Integrated Security Management Framework

Critical for Securing the Future of IoT

Nampuraja Enose

Principal Consultant- Industry 4.0 / Industrial Internet

17 Nov 2016

Internet Of Things – The Vision

Instrumented

Ability to sense, measure and monitor the condition of almost everything

Integrated

Equipment and Systems seamlessly interconnected to collaborate with each other in entirely new ways

Informed

Leveraging big and small data to draw real-time visibility to drive innovation and growth

Intelligent

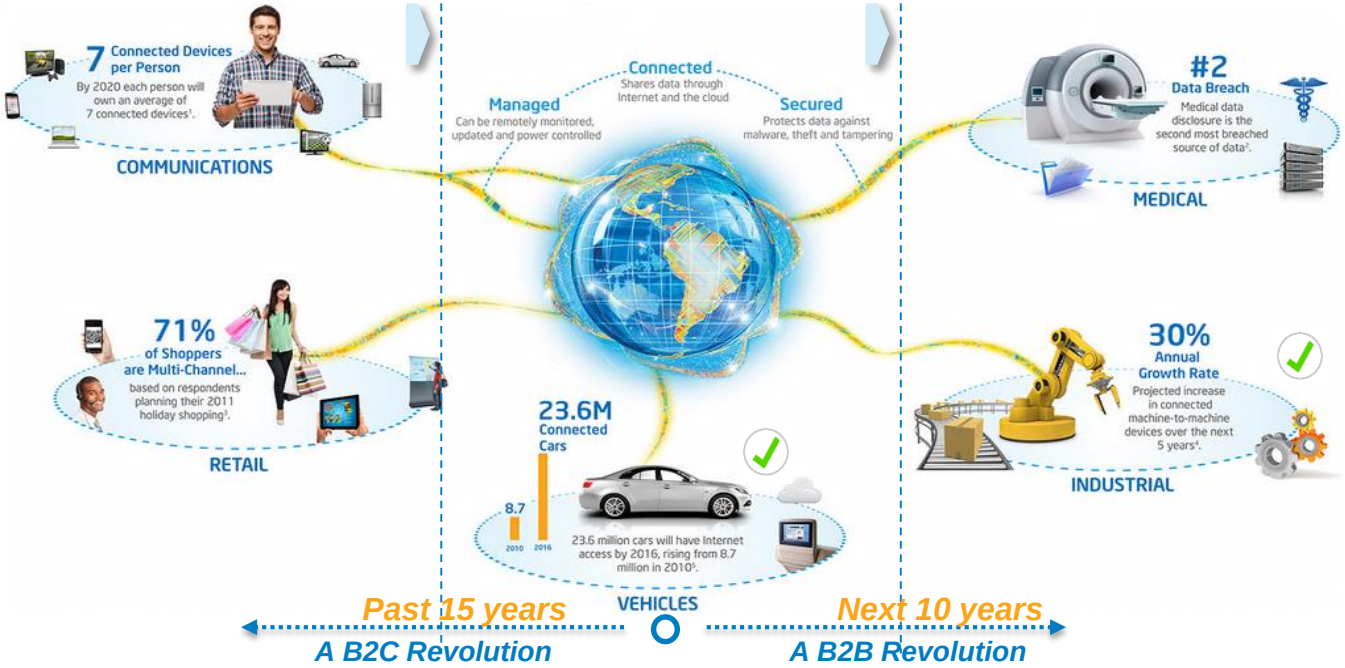
Advanced analytics and data-driven diagnostics to optimize processes leading to autonomy

Disruptive Technologies

Cyber-Physical Systems	*Interoperable Networks*	*Big Data Processing*	*Real-time Visualization & Advanced Analytics*	*Enabling Platforms*

MONITOR ⇨ **MANAGE** ⇨ **AUTOMATE**

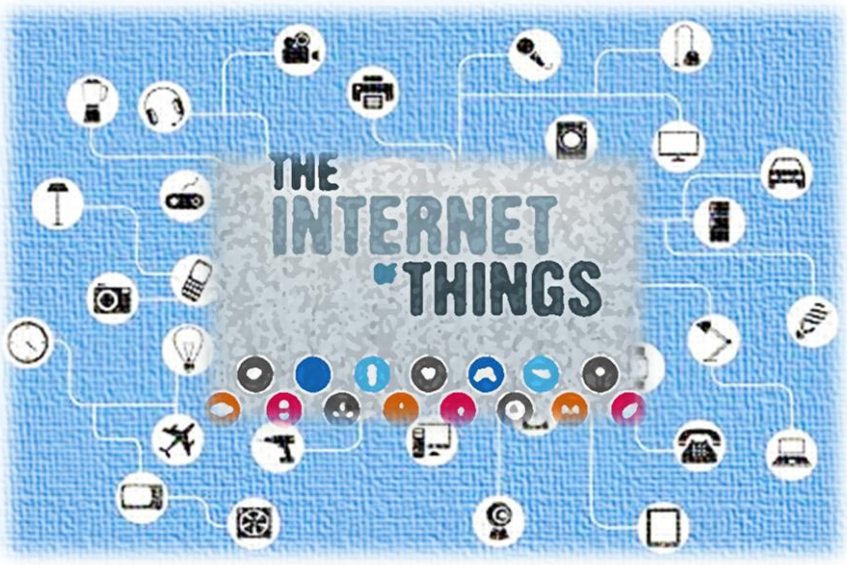
It is Happening!



- ***Cisco*** *projects 40 billion intelligent things connected by 2019*
- ***ABI Research*** *estimates 35 billion networked devices by 2019*
- ***IDC*** *predicts 212 billion devices connectable by 2020*
- ***Gartner*** *anticipates 19 billion IoT devices by 2019 & 25 billion by 2020*
- ***Harbor*** *projects 21.7 billion IoT devices by 2019*
- ***Business Insider Intelligence*** *estimates 23.4 billion IoT devices by 2019*

Source: Intel Intelligent Systems

The Billions of Devices and Trillions in Impact



Performance Efficiency	↑	**20-25%** Equipment Efficiency & Effectiveness
Maintenance Efficiency	↑	**20-40%** Increase in Equipment Lifetime
Information Efficiency	↑	**5- 10%** Saving in Business Expenditure
Service Efficiency	↑	**30 - 40%** Service Margin
Energy Efficiency	↓	**25%** Reduction in Energy Consumption

$3.9 trillion -11.1 trillion per year in 2025- McKinsey

Add about $15 trillion to global GDP by 2030

- GE

To grow at CAGR of 7.9% reach $8.9 trillion by 2020

- IDC

IOE a $19 Trillion opportunity

- Cisco

Projected Economic Benefits

Source: McKinsey Global Institute (MGI); Findings from the Infosys – FIR Joint Study on Industry 4.0 'The state of the Nations'

Delayed IoT Adoption? Security and Privacy may be the Reason

The Security threat is more serious than you think

securityledger.com

Major Challenges

1 Fears about privacy and security

53% Expressed concern about data sharing

51% Are worried about hacking

Microsoft

Top Trends in IoT Security

Cyber threats are more sophisticated than ever before.

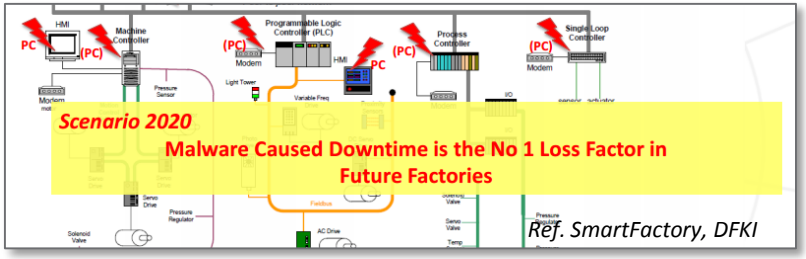
#1 obstacle to corporate IoT adoption through 2017: Security

78% Year-over-year growth of cybersecurity breaches in 2014.

New malware every ½ second

Global Threat Intelligence
- 1,200+ experts worldwide

80 Percent of Best-Selling Small Office/Home Office (SOHO) Wireless Routers Have Security Vulnerabilities



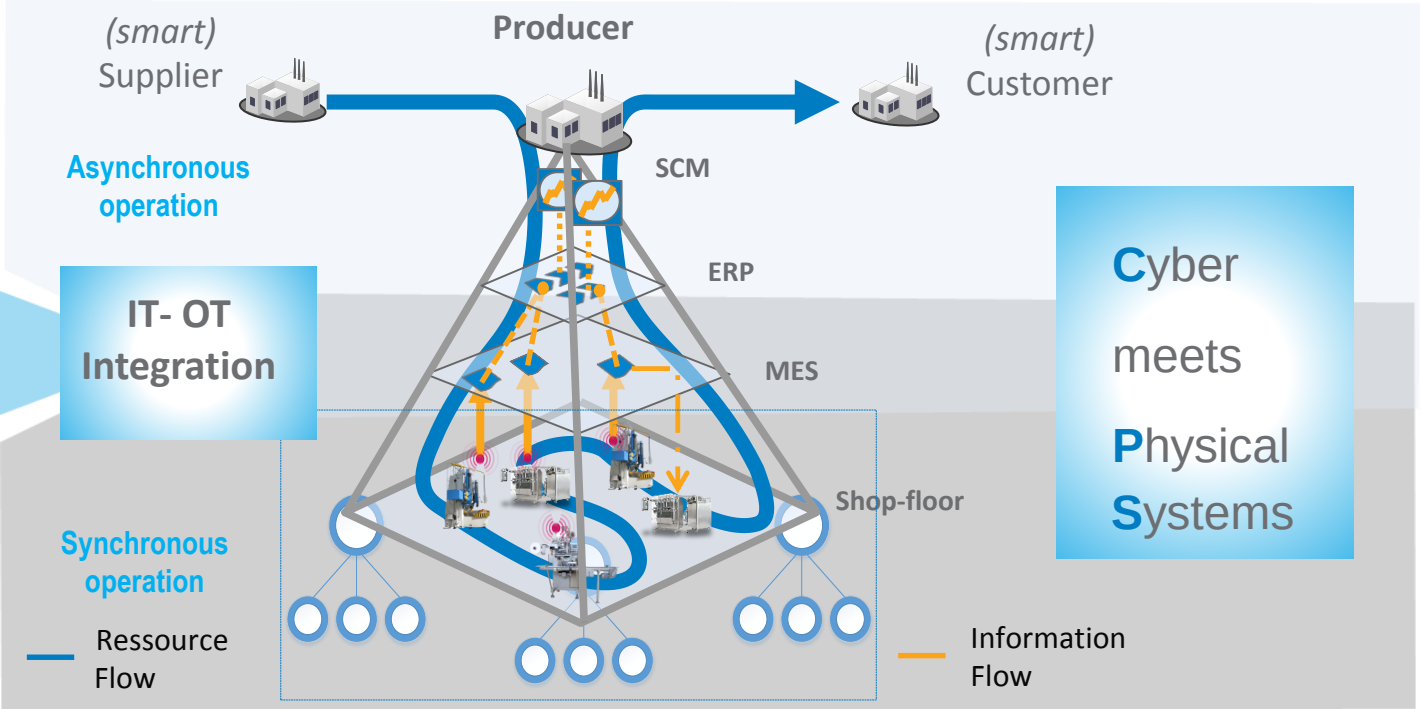
Control systems, vehicles, homes and even the human body can be accessed and manipulated causing injury or worse – CSA (cloud security alliance)

Security is definitely one of the biggest barrier for IoT adoption

What does it Mean to be on "Internet of Things?

The IT – OT Convergence

- Smart Applications & Services
- Advanced Analytics
- Big Data Processing
- Seamless Interoperability
- Cyber Physical Systems



"cyberizing the physical"
Amplifying physical subsystems with computational abstractions

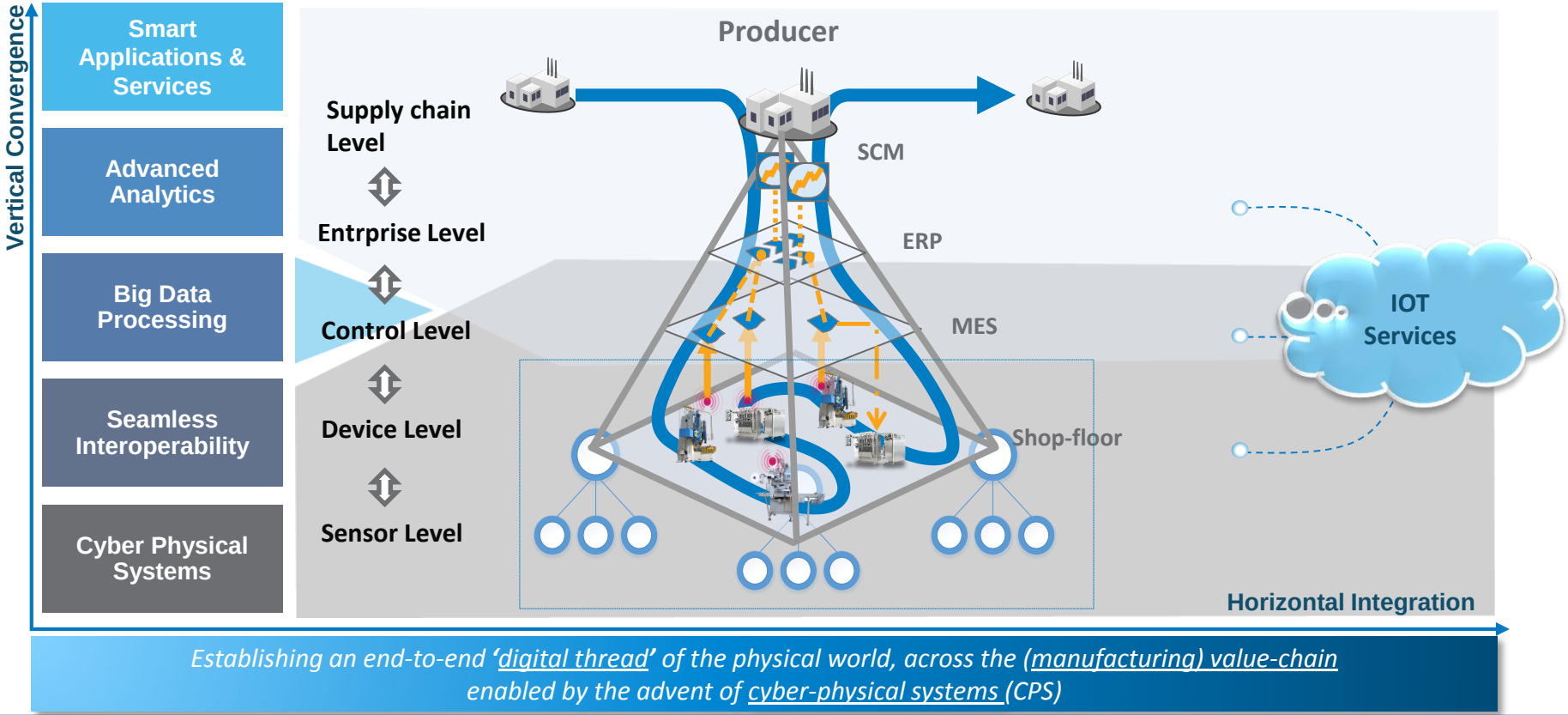
"physicalizing the cyber"
expressing abstractions of software components to represent physical systems

- Edge Intelligence
- Semantic Interoperability

Source: Infosys & FIR

What does it Mean to be on "Internet of Things?

The Horizontal and Vertical Convergence

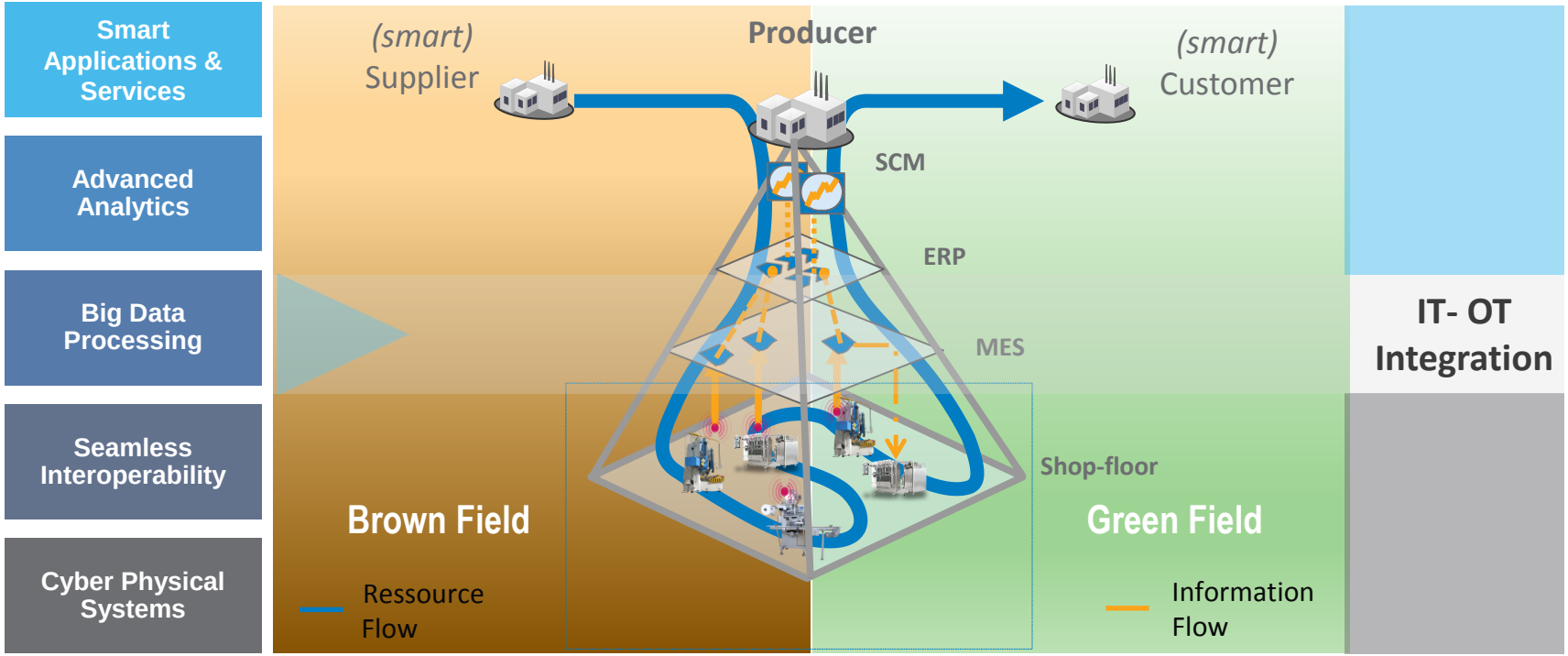


Establishing an end-to-end 'digital thread' of the physical world, across the (manufacturing) value-chain enabled by the advent of cyber-physical systems (CPS)

Source: Infosys & FIR

What does it Mean to be on "Internet of Things?

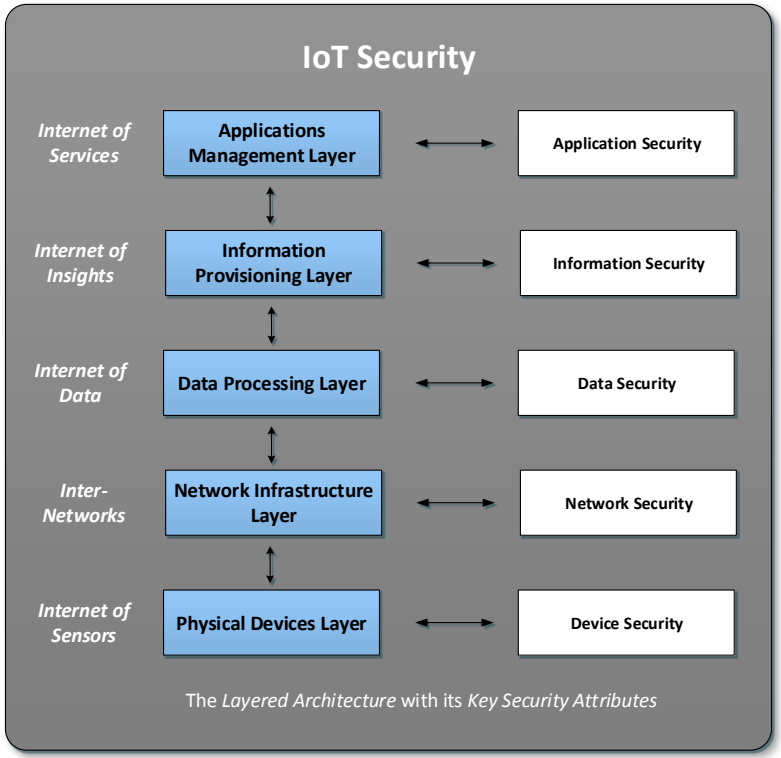
The Brown-Field and the Green-Field



The IoT architecture may be built from the ground up to leverage IoT (greenfield) or may be legacy devices that will have IoT capabilities added post-deployment (brownfield)

Source: Infosys & FIR

Establishing an Integrated Security Management Framework

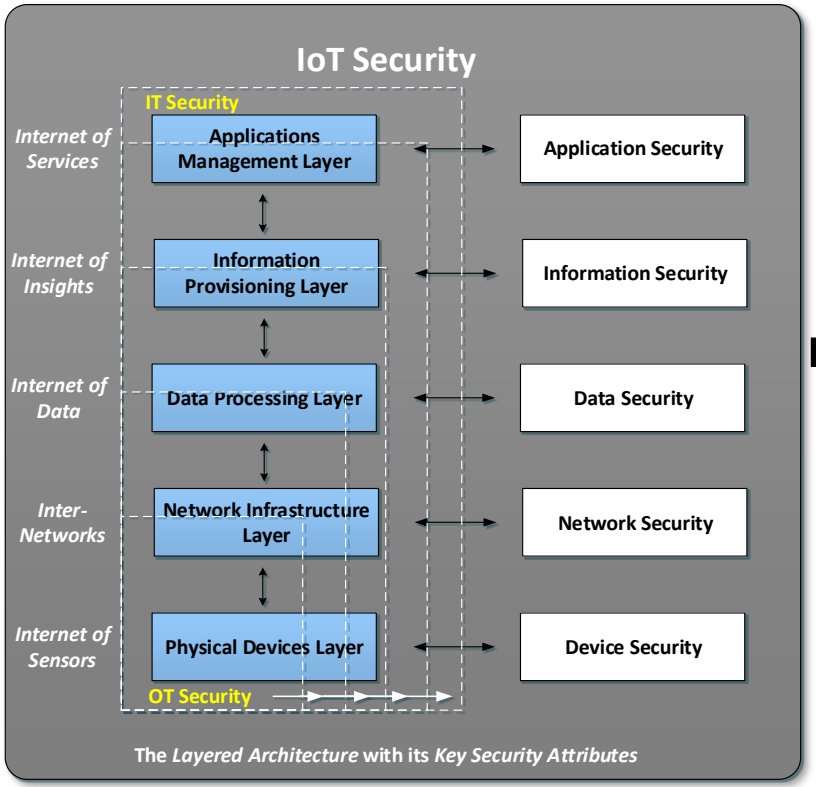


- ✓ Layered and Flexible Security Architecture – for optimal security
- ✓ IT – OT Security
- ✓ Building Security from the ground up (greenfield) or top down (brownfield)

Device Security	Network Security	Data Security	Information Security	Application Security
End point Authorization	Interoperability	Encrypted storage	PII Security (Privacy)	Usage policy Enforcement
End point Authentication	Network Firewalls	Signature data Memory	Data Obfuscation	User identity ´management
Device Identity	Transport Layer Security	Memory Integrity Checks	Digital Signatures	Application Integrity
Intrusion Detection	Dynamic traffic shaping	Advanced Encryption Std.	Configuration Data Protection	Malware Protection
Physical Security	Network Segmentation	Machine data management	Stored data Encryption	Anti-virus
Device/ Data Integrity	Routing protocol security	Data accessibility management	Hybrid cloud security	Sandboxing
Identity Management	Wrapper and Proxy	Notification Services	Masking Engines	API Security
Autonomous device coordination	Lightweight Cryptography			

Recommended Security Controls

Establishing an Integrated Security Management Framework



- ✓ Layered and Flexible Security Architecture
- ✓ IT – OT Security
- ✓ Building Security from the ground up (greenfield) or top down (brownfield)

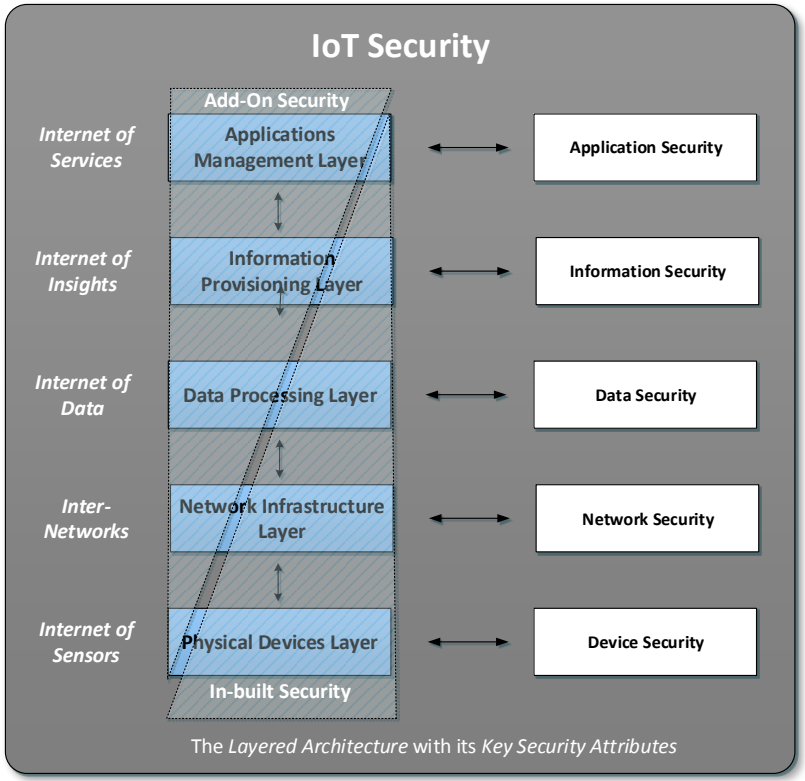
- Physical Security
- Access Controls
- Patch Management for industrial control systems
- Firmware Security
- OS security

OT Security

IT Security

- Data At Rest (DAR)
- Data In Transit (DIT)
- Data In Use (DIU)
- Data Loss Prevention (DLP)
- Data Integrity
- Aggregation Policies

Establishing an Integrated Security Management Framework



The *Layered Architecture* with its *Key Security Attributes*

- ✓ Layered and Flexible Security Architecture
- ✓ IT – OT Security
- ✓ Building Security from the ground up (greenfield) or top down (brownfield)

In-built Security

- Security in Design
- Secure Systems Engineering approach
- Green Field
- Bottom up

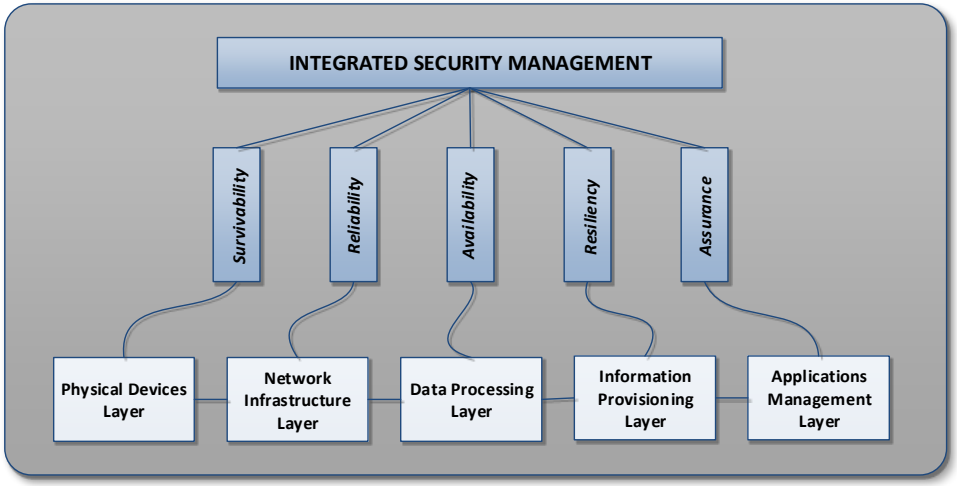
Add-On Security

- External Security Layers
- Brown Field
- Top down

Integrated Security Management - Implementation

The Key Principles

Distributed	*Decentralized*	*Lightweighted*	*End to End*	*Collaborative*
• Blockchain	• Edge Intelligence • Autonomy	• Peer to peer	• Threat Modelling • Incident Response • Lfe cycle controls / Audit	• All stakeholders



Thank You

nampuraja_enose@infosys.com

Infosys® | Building Tomorrow's Enterprise

Integrated Security Management - Implementation

Key Principles

- ✓ Distributed
  - – Blockchain
- ✓ Decentralized
  - – Edge Intelligence
  - – Autonomy
- ✓ Light weight
  - – Peer to Peer
- ✓ End to End perspective
  - – Threat Modelling
  - – Optimum approach