



Solving IIoT Security Challenges

10 May 2018





“A fundamental new rule for business is that the Internet changes everything.”

-Bill Gates, 1999

Or has it?





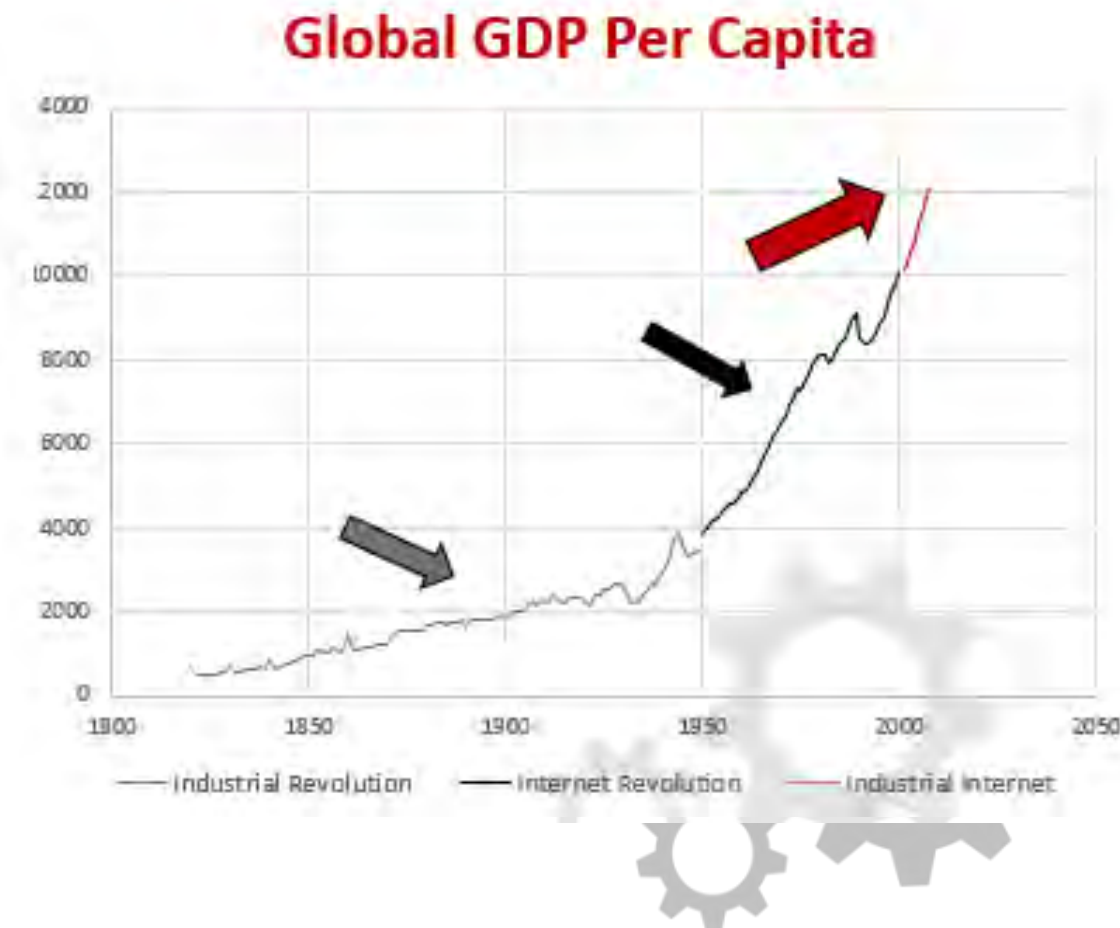
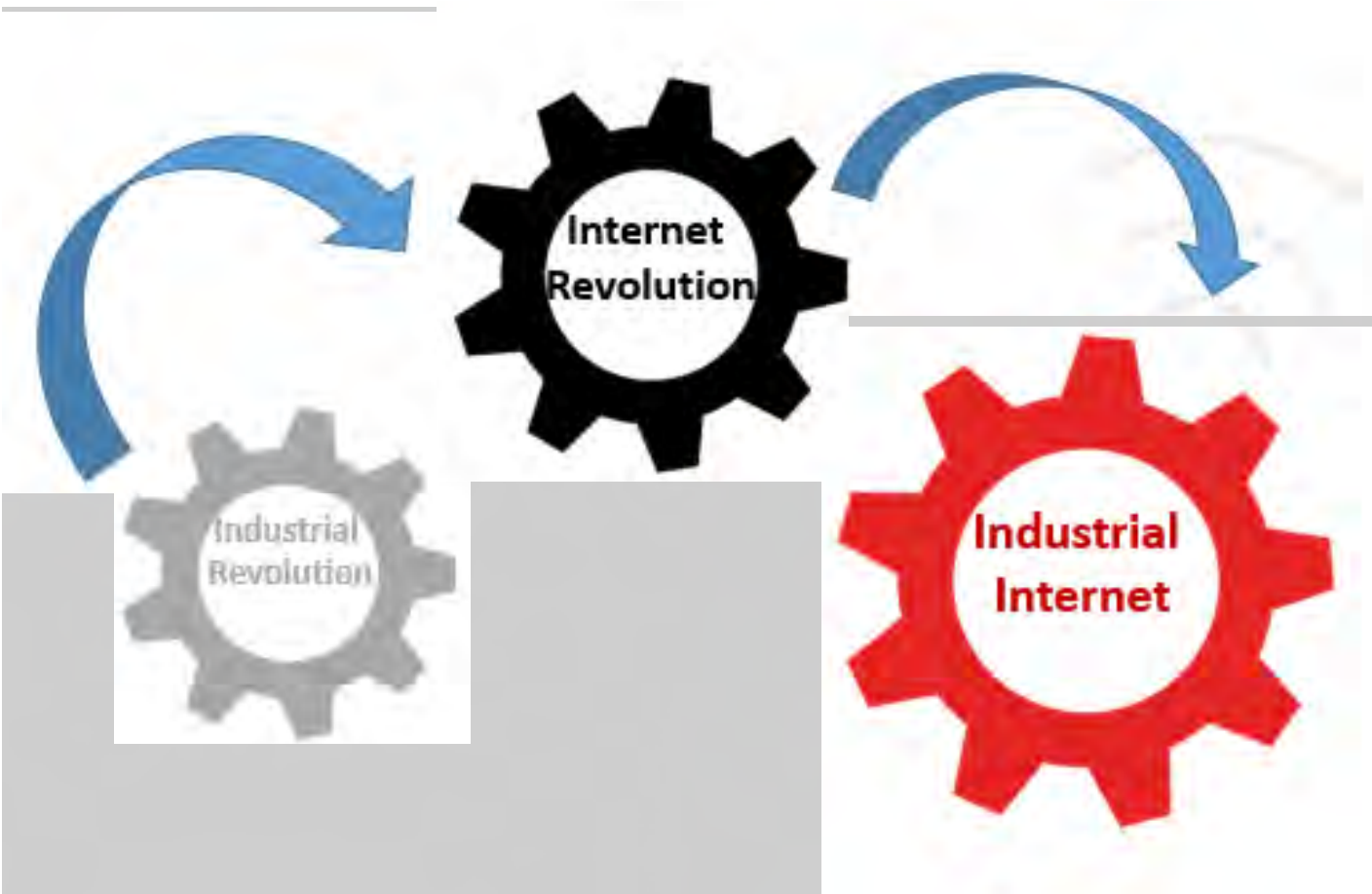
No, the Internet Didn't Change Everything

There is much more to be done:

- Oil & Gas Exploration
 - Geological data integration from multiple sensing sources
 - Jet engine performance management
 - Electric grid transmission management
 - Rail & other transportation
 - Failure sensing and automatic rerouting of multimodal systems, far more extensive than JapanRail automatic stop
 - Smart homes & smart energy usage
 - And on... and on... and on...
-
- *“Internet Thinking” is key to Smart Manufacturing, Smart Connected Products, and Smart Product Data*

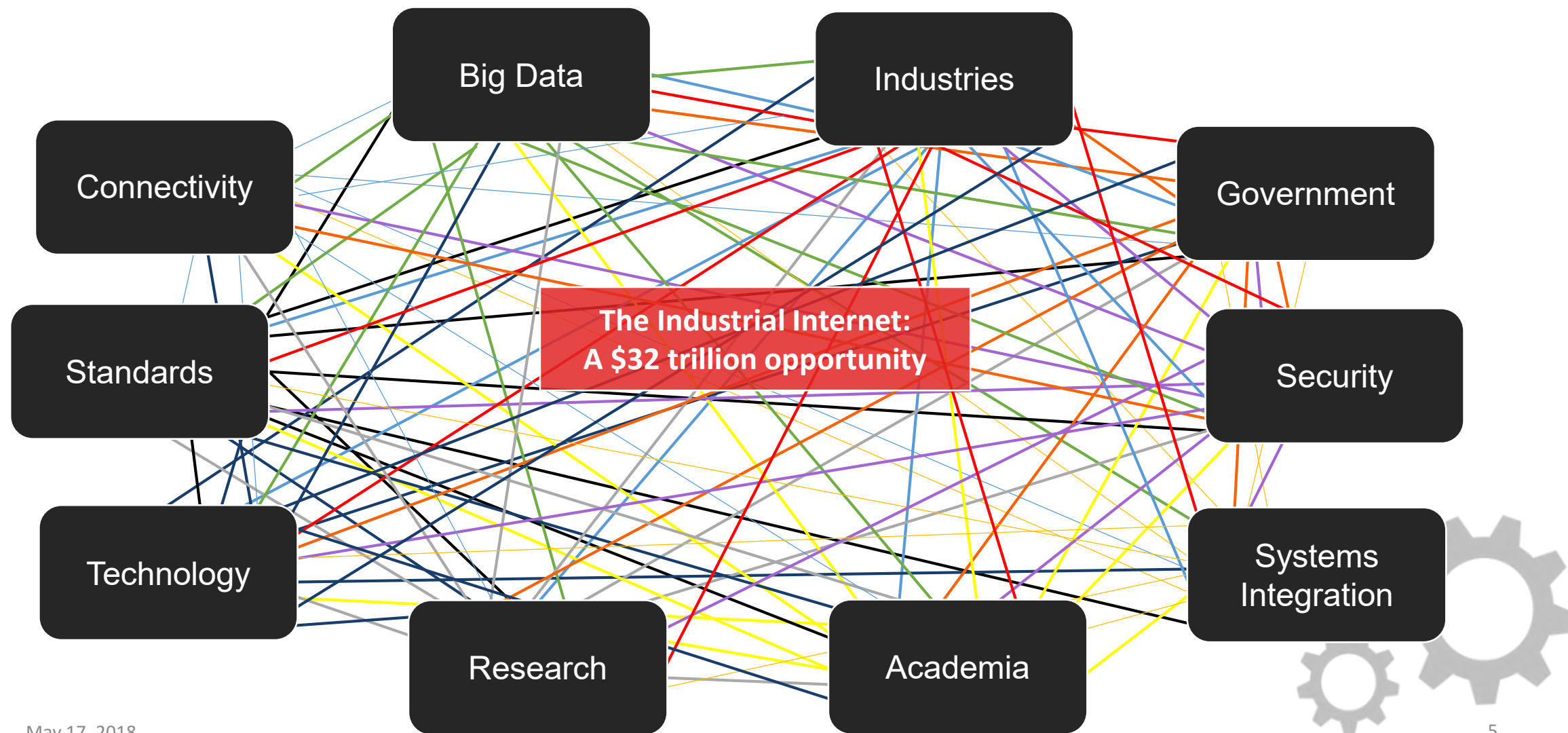


The Industrial Internet is leading the next economic revolution



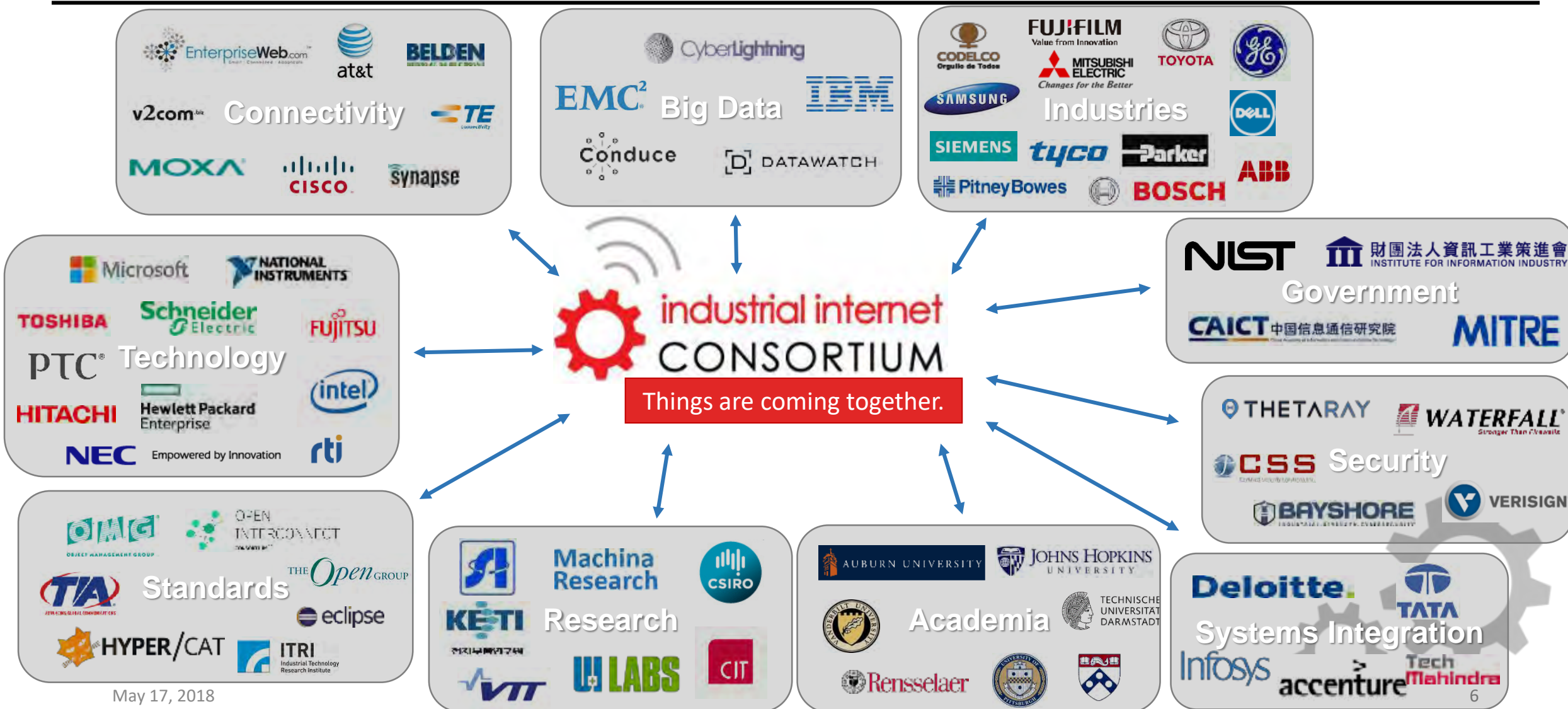


Adoption is Hampered in a Disconnected Environment





The IIC: Things are coming together



Industrial Internet Consortium

Mission

To **accelerate growth** of the Industrial Internet by **coordinating ecosystem** initiatives to connect and integrate objects with **people, processes and data** using common architectures, interoperability and open standards that lead to **transformational business outcomes**.

Launched in March 2014 by five companies:



About 250 Member Organizations
Spanning 30 Countries



The IIC is an open, neutral “sandbox” where industry, academia and government meet to collaborate, innovate and enable.



IIC Founders, Contributing Members, & Large Industry Members

IIC Founding and Contributing Members



IIC Founders, Contributing Members, & Large Industry Members



IIC Small Industry Members



IIC Small Industry Members





IIC Nonprofit, Academic, & Government Members



INDUSTRIE (IFI)



財團法人資訊工業策進會
INSTITUTE FOR INFORMATION INDUSTRY



YNU 横浜国立大学
YOKOHAMA National University



NIST



KEDGE
BUSINESS SCHOOL

CAICT 中国信息通信研究院
China Academy of Information and Communications Technology



wireless
@mit



TECHNISCHE
UNIVERSITÄT
DARMSTADT

MITRE

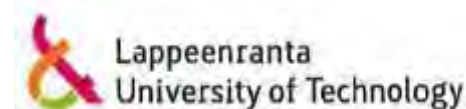
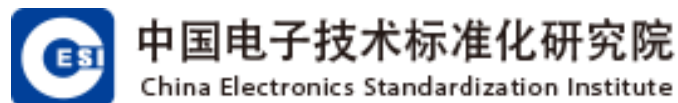


fimecc

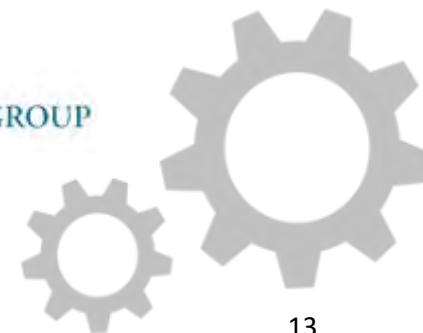




IIC Nonprofit, Academic, & Government Members



TAMPERE UNIVERSITY OF TECHNOLOGY



The IIC and Standards Organizations

The IIC is ***not*** a standards organization. We evaluate and organize existing standards to :

- advocate for open standard technologies, and
- influence the global standards development

The IIC has a formal Liaison team that evaluates potential formal agreements with other organizations.

We are an open membership organization and we work collaboratively on an informal basis with many other organizations, including Industrie 4.0.

The Technology Working Group is currently:

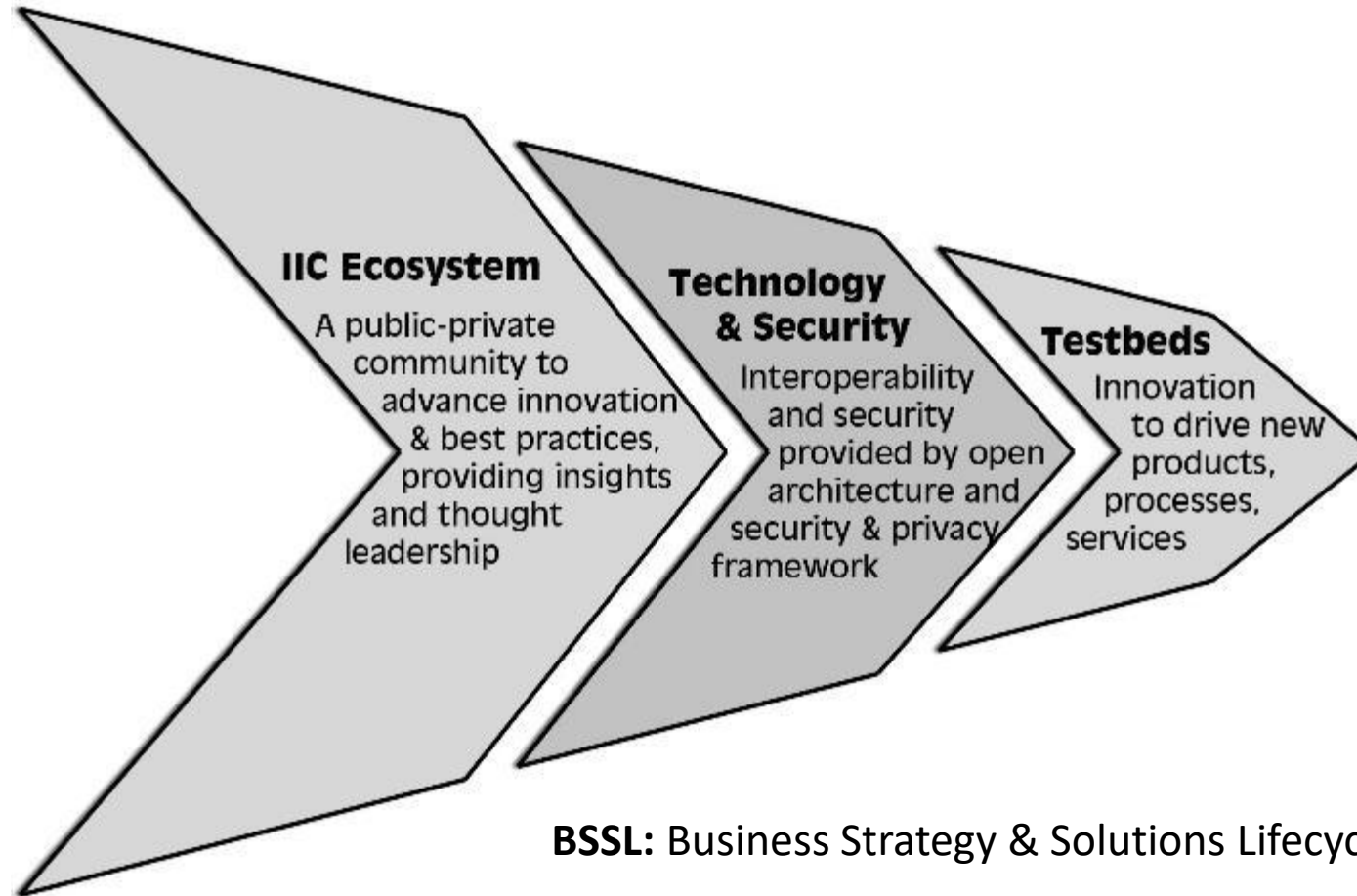
- Evaluating existing standards
- Identifying requirements for the Industrial Internet

IIC Formal Liaisons as of June 2015

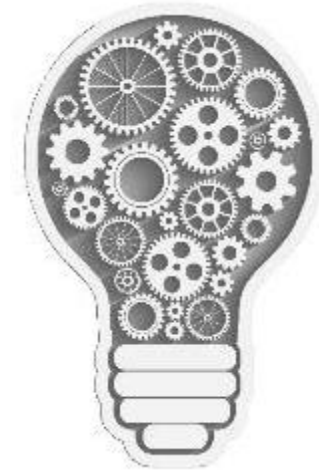




The IIC has three primary areas of activity: Community Engagement, Technology & Security, and Testbeds



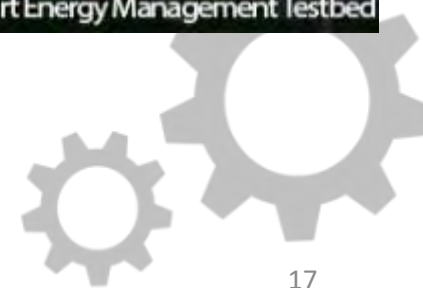
BSSL: Business Strategy & Solutions Lifecycle



Current Publicly Announced Testbeds



Track and Trace: Results from our first testbed





Example IIC Testbed: Track & Trace

Industrial Internet Consortium Member participants:

- Bosch, TechMahindra, Cisco, National Instruments

Market Segment

- Industrial Manufacturing
- Power Tool Fleet Management

Goal

- Manage smart, hand-held tools in manufacturing, maintenance and industrial environments

Features & Commercial Benefits

- Asset Management, Work Management
- Integration with Factory Manufacturing Systems
- Improved Safety and Operational Performance
- Monitor/Control Quality



INFINITE: Learning from the data





Example IIC Testbed: International Future Industrial Internet (INFINITE)

Participants:

- Members: EMC Corporation and Cork Institute of Technology
- Other Participants: Vodafone, Irish Government Networks, Asavie, and Cork Internet Exchange

Market Segment:

- The scale and scope of the project means INFINITE can be used across a wide and diverse range of industries and sectors

Solution:

- Completely virtual domains that are able to be connected via mobile networks
- A solution that allows multiple virtual domains to securely run via physical network.

Commercial Benefits:

- Ideal for mission-critical systems
- Industrial Internet applications in an environment that resembles real-world conditions





Key Safety Challenges of Securing the IIoT

Industrial sectors have long-established approaches to safety, the approaches and standards are still evolving to address new and unique safety challenges that IIoT brings. Key challenges unique to the IIoT that effect safety characteristics:

- **Increased security risks due to an increased attack surface**
- **Convergence of IT and OT**
- **Pervasive autonomy**
- **Inadequate regulatory framework and evolving standards.**





Security Working Group

Charter: To define a security and privacy framework to be applied to technology adopted by the IIC. The framework will establish best practices and be used to identify security gaps in existing technologies.

- **Drive industry consensus**
- **Promote IIoT security best practices**
- **Accelerate the adoption of those practices.**





Industrial Internet Security Framework

- Published September 2016
- Addresses Industrial Internet security issues
- Delivers the adoption model to apply IIoT security techniques
- Unifies Industrial characteristics in terms of trustworthiness
 - Security to enable: safety, reliability, resilience and privacy
- Provides system-wide, top-to-bottom assurance of Trustworthiness
- Applies techniques spanning: endpoints, communications, monitoring, and management
- Tracks future security trends to bring into Industrial Internet when mature





Expanding on the IISF

Expanding on the building blocks of the Industrial Internet Security Framework and The Business Viewpoint of Securing the Industrial Internet

Recently Published

- [Key Safety Challenges for the IIoT](#)
- [Endpoint Security Best Practices](#)
- [Security Maturity Model](#)



Upcoming:

- Communication Security Best Practices
- Data Protection Best Practices
- Automotive Trustworthiness





Trustworthiness: Basis for Industry Adoption of IIoT

- **Industrial Business Benefits from IIoT Trustworthiness**
- **Leverage Trustworthiness to Manage Risk:**
 - increase likelihood of correct business decisions
- **Permeation of Trust:**
 - Assure Trust across the entire Industrial System
 - Component Builders
 - System Builders
 - Operational Users





Endpoint Security Best Practices Document

The Industrial Internet Consortium Endpoint Security Best Practices document recommends best practices for endpoint security in industrial applications under the broader scope of industrial internet security.

- **Provides a common benchmark that may be used to analyze risk and encourage security improvements.**
- **Provides a clear description of what countermeasures and controls are generally recommended for each of 4 levels of security.**
- **Offers guidance for industrial equipment manufacturers, integrators, and industrial equipment owners and operators.**





What is the SMM?

The IISF explains how security fits within the business of industrial operations, relates to the IIC Industrial Internet Reference Architecture (IIRA), defines functional building blocks for addressing security concerns and provides guidance and practical techniques for IIoT security implementations.

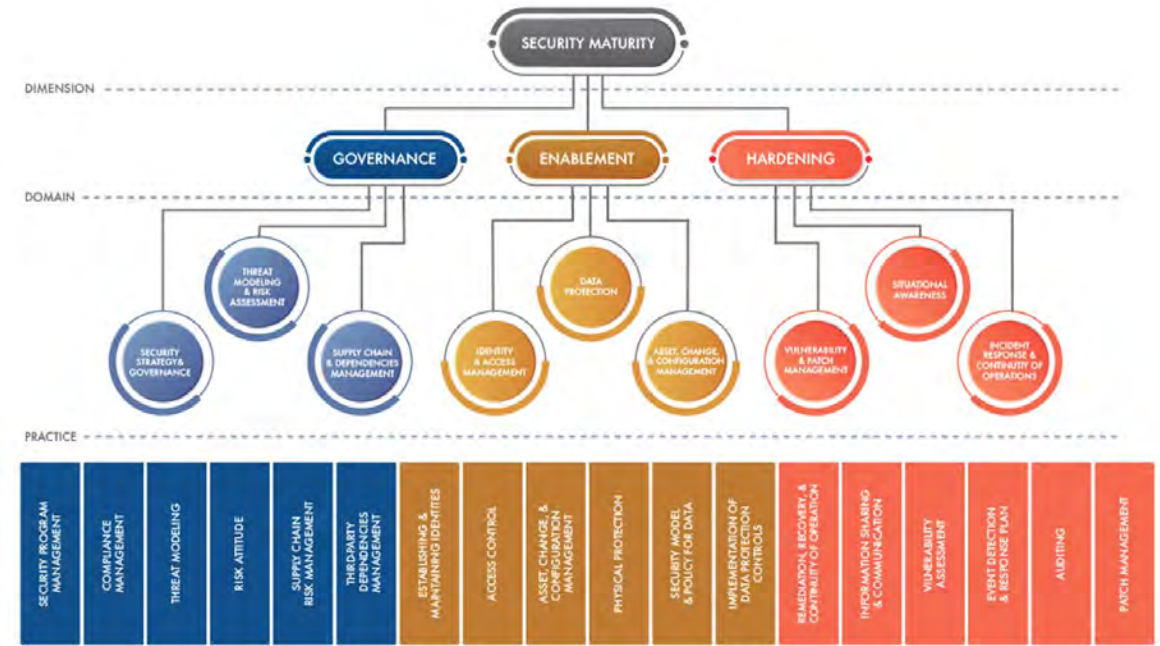
The Security Maturity Model (SMM) builds on IISF concepts, providing actionable guidance for specific IoT scenarios. The goal of a SMM is to enable IoT providers to invest appropriately in security mechanisms to meet their requirements. The SMM helps them understand and make intelligent choices about which mechanisms to use and the mechanism strengths needed considering their specific deployments.





Security Maturity Model: The Challenge

- How can you tell if your IoT solutions is sufficiently secure to address your needs?
- Does it address your requirements and threat environment?
- How do you evaluate the risk consistently?
- How do you identify the actions you need to take including
 - Process improvements
 - Security techniques
 - Security mechanisms





The Future

How will we reduce jet engine failure & maintenance costs?



How will we minimize unplanned factory downtime?

How will we save lives through better patient care?



How will we reduce passenger fatalities?



How will we reduce waste of natural resources?



Things are coming together.





Community. Collaboration. Convergence.

Things are coming together.

www.iiconsortium.org





Richard Mark Soley, Ph.D.

Chairman and Chief Executive Officer, OMG

Executive Director of the Industrial Internet Consortium

109 Highland Avenue

Needham, MA 02494

USA

Phone: +1-781-444-0404

Email: soley@iiconsortium.org





For more IIC information

- About IIC: <http://www.omg.org/intro/IIC-flyer.pdf>
- IIC Fact Sheet: http://www.iiconsortium.org/pdf/IIC_FACT_SHEET_2015.pdf
- IIC Smart Factories: <https://workspace.iiconsortium.org/kws/public/download/5350/IIC-Smart-Factory-1-pager.pdf>
- IIC Quarterly Update: http://www.iiconsortium.org/pdf/IIC_Progress_Report_2016_July.pdf
- IIC and Industrie 4.0: <https://workspace.iiconsortium.org/kws/public/download/5351/IIC-4-0-1-Pager-web-Final.pdf>
- Industrial Internet Interoperability Coalition: <http://www.iiconsortium.org/accelerating-innovation.htm>
- IIC meetings and on stage: <http://www.iiconsortium.org/events.htm>





For information about OMG

- About OMG: <http://www.omg.org/intro/OMG-Backgrounder.pdf>
- OMG and the IIoT: <http://www.omg.org/intro/IIoT.pdf>
- OMG Consumer Device Safety:
http://www.omg.org/intro/Consumer_Device_Safety.pdf
- Data-Distribution Service: <http://www.omg.org/intro/DDS.pdf>
- Modeling Languages at OMG: <http://www.omg.org/intro/MLS.pdf>
- OMG Quarterly Technical Meetings:
<http://www.omg.org/news/schedule/upcoming.htm>

