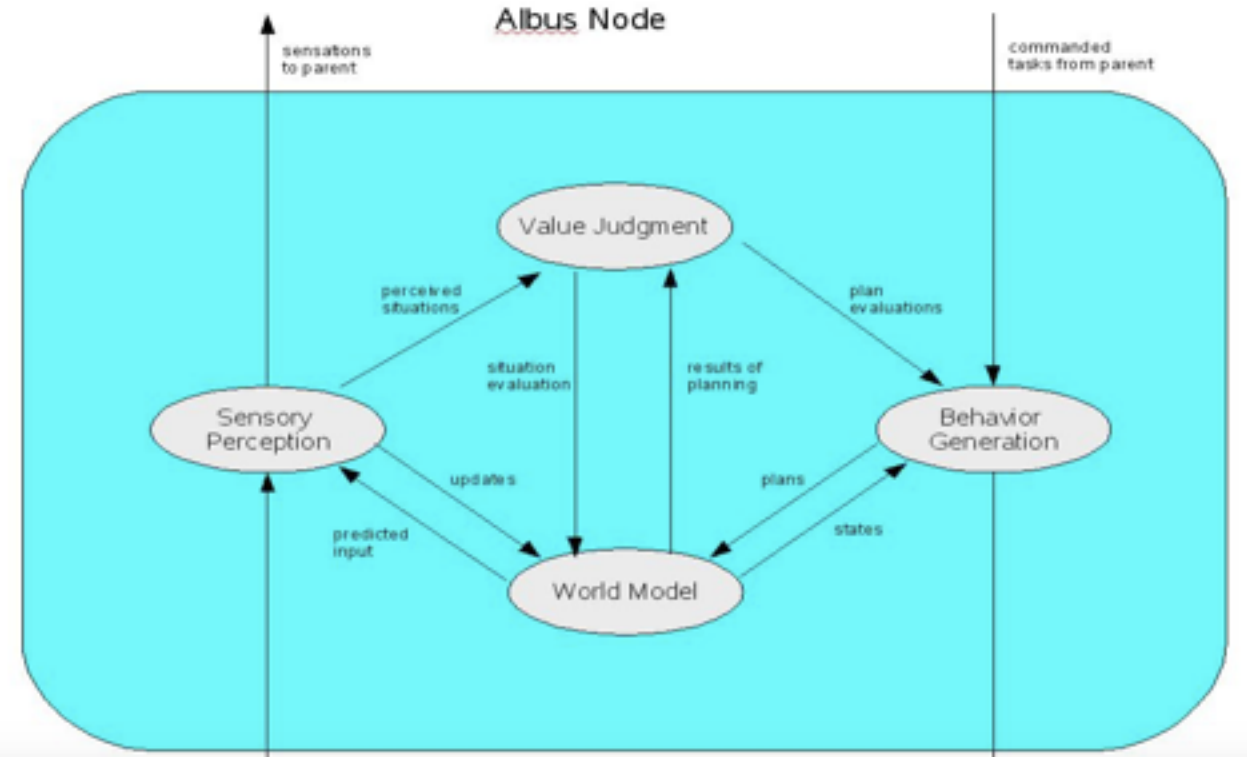


Figure 9, Node in a Hierarchical Real-Time Control System from James Albus

The “CPS Hub” in Figure 10 from http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems is an extension of the Data Hub that provides similar capabilities to the Albus Node.

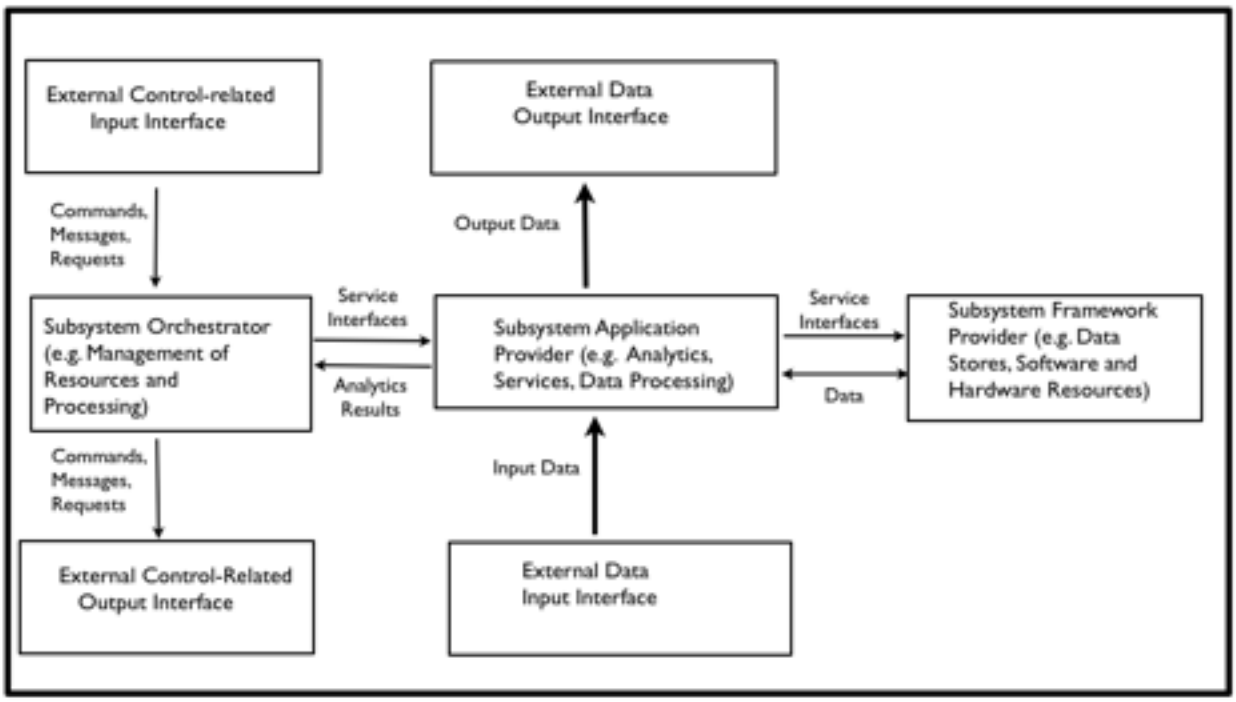


Figure 10. CPS Hub extension to Data Hub

Albus interfaces nodes to form a Hierarchical Real-Time Control System as shown in Figure 11 from https://en.wikipedia.org/wiki/Hierarchical_control_system

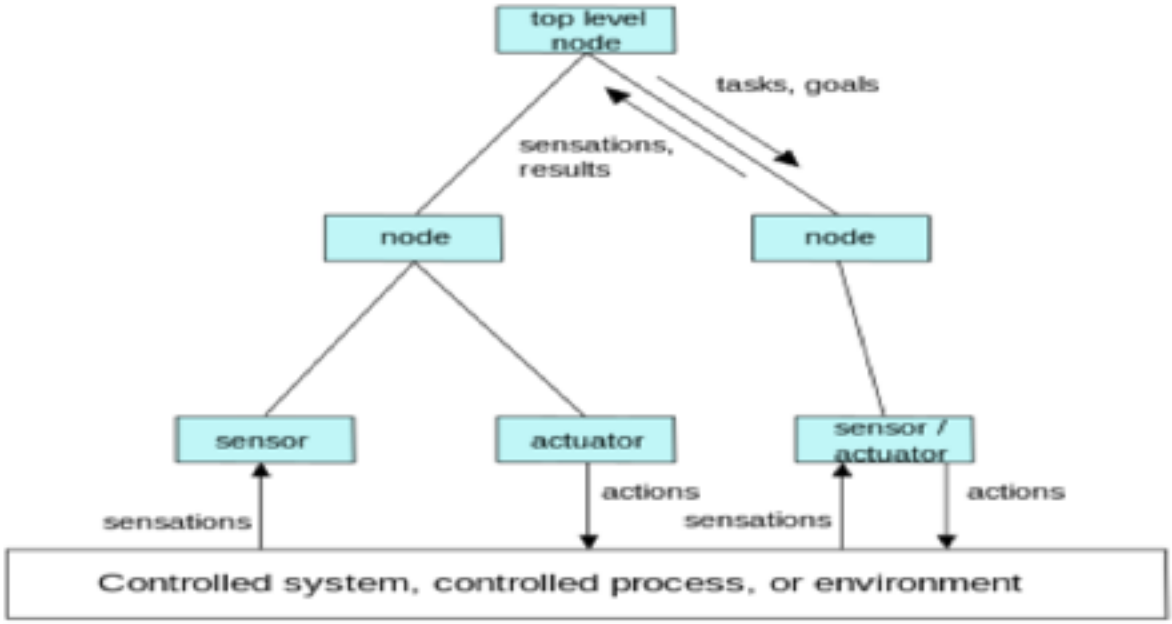


Figure 11. Hierarchical Real-Time Control System from James Albus

Similar connections among CPS Hubs are in Figure 12 from http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems

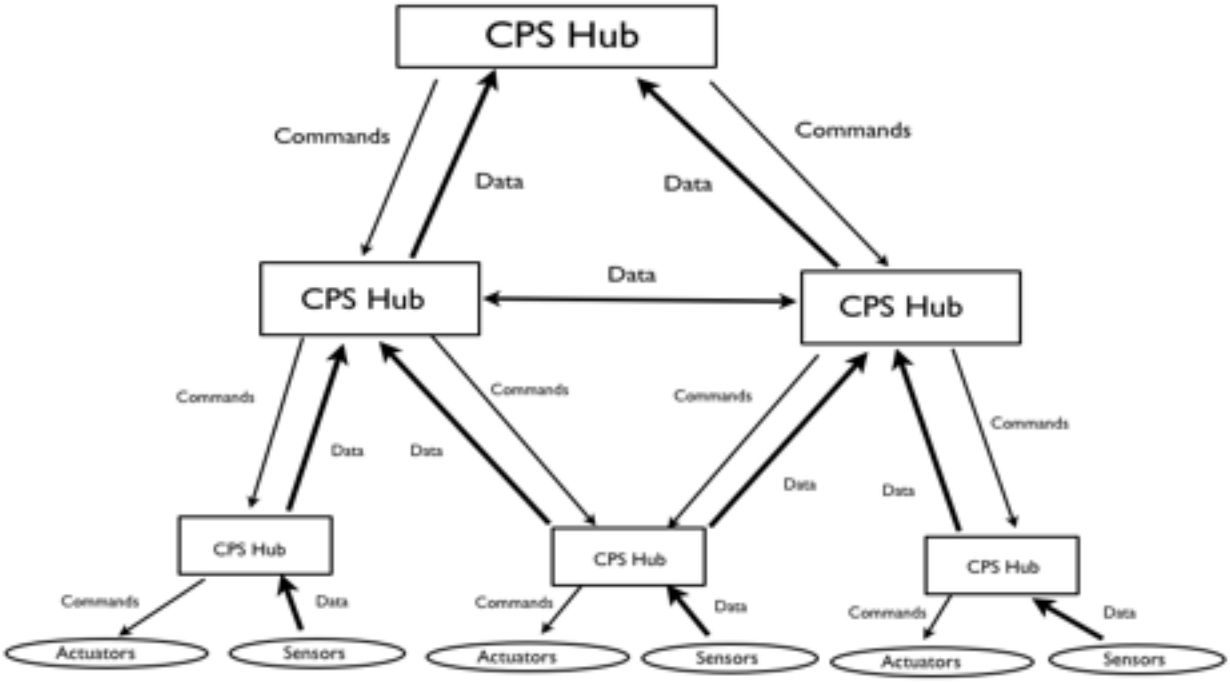


Figure 12. Hierarchical Real-Time Control System using CPS Hubs

A Control Architecture for IoT by City University New York (CUNY) is shown in Figure 13 from http://cps-vo.org/file/22521/download/66384

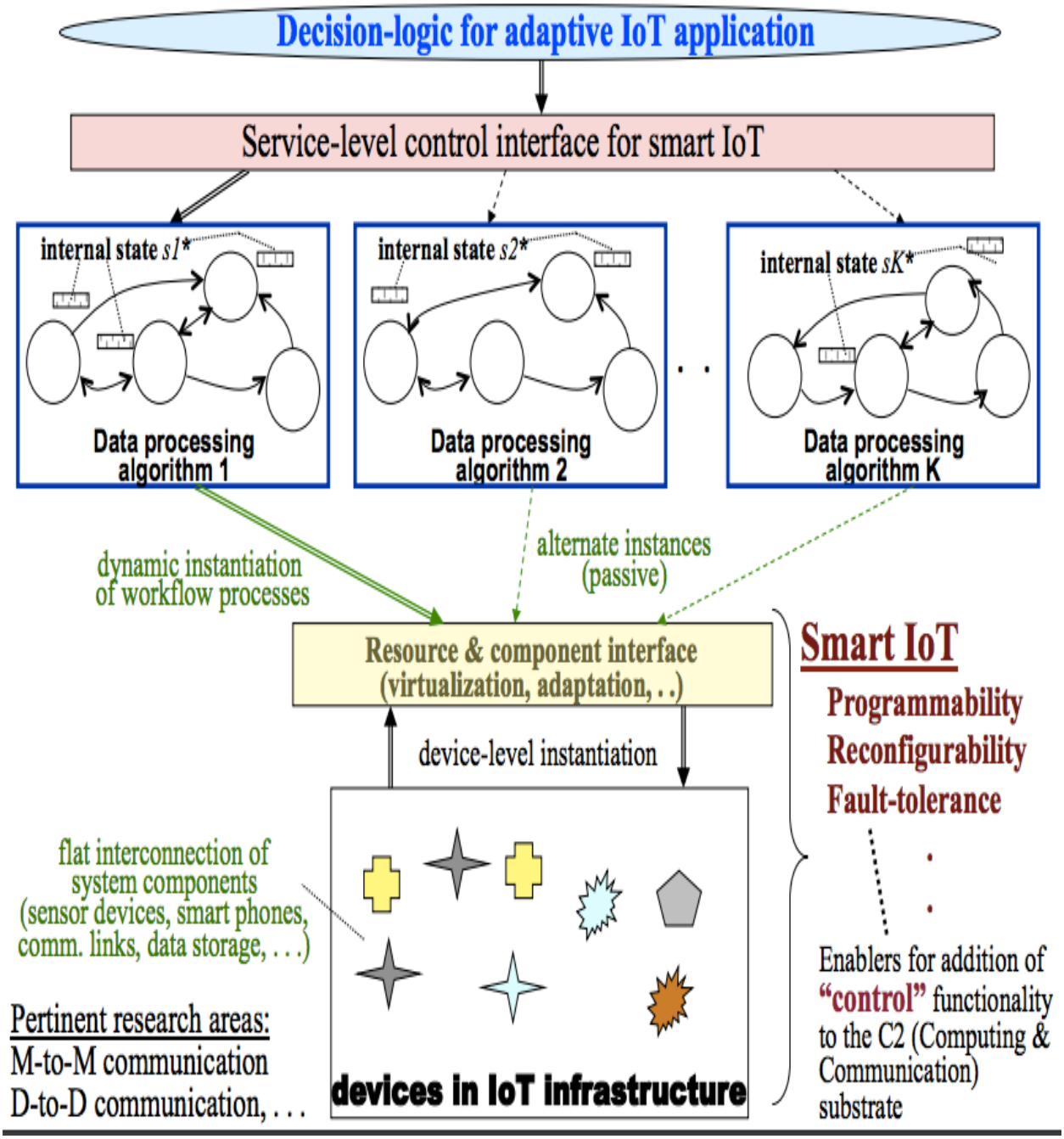


Figure 13. A Control Architecture for IoT from CUNY

Challenge 4: Management of IoT Elements (Devices, Power, Time, and Networking). See http://www.slideshare.net/bobmarcus/management-for-cps Some of the management issues for IoT from http://cnds.eecs.jacobs-university.de/slides/2013-im-iot-management.pdf are listed below

Management System/Architecture

- Support multiple device classes.
- Minimise state maintained on constrained devices.
- Support for lossy and unreliable links.

Management Protocols

- Modular implementations with a basic set of protocol primitives.
- Compact encoding of management data.
- Protocol extensibility.

Configuration Management

- Self-configuration capability.
- Asynchronous Transaction Support.
- Network reconfiguration.

Implementation Requirements

- Avoid requiring large application layer messages.
- Avoid reassembly of messages at multiple layers.

Monitoring

- Device status monitoring.
- Current and estimated device availability.
- Network status monitoring
- Network topology discovery.
- Notification.
- Logging.

Security

- Authentication of management systems and managed devices.
- Access control.
- Security bootstrapping mechanisms.
- Efficient cryptographic algorithms.

Energy Management

- Management of energy resources.
- Dying gasp.

Many of the issues in Time Management can be found at NIST's Time-Aware Applications, Computers, and Communication Systems (TAACCS) document at http://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.1867.pdf

Challenge 5: Engineering Large-Scale CPS Systems of Systems. See http://www.slideshare.net/bobmarcus/engineering-large-scale-cyberphysical-systems

The features of CPS SoS is shown in Figure 14 from the EU CPSoS.org at www.cpsos.eu/wp-content/uploads/2015/12/Roadmap-ICT-Info-Day-Brussels-Dec.-1-2015.pdf

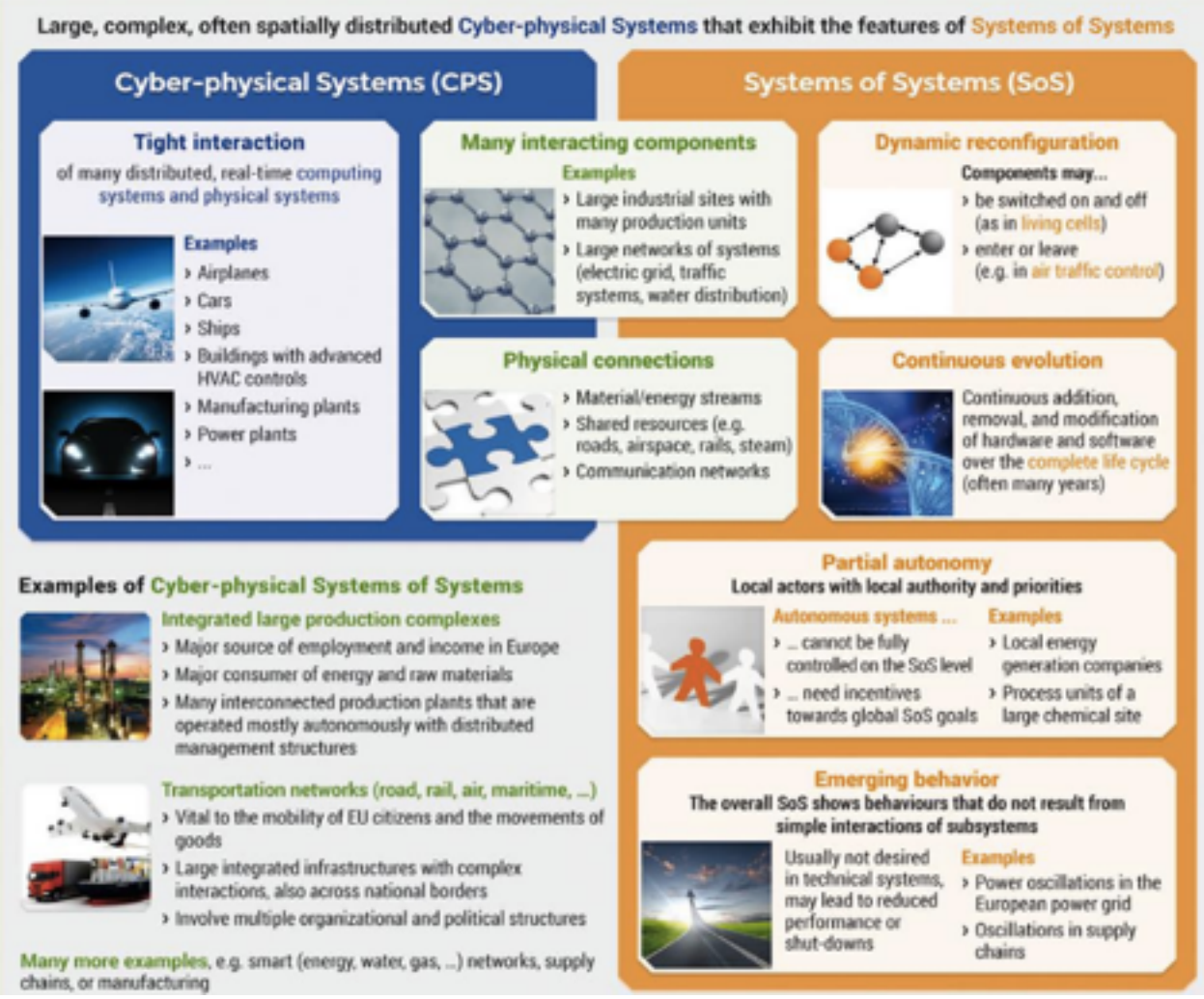
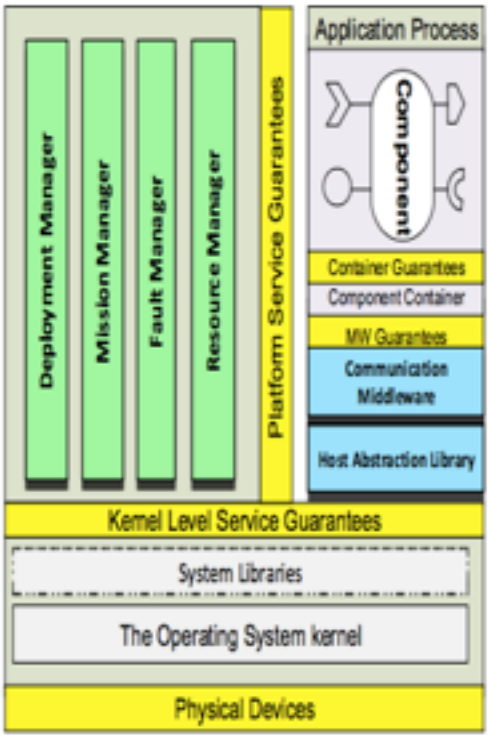


Figure 14. Features of CPS SoS from the European CPSoS.org

Managing Scale and Heterogeneity in CPS SoS is shown in Figure 15 from Vanderbilt University at http://cps-vo.org/file/20908/download/60342f

- *Interactions across engineering domains which require interoperation across multiple system dynamics, constraints and interactions:*
  - Well-defined interaction semantics and support of cross platform robust middleware
  - Support for well-defined data model.
- *Tradeoffs between Privacy, Security and Safety from both theoretical and operational perspectives:*
  - Good analytical tools
  - Built-in support across the layers for privacy and security
- *Distribution of Adaptive and Autonomous Platform Management:*
  - Support for adaptive deployment, configuration and application management architecture
- *Timely Dissemination of Massive Amounts of Information Reliably, Securely and Scalably:*
  - Support for enforcing quality of service and strong implementation of time synchronization protocol such as IEEE Precision Time Protocol.



More information is available on Drems.isis.vanderbilt.edu

Figure 15. CPSoS Engineering Requirements from Vanderbilt University

Challenge 6. Security and Privacy. See http://www.slideshare.net/bobmarcus/security-in-cyberphysical-systems . The areas of security, privacy, and trust have been addressed by defense-related projects but are emerging technologies in many of the Smart X domains.

The Clouds Standards Council Architecture for IoT at http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf includes many security and privacy requirements.

Security - Security in IoT deployments must address both information technology (IT) security as well as operations technology (OT) security elements. Furthermore, the level of attention to security, and in which topic areas will vary depending upon the application environment, business pattern, and risk assessment. A risk assessment will take into account multiple threats and attacks along with an estimate of the potential costs associated with such attacks.

There are several areas of security to consider:

- Identity and Access Management
- Data Protection
- Security Monitoring, Analysis, and Response
- System, Application, and Solution Lifecycle Management

Each of these areas is briefly discussed below.

Security Monitoring, Analysis, and Response - Every system must have monitoring of the environment built in so that active attacks as well as anomalous behavior will be detected and acted upon. Because of the scale of IoT systems, both in the number of devices as well as the amount of information being processed, there is a large requirement for automated response to known attacks as well as automatic detection of suspicious behavior. Response to attacks and suspicious behavior may include temporary isolation, quarantine, or removal of parts of the IoT system as well as having formal incident response processes for addressing vulnerabilities which are discovered long after the systems have been put into service. Like IT security, there is a need for disclosure of vulnerabilities such that appropriate mitigations, changes, and updates can be implemented in a timely manner by all affected parties.

System, Application, and Solution Lifecycle Management - Lifecycle management of the IoT system is complex, multi-faceted, and has relationships with identity management, device management, as well as involving the supply chain, application and software development, through to system operations and change management of deployed and in-service systems. Attention to security in all of these areas is required in order to prevent a variety of attacks ranging from malicious code insertion to inappropriate firmware/software deployment, to effective cryptographic key management. Code, key material, and even physical components must be verified as they flow from procurement and creation through to their installation into the devices, gateways, and systems which provide the IoT solution. The IoT system should also provide the capability to update individual components in a secure way, both to address vulnerabilities and also to address functional enhancements over the lifetime of the system.

Identity and Access Management - As with any computing system, there must be strong identification of all participating entities – users, systems, applications, and, in the case of IoT, devices and the gateways through which those devices communicate with the rest of the system. Device identity and management necessarily involves multiple entities, starting with chip and device manufacturers, including IoT platform providers, and also including enterprise users and operators of the devices. In IoT solutions it is often the case that multiple of these entities will continue to communicate and address the IoT devices throughout their operational lifetime.

Data Protection - Data in the device, in flight throughout the public network, provider cloud, and enterprise network, as well as at rest in a variety of locations and formats must be protected from inappropriate access and use. Multiple methods can be utilized, and indeed, in many cases, multiple methods will be applied simultaneously to provide different levels of protection of data against different types of threats or isolation from different entities supporting the system. Communications link protection may be used in addition to individual data field level encryption and/or signing done at/in the device in order to provide both end-to-end and point-to-point communications protection. Data at rest in different formats may be encrypted at the field, database, and even whole disk/media level to protect against leakage and improper usage. Increased data collection also results in a need to consider potential privacy implications, requiring additional attention to data segregation, redaction, and special handling requirements.

It is important to consider whether the data involved in an IoT system is personally identifiable information (PII) – in many cases, devices may be directly associated with individuals, or individuals may be the physical objects that are the target of sensors. Such PII is usually the subject of laws and regulations with the result that the IoT system must be designed to give appropriate protection to this data.

c. What are the most significant new opportunities and/or benefits created by IoT, be they technological, policy, or economic?

A Table showing the Impact of Cyber Physical Systems from NIST Study at http://tinyurl.com/javobbr is shown in Table 2.

Innovative Products or Applications	Cyber-Physical Systems	Impacts
Smart Manufacturing and Production		
• Agile manufacturing • Supply chain connectivity	• Intelligent controls • Process and assembly automation • Robotics working safely with humans	• Enhanced global competitiveness • U.S.-based high tech manufacturing • Greater efficiency, agility, and reliability
Transportation and Mobility		
• Autonomous or smart vehicles (surface, air, water, and space) • Vehicle-to-vehicle and vehicle-to-infrastructure communication	• Drive by wire vehicle systems • Plug ins and smart cars • Interactive traffic control systems • Next-generation air transport control	• Accident prevention and congestion reduction (zero-fatality highways) • Greater safety and convenience of travel
Energy		
• Electricity systems • Renewable energy supply • Oil and gas production	• Smart electric power grid • Plug-in vehicle charging systems • Smart oil and gas distribution grid	• Greater reliability, security, and diversity of energy supply • Increased energy efficiency
Civil Infrastructure		
• Bridges and dams • Municipal water and wastewater treatment	• Active monitoring and control system • Smart grids for water and wastewater • Early warning systems	• More safe, secure, and reliable infrastructure • Assurance of water quality and supply • Accident warning and prevention
Healthcare		
• Medical devices • Personal care equipment • Disease diagnosis and prevention	• Wireless body area networks • Assistive healthcare systems • Wearable sensors and implantable devices	• Improved outcomes and quality of life • Cost-effective healthcare • Timely disease diagnosis and prevention
Buildings and Structures		
• High performance residential and commercial buildings • Net-zero energy buildings • Appliances	• Whole building controls • Smart HVAC equipment • Building automation systems • Networked appliance systems	• Increased building efficiency, comfort and convenience • Improved occupant health and safety • Control of indoor air quality
Defense		
• Soldier equipment • Weapons and weapons platforms • Supply equipment • Autonomous and smart underwater sensors	• Smart (precision-guided) weapons • Wearable computing/sensing uniforms • Intelligent, unmanned vehicles • Supply chain and logistics systems	• Increased warfighter effectiveness, security, and agility • Decreased exposure for human warfighters and greater capability for remote warfare
Emergency Response		
• First responder equipment • Communications equipment • Fire-fighting equipment	• Detection and surveillance systems • Resilient communications networks • Integrated emergency response systems	• Increased emergency responder effectiveness, safety, efficiency, and agility • Rapid ability to respond to natural and other disasters

Table 2. Impacts of CPS Systems

2. The term “Internet of Things” and related concepts have been defined by multiple organizations, including parts of the U.S. Government such as NIST and the FTC, through policy briefs and reference architectures. What definition(s) should we use in examining the IoT landscape and why? What is at stake in the differences between definitions of IoT? What are the strengths and limitations, if any, associated with these definitions?

Some definitions of IoT from major sources are below. See the IEEE paper (86 pages) entitled “Towards a Definition of the Internet of Things (IoT) at http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf for a more complete discussion.

http://www.internet-of-things-research.eu/about_iot.htm
IoT is "A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.".

https://en.wikipedia.org/wiki/Internet_of_Things
The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items—embedded with electronics, software, sensors, and network connectivity that enables these objects to collect and exchange data. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities.

http://www.gartner.com/it-glossary/internet-of-things/
The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.

4. **Are there ways to divide or classify the IoT landscape to improve the precision with which public policy issues are discussed? If so, what are they, and what are the benefits or limitations of using such classifications? Examples of possible classifications of IoT could include: Consumer vs. industrial; public vs. private; device-to-device vs. human interfacing.**

Classifications Categories for IoT include:

Category 1. Research and Testbeds: (Recommendation - Government Funding Support) CPS research and testbeds should be supported by government grants. These grants should be focused on key areas of CPS technology. Some examples include systems of systems implementations, advanced CPS analytics, and interoperability across diverse devices.

Category 2. Private industrial: (Recommendation - Government Standardization Support) . CPS industrial applications (e.g. Smart Manufacturing)will usually be privately deployed and managed. However these initiatives will strengthen US economic competitiveness. Government should support standardizations in this area

Category 3. Public Consumer: (Recommendation - Government Regulate) CPS consumer applications (e.g. Smart Home) will usually be privately developed. Government should supply regulations guaranteeing factual marketing, privacy and security for consumers. Governments could mandate specific capabilities and standardizations if necessary.

Category 4. Public Governmental (Recommendation - Government Managed) CPS governmental applications (e.g. Smart City) should be managed by Government executive leadership. Some technology development and system integration can be performed by commercial vendors using Government specifications.

Category 5. Defense and Intelligence (Recommendation - Government Owned) CPS defense and intelligence applications should be owned by the Government and developed under the appropriate security regulations and Government standards . Contractors should be required to meet these regulations and standards and be carefully supervised.

Example of Category 1 (Research and Testbeds): An IoT Cloud research testbed is shown in Figure 16 from the University of Indiana at grids.ucs.indiana.edu/ptliupages/publications/intelligent_iot_cloud_controller.pdf
(ROS = Robot Operating System at ros.org)

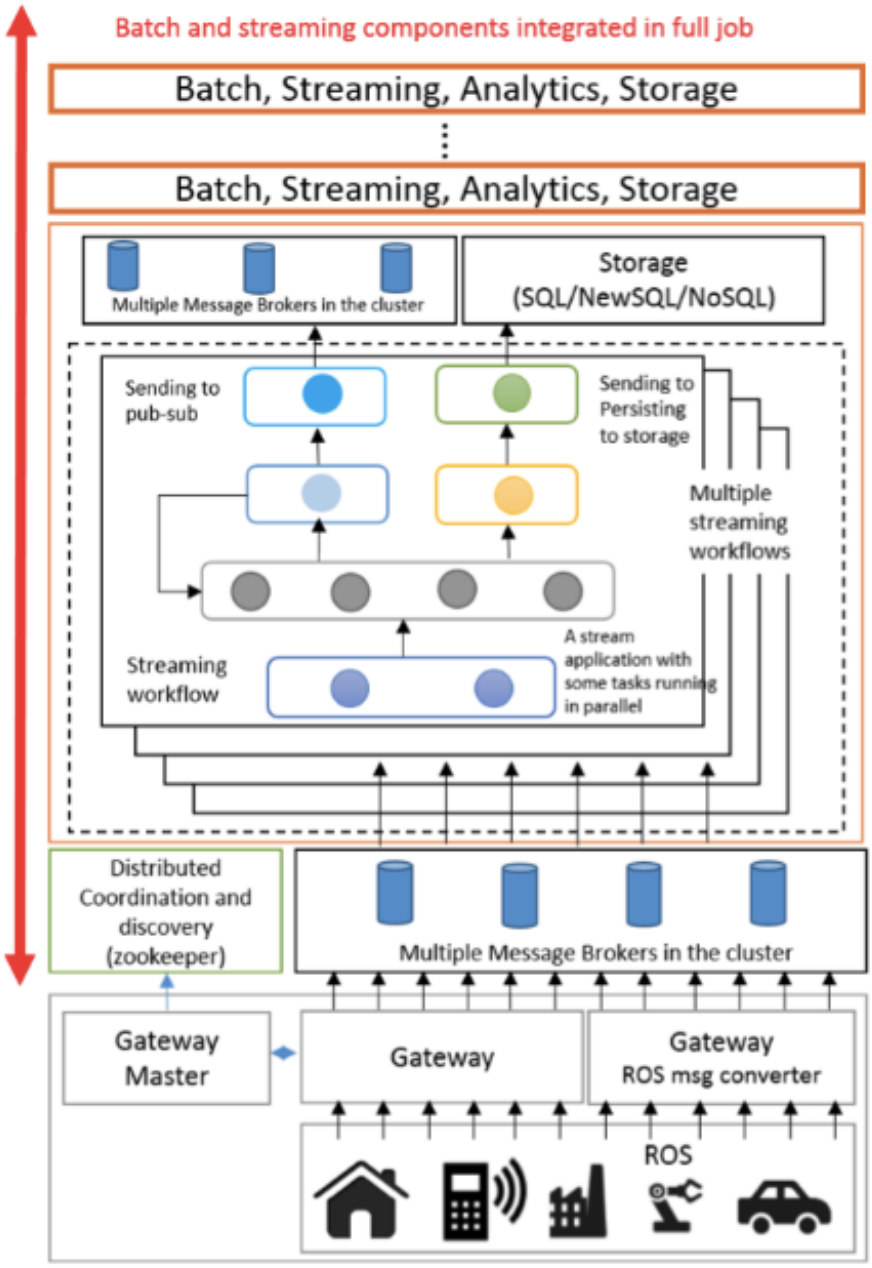


Figure 16. IoT Research Testbed from the University of Indiana

Example of Category 2 (Private Industrial): The Functional Domain Architecture from the Industrial Internet Consortium is shown in Figure 17 at http://www.iiconsortium.org/IIRA-1-7-ajs.pdf

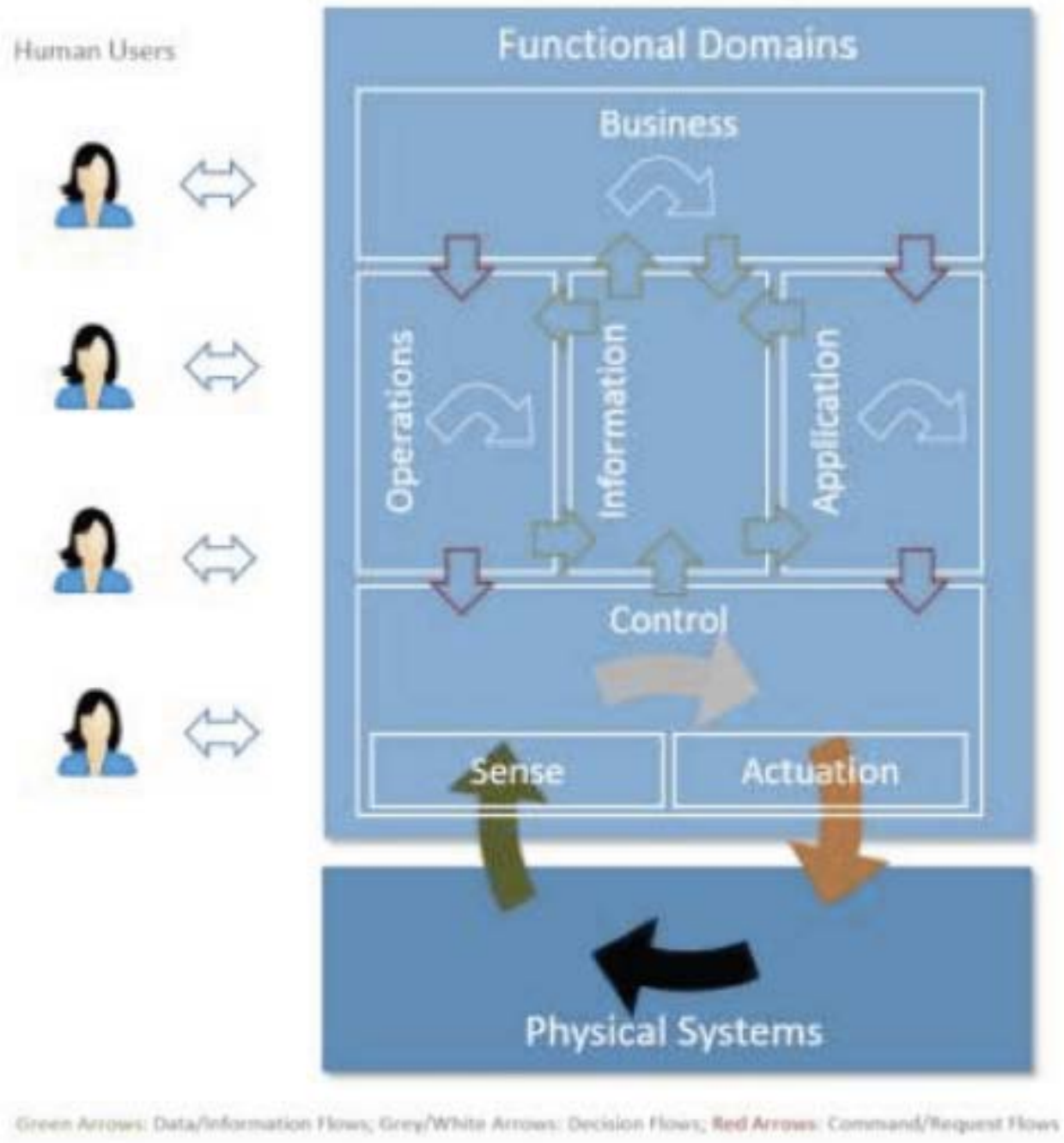


Figure 17. Industrial Internet Consortium's Functional Domain Architecture

Example of Category 3 (Public Commercial). A Cloud-supported Smart Home Architecture is shown in Figure 18 at https://www.marsdd.com/wp-content/uploads/2014/10/Oct28-MaRS-ConnectedWorld-ConnectedHome.pdf

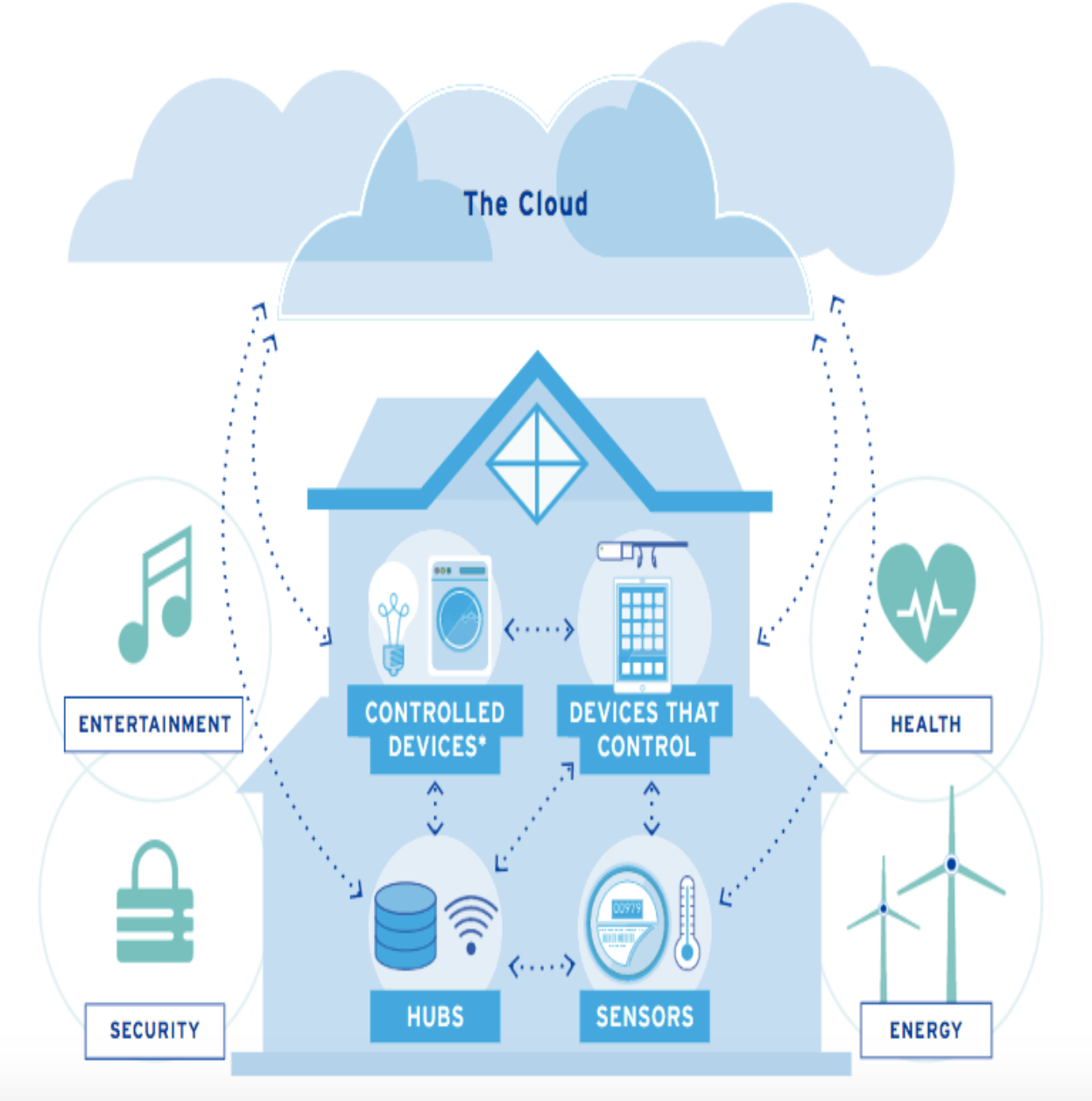


Figure 18. Cloud-supported Smart Home Architecture

Example of Category 4 (Public Governmental). The Hierarchical Smart City Architecture from the University of Rhode Island in Figure 19 is from http://dl.acm.org/citation.cfm?id=28188982

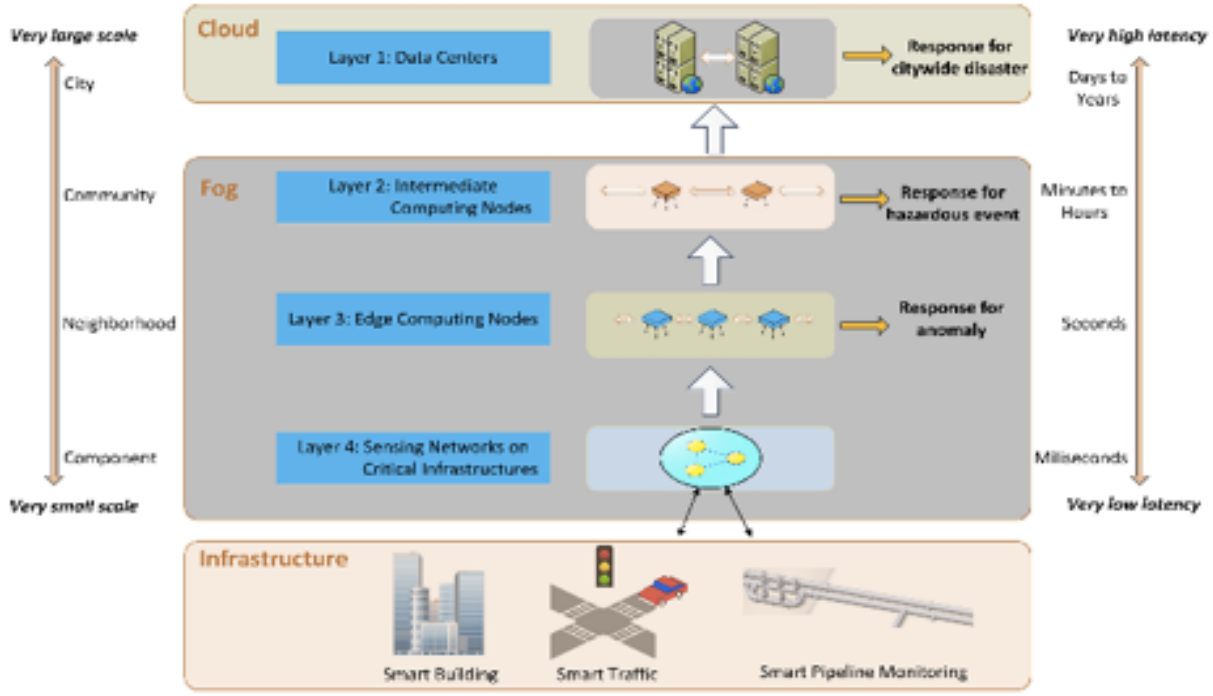


Figure 19. Smart City Architecture from the University of Rhode Isalnd

Another Example of Category 4: Three different types of IoT applications with a high level federation are shown in Figure 20 at http://dw.connect.sys-con.com/session/2999/Dennis_Ward.pdf

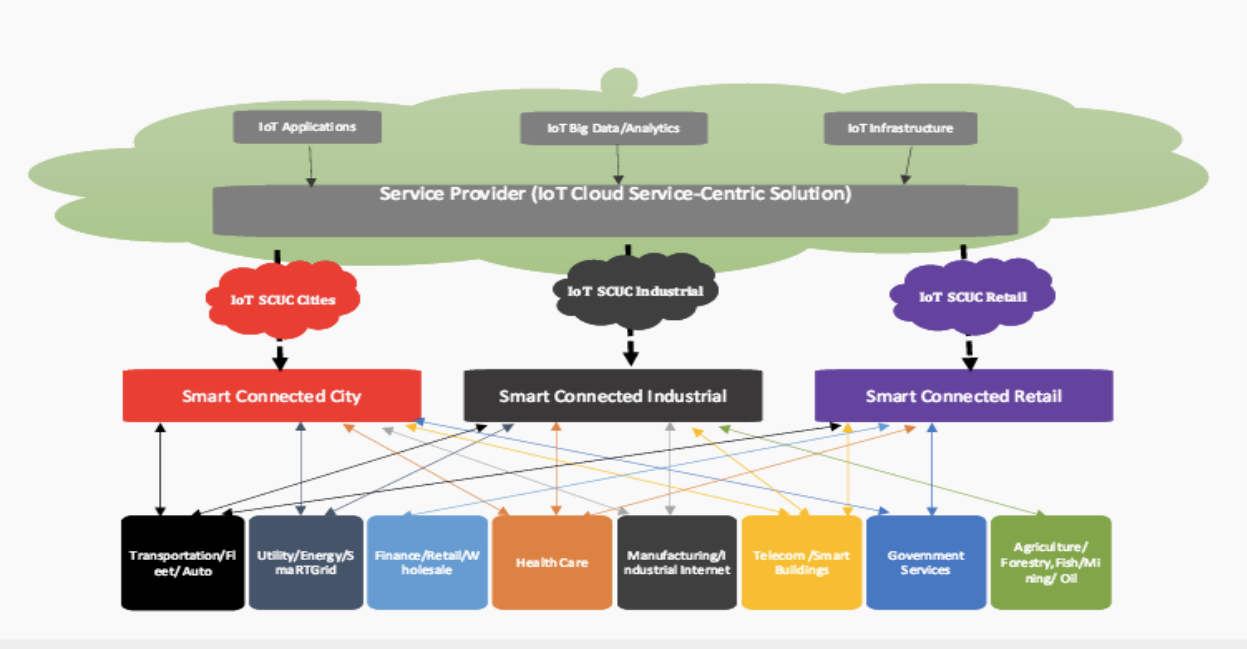


Figure 20. Federated Smart X Applications

Example of Category 5 (Defense and Intelligence). The Global Information Grid is shown in Figure 21 from https://publicintelligence.net/ufouo-dod-global-information-grid-2-0-concept-of-operations/

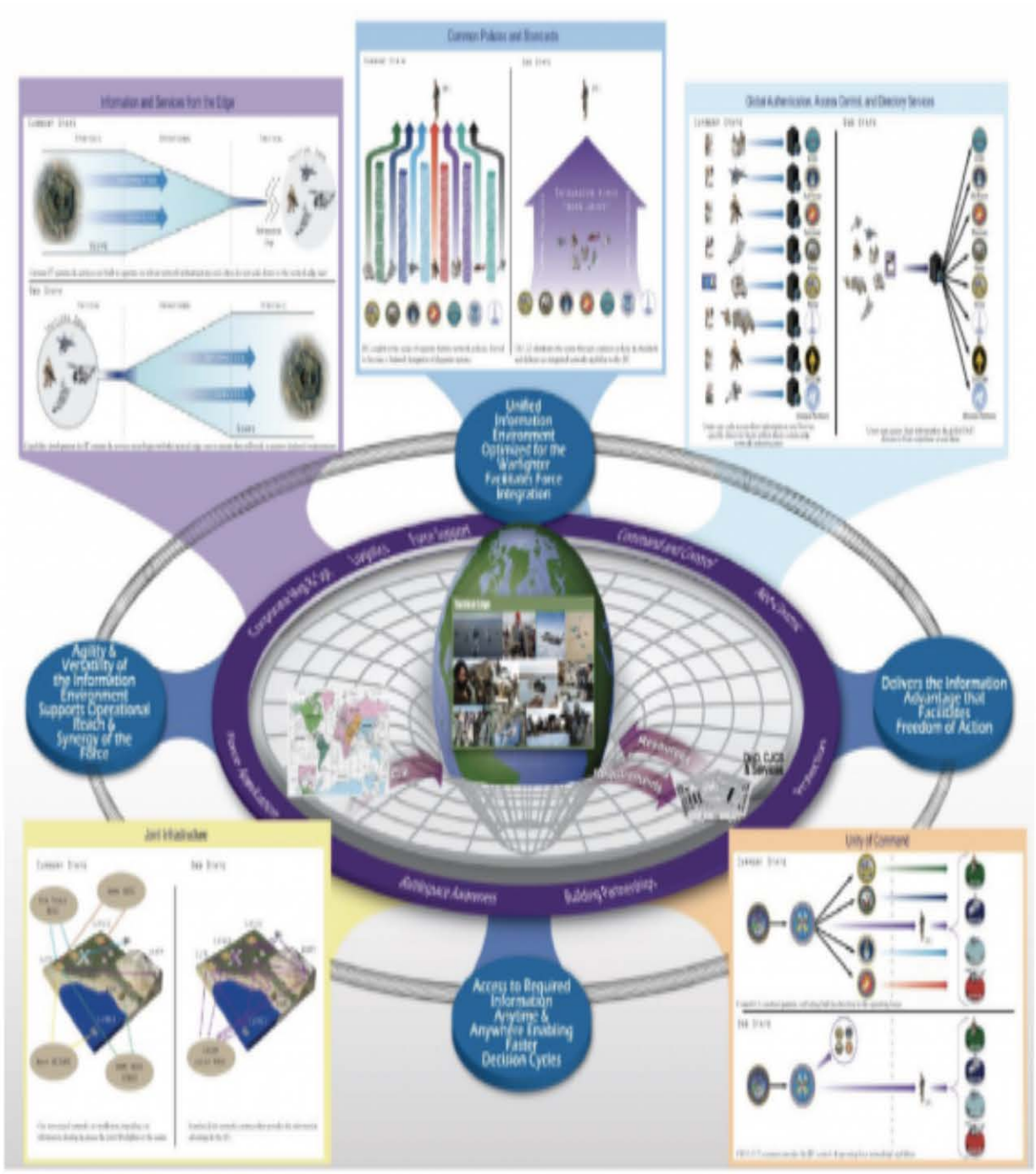


Figure 21. Concept of Operations for Global Information Grid 2.0

5. Please provide information on any current (or concluded) initiatives or research of significance that have examined or made important strides in understanding the IoT policy landscape. Why do you find this work to be significant? Technology: Technology is at the heart of IoT and its applications. IoT development is being driven by a very diverse set of stakeholders whose expertise in science, research, development, deployment, measurements and standards are enabling rapid advances in technologies for IoT. It is important to understand what technological hurdles still exist, or may arise, in the development and deployment of IoT, and if the government can play a role in mitigating these hurdles.

Research and Testbeds. See http://www.slideshare.net/bobmarcus/research-and-testbeds-in-cyberphysical-systems

The NIST CPS and Smart Grid Testbed in Figure 22 from http://www.nist.gov/smartgrid/upload/Smart-Grid-Testbed-Update.pdf is a valuable contribution

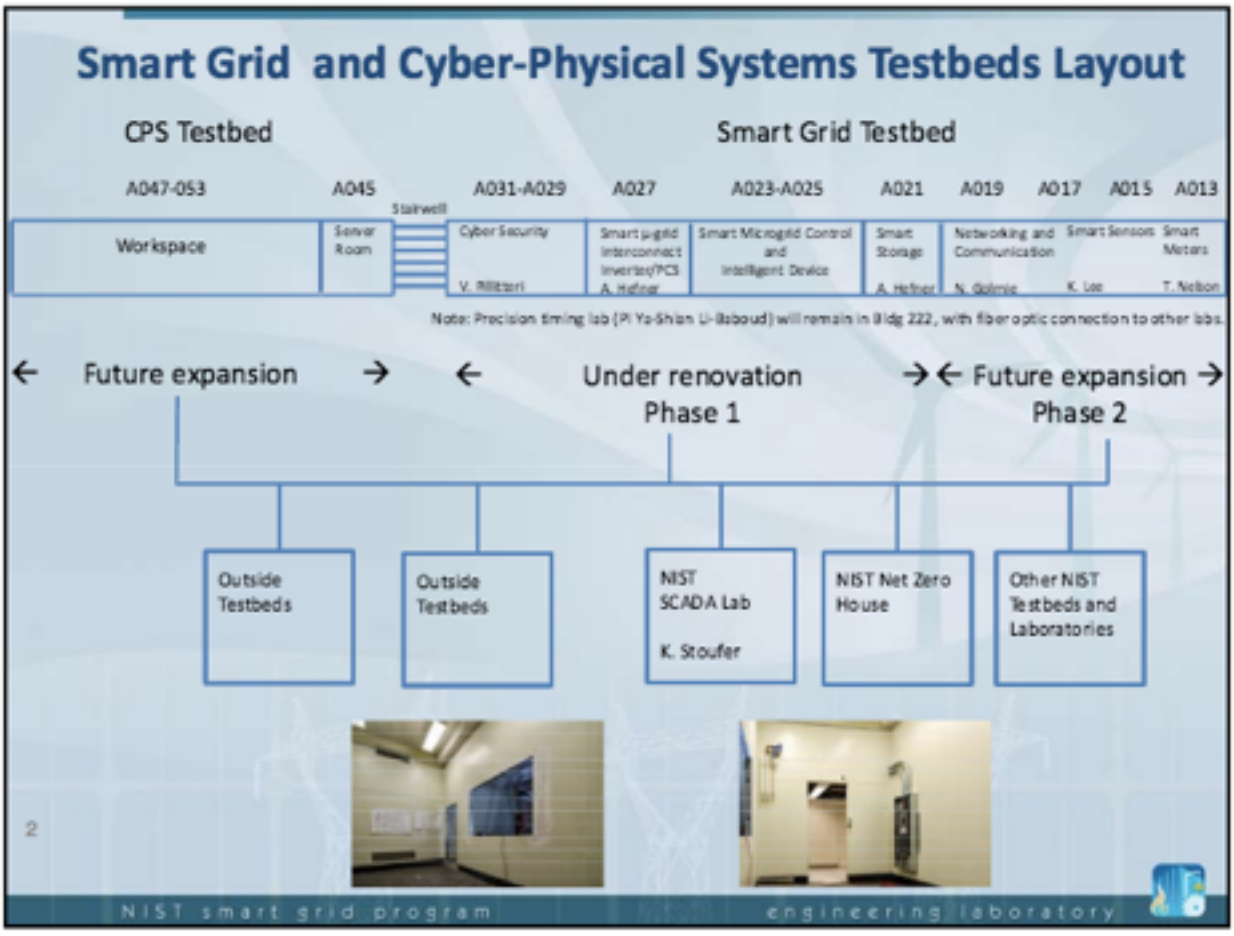


Figure 22. Smart Grid and CPS Testbeds from NIST

The Industrial Internet Consortium is supporting multiple Smart Manufacturing testbeds pictured in Figure 23 at http://www.iiconsortium.org/test-beds.htm

Figure 23. Testbeds from the Industrial Internet Consortium

6. What technological issues may hinder the development of IoT, if any?

a. Examples of possible technical issues could include:

i. Interoperability

ii. Insufficient/contradictory/proprietary standards/platforms

See http://www.slideshare.net/bobmarcus/standards-and-open-source-for-big-data-cloud-and-iot

Several standards organizations are listed in Figure 24 from http://tinyurl.com/gv38c78

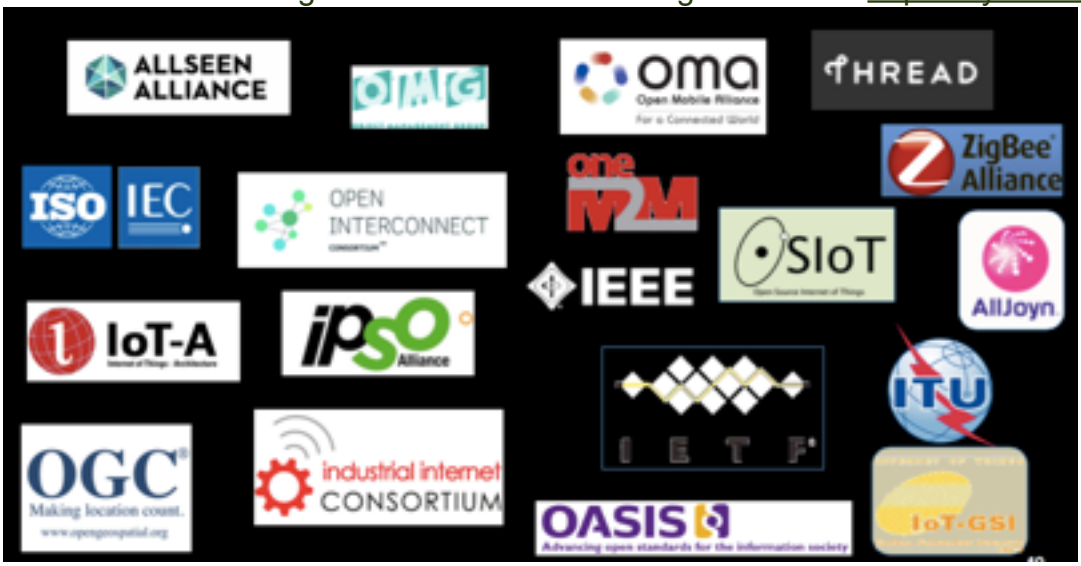


Figure 24. Some Standards Organizations with IoT-related Activities

The Internet of Things Standards Stack below is described in Figure 25 at http://www.slideshare.net/MichaelKoster/ietf91-ad-hoccoaplwm2mipso-4157527

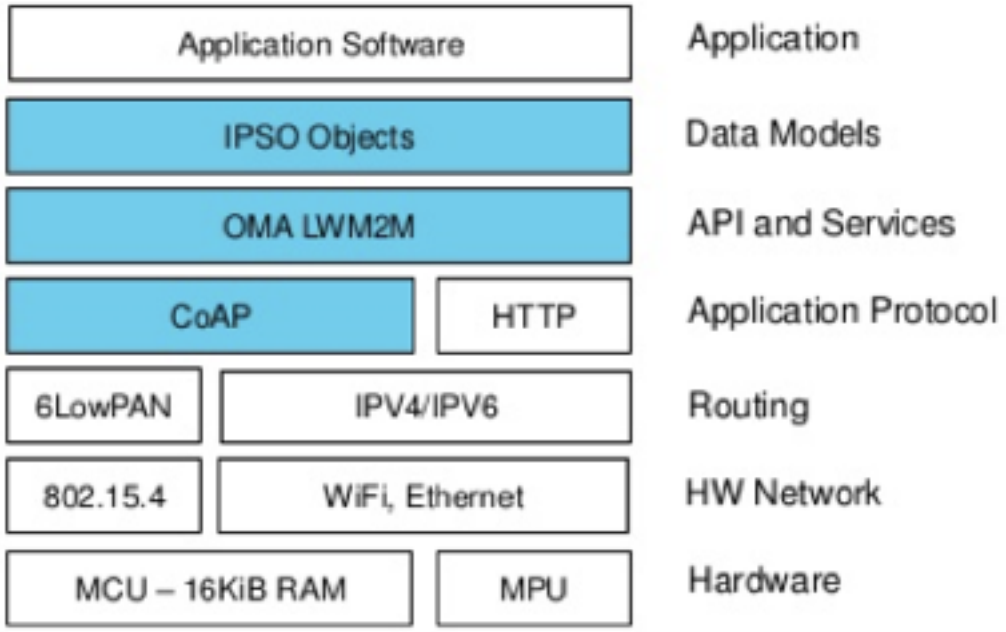


Figure 25. An Internet of Things Standards Stack

iii. Spectrum availability and potential congestion/interference
iv. Availability of network infrastructure

See http://www.slideshare.net/bobmarcus/iot-nodesosmiddlewareplatforms
Software Defined Networking (SDN) for IoT is a potential solution for network issues. For example, see the MulL SDN Platform in Figure 26 from http://www.openmul.org/

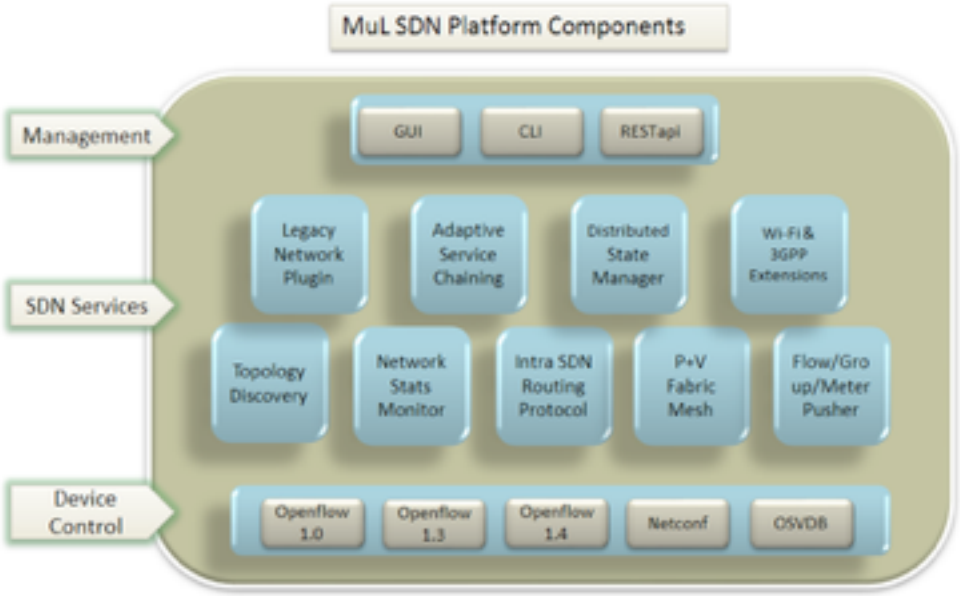


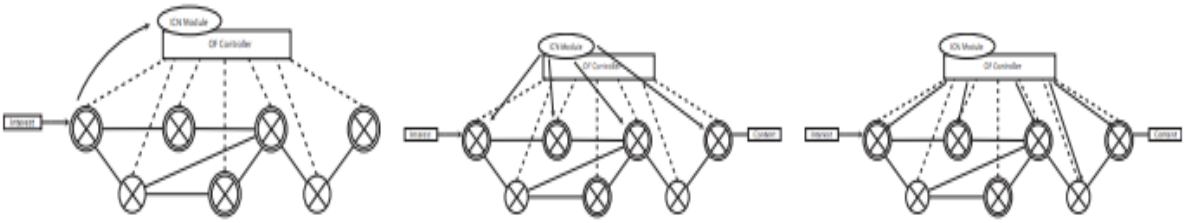
Figure 26. Software Defined Networking (SDN) Platform from MuL

Named Data Networking (NDN) for IoT can also support enhanced networking. See the mapping between IoT requirements and NDN features in Table 3 from http://tinyurl.com/grpto7t

IoT requirement	NDN features
Scalability and robustness	hierarchical application-specific names, in-network caching, Interests aggregation, anycasting
Security	data integrity and origin authentication via per-packet signature, possibility of encryption
Energy efficiency	in-network caching, Interest aggregation, anycasting
Heterogeneity	unbounded application-specific namespaces, high customization of transport and forwarding strategies and caching policies
Mobility	location-independent names, receiver-driven connectionless communications, multi-source retrieval
Reliability	Interest retransmissions from original consumers and retries from intermediate nodes, in-network caching, multi-path routing

Table 3. IoT Requirements mapped to Named Data Networking (NDN) Features

A Named Data Networking can also be layered over a Software Defined Network. See the Figure 27 at https://www.nas.ewi.tudelft.nl/people/Fernando/papers/NDNflow.pdf



(a) Step 1, local NDN daemon receives an unassociated Interest and forwards this Interest to the ICN module of the OpenFlow Controller.

(b) Step 2, with the knowledge on topology and ICN capabilities, the ICN module computes a feasible path and configures the appropriate ICN-enabled switches accordingly.

(c) Step 3, the ICN module instructs the legacy OpenFlow controller to configure the necessary IP/Ethernet rules on all intermediate OpenFlow enabled switches.

An overview of the steps necessary to configure an ICN flow over an OpenFlow-enabled network. All switches are OpenFlow capable, doubly-circled nodes additionally have ICN capabilities.

Figure 27. Named Data Networking Layered over a Software Defined Network

v. Other

Engineering of Large-scale CPS Systems of Systems: See http://www.slideshare.net/bobmarcus/engineering-large-scale-cyberphysical-systems

Systems Engineering Guide for Systems of Systems (SoS)
http://www.acq.osd.mil/se/docs/SE-Guide-for-SoS.pdf

SoS 1.Translating SoS Capability Objectives into High-Level SoS Requirements

SoS 2.Understanding the Constituent Systems and Their Relationships

SoS 3. Assessing Extent to Which SoS Performance Meets Capability Objectives

SoS 4. Developing, Evolving and Maintaining an Architecture for the SoS

SoS 5. Monitoring and Assessing Potential Impacts of Changes on SoS Performance

SoS 6. Addressing SoS Requirements and Solution Options

SoS 7.Orchestrating Upgrades to SoS

b. What can the government do, if anything, to help mitigate these technical issues? Where may government/private sector partnership be beneficial?

Set up standards maturity matrix for specific capabilities similar to Cloud as shown in Table 4 from http://www.slideshare.net/bobmarcus/2011-iaas-standards-report-from-ad-hoc-wg

Availability Level	Description	Recommendation
1. No Standards	Standardization needed	Encourage standards development
2. Under Development	Discussions within standards groups. Open source project launched.	Monitor and provide feedback to standards development
3. Specification Document Published	Initial specification posted for public review	Review specification and plan testing
4. Initial Reference Implementation	Reference implementation available	Evaluate reference implementation
5. Early Third Party Testing	Evaluation in test environments	Pilot Projects should consider use
6. Initial Production Implementations	Successful use in production	Mainstream projects should consider use
7. Many Deployments	Widespread use by many groups	Projects should use the standard as a default
8. Accepted Standard	De facto or de jure acceptance as a standards	Projects should use unless special circumstances require exemption
9. Aging Standards	New standards are under development	Projects should explore alternatives

Table 4. Standards Maturity Matrix

Set up Testbeds for Government CPS SoS including Standards Evaluation. A Live, Virtual, and Constructive Simulation Testbed for SoS is shown in Figure 28 from http://www.et-strategies.com/great-global-grid/emerging-trends.pdf

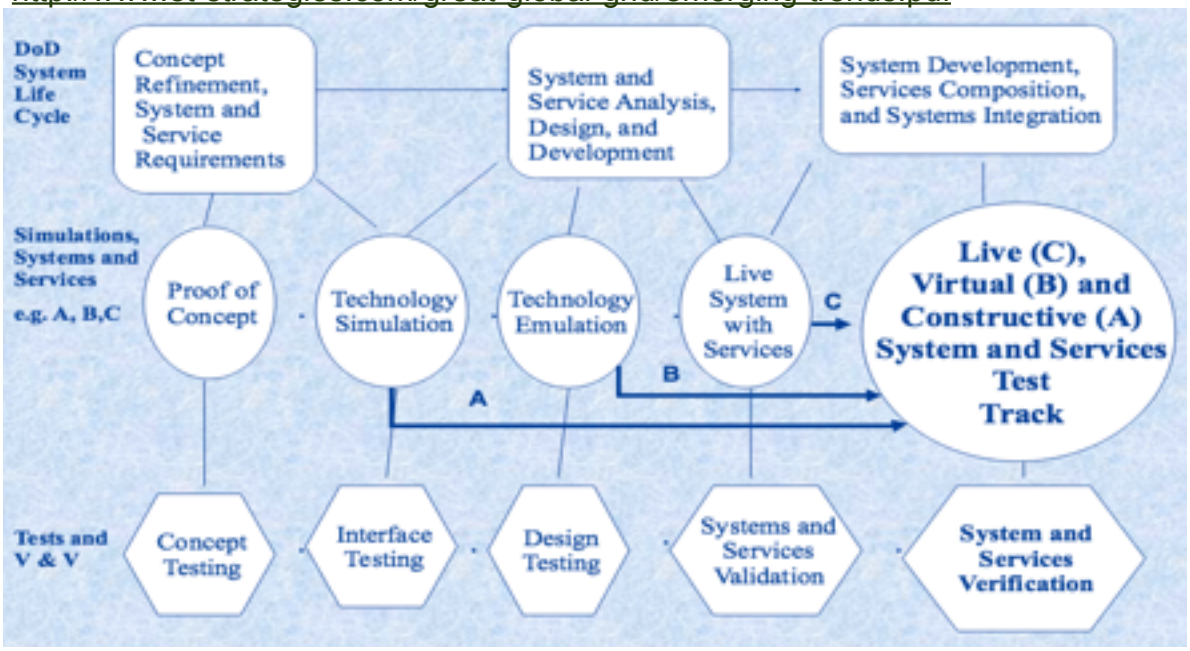


Figure 28. Live, Virtual, Constructive Simulation Testbed for SoS

An Architecture Delivery Process for engineering SoS is shown in Figure 29 from http://www.slideshare.net/Zubin67/soa-architecture-delivery-process-presentation

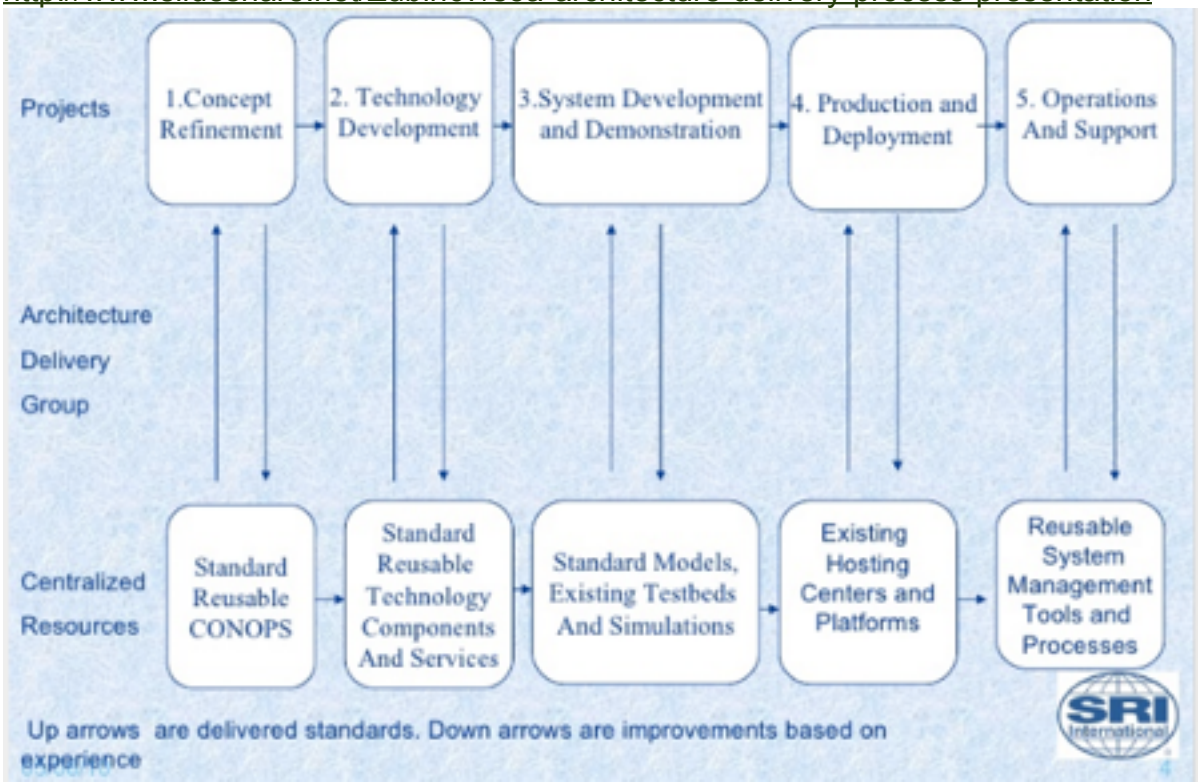


Figure 29. Architecture Delivery Process for Engineering Systems of Systems

7. NIST and NTIA are actively working to develop and understand many of the technical underpinnings for IoT technologies and their applications. What factors should the Department of Commerce and, more generally, the federal government consider when prioritizing their technical activities with regard to IoT and its applications, and why? Infrastructure: Infrastructure investment, innovation, and resiliency (such as across the information technology, communications, and energy sectors) will provide a foundation for the rapid growth of IoT services.

NIST should establish a collaborative Working Group combining Cloud, Big Data, and CPS to extend current Reference Models to support Smart Grid and Smart City. See http://www.slideshare.net/bobmarcus/reference-architectures-for-layered-cps-system-of-systems and http://www.slideshare.net/bobmarcus/nist-cpsrelated-slides and http://www.slideshare.net/bobmarcus/iotenabled-smart-city-framework

The current Cloud Reference Model is shown in Figure 30 from http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505

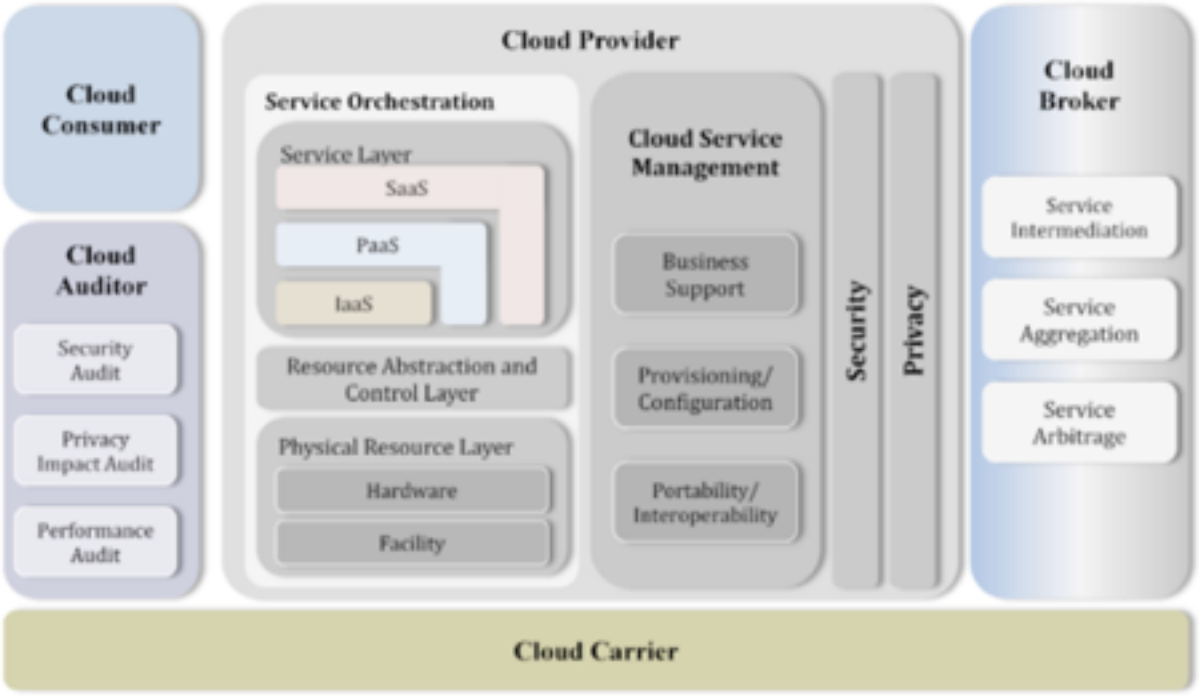


Figure 30. NIST Cloud Reference Model

The current NIST CPS Reference Framework is shown in Figure 31 from http://www.cpspwg.org/Portals/3/docs/CPS%20PWG%20Draft%20Framework%20for%20Cyber-Physical%20Systems%20Release%200.8%20September%202015.pdf

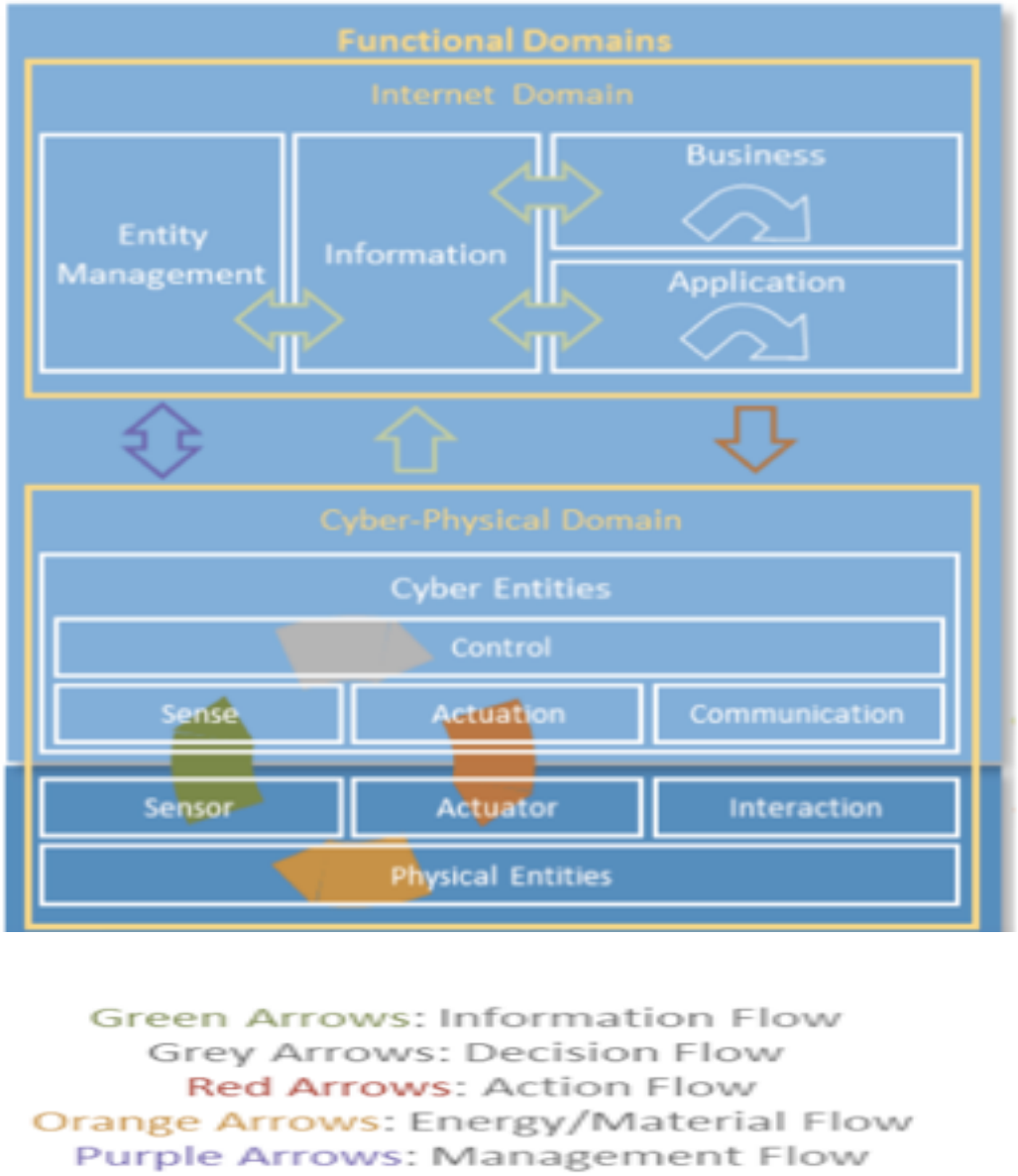


Figure 31. NIST CPS Reference Framework

The current NIST Big Data Reference Architecture is shown in Figure 32 from http://bigdatawg.nist.gov/_uploadfiles/M0397_v1_2395481670.pdf

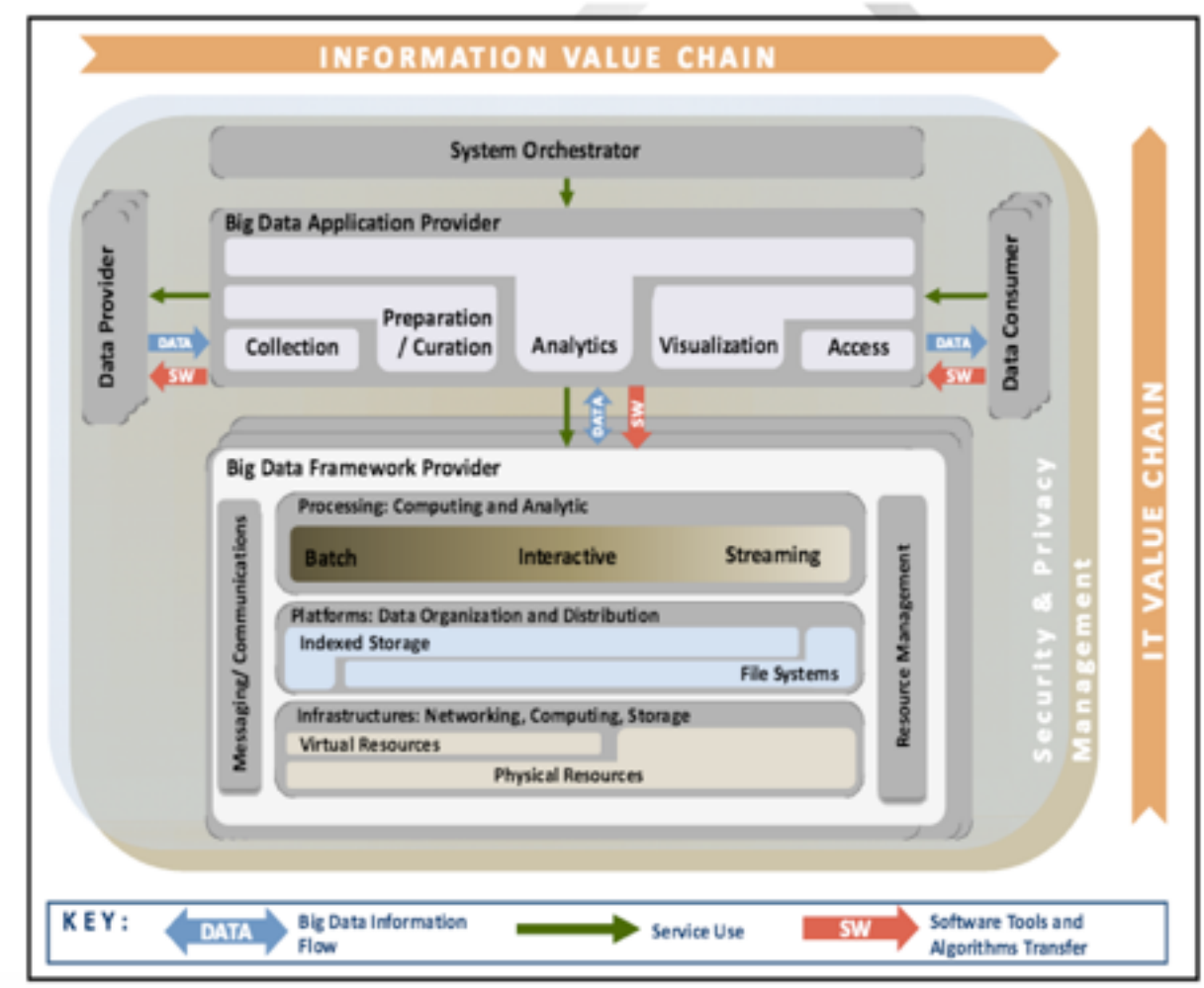


Figure 32. NIST Big Data Reference Architecture

8.How will IoT place demands on existing infrastructure architectures, business models, or stability?

Challenges. See http://www.iiconsortium.org/pdf/IIC_Investment_Strategies_White_Paper-2015.pdf

“What we found was that traditional investment models simply don’t work. As one Venture Capital executive told us, IoT is turning the Venture Capital model upside down. We dub this new role the Venture Industrialist, a new role played by new rules.The goals and timelines have shifted.

In Industrial Internet environments, ideas don't have to be broad and fine-tuned; they can be narrowly focused and under development. Speed and flexibility are critical success factors. In this area, the goal is to transform existing businesses or to create an entirely new business. The new investment hot spots are around innovation that targets operational efficiencies that can save companies tens of millions of dollars. "

The roles of the many infrastructure layers from Physical Environment to Business Goals are shown in Figure 33 from http://www.nuigalway.ie:85/media/publicsub-sites/engineering/files/Time-AwarenessIoT.pdf

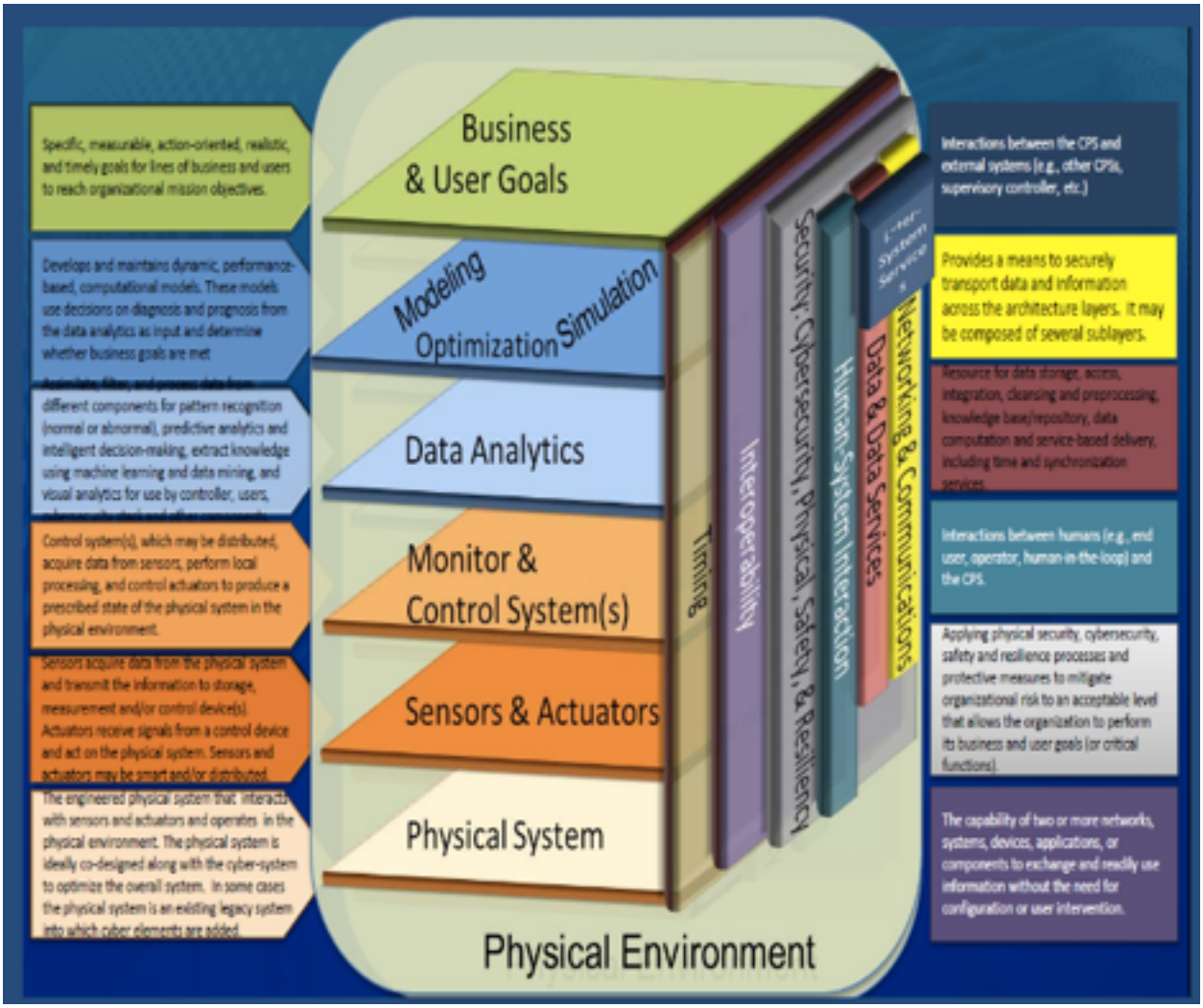


Figure 33. Infrastructure Layer Roles in CPS Systems

9. Are there ways to prepare for or minimize IoT disruptions in these infrastructures? How are these infrastructures planning and evolving to meet the demands of IoT?

Engineering Large-Scale CPS System of Systems http://www.slideshare.net/bobmarcus/engineering-large-scale-cyberphysical-systems

A key problem for the future of Large Scale CPS System of Systems will be the robust interfacing of heterogeneous systems. Some initial success should be achievable horizontally and vertically across systems in the same domain using emerging standardizations and tools as shown in Figure 34 from http://www.slideshare.net/bobmarcus/engineering-large-scale-cyberphysical-systems. However applications such as Smart Cities will require the interfacing of systems from many different domains with diverse application models, data processing and control structures.

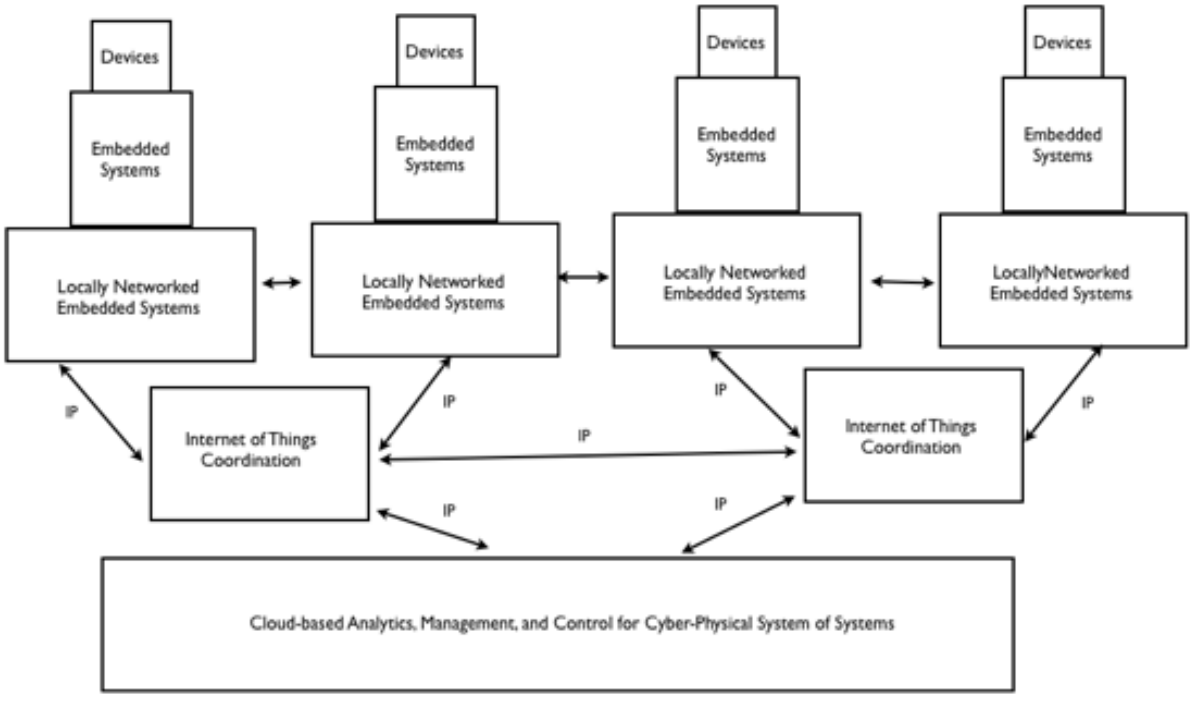


Figure 34. Horizontally and Vertically Connected CPS Systems of Systems

The many capabilities that must be engineered into an IoT Platform are shown in Figure 35 from http://www.slideshare.net/IoTBruce/the-iot-food-chain-picking-the-right-dining-partner-is-important-with-dean-freeman-of-gartner/28

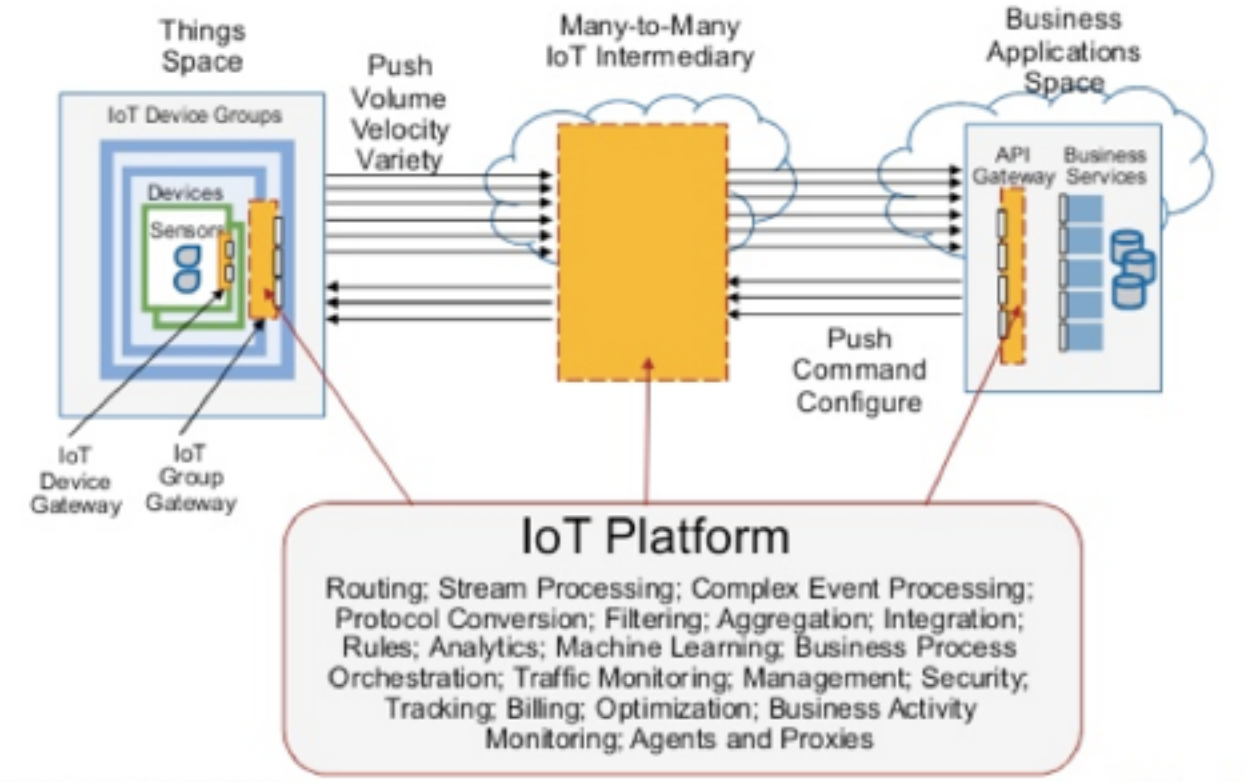


Figure 35. IoT Platform Capabilities from Gartner Group

13. What impact will the proliferation of IoT have on industrial practices, for example, advanced manufacturing, supply chains, or agriculture?

a. What will be the benefits, if any?

b. What will be the challenges, if any?

c. What role or actions should the Department of Commerce and, more generally, the federal government take in response to these challenges, if any?

Many examples of IoT Smart X applications can be found at http://www.slideshare.net/bobmarcus/iot-use-cases. Figure 36 from General Electric at http://www.ge.com/docs/chapters/Industrial_Internet.pdf shows the impact of industrial IoT on different industries

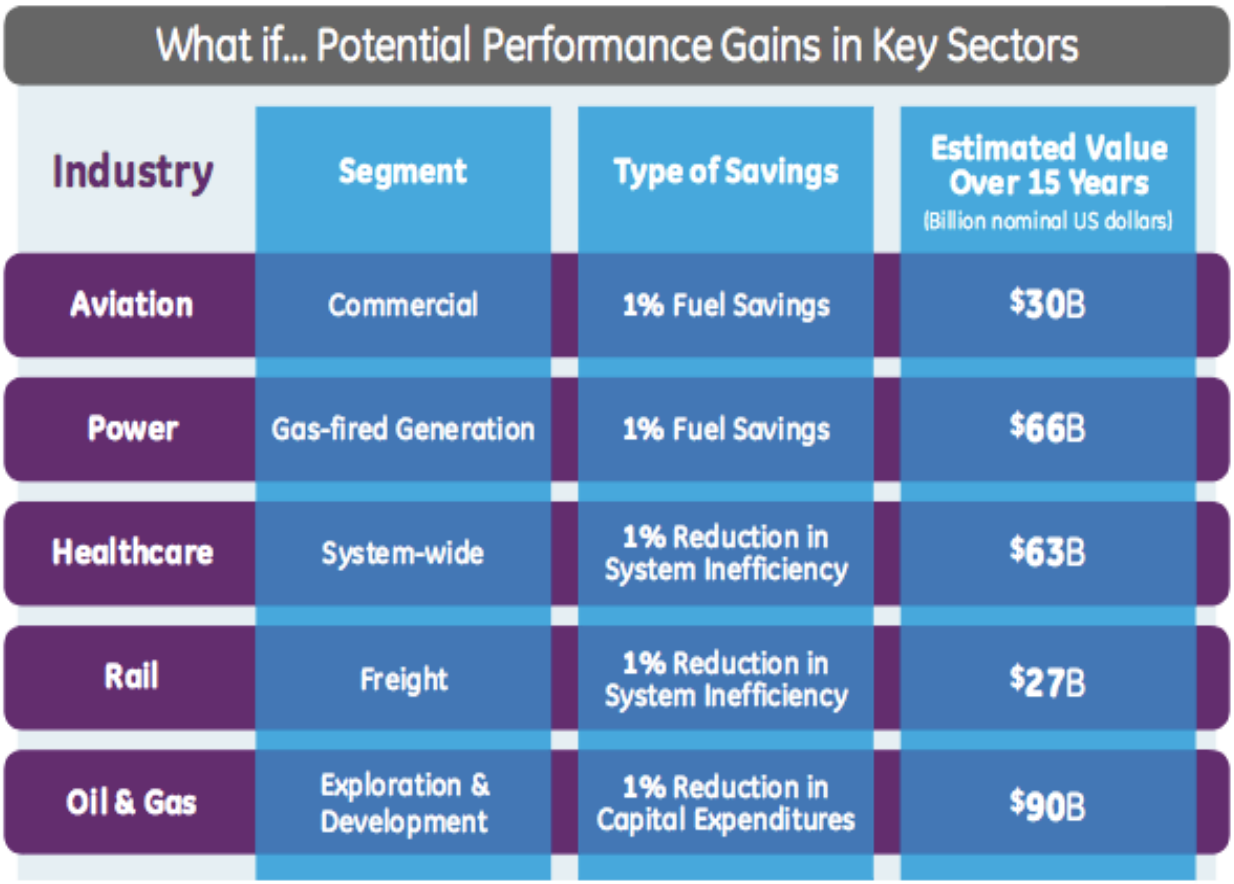


Figure 36. Potential Gains from IoT in Key Sectors from GE

16. How should the government address or respond to cybersecurity concerns about IoT?

a. What are the cybersecurity concerns raised specifically by IoT? How are they different from other cybersecurity concerns?

b. How do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to IoT cybersecurity, if any?

Many slides on CPS Security are at http://www.slideshare.net/bobmarcus/security-in-cyberphysical-systems. Security Requirements from the European Research Cluster on the IoT (IERC) www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

" DoS/DDOS attacks are already well understood for the current Internet, but the IoT is also susceptible to such attacks and will require specific techniques and mechanisms to ensure that transport, energy, city infrastructures cannot be disabled or subverted.

** General attack detection and recovery/resilience to cope with IoT-specific threats, such as compromised nodes, malicious code hacking attacks.*

** Cyber situation awareness tools/techniques will need to be developed to enable IoT-based infrastructures to be monitored. Advances are required to enable operators to adapt the protection of the IoT during the lifecycle*
of the system and assist operators to take the most appropriate protective action during attacks.

** The IoT requires a variety of access control and associated accounting schemes to support the various authorization and usage models that are required by users. The heterogeneity and diversity of the devices/gateways that require access control will require new lightweight schemes to be developed.*

** The IoT needs to handle virtually all modes of operation by itself without relying on human control. New techniques and approach e.g. from machine learning, are required to lead to a self-managed IoT"*

17. How should the government address or respond to privacy concerns about IoT?

a. What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

b. Do these concerns change based on the categorization of IoT applications (e.g., based on categories for Question 4, or consumer vs. industrial)?

c. What role or actions should the Department of Commerce and, more generally, the federal government take regarding policies, rules, and/or standards with regards to privacy and the IoT?

Many slides on CPS Privacy are at http://www.slideshare.net/bobmarcus/security-in-cyberphysical-systems. Privacy Requirements from the European Research Cluster on the IoT (IERC) www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

“ Cryptographic techniques that enable protected data to be stored processed and shared, without the information content being accessible to other parties. Technologies such as homomorphic and searchable encryption are potential candidates for developing such approaches.*

** Techniques to support Privacy by Design concepts, including data minimization, identification, authentication and anonymity.*

** Fine-grain and self-configuring access control mechanism emulating the real world. There are a number of privacy implications arising from the ubiquity and pervasiveness of IoT devices where further research is required, including*

** Preserving location privacy, where location can be inferred from things associated with people.*

** Prevention of personal information inference, that individuals would wish to keep private, through the observation of IoT-related exchanges.*

** Keeping information as local as possible using decentralised computing and key management.*

** Use of soft Identities, where the real identity of the user can be used to generate various soft identities for specific applications.Each soft identity can be designed for a specific context or application without revealing unnecessary information, which can lead to privacy breaches”*

Trust Requirements from the European Research Cluster on the IoT (IERC**)**
www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf

“ Lightweight Public Key Infrastructures (PKI) as a basis for trust management. Advances are expected in hierarchical and cross certification concepts to enable solutions to address the scalability requirements.*

** Lightweight key management systems to enable trust relationships to be established and the distribution of encryption materials using minimum communications and processing resources, as is consistent with the resource constrained nature of many IoT devices.*

** Quality of Information is a requirement for many IoT-based systems where metadata can be used to provide an assessment of the reliability of IoT data.*

** Decentralized and self-configuring systems as alternatives to PKI for establishing trust e.g. identity federation, peer to peer.*

** Novel methods for assessing trust in people, devices and data, beyond reputation systems. One example is Trust Negotiation. Trust Negotiation is a mechanism that allows two parties to automatically negotiate, on the basis of a chain of trust policies, the minimum level of trust required to grant access to a service or to a piece of information."*

** Assurance methods for trusted platforms including hardware, software, protocols, etc.*

** Access Control to prevent data breaches. One example is Usage Control, which is the process of ensuring the correct usage of certain information according to a predefined policy after the access to information is granted*

20. What factors should the Department consider in its international engagement in:

a. Standards and specification organizations?

b. Bilateral and multilateral engagement?

c. Industry alliances?

d. Other?

The 30 organizations below are working on aspects of IoT and CPS standardization.

The Department of Commerce should track and collaborate with them when appropriate. See http://www.slideshare.net/bobmarcus/standards-and-open-source-for-big-data-cloud-and-iot for more information.

• NIST Cloud, Big Data, and CPS Public Working Groups
http://www.nist.gov/itl/cloud/ and http://bigdatawg.nist.gov and http://www.cpspwg.org/

• Industrial Internet Consortium and Cloud Standards Customer Council and OMG DDS
http://www.iiconsortium.org/ and http:// www.cloud-council.org/ and http:// portals.omg.org/dds/

• Open Fog Alliance
http://www.openfogconsortium.org/

• IETF (CoAP and 6LoWPAN)
http://coap.technology/ and https://en.wikipedia.org/wiki/6LoWPAN

• OASIS MQTT
https://www.oasis-open.org/committees/mqtt/charter.php

• ITU-T IoT Study Group + Big Data and Cloud Requirements and Capabilities
http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx and
https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.3600-201511-I!!PDF-E&type=items

• ISO (Reference Architecture under development)
http://www.iso.org/iso/internet_of_things_report-jtc1.pdf

• IEEE IoT
http://iot.ieee.org/

• W3C Web of Things
https://www.w3.org/WoT/

• Open Interconnect Consortium (OIC) with IoTivity open software
http://openconnectivity.org/wp-content/uploads/2016/01/OIC_Specification_Overview_201501131.pdf
https://www.iotivity.org/

• New Open Connectivity Foundation (OCF) incorporating OIC
http://openconnectivity.org

• OneM2M
http://www.onem2m.org/

• Open Mobile Alliance (LWM2M)
http://openmobilealliance.org/about-oma/work-program/m2m-enablers/

• Open Web Application Security Project (OWASP) IoT Projects
https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

• IoT European Research Cluster(IERC)
http://www.internet-of-things-research.eu

• ETSI Internet of Things
http://www.etsi.org/technologies-clusters/technologies/internet-of-things

• Open Group IoT Working Group
http://www.opengroup.org/getinvolved/workgroups/iot

• Fiware Technologies
http://www.europeanpioneers.eu/en/fiware-technologies.html

• Weightless for LPWAN
http://www.weightless.org/

• AllSeen Alliance (AllJoyN)
https://allseenalliance.org/framework

• Thread
http://www.threadgroup.org/

• Zigbee Alliance
http://www.zigbee.org/

• Bluetooth
https://www.bluetooth.com/

• XMPP-IoT and Sensei IoT Semantic Web 3.0 Standard for IoT
http://www.xmpp-iot.org/ and http://www.sensei-iot.org/

• IPSO Alliance (Smart Objects)
http://www.ipso-alliance.org/

• IoT European Research Cluster(IERC)
http://www.internet-of-things-research.eu

• OGC SensorThings API
http://www.opengeospatial.org/projects/groups/sensorthings

• WS02 IoT
http://wso2.com/iot

• IoT6 Project in Europe
http://iot6.eu/

• Open Networking Users Group
https://opennetworkingusergroup.com/about/

• Cloud Standards Customer Council Architecture for IoT
http://www.cloud-council.org/deliverables/CSCC-Cloud-Customer-Architecture-for-IoT.pdf

26. What role should the Department of Commerce play within the federal government in helping to address the challenges and opportunities of IoT? How can the Department of Commerce best collaborate with stakeholders on IoT matters?

The Department of Commerce should issue periodic reports on the best practices and emerging standards for IoT and Smart X applications. For more details about bsst practices, see http://www.slideshare.net/bobmarcus/challenges-and-best-practices-for-iot-cloud-and-big-data-systems. For more details about standards, see http://www.slideshare.net/bobmarcus/standards-and-open-source-for-big-data-cloud-and-iot

27. How should government and the private sector collaborate to ensure that infrastructure, policy, technology, and investment are working together to best fuel IoT growth and development? Would an overarching strategy, such as those deployed in other countries, be useful in this space? If the answer is yes, what should that strategy entail?

See http://www.slideshare.net/bobmarcus/2009-federal-open-cloud-computing-initiative-foci-proposal for a draft on possible Federal roles in advancing Cloud Computing. A similar strategy could be developed for future government, private sector, and academic collaboration on IoT and Smart X applications. The benefits would include:

- Improve Government Operations
- Provide Training and Employment Opportunities
- Increase US Business Competitiveness
- Encouraging IoT R &D and Startups
- Support Future US Scientific Research

References:

Downloadable Publications Related to CPS
www.slideshare.net/bobmarcus/downloadable-publications-on-cps-cloud-and-big-data

NIST Related CPS-related Slides
http://www.slideshare.net/bobmarcus/nist-cpsrelated-slides

Inventory of my CPS Slide Sets
http://www.slideshare.net/bobmarcus/inventory-of-my-cps-slide-sets