IOT Week 2017: Industrial IOT

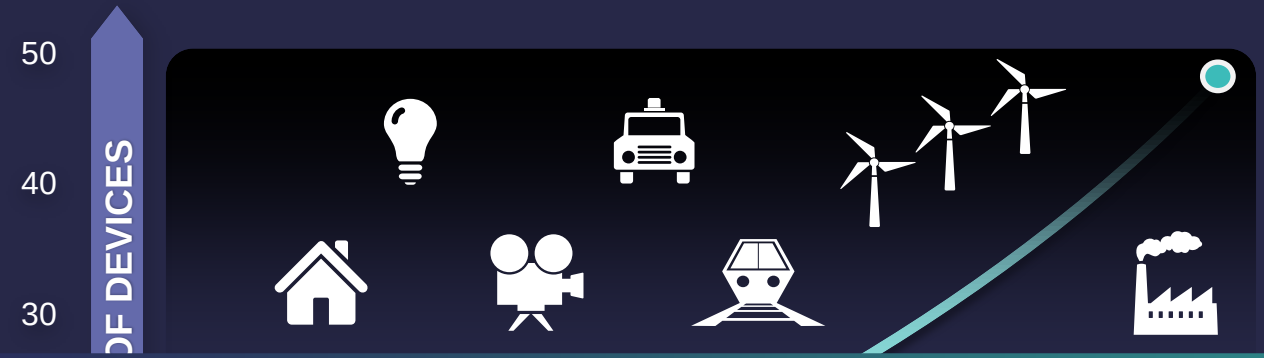
Patrick Wetterwald, CTAO IOT Standards and Architecture

ETSI IP6 Vice Chairman, IEC SEG8 Chair, IPSO Alliance Past President

pwetterw@cisco.com

June 6th , 2017

IoT Is Here Now – and Growing!

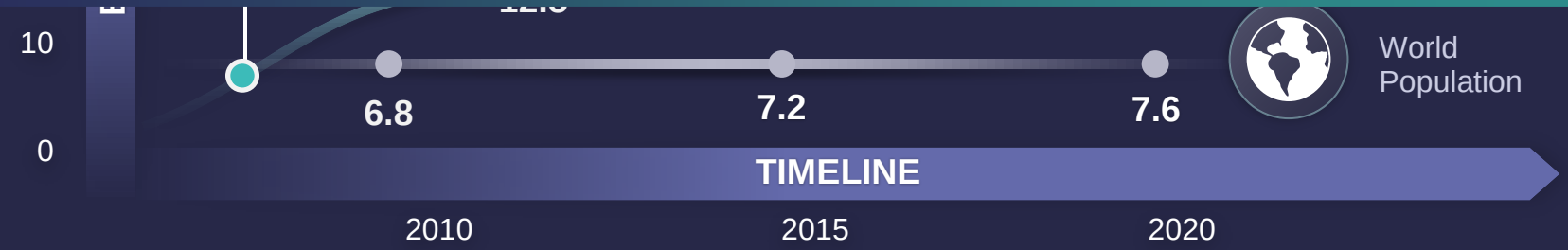


50 Billion

"Smart Objects"

Rapid Adoption Rate of Digital Infrastructure:

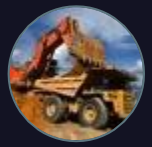
The New Essential Infrastructure



Source: Cisco IBSG, 2011

What Industries Are We Focused On?


Manufacturing


Mining


Energy-Utility


Oil and Gas


Transportation


City


Defense


SP/M2M



REAL TIME SCALE BIG DATA/ANALYTICS SECURITY



"In this decade, our industry will transform more than in the last century – through new markets, new technologies and new business models"

Dr. Dieter Zetsche
Chairman Daimler AG

"This is about a business change, to make our manufacturing facilities more flexible, more agile and more lean"

Kirk Gutmann GM Global Information Officer, Manufacturing and Quality

The New Digital World

Accelerate Business Processes, Introduce New Services

FANUC

Fanuc Robots

Lower Downtime

Maximize OEE

SUB-ZERO

Sub-zero

Faster New
Product Introduction

StanleyBlack&Decker

Stanley Operations

Reduce Defects

Increased Productivity

Continental

Continental Factory
Automation

Lower Inventory

Del Papa
Distribution Center

Reduce Risk

Increased Capacity

“Digital disruption will displace 40% of incumbent companies in the next 5 years.”

- John Chambers, Cisco 2015 Partner Summit

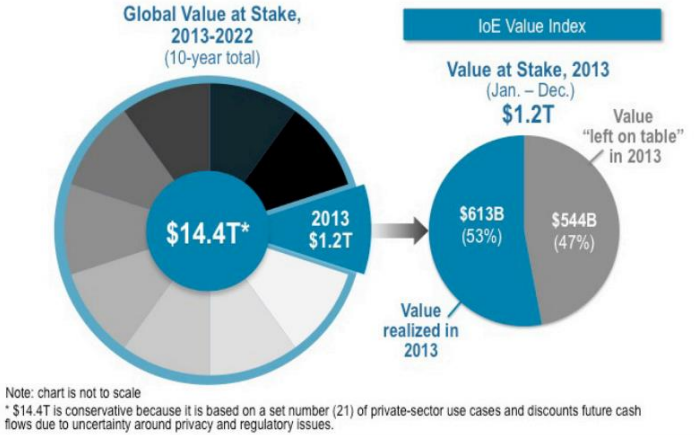
The Industrial Internet of (Every)thing

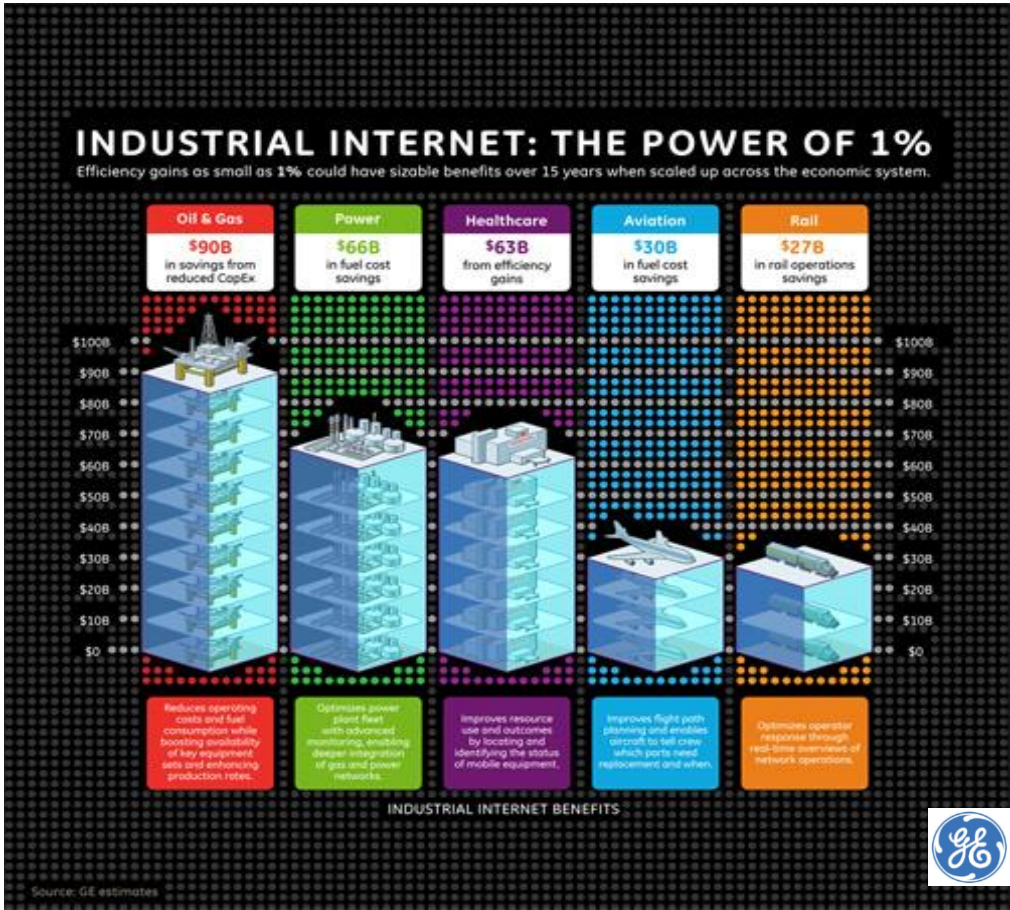
Converge Control Networks to IP

- Make IP operations more efficient
- Emulating existing Industrial protocols

Beyond Control and Automation

- Optimize processes (by 1%?)
- Leveraging IT, Live big data and Analytics





Digital Manufacturing

For higher operational efficiencies,
improved quality and reduced risks

Challenges and Trends Driving Change in Manufacturing

Challenges

- Speed
- Simplicity
- Innovation

Trends

Supply Chain

- Right- Shoring
- Capacity Rationalization
- Bigger Regulation and compliance standards

Demand Chain

- Mass Consumerization
- Fast Changing Consumer Trends
- New Digital business models

Connected Factory Solutions

Factory Analytics and Big Data

Factory Virtualization

Factory Wireless

Factory Network

Factory Compute

Factory Collaboration

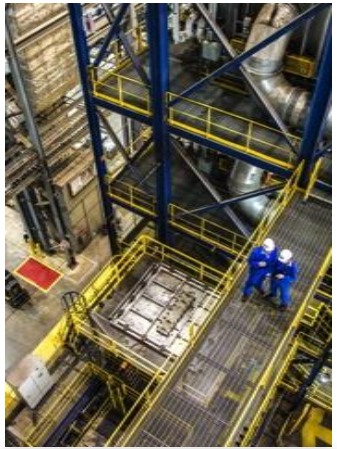
Connected Assets

Connected Machines

Factory Security

What If You Could…

Reduce downtime?



Introduce new products faster?

Achieve real-time visibility?

Better manage global supply chain?

Protect company from security threats?

Key Benefits

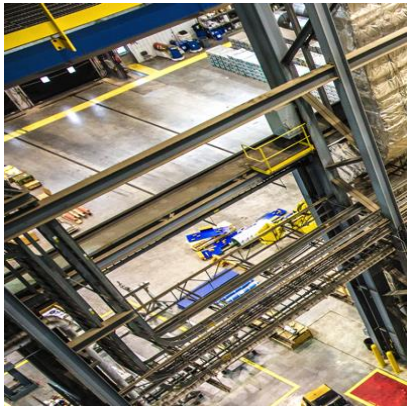
Agility

- Reduced NPI cycle
- Flexible Production
- Better Production planning

Visibility

- Improve quality
- Better asset tracking
- Lower inventory

Operational Efficiency



- Reduced downtime
- Increased OEE
- New business models

Safety and Security

- Real-time monitoring
- Reduce factory vulnerabilities
- Minimize Cyber theft

Converge Multiple Proprietary Systems onto a Single IP Network

Adopting the Converged Industrial Network

70% of manufacturing executives are focusing on plant floor data initiatives to drive **operational and business excellence**

– Empowering Decision Makers — Aberdeen Group

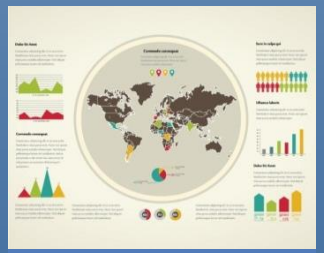
IT Enterprise

Manufacturing Floor

- **Reliability**
  - Wired and Wireless
  - Lower Latency
  - QoS
- **Real-Time**
  - Analytics
  - Access to plant performance
- **Immediate Access to**
  - IACS data (Historian)
  - Device, sensor and machine status

Convergence Driving Adoption of The Internet of Things

Sensors



Real Time Analytics

Personal Devices

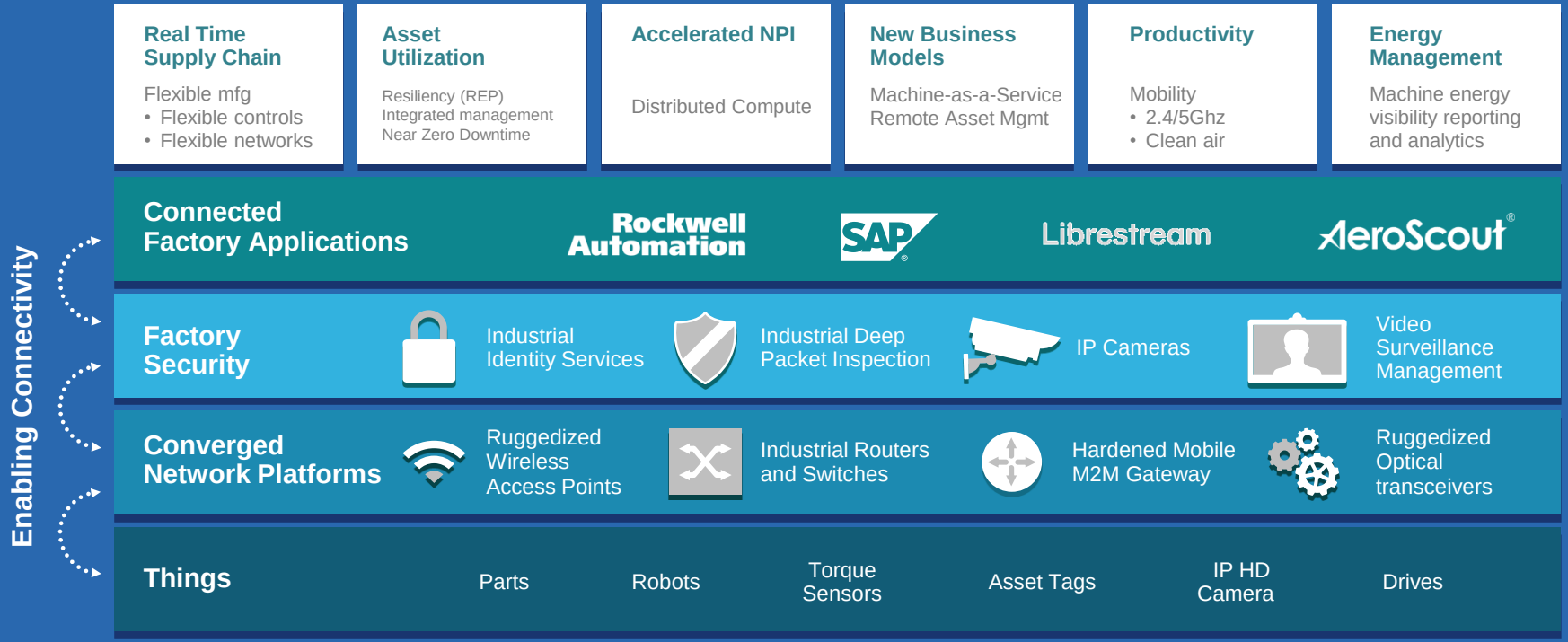
Robots

Security Devices

Sensors Everywhere | Machine-to-Machine | Pervasive Intelligence | Automation

Less Waste, More Efficiency, More Cost Savings
Constant Improvements in Productivity
Enhanced, Personalized Experiences

Building to the Factory of the Future



Real-Time Application Classes

	Process Automation	Factory Automation	Motion Control
			
Function	Information Integration, Slower Process Automation	Time-critical Factory Automation	Motion Control
Comm. Technology	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, etc.	Hardware and Software solutions, e.g. CIP Motion, PTP
Period	1 second or longer	10 ms to 100 ms	<1 ms
Industries	Oil & gas, chemicals, energy, water	Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical	Subset of factory automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing

Source: ARC Advisory Group

Time Sensitive Networking

Cisco Connected Factory for Industrie 4.0

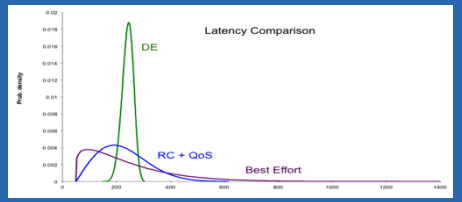
Time Sensitive Networking	Cisco Industrial Network Director	Connected Asset Manager for IoT Intelligence

Securely Connect, Extract, and Manage Data for Improved Business Operations

Deterministic Ethernet

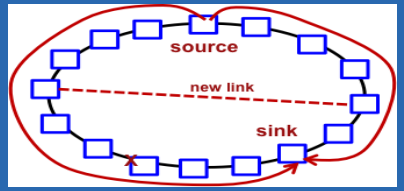
Characteristics for Real time applications

- Low Latency & Packet Jitter
  - Measured in microseconds



Automation & Control
Rate Constrained
Best Effort

- Control traffic immune from impact of other traffic
- Guaranteed delivery & resiliency



Multiple Deliveries

- Time Synchronization
  - Measured in nanoseconds

ARINC

TÜV Rheinland of North America, Inc. US

Example Deterministic Ethernet use cases today for controls

Wind Turbines

- Safety certified control system (integrated approach to networking and control)
- Reduced total cost of ownership for end user from higher availability of system

Oil and Gas

- Process control system
- Expanded existing control system with determinism
- Cost-effective to operate, simple to upgrade and maintain

Automotive
(from 2016)

- Automotive in-vehicle network for control
- High performance, cost-effective, weight reducing from integrating safety and non-safety traffic on one network

Space

- Spacecraft backbone Network, redundant fail- operational network
- Enabled robust network where maintenance is not an option

Aerospace and Defence

- Avionics Backbone network, simple redundant mechanisms that fulfill fail operational requirements
- Enabling highest performance

Deterministic Networks with TSN

IEEE 802.1 Key Advantages of TSN

Secure
Simple
Intelligent

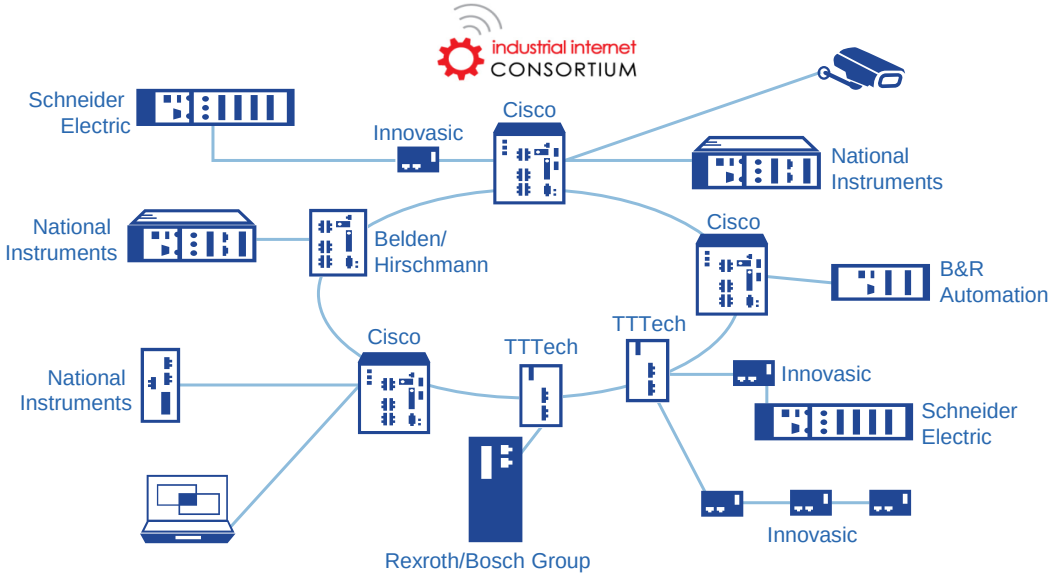
Guarantee delivery and bandwidth for critical data flow	Guarantee latency for data delivery	Converge networks save operating costs	Increase data availability	Leverage Ecosystem Expertise
100%				intel, TTTech, National Instruments, ABB, Schneider Electric, BOSCH

Growing Ecosystem of TSN Vendors at IIC

Secure
Simple
Intelligent

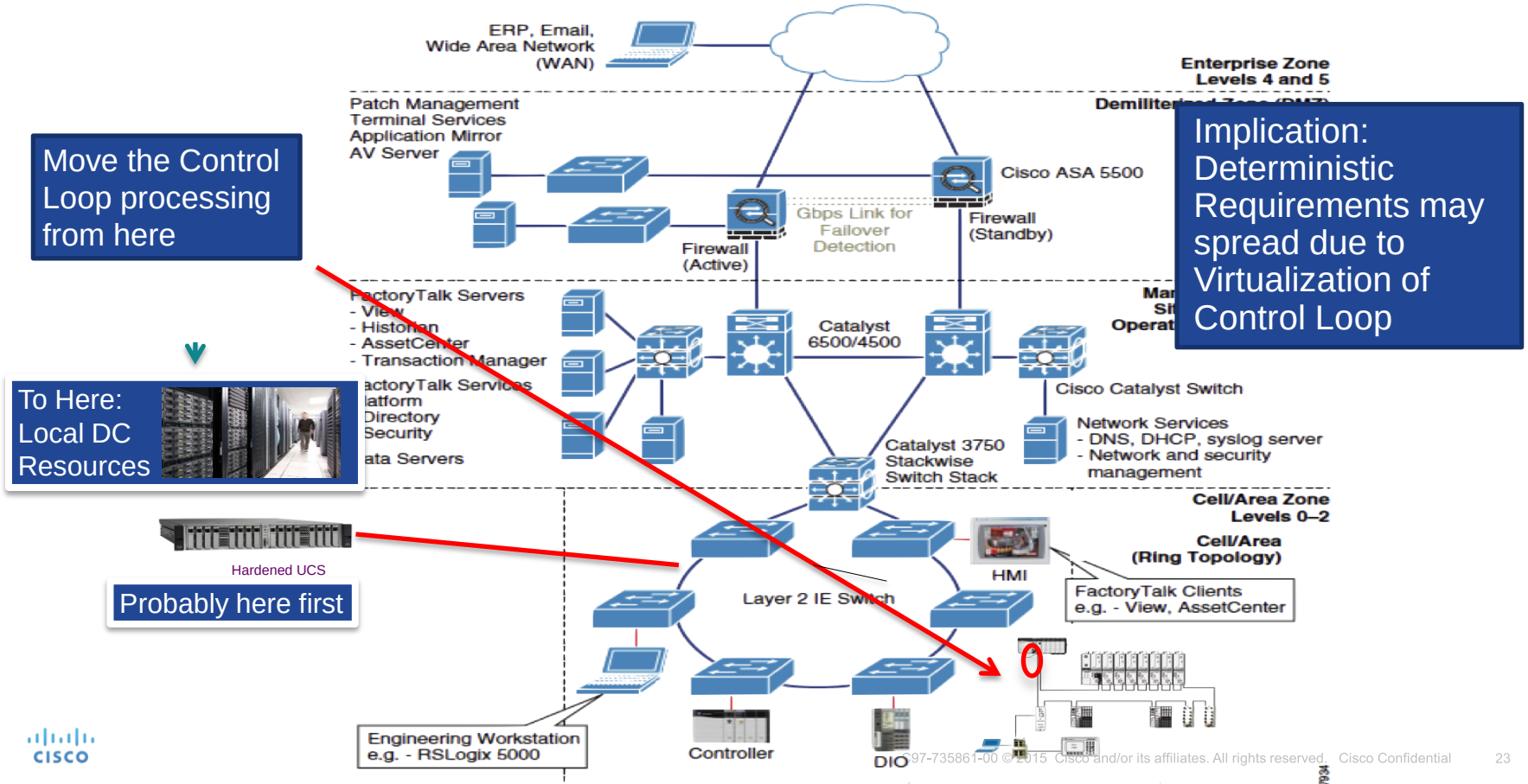
Key Facts:

- **18 Vendors** participating today
- **6 Plugfests** conducted
- **2 Testbed facilities**
- **Demonstrations at 6 major shows**
- **Collaboration with multiple standards**



AVNU · cisco · intel · HIRSCHMANN A BELDEN BRAND · ixia · Innovasic · NATIONAL INSTRUMENTS · OPC UA · B&R · ABB
Rexroth Bosch Group · Schneider Electric · TTTech · ANALOG DEVICES · SICK Sensor Intelligence. · RENESAS · hilscher · Calnex · KUKA · BOSCH

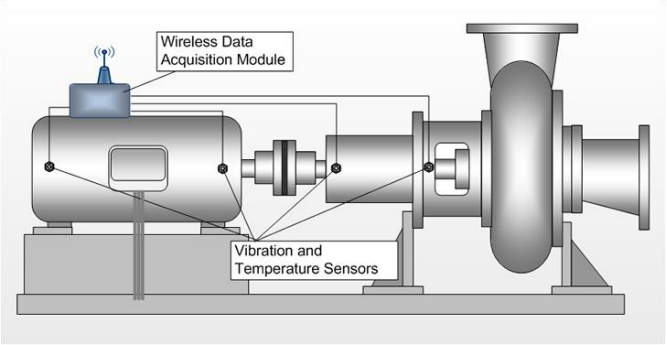
Moving the Control Loop out of the Cell Area expands the footprint of Determinism



Time Sensitive Networking and Wireless

Condition Monitoring and Large Scale Monitoring

- Not Process Control but “Missing Measurements”
  - Reliability and availability are important, which implies
  - Scheduling and admission control
- Scalability
  - 10’s of thousands of new devices
- Deployment cost factor is key

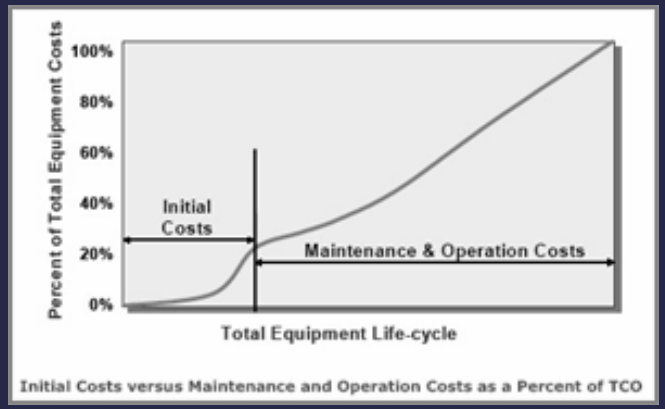


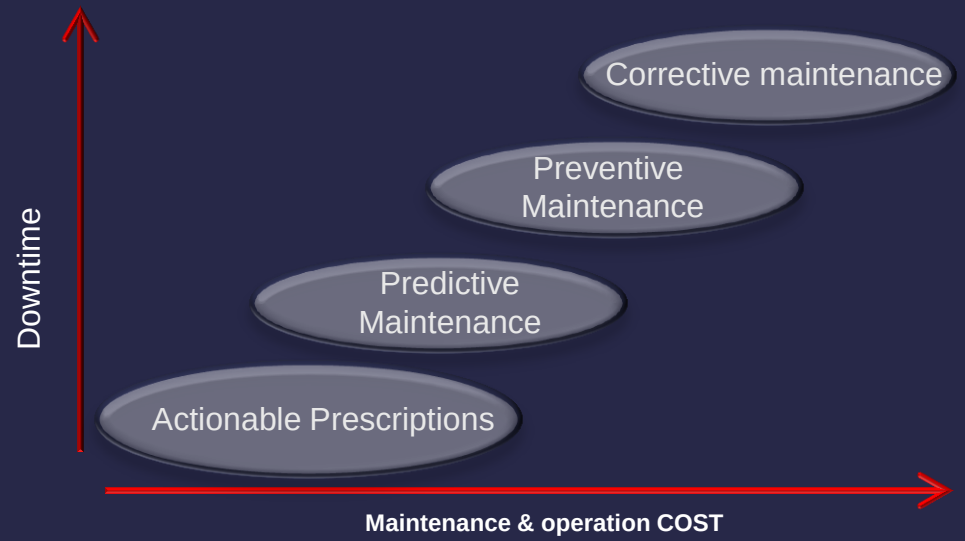
For Emerson this is the **second layer of automation**:

Typically missing are the measurements you need to monitor the condition of the equipment--temperature, pressure, flow and vibration readings you can use to improve site safety, prevent outages and product losses, and reduce maintenance costs of equipment such as pumps, heat exchangers, cooling towers, steam traps and relief valves.

Industrial Internet Application: OPEX reduction

Maintenance and operation represent 75% of the Total equipment cost





➔ Deployment of Wireless sensors is seen as an efficient solution

Wireless Connectivity

New level of cost effectiveness

- Deploying wire is slow and costly
- Low incremental cost per device

Reaching farther out

- New usages / types of devices
- Global Coverage from Near Field to Satellite via 3/4G

BUT

Lack of trust in Industrial vs. Wired
Multiple Interferers, ISM band crowded
Issues with IPv6 for scalability and Mobility

IEC 62591

WirelessHART

IEC based on HART 7.1.

TDMA

fixed time slots (10ms)

Mesh only

Shipped YE-2008.

Vendor driven

Emerson, E&H, ABB, Siemens

IEC 62734

ISA100.11a

ISA100 WIRELESS

IEC based on 2011 revision

TDMA+CSMA

Var. time slots

Star, mesh and hybrid topology

IPv6, 6LoWPAN, TCP-friendly

Shipped mid-2010

Mostly user driven

Honeywell, Yokogawa, Invensys

IEC 62601

WIA-PA

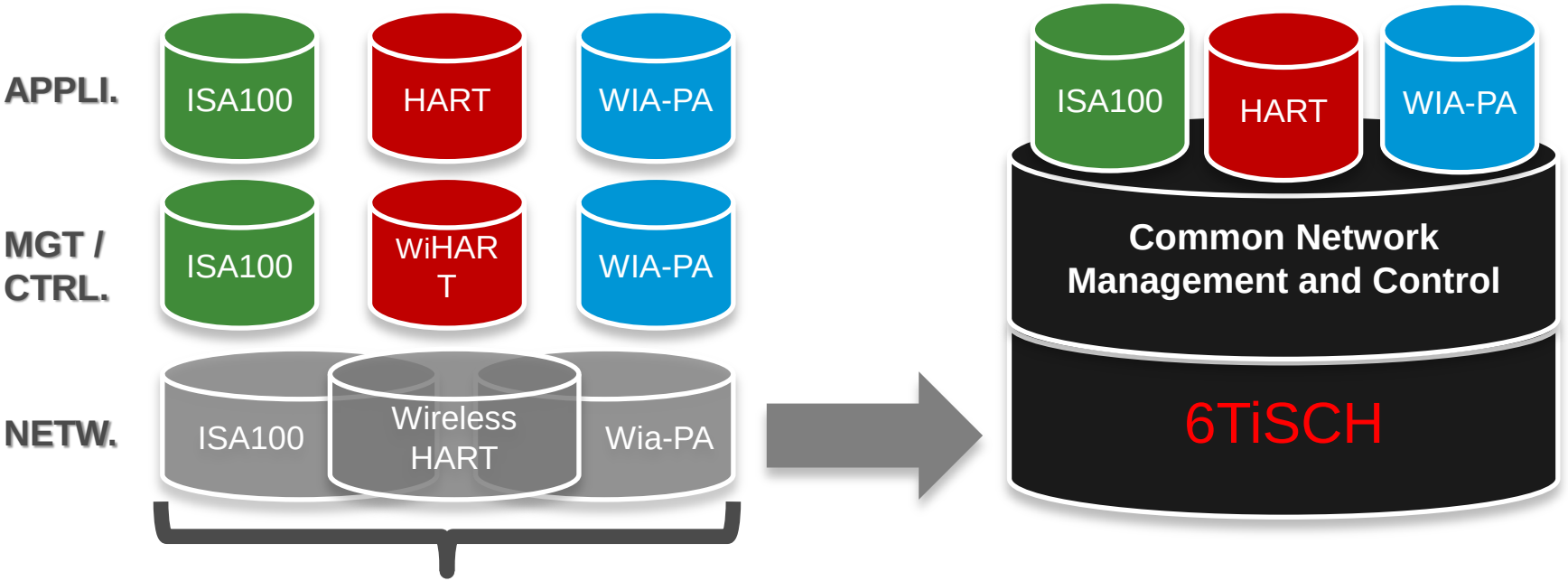
WIA 工业无线网络WIA Industrial Wireless Network WIA

Alternate from China

Star, mesh and hybrid topology

Standardization work started in 2006.

“Single protocol” vs. Converged Network and Control



Requirement for a new standard

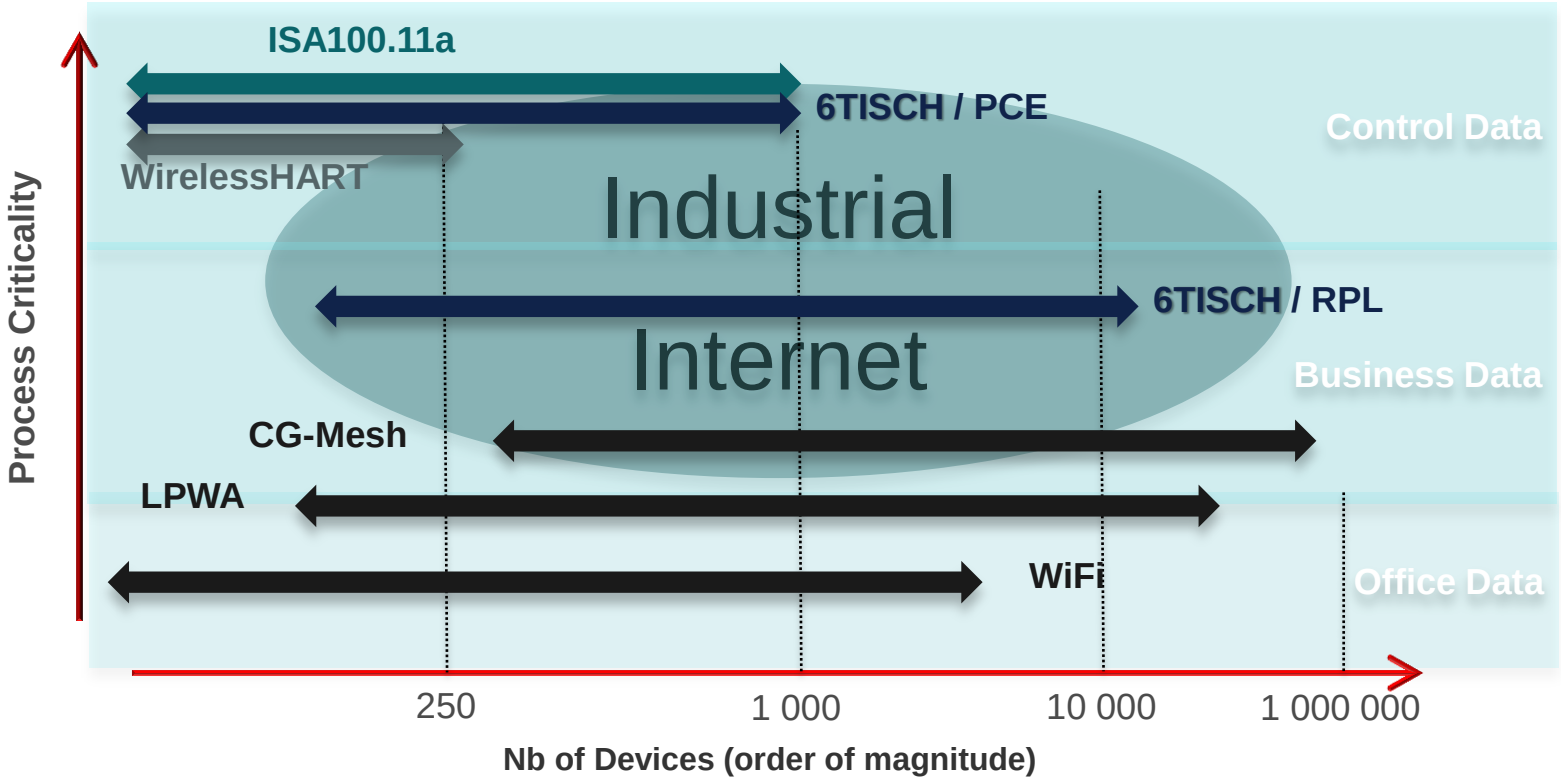
- Industrial requires standard-based products
- Must support equivalent features as incumbent protocols
- Must provide added value to justify migration
- 6TiSCH value proposition
  - Design for same time-sensitive MAC / PHY (802.15.4e TSCH)
  - Direct IPv6 access to the device (common network mgt)
  - Distributed routing & scheduling for scalability (for monitoring)
  - Large scale IPv6 subnet for mobility (50K +)

6TiSCH within Open Standards Reference Model

Open Standards: At All Levels to Ensure Interoperability and Reduce Technology Risk for Utilities

Future Proofing: Common Application Layer Services Over Various Wired/Wireless Communication Technologies

Technologies for the Industrial Internet



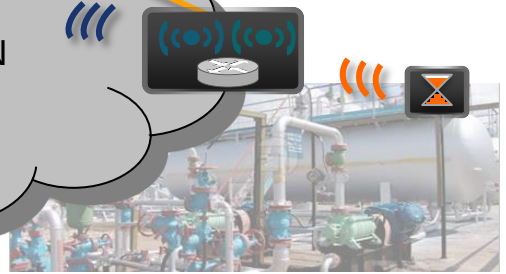
Future Architecture

Enterprise

Wi-Fi or Ethernet
(RPL Domain or IPv6 ND)

6LoWPAN
+ RPL

6LoWPAN
+ RPL



- Plant Firewall
- Wireless Lan Controller
- Integrated Plant Security & Identity services

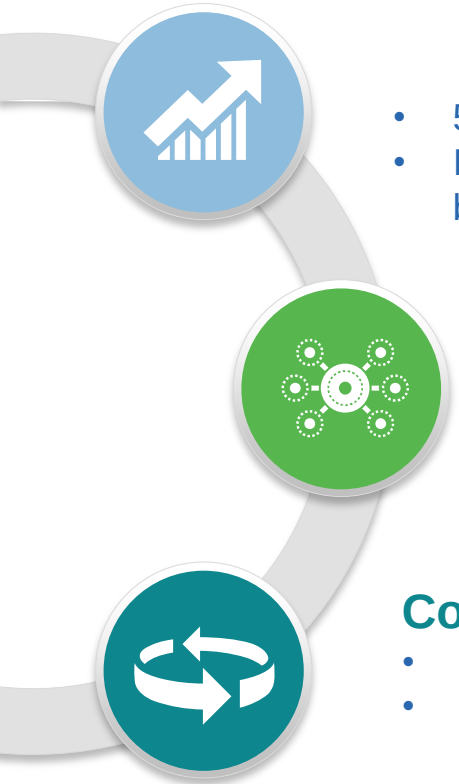
- Wi-Fi Border Router
- WiFi/6LoWPAN RPL Backbone Router
- WiHart Backbone Router
- ISA100 Backbone Router

- WiFi Host
- 6LoWPAN Host
- WirelessHART Host
- ISA100 Host

Securing Industrie 4.0 and the Industrial Internet of Things

Challenges, Frameworks, Architecture and Device Considerations

Challenges and Trends



- 50B connected things by 2020
- IoT devices predicted to account for 83% of all Internet connections by 2020

Connected ≠ Smart

- Devices without system resources to run security
- Security-immature vendors
  - Mirai botnet used hard-coded default credentials -> *not* sophisticated but devastating

Convergence of IT and OT

- IT progressively being given responsibility for security in OT networks
- OT shops cannot ignore security due to regulations and/or proliferation of attacks

Cyber Physical Security Framework
Core Functions

Identify	Protect	Detect	Respond	Recover
Risk Assessment	Access Control	Anomalies & Events	Response Planning	Recovery Planning
Risk Management Strategy	Data Security	Security Continuous Monitoring	Analysis	Communications
Asset Management	Information Protection	Detection Process	Mitigation	Improvements
	Awareness & Training		Improvements	
	Protective Technologies			

Source http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

Recommended Focus Areas
Device Manufacturers

Endpoint Security

- Define different security levels and profiles for IoT endpoints
- Hardware and software development strategy
- Business strategy

Access and Commissioning

- Identify gaps in existing Network Access Security solutions
- Secure Network vs. Controlled Cloud Access
- Commissioning Security

Cloud-based Security Services

- Asset Registration, Configuration Management, Context Service, and Configuration Management.
- Centralized Trust Management vs. Ownership Transfer

Data Analytic and Intelligence

- Data collection and aggregation of IT and OT data
- Network behavior modeling and anomaly detection
- Rule-based security operations

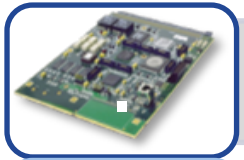
Trustworthy Device Considerations

- Product Assurance

Hardware & Software Authenticity
Counterfeit & Illegal Upgrade Protection
Immutable Product Identity

- Trusted Execution

Boot-Time & Run-Time Integrity
Cyber Resiliency & Tamper Resistance
Strong Crypto & Certifiable Entropy



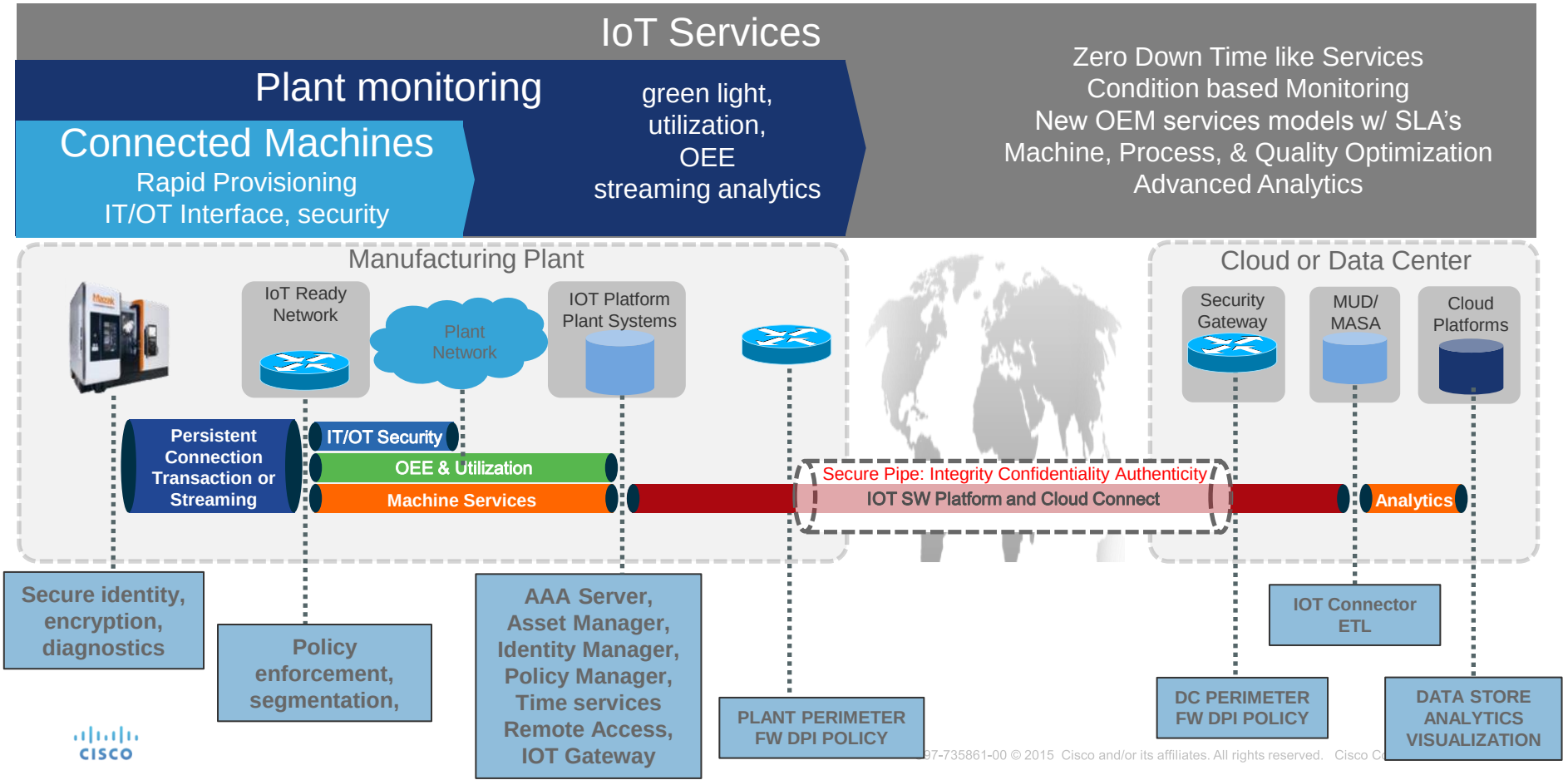
- Embedded Application Security

Secure (Application) Key Storage
Secure Crypto
IP & DRM Protection

- Secure-By-Default & Trustworthy Solutions

Strong Device/Network Authentication
Secure Communication (e.g. TLS, DTLS)
Customer Visible Trustworthy Status

Security Architecture



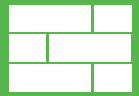
Network Considerations

Visibility & Analysis

Identify & authenticate devices, analyze potential dangerous behavior

Stealthwatch, NGFW-IPS, ISE, Umbrella, Cognitive Threat Analytics (CTA)

Segmentation



Segmented access control of both IT and OT environments

NGFW, ISE/TS, Cognitive Threat Analytics (CTA)

Remote Access

Secure remote access into the OT network

AnyConnect

Security Services

Prioritize critical areas of risk from lower risk

Risk Assessment, Operations/Incident Response

This solution helps to build stronger protection across the IoT environment to reduce unplanned downtime and negative business impact

key take away

Cisco Connected Factory for Industrie 4.0

Secure
Simple
Intelligent

Delivering Business Outcomes for Manufacturers

Security

- Reduce risk
- Protect your IP
- Ensure production integrity

Simplicity

- Automated factory network deployment & Simple management
- Simple plug and play network deployment and replacement
- Easy to configure data visualization and exception reporting

Intelligence

- Manage data in the factory
- Transform data at machine cell edge for improved agility
- Bridge network silos

Thanks You


There's never been a better time to
DIGITIZE MANUFACTURING