Bolstering U.S. Competitiveness & National Security through IoT

July 8, 2016 | Capitol Hill | Rayburn Building

Chuck Evanhoe

- **President & CEO | Evanhoe & Associates**
- **Chairman | AIM, Inc.**
- **Chairman | INCITS IoT10 Technical Committee on ISO/IEC IoT Standards**

Welcome ladies and gentleman to the Internet of Things Caucus discussion on IoT U.S. Competitiveness and national security.

My name is Chuck Evanhoe and I am Chairman, AIM Board of Directors, as well as the Chairman IoT10-US Technical Committee, ISO/IEC JTC1/WG10—IoT Standards Working Group and the Chairman, ADC1-US Technical Advisors Group, ISO/IEC JTC 1/SC31—Barcode & RFID Standards. In my spare time, I'm the President, Evanhoe & Associates, Inc., a full-service IT Solutions Provider and Systems Integrator, a service-disabled, veteran-owned small business (SDVOSB) focused on accurate, actionable data provided by data capture, management, cleansing, aggregation and presentation solutions.

Our panelists will discuss IoT competitiveness, provide interesting international updates, give an overview of global standards and their potential impact on U.S. industries, and discuss opportunities for DoD and the Federal government as IoT end users. In addition, we provide our opinion as to what is missing from a U.S. perspective and we suggest might be done to help U.S. competitiveness in the IoT space.

Our panelists will include:

- David Coons, *Vice President, Software and Advanced Solutions, Asset Identification & Tracking Division, Zebra Technologies Corporation & Member, AIT Alliance*
  David Coons is Vice President of Software and Advanced Solutions for Zebra Technologies' Asset Identification and Tracking division. He is responsible for planning and management of Software and Firmware products for Zebra's printing business, and for the development of new solutions made possible by the innovative application of connected technologies in vertical markets. Of particular interest to David are applications in medical device identification, drug supply chain security and healthcare asset management. David has a bachelor's degree in mechanical engineering and a master's degree in electrical engineering, both from Rochester Institute of Technology.

- Bob Fudge, *Chairman, Automatic Identification Technology Alliance (AIT Alliance) & Vice President, Evanhoe & Associates, Inc.*
  Bob Fudge is Vice President of Public Sector Business for Evanhoe & Associates. He is also the Chairman of the AIT Alliance, an industry association focused on fostering education and adoption of automatic identification technologies in the federal government, including the

Department of Defense. Having served 25 years in the United States Air Force as an aircraft maintainer, he is passionate about the need for improving logistics data capture processes that will improve mission capability, save taxpayer dollars, and improve the lives of our service members. Bob has a Bachelor's degree in Government and Politics from the University of Maryland and a Juris Doctor degree from Marquette University Law School.

- Gary Moe, *President, ID Integration, Inc. & Member, AIT Alliance*
  Gary Moe is President of ID Integration and is an authority on RFID systems Integration and direct part marking, reading and verification of 2D barcodes on parts and tools. He has over 30 years of experience in implementing engineered systems in Aerospace, Military, Medical, Automotive and Microelectronics industries. Customers of ID Integration include Boeing Commercial and Defense, US Army, US Navy, Lockheed Martin, Northrop Grumman, Sikorsky Helicopter, Bell Helicopter, Raytheon, Rockwell Collins, Honeywell Aerospace and Engines, GE Aircraft Engines, Goodrich Aerospace, United Airlines and Parker Aerospace.

We'd all be pleased to take questions at any time during our presentations but have left time to have a robust Q&A at the end.

So who is AIM and what perspective are we bringing to this discussion.

AIM is the association for automatic identification and data capture to advance the success of our members in the application of AIM technologies. AIM is GLOBAL with chapters across the world with over 400 member companies.

Automatic Identification and Data Capture (AIDC) are the technologies that provide the ability to automate data collection in business eliminating keyboard entry. For example:

- Bar codes – UPC, Code 39, Code 128, etc.
- 2D Symbology – QR Code, DataMatrix, etc.
- RFID – passive also known as RAIN, active, near field communication (NFC), etc.
- RTLS – real-time locating systems using RF, infrared, beacons, etc.
- Biometrics – fingerprints, blood vessels, retinas, etc.
- As well as many others

AIM technologies identify the things in the Internet of Things so our technologies are the first millimeter, centimeter, meter, or kilometer of the Internet of Things!

When people discuss the IoT, they are generally talking about directly connect devices, usually with an IP (internet protocol) address normally found on a network. AIM technologies are generally not directly connected to a network but act as the sensor or trigger for network connected devices such as a scanner or RFID reader. But without AIM technologies such as a bar code or RFID tag, it is difficult to know what a "thing" is. So while we are not the traditional connected technologies, our technologies enable the IoT to function better and identify the things.

So why is AIM here? It's our mission to be an unbiased resource for networking, education, advocacy, and standards to help our members grow their business by fostering the effective use of Automatic Identification and Data Capture (AIDC) solutions. This is especially important in this burgeoning IoT space where people think about the internet part of IoT but forget about the things.

To accomplish our mission, AIM has several active committees both internationally, such as the IoT and RFID Experts Group Committees, as well as those that are chapter specific like North America's AIT Alliance which is focused on the effective use of AIDC in the federal government. We have been very

helpful to both the DoD and FDA on several automatic identification technology related efforts such as the DoD Item Unique Identification (IUID) requirement and FDA's Unique Device Identification (UDI) regulation.

Our first panelist is David Coons, Vice President of Software and Advanced Solutions for Zebra Technologies. He is here to provide a view on U.S. IoT competiveness.

David Coons

- **Vice President – Software & Advanced Solutions | Asset Identification & Tracking Division Zebra Technologies Corporation**
- **Member, AIT Alliance**

Hello and good afternoon. Thank you for attending this AIM briefing on the Internet of Things and US competitiveness. I'd like to start with a brief overview of Zebra Technologies Corporation and the work we're doing in the IoT space, and then I'll give a Solution Provider's view on the importance of the Internet of Things and what it means to US commercial competitiveness and technology leadership.

Zebra Technologies Corporation is a global leader in bringing enterprise Internet of Things solutions to Business-to-Business and Business-to-Government markets. With revenues of approximately $3.6 billion and 7,000 employees in more than 40 countries, Zebra is a trusted business partner of the more than 95 percent of all Fortune 500 companies that we serve. In addition, Zebra leads the growing category known as Enterprise Asset Intelligence (EAI) which describes the ability of businesses, government agencies and other organizations to track critical assets within their operations and know exactly **what** they are, **where** they are and their **condition** so they can make smarter, faster decisions that improve their bottom line. EAI leverages and recognizes the fact that people, assets and devices – especially mobile devices – are becoming increasingly connected and that this trend is advancing at an exponential rate.

I'd also like to highlight some other recent engagements we've had on the Hill regarding IoT policy and technology.

It is difficult to understate the importance of the IoT and the impact it is having on industry and government. You heard Chuck describe what he called "AIM Technologies" – RFID tags and readers, bar code printers and scanners, Real time location systems, and mobile terminals. These technologies have been, and will continue to be, some of the most fundamental tools that give "things" – Packages, Containers, Equipment, Instruments, etc. – a digital identity. In different forms, these same technologies also help identify workers, soldiers, and students around the world. With the advent of the IoT, these devices are being enhanced with additional sensing capabilities and are increasingly being connected to the internet. The flow of data from these sensors is beginning to permit unheard-of levels of real-time insight to the status and behavior of complex systems and processes. This visibility to operations through data allows an entirely new level of thinking about how organizations can optimize performance for competitive advantage, and it opens up new business models around how insight and analysis can be offered as a service.

A good way to measure the impact on commercial interest in IoT is to look at where venture capitalists are putting their money. Over the past three years we have seen a 10X increase in VC funding for IoT start-ups. And it is not all in the consumer space, though consumer products, like fitness monitors and smart watches, often get most press. Half of those new companies will be based on industrial devices and services. And spending **by** businesses on IoT technology and services is also increasing dramatically. At its November, 2015 Symposium and ITExpo, IT research firm Gartner projected that global spend on endpoint IoT **devices** would be $1.4 Trillion in 2016, with another $250 Billion in related

services, the majority of which will be spent on business applications. Surveys consistently show that IoT & cloud initiatives are at the top of enterprise investment strategies, and over 80% of surveyed firms agreed that IoT solutions will be **the** most strategic technology initiative for their organization in a decade. These firms represent the core of American enterprise - including retail, manufacturing, consumer products, transportation, healthcare, and government. As a Business to Business enterprise that serves all of these markets, Zebra's foundation in scanning, wireless LAN, and Mobile computing gives us a unique perspective from which to innovate and deliver on the benefits of the IoT.

Solution provider companies, like Zebra, are increasingly building strategies around the Internet of Things. In fact, we consider delivering **insight from data** to be the primary customer value proposition that will extend our 40-year history of technology and market leadership. Our ability to deliver on that opportunity **globally** hinges on being able to work within an evolving environment of connectivity and security standards. At this point in the life-cycle of IoT, there are myriad alliances and consortiums that are working to create standards for connectivity and interoperability. This will shake out over time, but what we consider to be most important is that US companies aren't under-represented in these consortia. We should drive for adoption of open standards and avoid ending up in a situation where, for example, we need to license a technology component in order to operate in a particular country. Technology providers will design "around" closed standards, but this just adds complexity, exposes security risks, and delays the day when companies can freely compete in global markets.

Despite the need for clear interoperability standards, history has shown that the tech industry isn't one to sit idle while standards are developed. Many technology battles are won or lost before standards are ever close to being ratified, but free-market forces eventually drive convergence. In the near term we will innovate as needed to satisfy our customers, but we are very interested in shaping and contributing to the evolution of standards which build upon the best work done by government, industry and academia. There is a tee shirt on display at the Computer History Museum in Mountain View, CA, that was produced by Cisco in the mid 70s, listing twenty-five network transport protocols that Cisco equipment supported in order to sell into a world of nascent, competing standards. Long story short - through some remarkable private sector collaboration and with some help from ARPA, these standards eventually reduced down to one primary protocol, known as TCP/IP, that powers the internet and most networks today. Similarly, efforts by the federal government to collaborate with U.S. companies on data security standards and the enforcement of intellectual property laws can play a key role in developing and protecting the infrastructure upon which IoT deployment and growth will rest.

As with all new technology platforms, there will be technical challenges with IoT that will produce an initial solution that will be subsequently subject to ongoing, continuous improvement. Among these challenges will be the need to ensure the security of connected **devices**, the **data** those devices capture and transmit and the **cloud platform** on which the devices interact. Privacy concerns, especially in areas such as health care, will also require thoughtful resolution. One frequently cited concern relates to the rapid pace of new product introduction in the device space. As improvements are made in security and connectivity protocols, will older products be "orphaned" in the marketplace, leaving known security vulnerabilities unaddressed? This is an appropriate question. In fact, in a blog post in February last year, FTC Chief Technologist, Ashkan Soltani wrote, "If a critical vulnerability is discovered, will an update be provided? Should modern refrigerators have a shelf life, much like the food contained within?" Perhaps. Keep in mind, though, that the very internet connectivity that creates security concerns is also the mechanism by which security patches can be pushed out to devices at the edge. Today, 30% of car owners ignore safety recall notices, because some people take the attitude that "if it's sunny today, it's never going to rain". Connected devices (and cars) will **at least** be visible and accessible for security updates, but responsibility and liability are difficult topics that need to addressed by policy makers. Zebra believes that it will be important to not dis-incent providers from building in this capability, and that regulatory statues around the world are as harmonized as possible.

Consequently, the primary policy challenge for policymakers is to foster an environment that supports the rapid development, deployment and subsequent advancement of secure IoT-enabled technologies in a manner that simultaneously addresses concerns over data security, encryption and privacy. The goal must be to encourage the rapid development and deployment of technologies which provide enhanced, secure and real-time visibility, and access to information in a way that empowers workers to undertake more effective and timely decisions and actions. It is for this reason that we urge Congress to take a thoughtful regulatory approach to governing the IoT and the countless solution applications it enables. Additionally, Zebra recommends that policy makers appreciate the fact that technology and policy issues attendant to B2B and B2G applications of IoT solutions and wearable technologies may differ – at least in some instances – from issues which arise in a B2C setting, and that legislative and regulatory action should take care to identify and appropriately manage any such potential differences. We got policy right with the Internet in the 1990s," said George Mason's Mercatus Center Senior Research Fellow Adam Thierer, "now we need to get it right for the IoT. We need a light-touch, market-driven approach without trying to anticipate problems."

Zebra considers competitiveness to be directly linked to connectedness in the IoT age, both for us as a solution provider, but even more so for our customers. Our customers compete globally, and we are excited to be delivering solutions based on data and insight that can drive higher supply chain efficiency, enhanced customer satisfaction, better product quality, and better patient care. The Internet of Things is core to our strategy for delivering those benefits.

We appreciate your interest in today's overview, and I thank you for your attention.

Chuck Evanhoe

- **President & CEO | Evanhoe & Associates**
- **Chairman | AIM, Inc.**
- **Chairman | INCITS IoT10 Technical Committee on ISO/IEC IoT Standards**

Global IoT Standards Initiatives and The Potential Impact On U.S. Industries.

I have the pleasure to provide some background on global IoT standards initiatives and the potential impact on U.S. industries. My task is to provide you with good background and food for thought and not put you to sleep.
AIM has a long history in standards. Every bar code has been introduced as a standard through AIM's Technical Symbology Committee (TSC). It is comprised of individuals from AIM member companies who are the world's leading experts on symbology design, as well as printing and decoding algorithms. Companies actively work with the committee to ensure a complete technical specification is available to the market. All of the symbologies published as AIM specifications have been adopted by the international community via the ISO standardization process.

In addition, AIM's RFID Experts Group (REG), founded in 2004, is the AIM committee responsible for addressing the standards and issues associated with radio frequency identification (RFID). The REG is currently comprised of over 40 organizations from the U.S., Europe, and Asia. The REG has authored five ISO Technical Reports (on Security, Recycling, ISO/IEC 18000-6C Labeling, installation of ISO/IEC 18000-6C reading systems and ISO/IEC TR24729-4-Tag Security.). The committee has also submitted The RFID Emblem (ISO/IEC 29160) as an ISO standard to assist in consumer notification of RFID and to assist in operational use of the technology. This emblem has now been adopted by CEN as the European required symbol for identifying RFID.

AIM is directly plugged into the international standards process for IoT as liaison organization with ISO/IEC JTC1/WG10 that is working on IoT standards, particularly a reference architecture, a standard on how new standards for IoT in specific vertical application should be designed, and an interoperability framework, or how things should be able to connect and talk in the IoT realm.

To lay a foundation, let me review the various groups involved in IoT standards development to give you a picture of the new "wild west".

First are ISO, the International Organization for Standardization, and IEC, the International Electrotechnical Commission, the international standards and conformity assessment body for all fields of electrotechnology. ISO and IEC also formed JTC 1, Joint Technical Committee One, as the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) who is supposed to have primacy in the area of IoT standards. In spite of this agreement within ISO and IEC, even other ISO and IEC committees are developing vertically oriented IoT standards.

But we also have a number of other organizations and consortia making their mark on IoT standards:

- IEEE – Institute of Electrical and Electronics Engineers
- IETF – Internet Engineering Task Force
- 3GPP – The 3rd Generation Partnership Project
- AIOTI – Alliance for Internet of Things Innovation, an EU initiative
- W3C – World Wide Web Consortium
- ETSI – European Telecommunications Standards Institute
- IIC – Industrial Internet Consortium
- OIC – Open Internet Consortium
- ITU-T – International Telecommunication Union, Telecommunication Standardization Sector
- And many, many others

So why is this alphabet soup important?

Standards set the way we design products as well as implement them into the market. This has profound and long lasting effect if done to favor certain countries, companies, or …

If you're old enough, you might recall the Betamax versus VHS video tape battle. Even though it was not technically superior, Panasonic wielded marketing and standards muscle over Sony to get VHS as the defacto standard for video tapes. What is to stop Huawei in China exerting it's muscle to become the IoT standard over Cisco or other technology companies?

In fact, IoT is part of China's infamous 5-year plan and they are spending billions of Yuan on IoT, even setting up entire cities and regions to be IoT hotbeds, such as Wuxi (near Shanghai). More to the point China has over a dozen experts at each of the WG10 meetings to ensure their view of IoT standards is preeminent over the views of experts from other countries such as US, UK and Sweden. China has made sure that its experts are the primary editor for the key Reference Architecture and Interoperability Framework standards. The Chinese government is expected to invest more than $600 billion in IoT through 2020. According to a GSMA report "How China is Set for Global M2M Leadership," China is the global leader in the adoption of M2M technology with more than 50 million connections in 2013. National policy support grew the M2M connectivity market, with the cooperation of China's largest mobile operators -- China Mobile, China Unicom, and China Telecom -- to nurture a vibrant ecosystem across sectors.

But China is not the only one. South Korea is holding the Chair and Secretariat of the WG10 committee and supplies the primary editor of the vocabulary for IoT. Likewise, they have nearly a dozen experts at each of the international standards meetings. South Korea is planning to invest $5b by 2020 in IoT and smart cars. It aims to increase the domestic market for the Internet of Things from KRW 2.3 trillion in 2013 to KRW 30 trillion ($28.9 billion) by 2020. The South Korean government has set aside KRW 50 billion ($49 million) over the next five years to grow the IoT market.

Let's not forget Europe with their AIOTI and Industry 4.0 initiatives. Europe has over 56 experts on the rolls with more than a dozen at each meeting. The EU is also spending billions on IoT. The EU is funding the AIOTI. EU had Framework 7 which invested 7 billion Euros in IoT research and now have Horizon 2020 – Going to Market with IoT (2014-2020) which has 80 billion Euros as the budget. Horizon 2020 is the financial instrument implementing the Innovation Union, a Europe 2020 flagship initiative aimed at securing Europe's global competitiveness. In the UK, as part of UK Prime Minister David Cameron's announcement to drive 5G research in partnership with Germany, Cameron unveiled a new set of measures that include a £45 million ($74 million) budget for IoT projects, tripling what was already available, and a £1 million ($1.3 million) European grant fund for companies investing in IoT. A UK government-backed consortium of companies has launched a new open specification called HyperCat, with £6.4 million ($10.5 million) in funding from the UK Technology Strategy Board, to support M2M interoperability by leveraging an online metadata catalog for universal communication between IoT devices. The UK financially supports their experts to attend standards meetings.

Industry 4.0 started as a German initiative. Industry 4.0, Industrie 4.0 or the fourth industrial revolution, is the current trend of automation and data exchange in manufacturing technologies. It includes cyber-physical systems, the Internet of Things and cloud computing. Industry 4.0 creates what has been called a "smart factory". Within the modular structured smart factories, cyber-physical systems monitor physical processes, create a virtual copy of the physical world, and make decentralized decisions. Over the Internet of Things, cyber-physical systems communicate and cooperate with each other and with humans in real time, and via the Internet of Services, both internal and cross-organizational services are offered and used by participants of the value chain. This initiative is highly focused on the German industrial complex and spearheaded by Bosch and Siemens.

So the reference architectures and interoperability framework efforts are being driven by forces outside of the U.S. What about things like Privacy and Security?

I think I can safely say that Privacy is being driven by the European Union. The French representative to ISO/IEC JTC 1/WG10 categorically stated that the European Commission is a forerunner for all privacy concerns. It has regulation governing privacy has now been published and that this regulation and approach will surely be extended to all IoT applications regardless of the data capture technology used. This is the ISO 29134 Privacy Impact Assessment—Methodology. What's the effect? What about the recent Facebook, Yahoo, Google, etc. data use issue?

And with China driving the IoT Interoperability Framework, I'd note that the key contributors are from Chinese universities, Wuxi Sensor Network, and Huawei. With these as the key players, I'd be surprised if the U.S. IoT security concerns are met or considered.

What missing from developing these standards? The U.S. has 40 registered experts but only 14 are active at a given time with less than a half a dozen at any given international meeting. In fact, at the last meeting in Berlin, the U.S. only had four experts, three of whom had never participated before.

Our next panelists are Gary Moe, President of ID Integration, and Bob Fudge, Vice President of Public Sector Business for Evanhoe & Associates. They are here to provide a view on opportunities for DoD and the Federal government as IoT end users. Gary & Bob….

Bob Fudge

- **Chairman | Automatic Identification Technology Alliance (AIT Alliance)**
- **Vice President | Evanhoe & Associates**

Precision Logistics and the Internet of Things. I was a maintenance officer with the B-2 Stealth bomber in 1996 when one of those aircraft demonstrated for the first time the ability for one aircraft to strike sixteen different targets on a single mission. Before that day, since the dawn of the aircraft in combat, we talked about how many aircraft it would take to neutralize one target. And yet we succeeded by arming and launching enough aircraft to do the mission…because that's what our nation's warriors do, accomplish the mission through whatever brute force it takes. These days we talk about the number of targets per aircraft because we've perfected the art of precision bombing…during Operation DESERT STORM less than 15% of the weapons we used were "smart bombs", resulting in an "on target" rate of roughly 25%. Nowadays we use less than 5% "dumb bombs" and have an "on target" rate of over 95%. Obviously, that revolutionary change was accomplished through technology like GPS and improved communications systems. Unfortunately, the logistics tail that supports getting those bombs on target has not yet undergone a similar revolution. Our data capture procedures are mostly paper-based and inefficient, but our troops still accomplish the mission through the brute force of throwing people, parts, and machinery at the problem. It's an unsustainable model in a fiscally constrained, technology-focused environment.

We have the technology to improve mission effectiveness; save taxpayer dollars; and make life easier on our troops. What we need is a strategy to accomplish it and the political will to make it happen. Insertion and adoption of autonomous data capture technology, when associated with smart "things", and combined with data analytics capabilities, will help us develop a precision logistics system.

Identify the Things

The exercise of uniquely identifying the "things" we want to track and associating those things with barcode, tag, or sensor will: 1) lay the foundation for machine-to-machine communication; 2) enable automated data capture; and 3) one we discovered with the US Air Force, will clean up the inventory accuracy, identifying excess, unneeded, or missing items. The DoD already has a policy for laying in the machine-to-machine communication foundation. DODI 8320.03 *Unique Identification (UID) Standards for Supporting DoD Net-Centric Operations,* dated November 4, 2015 (replacing the one from 2007), directs the adoption of unique identifiers for people (EDIPI), tangible personal property (IUID), organizations (OUID), real property (RPUID), and cargo (TTN). Those common identifiers reduce confusion and enable cleaner data exchanges across DoD and NATO information systems, and serve as the basis for enterprise asset visibility initiatives. So generally the things we want to track are people, parts, places, weapons systems, and transportation activities. The next question is where do I want to track them and why?

Define the Processes

Process analysis will help us identify visibility touch-points across the supply chain (by that I mean the entire life cycle of a weapons system and it's serially-managed parts) and applying the appropriate autonomous data capture method at those points with barcodes, pRFID, aRFID, GPS, etc. It's not necessarily economically feasible to track everything, everywhere, all the time. A business decision should be made at the enterprise level for choosing what to track. The next question is how, and related to the analysis above should meet the requirement at the lowest cost possible without compromising mission necessity.

Train the People
People are our most precious resource, but there are increasingly fewer troops available and they are busier than ever. And maintaining an overused, quickly aging fleet of aircraft (and ships, tanks, etc.). We need our troops operating in optimal health, with the ability to perform a cross-section of tasks in often austere and hostile environments. Two potential IoT applications include in-service passive health monitoring to ensure the human machine is optimized and skills identification and augmentation with situational augmented reality that could provide virtual on-demand job-aiding and training assistance.

Attach or Embed Sensors
Weapons systems and their components are currently tracked and maintained as if each of them is like the others. For example, all F-16s are removed from the operational when they reach 600 flying hours (these number are representative) because engineers have determined that some components on some F-16s have a risk of failing at about 700 hours. Uniquely identifying critical components and tracking actual life cycle events against that actual component will enable "condition-based maintenance" or CBM, which in most cases will allow aircraft to stay in the operational fleet longer and ultimately reduce the cost of maintaining the fleet. A logical extension of a CBM maintenance philosophy will be a just-in-time supply chain where parts arrive as needed instead of sitting on a shelf. Again, that will require enterprise visibility of the supply chain (suppliers, warehouse, transportation nodes, and item condition/status) supported by AIT and IT systems. Let me highlight that part…we have to smartly modernize our IT systems to support improved data transactions. Several of the services have spent billions of dollars on Enterprise Resource Planning systems that can't handle simple things like barcode scans, RFID reads, or the UID data elements discussed above.

The industrial base supporting a precision logistics environment presents another opportunity for budget shifting. Depot level maintenance described above results in the vast majority of the industrial energy expended by the Air Force. Installing environmental sensors throughout the depot complexes, when combined with reducing the depot workflow, will save millions of dollars that could be used to buy new aircraft, ships, tanks, etc.

What do we need to make it happen?

- Things identified
- Processes identified
- "Sensors" attached/embedded
- IT systems modernized and secured
- Infrastructure laid in/data capture devices fielded
- People trained

Gary Moe

- **President | ID Integration, Inc.**
- **Member | AIT Alliance**

IoT, people, and services are transforming the way manufacturers do business

Digital disruption means innovation and revenue - Industrial manufacturing companies reported an average 28.5% revenue increase from IoT[1]

Business must become more responsive - 40% of industrial manufacturers use digital technologies to monitor products sold to customers[1]

Customer experience matters most - 89% of leaders believe that customer experience will be their primary basis for competition by 2016[2]

Source: 1) TCS Global Trend Study – July 2015; 2) Accenture Technology Vision 2015

Manufacturing – IoT use cases - Top 3 Manufacturing Business Priorities

Design & Customer Service

- Product Monitoring with Telemetry – Connected Products, Connected Equipment
- Customer Insights from Product Usage
- Single view of customer / product / Customer Golden Record
- Insights for Improved Product Design

Manufacturing Optimization & Innovation

- Connected Manufacturing
- Yield & Quality Optimization
- Control Quality proactively with Real-time Manufacturing data Insights
- Predictive Equipment Maintenance to avoid manufacturing stoppages
- Warranty & Recall Management
- Energy Management

Supply Chain Efficiency

- Granular n-tier Supply Chain Visibility
- Assure Just-in-Time Delivery of Raw Materials
- Supply Chain Risk Management
- Connected Logistics
- Increase Operational Efficiency

Accenture reported that manufacturers using IoT for Predictive Analytics Reduce Maintenance Costs by 30% and Breakdowns by 70%

GE Aircraft Engines and Rolls Royce are using IoT for insights to improve aircraft performance, safety and maintenance. Engines have hundreds of sensors that communicate data to the Cloud. Results are:

- More efficient flight and maintenance plans
- Targeted and actionable fuel efficiency insights
- Quickly-generated reports and dashboards that tell compelling stories and deliver high-quality insights

Data volumes associated with the Industrial Internet are growing at twice the pace of other sources of Big Data, including social media - Wikibon Analysis

One final thought - it is imperative that we need to get good data and item/product traceability. Without traceability and good data we cannot get good data analytics to help with life cycle tracking, performance and condition based maintenance, financial accountability which impacts the readiness of our military and puts an extra burden on our warfighters!

Chuck Evanhoe

- **President & CEO | Evanhoe & Associates**
- **Chairman | AIM, Inc.**
- **Chairman | INCITS IoT10 Technical Committee on ISO/IEC IoT Standards**

In Summary. What's missing from a U.S. perspective?

- Defined National Strategy that supports the open market environment but ensures that the U.S. ability to compete is not overwhelmed by other national or international bodies.
    - Coordination and agreement between Executive and Legislative Branches
    - Map out concerns and paths forward
        - National security
        - National interests – commercial and consumer
        - Privacy
        - Security
        - Interoperability
        - Bandwidth
        - Standards
- We need more experts who are active in standards to ensure that U.S. views are not discarded at the international level.
    - Some major U.S. entities are not as invested as we need to achieve results that are inclusive of U.S. interests
    - Working group activities are based on experts, not national bodies
    - US has only averaged 4 experts at the recent meetings
    - China and Korea average more than a half dozen experts to meetings to help achieve consensus around their ideas
- More interested US entities involved in developing open standards through ISO/IEC JTC1 process
- Who's missing?
    - Google
    - DoD
    - Many others
- Who's pulling back due to the turmoil created by Chinese and South Korean dominance, funding and other similar issues?
    - NIST
    - Microsoft
    - Oracle

Who's missing from your district or state?

AIM Perspective

"The best way to predict the future is to create it." – Abraham Lincoln

- IoT is here and the IoT market is exploding
- IoT can make consumers and businesses more connected and productive
- Consumers will be key IoT users, but this is more than a wearable...Fitbit, Apple Watch, etc.
- Privacy and security concerns need to be addressed
- IoT will drive "Big Data" both for good and bad
- Foreign interests are leading the charge and are not necessarily in the best interests of the US

AIM is an unbiased, global organization and is here to help!

AIM members are leading in IoT standards and technologies both in the US and globally but AIM technologies only enable the IoT...we want to help others use the data we capture and provide.

Automatic Identification and Mobility (AIM)
AIM is a not for profit international industry association, resource, and authority for automatic identification & data capture innovation and technologies, such as barcode, radio frequency identification (RFID), the Internet of Things, among others, serving members as a trusted resource for nearly 50 years. AIM members are manufacturers, distributors, re-sellers and end-users of IoT and other automatic identification solutions.

AIT Alliance
The AIT Alliance is a not for profit trade association comprised of Automatic Identification Technology (AIT) suppliers and manufacturers dedicated to raising awareness about AIT and encouraging the adoption of AIT policies within U.S. government agencies, primarily the Department of Defense, and within the U.S. government contractor community.

Zebra Technologies Corporation
Zebra builds tracking technology and solutions that generate actionable information and insight, giving companies unprecedented visibility into their businesses by giving physical things a digital voice. Zebra's extensive portfolio of solutions give real-time visibility into everything from products and physical assets to people, providing very precise operational data not only about where things are, but what condition they are in.

Evanhoe & Associates, Inc.
Evanhoe & Associates, Inc. is a full-service IT Solutions Provider and Systems Integrator. Evanhoe is a service-disabled, veteran-owned small business (SDVOSB) and focused on accurate, actionable data provided by data capture, management, cleansing, aggregation and presentation solutions.

ID Integration
Is a leading systems integrator for direct part marking systems in manufacturing facilities for regulations specified by the United States Department of Defense (DoD) and the aerospace industry. Their expertise lies in integrating marking, reading, and verification systems into their clients' ongoing processes to permanently mark parts with machine-readable barcodes, including data-rich 2D Data Matrix barcodes.